



Anonymous Reporting

Prepared for the U.S. Government

May 11, 2011

Document Control

This document can be shared with personnel who have a valid "need to know" within your federal agency or network, typically defined as a person or group that has a direct role in securing federal networks. Recipients of this document cannot add, edit, change, or modify it in any way. This document contains the proprietary information and intellectual property of an independent contractor, iSIGHT Partners, Inc., and the document is protected from unauthorized disclosure or use. The information in this report is not subject to disclosure under any federal, state, or local freedom of information law or regulation. Further, Federal laws may protect the disclosure of information in this document. 18 USC Section 1905 ("Disclosure of Confidential Information Generally") prohibits government employees from disclosing company proprietary information under criminal statutes. This information or document, or portions thereof, may only be used for research purposes and such information or any information derived therefrom, or any person or persons involved in its creation, may not be used or deposited in any criminal or other proceeding (including but not limited to use in search/arrest warrants or affidavits or grand jury subpoenas and proceedings). Users must adhere to any intellectual property rights contained in this document or in material in linked websites.

Contents

"Anonymous" Members' Calls to Action Against Politicians Affiliated with Recent Website Shutdowns ...	7
Overview	7
iSIGHT Partners' Assessment	7
Situational Awareness Report: Overview of "Anonymous" Attacks Against Websites Associated with Anti-WikiLeaks Activity	8
Executive Summary.....	8
Methodology.....	8
Timeline of Attacks	9
Participants	10
Possible Future Developments	10
iSIGHT Partners' Assessment	10
Situational Awareness Report: Update on "Anonymous"-Related DDoS Activity	12
Chronology of Attacks.....	12
Potential Future Targets	12
Misinformation Campaigns.....	13
Additional Tools and Attack Methods	13
Likely Attacks by "Traditional" Botnet	14
Attribution.....	14
Dutch Law Enforcement Action Against Suspected Anonymous Administrator	15
Outlook	15
Situational Awareness Report: "Anonymous"-Related DDoS Attacks; Techniques, Actors Diversifying ...	16
Target Update	16
Diversification of Attacks	16
Continued LOIC Attacks	16
Increasing Attention from Other Hacking Communities	17
Continued Misinformation Campaigns Surrounding Supposedly Leaked Credit Card Information	18
Outlook	18
Situational Awareness Report: Anonymous Movement Disorganized and Less Effective	20
Executive Summary.....	20
Fragmentation of Anonymous Movement	20
LOIC Controller Unavailable.....	20
New Tools Developed and Used	20
Changes in Future Targeting	20
Outlook and Implications.....	21
Situational Awareness Report: Anonymous DDoS Attacks Wane	22

Executive Summary.....	22
Infrastructure	22
Regional Variations	22
Outlook	23
Anonymous Actors Conduct Successful DDoS Attacks on Embusa.es	24
Overview	24
Attacks Target Embusa.es	24
Operator Identified	24
Ley Sinde Legislation	25
Operation Ley Sinde Phase 1 and 2	25
Implications.....	26
Anonymous Movement Increasingly Focused on Government Targets and Geopolitical Rhetoric Through January 2011	27
Overview	27
Operations in Late December 2010 through January 2011.....	28
Past Operations Attributed to Anonymous or Anonymous-Associated Actors.....	32
Tools and Adaptability	33
Organization and Communication Channels	33
Outlook and Implications.....	34
Anonspain Planning Attacks Against Spanish and US Government Sites	36
Overview	36
Anonspain Plans Attacks	36
Implications.....	36
Anonymous Member's Media Statements Declaring "Cyberwar" on United States Interests Likely Not Credible	37
Executive Summary.....	37
Origin of Operational Concept.....	38
Operational Evolution and Early Termination	38
Indications of Possible Involvement by Wintermute (aka q) in Fraud Operations.....	39
Implications and Outlook.....	40
Anonymous Targeting of Koch Industries	41
Executive Summary.....	41
Discussions of Targeting Koch Industries.....	41
DDoS Attacks.....	43
Intrusion Operations and Collecting "Dox"	47
Additional Attack Options.....	50
Disenfranchisement with Operation.....	51

Actors	52
Implications	52
Anonymous Using Secondary Botnet to Support DDoS Activities	53
Overview	53
Secondary Botnet Undisclosed to General "Anonymous" Population	53
Botnet Uses Simple Python Script "vibot"	54
Infrastructure May Be Responsible for Recent Attacks	54
Previous Reporting on Anonymous	54
Outlook	55
Anonymous' Planned 'Operation Metal Gear' Ineffectively Targeting Government Contractors.....	56
Overview	56
Operation Metal Gear	56
Actor Involvement	57
Implications	58
Alleged Anonymous Actor Posts Communiqué Discussing Targeting Global Financial Institutions Dubbed "Operation Empire State"	59
Overview	59
Drone Attacking AnonOps Servers Identified	60
Overview	60
Anonymous Members Demonstrating Increased Intent and Capability to Conduct Planned and Opportunistic High-Profile Intrusions	61
Overview	61
Attack on Sony	61
Fox.com	62
Possible Motivations Behind the Attacks and Future Use of Data	63
Implications and Outlook.....	63
New Anonymous Operation Targeting Financial Institutions in Spanish-Speaking Countries	64
Anonymous Announces Operation "Hipoteca"	64
Implications	65
AnonOps Attacked by Splinter Group; Adopts Web Server Attack Tool 'Slow Post' for New Campaigns..	66
Overview	66
Anonymous Splinter Group Successfully Attacks AnonOps.....	66
AnonOps Recovers and Conducts Attacks Against New Zealand and Iran	67
New DoS Tool Adopted Following Attacks.....	67
Implications.....	68
Anonymous Likely to Remain Viable Despite Leadership Schism.....	69
Outlook	69

Ryan Breaks with Anonymous	69
Implications	71
LulzSec Most Likely Anonymous Attribution Front.....	72
Overview	72
LulzSec Emerges	72
Relationship to Anonymous.....	74
Implications.....	75

"Anonymous" Members' Calls to Action Against Politicians Affiliated with Recent Website Shutdowns

Originally published on Dec. 6, 2010

Key Points:

- Members of the hacktivist community "Anonymous" have called for retaliation against several political figures associated with US Immigration and Customs Enforcement's (ICE) shutdown of websites selling counterfeit goods.
- Although the calls to action have attracted some positive responses, the probability of them occurring or their potential effectiveness is currently unclear.

Overview

On Nov. 29, 2010, the US Immigrations and Customs Enforcement agency launched "Operation in Our Sights v 2.0," executing seizure orders against the domain names of 82 websites believed to be selling counterfeit goods. Members of the hacktivist community "Anonymous" have reacted extremely negatively to news of the operation, and several members are calling for some form of retaliation. The most widely disseminated call to action appears to be "Operation Freedom," an attempt to gather exploitable information on political figures believed to be behind the ICE's operation, most notably Senator Patrick Leahy (D-Vermont). Other actors are calling for this operation to be merged into a "Mega" with two other ongoing operations that target Senators supporting a US copyright bill and an actor believed to be engaging in anti-Wikileaks activity. Finally, at least one actor is calling for denial-of-service (DoS) attacks against the websites seized by ICE.

iSIGHT Partners' Assessment

These calls for action have met with several positive responses, although at the time of this report it is too early to determine the likelihood of their occurrence, timeframes or potential effectiveness. Calls for action by "Anonymous" members are frequently received enthusiastically, but quickly abandoned. However, the motivation for these activities ties into other recent, successful activities by Anonymous (most notably "Operation Payback," a series of DoS attacks in support of online piracy), which could increase the likelihood of one or more of them gaining a receptive audience.

Situational Awareness Report: Overview of "Anonymous" Attacks Against Websites Associated with Anti-WikiLeaks Activity

Originally published on Dec. 8, 2010

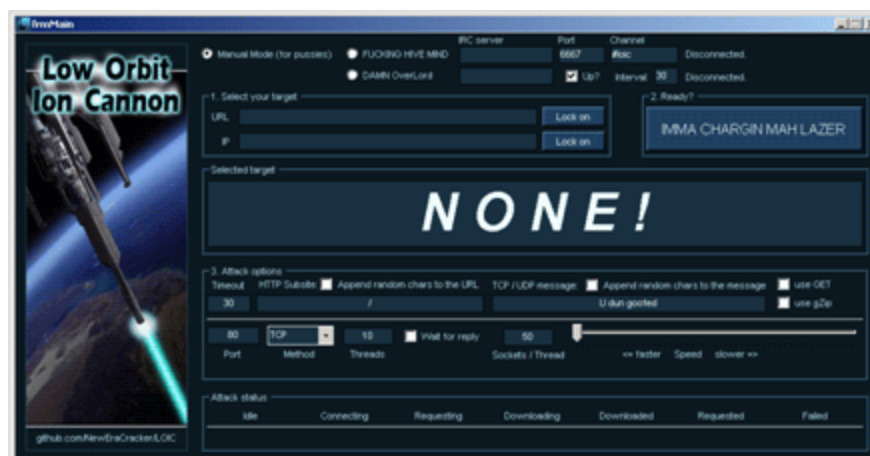
Executive Summary

Key Points:

- Between Dec. 4 and 5, 2010, the hacktivist community "Anonymous" launched an ongoing series of distributed denial-of-service (DDoS) attacks against the websites of organizations believed to have engaged in activity hostile to WikiLeaks.
- Participants in the attacks primarily use Low Orbit Ion Cannon (LOIC), a simple and widely available flooder tool.
- Recent attacks by Anonymous have benefited from increased coordination, both technical (a "Hivemind" C&C server), tactical (increased use of Twitter and other social media) and from the increased media attention paid to the WikiLeaks story.
- The attacks have drawn widespread media coverage and will likely continue and increase in effectiveness.

Over the weekend of Dec. 4 and 5, 2010, members of the loosely knit hacktivist community "Anonymous" began a series of attacks against websites believed to be engaging in activities harmful to WikiLeaks and its leader, Julian Assange. Targeted sites have primarily included payment providers who stopped processing donations to WikiLeaks, but have also included websites affiliated with the US and other governments. The attacks are ongoing as of Dec. 8, 2010, have been almost uniformly effective, have drawn significant press coverage and will likely increase in number of participants, effectiveness and prominence of targeted websites.¹

Methodology



Screenshot of LOIC interface
(iSIGHT Partners)

¹ iSIGHT Partners has reported extensively on Anonymous over the past few years; additional articles are available upon request.

The primary tool used in the attacks is Low Orbit Ion Cannon (LOIC), a simple, easy-to-use flooder tool widely available for free download since at least 2007. Recent versions of the tool (likely beginning the second half of 2010) have incorporated a "manual mode" (in which the individual operator selects the target) and a "Hivemind mode" that enables it to be controlled by an IRC command-and-control (C&C) server, in effect enlisting LOIC operators into a voluntary botnet. This has vastly increased the effectiveness of the attacks (automatically focusing all LOICs on a single target) and reduced the barrier to participation (since all an attacker needs to do is turn on his LOIC and ensure that it is selected for "Hivemind mode").

Coordination of the attacks is primarily taking place in several IRC chat rooms and advertised on several "chans" (simple message boards frequented by Anonymous members), Twitter streams and Facebook pages. The attacks appear to be drawing steadily increasing numbers of participants, with 1800 reported LOICs in the "Hivemind" as of noon EDT Dec. 8, 2010.

Timeline of Attacks

The following is a list of websites targeted by the "Hivemind" C&C. Except for the attack against paypal.com, all of the attacks have been successful, taking the targeted sites offline for the duration of the attacks.

- **Dec. 4-6, 2010** – against PayPal's blog at paypalblog.com. Unknown number of participants.
- **Dec. 6, 2010** – against paypal.com. More than 80 participating LOICs generating roughly 800Mbs of traffic.
- **Dec. 6, 2010** – against postfinance.ch (the finance department of the Swiss postal service). Roughly 200-250 participating LOICs.
- **Dec. 7, 2010** – against website of the Swedish prosecutor (hxxp://www.aklagare.se/). Roughly 120 participating LOICs.
- **Dec. 8, 2010** – against Mastercard.com. Roughly 800-1000 participating LOICs. According to publicly reported information, the attack on MasterCard has also disrupted the MasterCard SecureCode online transaction verification service. This disruption appears to have affected third-party payment processors that use the service.
- **Dec. 8, 2010** – against Visa.com. Approximately 2,000 participating LOICs. As of 4:15PM, Visa.com appeared to be down as a result of this attack.

Several other sites (such as Senator Joseph Lieberman's website at lieberman.senate.gov) have also come under limited attack. This is likely due to those sites being proposed as targets for the "Hivemind" in IRC chat rooms. While Senator Lieberman's site was not targeted by the Hivemind C&C, a number of individual Anonymous members were inspired to target the Senator's site with their LOIC bot set in "manual" mode.

A number of other sites were proposed as targets, but were not attacked by the Hivemind C&C. These proposed targets were likely targeted for attack by individual members running their LOIC bots in manual mode. Such sites include, but may not be limited to, Amazon.com, Sarah Palin's Sarahpc.com website and EveryDNS.

Participants

Although the primary language for coordinating the attacks is English, analysis of the attacking IPs² shows that a high proportion of the participants are from Western European countries, notably the Netherlands, Spain, Germany and UK. The majority of the actors iSIGHT Partners has identified as responsible for coordinating the "Hivemind" are also from Western Europe, which explains why the attack against MasterCard (for example) occurred during waking hours in that region.

Although "Anonymous" prides itself on being decentralized and faceless, iSIGHT Partners has identified several members as being responsible for maintaining the Hivemind C&C and, therefore, responsible for organizing the most significant attacks. These include:

- Evilworks
- fenniC
- iowa
- Jeroenz0r
- nerdo
- NewEraCracker
- Sharpie
- TomZ
- Tred

Possible Future Developments

As of Dec. 8, 2010, Anonymous members were discussing attacks against several entities, most notably Visa. The "holy grail" for the participants is a successful takedown of PayPal. Although they apparently do not believe they currently have sufficient members to carry out such an attack, they are actively seeking to recruit additional members for this operation and could possibly carry it out in the next few days.

One potential mitigating factor would be a disruption or takedown of the "Hivemind" server. Although attacks using LOIC's manual mode would almost certainly continue, they would likely be much less coordinated and therefore less effective.

Anonymous efforts to damage targeted organizations will very likely include media misinformation efforts. As of Dec. 8, 2010, actors affiliated with Anonymous were also attempting to coordinate a misinformation campaign claiming that MasterCard credit card databases had been compromised. The call to action was first identified on the 4chan message board website, although it is unclear how far it may have spread.

iSIGHT Partners' Assessment

Although Anonymous has been carrying out DDoS attacks for several years, their most recent operations show a marked increase in effectiveness. This is due to several factors, including the increased coordination and ease-of-participation provided by LOIC's "Hivemind" mode, increased use of social-media sites such as Twitter and Facebook for advertising attacks and increased media attention (which

² Since LOIC will not function properly through a proxy, it is highly likely that the IPs accurately represent the attackers' physical locations.

encourages the attackers and attracts new participants). Given the success of the recent attacks and the publicity surrounding them (and the likely continuing media attention revolving around WikiLeaks and Assange), it is likely that the attacks will continue until disrupted via technical, legal or other means.

Given that Anonymous appears to be at least partially selecting its targets based on media coverage, at this point, it is strongly recommended that organizations refrain from making any public statements, whether favorable or unfavorable, regarding Wikileaks.

Situational Awareness Report: Update on "Anonymous"-Related DDoS Activity

Originally published on Dec. 9, 2010

Chronology of Attacks

The list below shows all known attacks launched by Anonymous' "Hivemind" server from Dec. 4, 2010 to noon EST, Dec. 9, 2010.

- **Dec. 4-6**— paypalblog.com (PayPal's blog)
- **Dec. 6**— paypal.com
- **Dec. 6**— postfinance.ch (Finance Department of the Swiss Postal Service)
- **Dec. 7**— aklagare.se (Swedish prosecutor)
- **Dec. 8**— mastercard.com
- **Dec. 8**— visa.com
- **Dec. 8**— paypal.com
- **Dec. 9**— api.paypal.com

As mentioned in the previous version of this report, individual Anonymous members have also launched a number of attacks (such as the Dec. 7 attack against Lieberman.senate.gov) using individual resources operating outside of central direction. These attacks are typically inspired by communications within IRC chat rooms and likely vary widely in terms of numbers of attackers and intensity.

Potential Future Targets

As of noon, Dec. 9, 2010 EST, the Hivemind command and control (C&C) continues to target api.paypal.com. Anonymous members are calling for attacks against amazon.com and authorize.net (a payment-gateway service), although these have not yet occurred at the time of this report. Members are also continuing to call for attacks against PayPal.

Collaborative target selection remains ad-hoc and highly fluid. Not all proposed targets are attacked using the centralized Hivemind controller. However, individual members may independently attack proposed targets once nominated in initial discussions. Such individual attacks are far less likely to inflict significant effects against robust networks, especially in comparison to higher-volume traffic from Hivemind-directed attacks.

Misinformation Campaigns



OPERATION BANK-TROLL

Goal: Spread word all over the web that MasterCard servers have been breached and that private account details have been revealed. Make it viral, people panic out like the stock market, killing mastercard.

1. Post this on your Facebook, twitter, or any other social media:

"Millions of Mastercard details have been taken after today's attack, tell everyone you know to cancel their cards before it's too late, pass it on."

2. Google search "MasterCard deemed unsafe". Go to RefreshThing.com. Paste Google search URL into url bar. Press Go!

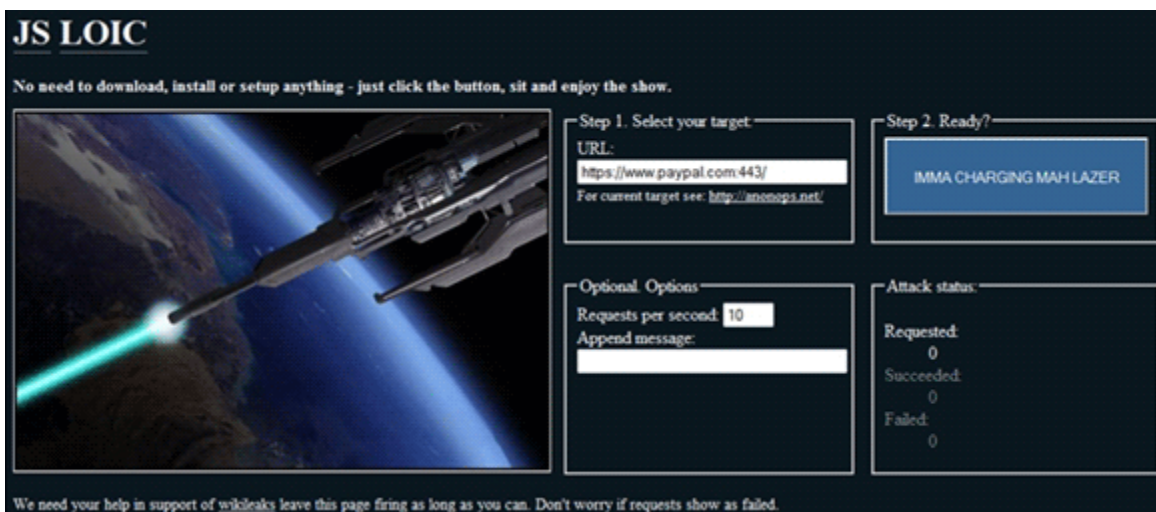
3. Contact media outlets explaining to them the breach, but claim that in order to avoid trouble MasterCard is trying to cover it up.

*"We are Right for we are Wrong."
- Captain Jack*

*Call-to-action for "Operation Bank-Troll"
(iSIGHT Partners)*

Anonymous members are also engaging in a variety of misinformation campaigns in order to cause additional brand-related damage to their targets. On Dec. 8, for example, Anonymous members began circulating calls for "Operation Bank-Troll," an attempt to convince users that Anonymous had compromised MasterCard credentials. This is likely related to the dissemination of a purported list of 10,001 compromised MasterCard numbers on late Dec. 8. It is unclear whether these numbers are genuine, and some Anonymous members have stated they did not directly obtain the accounts, but were merely disseminating them.

Additional Tools and Attack Methods



JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.

Step 1. Select your target:

URL:

For current target see: <http://anonops.net/>

Step 2. Ready?

IMMA CHARGING MAH LAZER

Optional. Options

Requests per second:

Append message:

Attack status:

Requested: 0

Succeeded: 0

Failed: 0

We need your help in support of wikileaks leave this page firing as long as you can. Don't worry if requests show as failed.

*Screenshot of "JS LOIC" tool
(iSIGHT Partners)*

Anonymous members are also circulating multiple web-based tools, such as the JavaScript "JS LOIC," although none of them appears to be in widespread use. In addition, Anonymous members are actively discussing additional attack methods, including attacks against key web services, APIs and CAPTCHA

authentication measures used by victim enterprises. However, LOIC will likely remain the most common attack tool until a new tool or technique is developed that is equally freely available and easy to use.

The LOIC tool is not designed to work through a proxy. Therefore, attackers risk revealing their own IP addresses, potentially identifying their participation in an illegal act. More sophisticated Anonymous members are utilizing options to reduce their exposure by hosting LOIC nodes on compromised drones accessed through common malicious web shells or open-source VPN software.

The group continues to explore alternative targeting options, including attacks against key web services APIs, CAPTCHA authentication protocols and other enabling technologies used by victim enterprises. Application-specific attacks discussed to date appear to contemplate only denial-of-service (DoS) through excessive or malformed requests, rather than any more sophisticated manipulation through intrusion for the purposes of disruption.

Likely Attacks by "Traditional" Botnet

Reports are also surfacing that a traditional botnet using malware-infected computers and not individual volunteer systems and incorporating about 30,000 drones was involved in the attacks against MasterCard and PayPal. Sensitive source reporting indicates that these reports are likely accurate, although the affiliation (if any) of the botnet operators to the LOIC operators is unclear.

Utilization of more traditional botnet infrastructure for continued attack operations likely represents further continuation of initial investigative defeat efforts intended to overcome design flaws of the LOIC tool.

Attribution

"Anonymous" prides itself on being decentralized and faceless, but the Hivemind functionality has somewhat changed this dynamic, as its success relies on a smaller, more organized and more skilled teams of actors running the C&C server. The Hivemind functionality provides unified direction of attacks, resulting in more significant degradation effects against targeted networks than previously observed in attacks using the LOIC tool.

Below is a list of actors iSIGHT Partners has identified as having access to the Hivemind C&C and, therefore, responsible for organizing (and launching) the most significant attacks. These include:

- **Jeroenz0r:** possible real-name attribution Jeroen Alexander, Netherlands. Possible address: Hazelaarstraat 23 2563 Segbroek, The Netherlands (near The Hague).
- **Rozza:** Possible real-name attribution Wouter van Eekelen, operator of hosting provider serverff.com, located at Piet Heinstraat 7, Schiedam, Netherlands.
- **Evilworks:** claims to be located in Zagreb, Croatia.
- **fenniC:** possible real-name attribution Jake Alexander Birchall, Neston, Cheshire, UK.
- **iowa:** possibly located in Toledo, OH.
- **nerdo:** possibly located in UK.
- **NewEraCracker:** claims to be named "Jorge" and located in Portugal.
- **Chronom, Nermd, Pro, sharpie, Switch, TomZ, Tred, Token, glomex, RootDisPI0x:** no information available.

Dutch Law Enforcement Action Against Suspected Anonymous Administrator



*Photo showing Dutch law enforcement raid on server farm
(iSIGHT Partners)*

In response to intelligence regarding attack planning and operations, Dutch law enforcement executed raids against a suspected Anonymous administrator late in the evening of Dec. 8, 2010. They seized equipment at one of the target locations, a datacenter in Haarlem near Amsterdam. The datacenter is operated by EvoSwitch and provides hosting services to a number of legitimate clients. It is believed that attack controllers were operated by Anonymous using rented servers at this location. Further action is anticipated against other potentially related targets.

Open-source information indicates that a juvenile was arrested in these raids. This individual is likely identifiable as the operator using the alias Jeroenz0r.

Outlook

Anonymous' operations are continuing to receive significant media attention, furthering a cycle in which successful attacks receive publicity, which draws additional members, which increases the likelihood of successful attacks. Likely near future targeting by the group is expected to concentrate on financial sector entities, including Amazon.com and authorize.net. Given widespread media attention, it is likely that adversary misinformation operations, alleging more significant effects such as a large-scale data breach, will continue. iSIGHT Partners is continuing to monitor the situation and will report on any additional developments as appropriate.

Situational Awareness Report: "Anonymous"-Related DDoS Attacks; Techniques, Actors Diversifying

Originally published on Dec. 9, 2010

Target Update

At the time of this report, the Hivemind continues to target api.paypal.com. Attackers continue to discuss a number of other potential targets, but this list has remained fairly static over the past 24 hours. Potential targets include amazon.com, twitter.com, authorize.net and Interpol.int.

Diversification of Attacks

As of Dec. 9, 2010, the attacks are shifting from primarily being conducted by individual Low Orbit Ion Cannon (LOIC) users, often connected to the Hivemind command and control (C&C), to incorporating a variety of techniques, including the following:

Continued LOIC Attacks

Anonymous is continuing to carry out LOIC attacks, although the IRC servers used to coordinate the attacks (by individuals and through the collective C&C of the Hivemind) are experiencing frequent downtimes. Anonymous is blaming this on "heavy traffic," although it is likely that they are also experiencing denial-of-service (DoS) attacks. Such attacks are more likely originating from rival hackers or groups rather than government entities, as the IRC rooms have become important intelligence sources for law enforcement (and the media).

As of the morning of Dec. 9, 2010, attack participants were being encouraged to visit eight new IRC servers located in Western Europe, the US and Canada, but these are also inaccessible at the time of this report. A large number of active Twitter and other social-media accounts are also disseminating targets and times for attacks and are likely serving as the primary information sources for many participants. However, the efficacy of the "Hivemind mode" is almost certainly being degraded by the IRC downtimes.

Compromised Servers Used to Host Web Shells



*Typical website defacement by Anonymous
(iSIGHT Partners)*

A dedicated group of actors within the Anonymous community have been actively compromising websites, both defacing them with pro-WikiLeaks messages and using them to host specific PHP web shells and PHP applications that use their servers' bandwidth to conduct additional UDP and HTTP flood attacks. To date, the majority of reported compromised websites are located in Western Europe, predominately impacting servers in Germany, the United Kingdom and France. While only a small number of compromised servers have been identified to date, this activity is consistent with previously identified attempts to leverage alternative attack tactics that offer greater challenges to attribution.

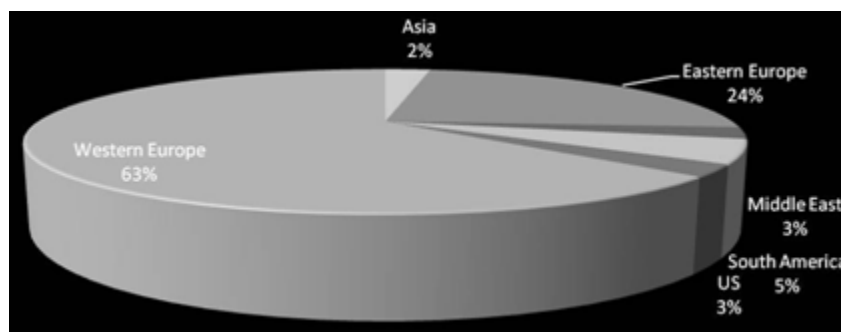


Chart showing distribution of compromised websites used for attacks (iSIGHT Partners)

Other Attack Tools

The increasing attention and first time participation in Anonymous-related attacks continues to motivate the existing community to attempt to best maximize these resources for ongoing distributed denial-of-service (DDoS) activity. As a result, alternative adaptations of the LOIC tool are rapidly proliferating. Each of these tools are client applications that rely on voluntary participation and are intended to allow participation by users relying on UNIX and Mac operating systems.

Although at least three alternative tools exist, the most widely advertised appears to be "JS LOIC," which performs only HTTP flooding attacks. One member has commented that requests from the tool include a suspect "Referrer" header that could be easily blocked by admins of targeted websites.

A second tool, the "Java LOIC" program, is being disseminated by Anonymous-affiliated actors who are recommending it for participants who use Linux or Mac operating systems. The tool is only capable of TCP and UDP flooding, and the original LOIC can perform HTTP flood attacks, although in any case most attacks have involved TCP flooding. Java LOIC cannot interface with the Hivemind server and, thus, can only be used for individual attacks. The program has the functionality to obtain targets from a given Twitter ID, but there is no indication that this is being used, and the setup guide for the tool instructs users to visit an IRC room and manually select targets as they are broadcast.

The third identified LOIC variant is an older tool known as WEBLOIC. This tool is not widely used and its effectiveness is unclear. Many new participants may be unaware of this alternative, given that attention is focused on newer variants.

Increasing Attention from Other Hacking Communities

There are strong indicators that other hacking/criminal communities may participate in the attacks in the near future. Calls for action are proliferating through a variety of regional hacking communities and this recruitment is likely to spur new attack alternatives using tactics, techniques and procedures that are more familiar within regional contexts. In particular, increased participation by South American

actors was observed during the course of Dec. 9, with Brazilian, Argentine and Mexican nationals represented among active participants. Localized translations of configuration manuals and other new participant guidance have also begun to circulate within these communities.

Additionally, a member of a Romanian hacking forum unaffiliated with Anonymous recently posted calls to attack Visa's website, and it is highly likely that calls for action are also disseminating through other underground channels. There is also a strong possibility that members of these communities will launch attacks against websites in their home countries that are believed to be engaging in anti-WikiLeaks or anti-piracy activity.

Anonymous members clearly anticipate the operational benefits that may be derived from increased participation by other hacker communities. Particular interest has been displayed in acquiring additional botnet resources. This is likely motivated in part by the earlier effects generated by a 30,000-node botnet that was utilized in attacks against MasterCard and PayPal.

While such infrastructure may be acquired at relatively low cost and effort, these operations typically require greater sophistication and technical skill than exhibited in Anonymous operations to date. Leveraging external assistance would therefore likely allow Operation Payback administrators to cross a critical threshold of potential effectiveness and sustainment in the face of continued law enforcement and security industry pressure.

Continued Misinformation Campaigns Surrounding Supposedly Leaked Credit Card Information

Around 2pm EST on Dec. 9, Anonymous members claimed that they had been given a list of compromised Visa card numbers (as a follow up to the list of purported MasterCard numbers they posted on Dec. 8), but had decided not to publish them. It is unclear whether the numbers were genuine (Anonymous only stated that they "seem[ed]" legitimate). Anonymous could have actually received the list, or their mention of it could have been a continuation of "Operation Bank-Troll," a likely ongoing attempt to target the reputation of financial institutions (particularly those also targeted by the DDoS attacks) by spreading misinformation about the security of their customers' accounts. While this misinformation campaign has been relatively ineffective to date, it has generated media coverage and concerns by private industry sources, and follow-on action is expected.

The emphasis in recent media on the alleged "insurance" file released by WikiLeaks may also inspire similar misinformation strategies by Anonymous. The encrypted file, widely distributed through peer-to-peer (P2P) torrent sharing mechanisms, is claimed to contain previously unseen classified material and remains sealed pending release of the cryptographic key. This key will allegedly be publicized in the event of unspecified negative action against WikiLeaks or its founder. Anonymous members may mimic such releases using material allegedly sourced from data breaches resulting from intrusion or attack activity against identified targets. The additional uncertainty created by encrypted materials, even if simply forged random files, will likely be difficult to as readily debunk as earlier misinformation activities.

Outlook

The potential impact of diversification and the current disruption of Anonymous' IRC structure remain unclear. One possible outcome is that the attacks will become dispersed and less effective and, therefore, draw increasingly fewer participants. However, another possibility is that they could attract

the participation of more sophisticated actors, such as operators of traditional botnets with much greater traffic-generating capabilities than the LOIC/Hivemind infrastructure. The reputation and emotional value accruing to many participants in the campaign may, in the short term, increase should the engagements escalate with new resources. However, in the longer term, many participants may be sidelined by the more technically complex, and likely more secretive, actions executed by more sophisticated and experienced hackers. It remains to be seen if the perceived importance of association with what may be increasingly seen as a "historic" event will outweigh the risks and the challenges of continued participation for many adversary actors.

Regardless, the targeting of the attacks continues to be driven by media coverage of Julian Assange and WikiLeaks in general, and any entities that are portrayed as engaging in behavior counter to either of these entities' interests are potential targets. Organizations not currently targeted by Anonymous may find corporate communications strategies that serve to minimize any potential association with the ongoing controversy an effective mitigation option.

Situational Awareness Report: Anonymous Movement Disorganized and Less Effective

Originally published on Dec. 10, 2011

Executive Summary

Key Points:

- The Anonymous movement shows signs of fragmentation and disorganization.
- Technical difficulties have reduced the availability of the Low Orbit Ion Cannon (LOIC) controller.
- Members are developing and experimenting with new distributed denial-of-service (DDoS) attack tools.

Fragmentation of Anonymous Movement

As of Friday, Dec. 10, 2010, the Anonymous movement was showing signs of fragmentation. Affiliated members of the movement were attempting to coordinate actions across a wider range of IRC channels. As more channels were created, the conversations continued to fragment and represent the interests of those members within a particular channel. For example, many channels catering to regional self-identified Anonymous members were created. Regional channels include, but are not limited to, Romania, the Netherlands, Italy, China, Mexico, Puerto Rico, Brazil, Portugal and a more general Hispano channel. The creation of these new channels increased the fragmentation of the movement.

LOIC Controller Unavailable

In addition, the centralized LOIC control server is suffering from increased instability and downtime. The loss of the central control server impedes the Anonymous operators from effectively controlling those members running their LOIC bots in Hivemind mode. As a result of this instability, many members have placed their LOIC bots in manual mode and are executing attacks on their own devoid of centralized coordination.

New Tools Developed and Used

Further, Anonymous members continue to develop new and experiment with other DDoS attack tools. Newly released tools include the High Orbit Ion Cannon (HOIC) and Geosynchronous Orbital Ion Cannon (GOIC). The HOIC tool is an HTTP flooder capable of targeting multiple sites in one session. An anonymous member can program the tool against multiple targets, and the HOIC tool will flood each target in serial. This tool is slightly more sophisticated than the LOIC, which generated easy to detect and filter UDP packets.

Changes in Future Targeting

The fragmentation of unitary operations through the Hivemind command and control (C&C) mechanism will likely change future Anonymous targeting processes during Operation Payback. The proliferation of smaller, but uncoordinated, communications channels will continue to challenge belief formation processes that were required to establish consensus for future target selection. In the absence of such consensus, individual attacks may be sporadic, with effects dependant on individual resources employed

for specific operational thrusts. Target selection will also likely be more dynamic, with individual attacks emerging more frequently against a larger range of targets that are attacked for a shorter duration.

Media feedback cycles will likely be a key determinant of duration for these smaller attacks, with even initial reporting providing emotional and reputational benefits to the attackers that may be a disincentive to sustained attack. However, should an effective attack occur, it is possible that other participants will join the effort in an attempt to capture a share of credit for their participation. In this scenario, an attack cascade may materialize, with subsequent re-attack waves against publicized targets. Such waves may exhibit classic long-tail dynamics, as the most publicized successes capture disproportionate attention and resourcing.

Outlook and Implications

If all participating members continue to be able to manually coordinate attacks, it is likely that the movement will continue to be able to disrupt targeted sites. However, it is unlikely that Anonymous will be able to continue to maintain its cohesive coordination due to the fragmentation of its communications infrastructure and the loss of its LOIC botnet controller. As a result, intense, but sporadic, attacks are expected to continue throughout the weekend.

These attack dynamics may be mitigated, in part, by substitution effects, as other activities capture the ephemeral attention of participants absent centralizing forces that serve to hold together otherwise highly autonomous individuals. These may include new efforts to publicize the content of alleged classified materials improperly released by WikiLeaks as part of Operation Leakspin, a task that requires less technical sophistication, but will likely consume participants' time and energy. Equally, frustration at technical challenges created by ongoing disruption of common coordination and communications channels may cause some participants to abandon attack efforts. However, a new media event or other significant driver may reinvigorate interest in the attacks. At this time, these effects cannot be quantified and their future impact on Operation Payback activities remains unclear.

iSIGHT Partners will continue to monitor this situation and pass updates if significant developments warranting attention emerge.

Situational Awareness Report: Anonymous DDoS Attacks Wane

Originally published on Dec. 13, 2010

Executive Summary

Over Dec. 11-12, 2010, the Anonymous community continued to launch scattered attacks against members of its traditional target set, particularly mastercard.com. These attacks were less effective than attacks over the previous week; MasterCard, for example, suffered only scattered downtime on Dec. 11. Anonymous successfully recreated much of its IRC infrastructure over the past 72 hours and was able to keep its Hivemind server online for much of the weekend (at the time of this report, it is online, but not specifying any attacks). Despite this, interest in conducting further attacks continues to wane as participants' attention is diverted elsewhere, including follow-on operations involving more traditional activist campaign tactics.

Infrastructure

Significantly, elements of this IRC infrastructure migrated to servers acquired through the hosting reseller Heihachi. This Russian service has previously been used as a component of infrastructure established by a number of bulletproof hosting providers active within the eCrime underground. The shift to more resilient hosting infrastructures also saw appeals for funding to support new acquisitions, but it is unclear the extent to which participants were willing to contribute financial resources to the action.

Although the number of participants remains down, the overall amount of traffic generated by the attacks has increased, which is likely due to increased use of web shells and other technologies instead of the LOIC tool, as well as the participation of more-sophisticated actors unaffiliated with Anonymous. The community continues to develop new tools inspired by LOIC, including a Java peer-to-peer (P2P) tool and an Android app, and is widely encouraging use of the "JS LOIC" web-based tool.

The P2P attack tool, Inter Stellar Cluster Ion Cannon (ISCIOC), was intended to provide resiliency for unified command and control (C&C) of attack infrastructure through a new design that sought to overcome weaknesses of the LOIC Hivemind architecture. The code is compiled for the Cygwin Windows-based Linux development environment, likely in an attempt to ensure broader accessibility for the large number of attack participants using the Windows operating system, but this tool remains immature. P2P traffic is carried over the UDP protocol, without command acknowledgement or authentication. To date, active denial-of-service (DoS) traffic generation functionality has not been successfully incorporated in early developmental versions circulating within the Anonymous community. The tool does offer spam functionality, which may be exploited in later Anonymous campaigns.

Regional Variations

Regional spinoff targeting efforts emerged early in the weekend, including discussions of new attacks against additional financial sector and media targets. Unconfirmed reporting indicates that additional botnet infrastructure may have been acquired for use in these potential attacks. However, participants were apparently unable to reach consensus regarding attacks on new targets, and no active engagements were observed. Low-level defacement-related intrusion activity did continue, involving opportunistic exploitation of common vulnerabilities in targeted websites and associated content management databases. Successful opportunistic exploitation was observed against UK and Turkish

government servers, although this action does not appear to have been coordinated with the larger campaign.

Outlook

Overall, Anonymous and its sympathizers' attention appears to be shifting to "Operation Leakspin," an effort to disseminate and use crowdsourcing techniques to analyze large numbers of WikiLeaks cables. Actors are constructing several sophisticated websites for this purpose, such as operationleakspin.org and the search engine leakysearch.com. Although Anonymous-inspired distributed denial-of-service (DDoS) attacks will likely continue, "Leakspin" will likely draw a higher level of media attention and be portrayed in a more positive and productive light than "Operation Payback," attracting users who chose not to participate in the DDoS attacks.



*"Operation Leakspin" call to action
(iSIGHT Partners)*

Anonymous Actors Conduct Successful DDoS Attacks on Embusa.es

Originally published on Jan. 17, 2011

Key Points:

- On Jan. 17, 2011, members of Anonymous initiated successful distributed denial-of-service (DDoS) attacks against the website embusa.es, which mirrors content from the official website of the US Embassy of Spain at madrid.usembassy.gov.
- Attacks are being carried out using the Low Orbit Ion Cannon (LOIC) and coordinated by an actor using the alias Alcaparran.
- Attacks are part of Operation Ley Sinde: Phase 2, a campaign carried out in response to Spanish intellectual property legislation that Anonymous actors believe is backed by the United States.

Overview

Anonymous-affiliated actors initiated successful DDoS attacks against embusa.es, a mirror site of the official website of the US Embassy of Spain on Jan. 17, 2011. Attacks are being conducted using the LOIC as part of Operation Ley Sinde: Phase 2, a campaign carried out in response to intellectual property legislation that is believed to have been influenced by the US government. Attacks are one of several recent engagements following the larger Operation Payback attack series.

Attacks Target Embusa.es

On Jan. 17, 2011, members of Anonymous initiated DDoS attacks against the website embusa.es, which mirrors content from the official website of the US Embassy of Spain at madrid.usembassy.gov. Attacks are part of a coordinated campaign called Operation Ley Sinde being carried out against Spanish government targets by members of Anonymous in protest of controversial copyright legislation. Access to embusa.es was disrupted throughout the morning of Jan. 17, 2011.

Embusa.es is an English-language mirror of the official American Embassy website at madrid.usembassy.gov. Registration indicates that embusa.es is also registered to the Embassy of the United States, though contact information is self-referential. Additionally, the site is the top response for Google searches of "Embajada de los Estados Unidos Espana."

Attacks on embusa.es are being carried out by an independent hivemind LOIC tasked to this specific attack. The target nomination process utilized by the group controlling this hivemind has been automated through a simple IRC polling tool, and embusa.es is among the most requested targets, which also include pp.es, the official website of the Partido Popular (People's Party) of Spain and senado.es, the official website of the upper house of the Spanish parliament. Both sites were successfully attacked over the weekend of Jan. 15-16, 2011. Embusa.es is the only observed nominated target associated with the US government.

Operator Identified

An individual using the alias Alcaparran issued the command to designate embusa.es as the target for the attacking hivemind. The actor has been observed communicating with attack infrastructure through IP address 188.126.70.127, a host associated with vpntunnel.se. The use of anonymization infrastructure indicates advancement in operational security measures by attack organizers, likely adopted in response

to widely publicized law enforcement action against identified operators in earlier Anonymous-affiliated attacks.

Ley Sinde Legislation

Attacks are part of an Anonymous campaign conducted in response to proposed intellectual property legislation, known as Ley Sinde, under consideration by Spanish lawmakers. The law would allow the government to black list sites associated with intellectual property violations. Significant controversy surrounds the legislation, particularly concerning US involvement in its adoption. This involvement, which Anonymous actors believe is detailed in diplomatic cables released through WikiLeaks, has led to significant focus of retributive activity on the US diplomatic presence in the country.

Ley Sinde legislation, which was attached as an amendment to a Sustainable Economy Bill, failed to pass through the lower house of Parliament in December. However, a new version of the legislation, which has received significant support from the Socialist party, is under reexamination and is expected to be voted on in February.

Operation Ley Sinde Phase 1 and 2

The current campaign is the second wave of attacks conducted in response to Ley Sinde legislation, known as Operation Ley Sinde. In December, the same infrastructure was used to conduct attacks against similar targets, which included sites associated with political parties and the parliament. There is no indication that the website of the US Embassy or other sites associated with the US government were targeted during this timeframe.



Anonymous poster advertising Operation Ley Sinde: Phase 2

Implications

This incident is one of several recent engagements against government entities in response to regional political issues following the larger Operation Payback attack series. Anonymous operations may continue to capitalize on future WikiLeaks disclosures, particularly those highlighting US involvement in controversial local political issues, to generate consensus for new attacks.

Anonymous Movement Increasingly Focused on Government Targets and Geopolitical Rhetoric Through January 2011

Originally published on Jan. 28, 2011

Key Points:

- The 'Anonymous' movement, a loosely knit association of Internet activists, garnered significant attention for its activities throughout late 2010, most notably with Operation Payback and other activities surrounding the controversy around WikiLeaks.
- The recent series of activities throughout January 2011 perpetrated by Anonymous actors (or actors capitalizing on the Anonymous "brand" and modus operandi) are gaining momentum with a number of geopolitically oriented operations that appear to be spurred on by increasingly sententious rhetoric surrounding Anonymous' perceived role and duty in fomenting political unrest.
- The broader Anonymous movement, which includes but is not limited to AnonOps or participants in specific operations, is dynamic and evolving and comprised of components with shifting alliances. However, a dominant model seems to have emerged to help interpret the movement's functions and processes and, while preventative measures against the movement and its targeting may prove complicated, there is a predictive element in anticipating a pattern of behavior.
- The January 2011 wave of attacks suggests that law enforcement activity does not necessarily carry deterrence measures, the adversary is relatively nimble in responding to obstacles, there are democratic processes at work in target selection and actors appear to be increasingly motivated by the perception that they are actualizing revolutionary change on a number of fronts.

Overview

The Anonymous community, loosely characterized as a movement of Internet activists of a generally nonlinear structure, has initiated a number of operations throughout late December 2010 and January 2011 since the Operation Payback wave of attacks through December 2010. The recent series of activities perpetrated by Anonymous actors (or actors benefiting from the Anonymous "brand" and standard operational patterns) are gaining momentum with a number of geopolitically oriented operations surrounded by increasingly political rhetoric. This rhetoric moves beyond Anonymous' traditional mission statement, which evolved over time to opposition to Internet and other forms of censorship, broadly interpreted. The broader Anonymous movement - as opposed to the "leadership" cell of AnonOps or participants in specific Operations - is dynamic and evolving and comprised of components with shifting alliances. However, a dominant model seems to have emerged to help interpret the movement's functions and processes and, while preventative measures against the community and its targeting may prove complicated, there is a predictive element in anticipating the group's general behavior. The January 2011 wave of attacks suggests that law enforcement activity, such as arrests, does not necessarily act as a deterrent, that the adversary can respond to obstacles with flexibility and innovation, that there are democratic processes in deciding target selection and that actors appear to be increasingly motivated by the perception that they are actualizing revolutionary change on a number of fronts.

Operations in Late December 2010 through January 2011

Operation Zimbabwe

Anonymous actors launched #OpZimbabwe from Dec. 27, 2010 through at least Dec. 30. An Anonymous affiliate claims to have targeted the website of President Robert Mugabe's administration for withholding information about Zimbabwe-related WikiLeaks cables and because Mugabe's wife was reportedly suing a Zimbabwean newspaper for \$15 million USD after the newspaper published a purported cable claiming the Mugabe financially benefited from illegal diamond trading. Anonymous' message focused on dissident themes stating, "We are targeting Mugabe and his regime in the ZanuPF who have outlawed the free press and threaten to sue anyone publishing WikiLeaks."

Actors targeted websites of the Mugabe administration, including the official government website, www.gta.gov.zw, and the official website of the ruling ZANU-PF party, which was offline for a reported 40 hours. Zimbabwe's Finance Ministry's website was also defaced with the now ubiquitous Anonymous message, "We are Anonymous, all your base belongs to us – 28th Dec 2010, We are Anonymous, we are Legion, we do not forgive, we do not forget, Expect us"



Screenshot of Operation: Zimbabwe defacement on the Ministry of Finance website

Operation Tunisia

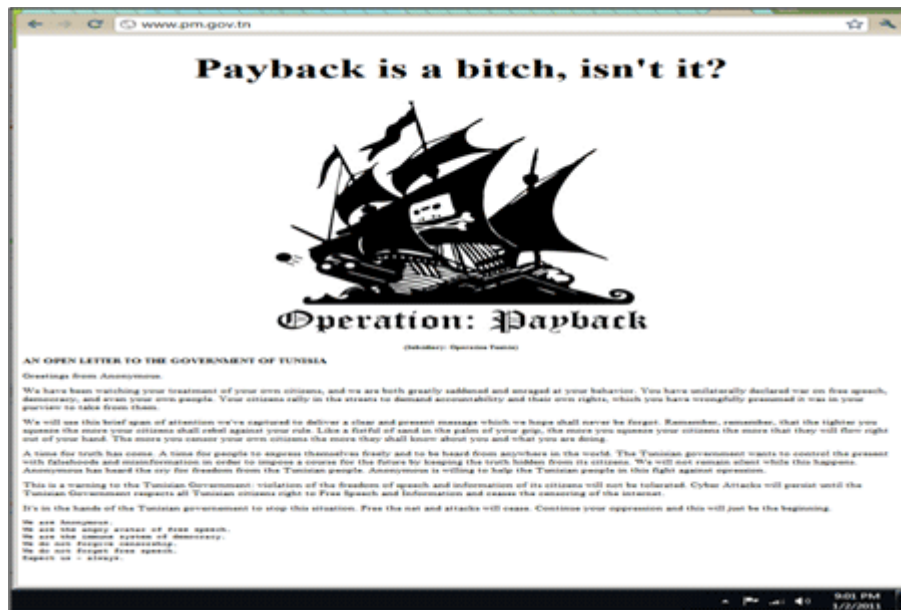
Anonymous targeted at least eight Tunisian government websites in protest of Tunisia's alleged "war on free speech" starting on Jan. 2, 2011, with the bulk of major disruptions lasting through Jan. 4, but on and off through at least Jan. 20. While some online news outlets speculate that Anonymous targeted Tunisia because of perceived anti-WikiLeaks censorship, Anonymous circulated a press release claiming it launched OpTunisia to raise awareness over Tunisian government censorship of internal protests over youth unemployment and general Internet and press censorship. In December, the Tunisian government blocked access not only to WikiLeaks, but also to various news sources that referenced Tunisia unfavorably in the WikiLeaks cables, including access to Tunileaks, a Tunisia-focused WikiLeaks-like site.



Anonymous' recruitment materials for attacking Tunisian government websites

The denial-of-service (DoS) attacks were directed against the websites of the Tunisian government, the stock market and Tunisia's primary DNS server. The latter target's compromise allegedly successfully brought down many websites with the .TN top-level domain. "Operation Tunisia" did not consist solely of DoS attacks, but also included defacements, including posting Anonymous' open letter on a compromised government website and an assurance that Anonymous "[took] steps to ensure that Tunisians can connect anonymously to the Internet and access information that their government does not want them to see." This likely refers to the circulation of various proxy and other connection address anonymizing tools among the hactivists involved in anti-government actions. The following Tunisian government websites were targeted by DoS attacks:

Tunisie.gov.tn	Official Website of Tunisian Government
bmv.t.com.tn	Tunisian Stock Exchange
sicad.gov.tn	Tunisian Ministry of Foreign Affairs
industrie.gov.tn	Tunisian Ministry of Industry
commerce.gov.tn	Tunisian Ministry of Commerce
carthage.tn	Carthage Palace: Presidency of Tunisia
benali.tn	Presidential Elections Site
ministeres.tn	Tunisian Government Site listing various Tunisian Ministries
Marchespublics.gov.tn	Ministry of Procurement
Pm.gov.tn	Office of the Prime Minister of Tunisia



Screenshot of the defaced website of Tunisia's Prime Minister

Through mid-late January 2011, OpTunisia participants were still discussing how best to disseminate information, general conversations related to the current situation with the country's new government and sophomoric political discussion related to a broad range of topics. OpTunisia was ongoing as of Jan. 20, but when OpEgypt began, several members posted messages in the OpTunisia IRC channels directing members to OpEgypt. Targeting instructions included agreed-upon target IPs, links to tools (such as LOIC and variants) and general information on boosting the anonymity of one's online presence.

The situation in Tunisia escalated to violence and increasingly vociferous protests. In a likely effort to exert control of the situation and stymie the protesters' organizing, on or around Jan. 11-13, reports claimed the Tunisian government began using a number of tactics to disrupt protesters' online activities. Anonymous particularly focused on allegations that the Tunisian government was leveraging its control of telecommunications infrastructure to monitor and alter the communications via popular webmail and social networking sites, including Google, Yahoo and Facebook. Independent technical analysis indicates that access to accounts was accomplished through the surreptitious addition of malicious JavaScript to legitimate login pages.

Code samples recovered from third parties believed to be the JavaScript code in question are designed to capture login credentials and extricate them through a unique mechanism. When users of affected sites attempt to login, the JavaScript identifies user login identification and password and encodes the data with an algorithm. This information, along with five random additional digits, is then sent via a GET request to a nonexistent URL.

Several commentators have claimed that the delivery method of the malicious code and the use of a nonexistent URL indicate malicious activity at the ISP level, as it would be the most likely method of inserting JavaScript into the pages and the best way of exfiltrating credentials sent to nonexistent URLs. Given its intimate control of these resources, the Tunisian government has been widely implicated in the monitoring scheme.

Tunisian President Ben Ali declared a state of emergency on Jan. 14, and later that day the government was dissolved and Prime Minister Ghannouchi assumed power.

Jan. 15, 2011 Planned "Day of Protest"

AnonOps publicized a day of protest to "Stand up for Freedom" on Jan. 15 as the first of a series of global protests in defense of WikiLeaks and to promote freedom of expression. While the rhetoric was circulated widely, news coverage of actual protests was limited at best. Anonymous activists were particularly aggrieved by the US Department of Justice's actions subpoenaing Twitter for subscriber account information of individuals linked to WikiLeaks activities.

Operation Venezuela

Beginning on Jan. 19, Anonymous actors coordinating through AnonOps, a sort of figurehead within the greater Anonymous movement that provides a semblance of leadership, started discussing OpVenezuela on its Twitter feed and in IRC channels, additionally circulating a press release that day. Operators included a link justifying their behavior to a Dec. 20 BBC news story about Venezuelan lawmakers approving a bill in Parliament to expand a bill on media content control to include the Internet, widely interpreted as increasing censorship, but under the auspices to "protect citizens against online crimes." OpVenezuela targeted and took down www.presidencia.gob.ve, the website of the government of Venezuela. A few days prior to the launch of the Operation, a "concerned Venezuelan blogger" reached out to Anonymous about the "horrible situation" in Venezuela and the perceived increase in censorship on behalf of Chavez's regime.

A simple website designed to facilitate communication between participants and to flesh out targeting strategies, a common Anonymous means of communication, included discussions encouraging participants to educate themselves on the political situation in Venezuela writ large beyond a cursory Internet search and suggested non-technical and more traditional means of protests such as sending letters to relevant lawmakers and other stakeholders. There was some discussion as to the utility of DoS attacks vice defacements and the relative pros and cons of both types of attacks. However, these discussions did not appear to substantively influence the group's operational approaches.

Operation Algeria

On Jan. 20, Anonymous released a press release warning the Algerian Government that Anonymous was monitoring the "causalities of repression...human rights violations....and injustice" and told people to "make history now by fighting against oppressive powers." As of this writing, there were discussions on OpAlgeria circulating, but no substantial activity yet. The increasingly politicized rhetoric and calls to Anonymous members to "make history" echo the verbiage and moral imperatives voiced in earlier and simultaneous Operations and suggest a broader mandate being adopted by Anonymous actors beyond fighting censorship.

Operation Egypt

Protests against Egyptian President Hosni Mubarak and general perceived corruption among the Egyptian elite started to gain considerable momentum on Jan. 25, the "Day of Anger," and escalated the next day with breakouts of violence. Many protesters planned activities via social networking sites such as Twitter and Facebook. Anonymous released a press release dated Jan. 26 citing that Anonymous "can not (sic), and will not, stand idly by while people are being denied their basic rights and human liberties....The Egyptian people are living under inhuman conditions" and are allegedly being denied a catalog of basic human rights. The press release then challenged the Egyptian government to offer unfettered access to uncensored media throughout the country and stated that if the government failed

to do so, Anonymous will attack Egyptian government websites and ensure that the international media "sees the horrid reality" the Egyptian government imposes on the Egyptian people.

Reported targets include www.moiegypt.gov.eg, the website of Egypt's Ministry of Interior, and www.mcit.gov.eg, which have been intermittently unavailable or considerably slower.

On Jan. 26, the Egyptian government blocked its citizens' access to Twitter and Facebook, echoing similar actions in Tunisia, likely in an effort to disrupt opposition communication channels and planning mechanisms. On Jan. 28, the government further imposed sweeping restrictions on Internet and other telecommunications services, including mobile telephony, in reaction to widespread civil unrest. These escalating measures increasingly reflect little Anonymous influence, but rather are directed against traditional forms of domestic opposition that also play out in the physical environment in classic venues such as the Friday prayer sessions at local mosques, which have also been subject to increasingly authoritarian restrictions.

Past Operations Attributed to Anonymous or Anonymous-Associated Actors

iSIGHT Partners has previously published coverage of two Anonymous-related incidents in January 2011 (Operation Ley Sinde and an operation against a Maldives telecom provider). In addition, an operation against an Irish political party website claimed to be by Anonymous-related actors, but exhibited slightly different tradecraft, indicating it may have been perpetrated by copycat actors.

Operation Ley Sinde

The Spanish attacks were part of Operation Ley Sinde: Phase 2, a reactionary campaign to Spanish intellectual property legislation perceived to be censorship leaning and supported by the U.S. The distributed denial-of-service (DDoS) attacks were initiated against embusa.es, which mirrors contents from the US Spanish Embassy's official website, and ppa.es, the official website of the People's Party of Spain. In this case, attacks were carried out by independent hivemind LOIC tasked to this specific attack, and the target nomination process was automated through a simple IRC polling tool, with embusa.es and ppa.es as the most requested targets. Both sites were successfully attacked over the weekend of Jan. 15-16, 2011. One of the identified actors who issued the hivemind's commands to target embusa.es used anonymization infrastructure to increase operational security, likely in reaction to press reports of the arrests of suspected perpetrators of other Anonymous-linked attacks.

Maldives

The Maldives telecom provider DDoS actors claimed to be part of the Anonymous movement and very explicitly stated they were inspired by Anonymous' activism. This operation began on Dec. 30, 2010 and continued through at least Jan. 3, 2011 (for further information on Operations that took place in Spain under Operation Ley Sinde on Jan. 17, 2011 and Anonymous-related actors in the Maldives, see iSIGHT Partners *ThreatScape Network Conflict*, "Anonymous Actors Conduct Successful DDoS Attacks on Embusa.es," Intel-339646, Jan. 17, 2011; "DDoS Attack Against Maldives Telecom Provider Dhiraagu in Protest over Pricing, Service," Intel-335718, Jan. 6, 2011).

Fine Gael

On Jan. 9, 2011, administrators from the Fine Gael political party's website claimed that hackers had stolen personal information of voters from its website. Fine Gael is the main opposition party and second-largest political party in Ireland. Two actors purporting to be part of the Anonymous group

claimed responsibility for the attack and said they defaced and compromised the website because the party was censoring the public's comments. The personal information stolen included the names, e-mail addresses, phone numbers, constituency and IP addresses of approximately 2,000 of the website's registrants. Fine Gael's website was also defaced, and the title was changed from "One of the big failing of politicians is that they talk too much and don't listen enough," to "The problem with politicians is that they lie," and "Nothing is safe, you put your faith in this political party and they take no measures to protect you. They offer you free speech yet they censor your voice. WAKE UP!"

Speculation abounds on whether the actors who claimed responsibility, Palladium and Raepsauce, are actually working on behalf of Anonymous because Fine Gael was not on the group's official target list, nor did the defacement contain the group's usual message of "We are Anonymous, we do not forgive, we do not forget." The theft of personal data seems out of the traditional observed behavioral pattern of most Anonymous operations, suggesting that the actors were using Anonymous as a false flag or were copycats. As Anonymous' profile increases, copycat attacks or actors using the group's name in an attempt to obscure criminal intent are likely to increase.

Tools and Adaptability

The most commonly used and advertised tools from several Anonymous DoS attacks are the Low Orbit Ion Canon (LOIC), Longcat Flooder and Unicorn. These tools are relatively easy to use and freely available, and Anonymous members have, at times, circulated their own, improved-upon variants. Other tools include webLOIC, a web-based DDoS tool that uses JavaScript; Slowloris, which continually sends partial HTTP requests; High Orbit Ion Canon (HOIC); Geosynchronous Orbital Ion Canon (GOIC); a few web-based PHP flooders and some utilization of botnets and fast servers. Disruptions in one mechanism of centralized C&C (the hivemind) led to flexibility and adaption on behalf of the adversary and likely led to forced innovations in these types of tools to ensure a robust attack. Despite extensive discussions around multiple separate development efforts, DDoS tool selection nonetheless remains largely consist with operations in December 2010.

Not all of Anonymous' activities are DoS focused. Other activities include Google bombing (ensuring offensive search terms appear as high-ranking Google results), posting offensive content to targeted social networking sites and website defacements.

Organization and Communication Channels

As a movement, Anonymous tends to communicate through social networking platforms such as Twitter and Facebook, IRC channels dedicated to various operations, message boards (or "chans") and simple websites, also usually tailored to specific operations. As the operations in mid-December 2010 (especially those related to disrupting anti-WikiLeaks organizations) increased in strength and numbers, Anonymous showed signs of fragmentation as IRC channels increased and became more targeted toward the specific operation or the members' regional orientation. The increase in the number of IRC channels and their increasing specialization, along with only limited overlap in channel leadership, suggested somewhat of a fragmentation. Note that channels are not only Operation-based or regional-focused, but also thematic (e.g., #support, #deface, #target, #loic, #help, #anonnews, etc.).

Anonymous IRC servers continue to suffer extensive disruption from third-party DDoS attacks, law enforcement and private cyber security takedown efforts. The group continues efforts to combat this instability through shifting network provisioning and separation of attack C&C (hivemind) functions from other communications channels.

There appears to be a perceptible threshold for picking operations and targets on larger scales to get a perceived Anonymous "institutional buy-in," although consensus has, to date, been relatively easy to achieve for most proposed attacks. However, the lesser incidents capitalizing on Anonymous' name and brand, whether or not they are officially part of AnonOps or "sanctioned" by Anonymous, did not appear to result in any sanction against splinter elements using the Anonymous name. There is some negative commentary in various online discussion boards about how a certain attack was or was not up to "standard," which was not defined, and participants were likely referring to the size of the attack and the sequence of events throughout the Operation. An interview with an information security magazine with an alleged Anonymous member involved in OpTunisia, and corroborated by sensitive source reporting, confirmed that there is a level of coordination and cooperation in the IRC channels related to specific operations and that there is some level of organizational structure in that members with specific skill sets (such as programming competencies) were identified and used as resources, if the occasion called for it.

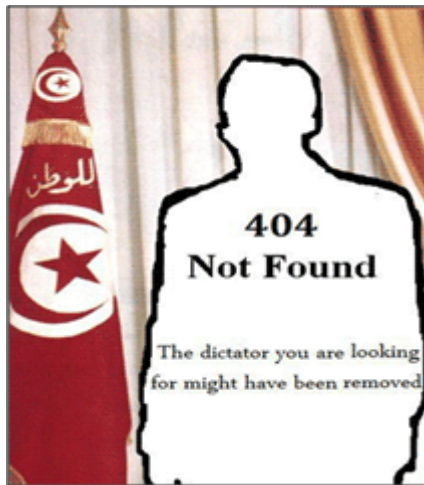
Targets in the most-recent operations seem to be chosen in a roughly democratic manner, where participants suggest websites, and IPs are discussed. In at least one instance, an IRC bot was used to receive and calculate votes, and sensitive source reporting indicates that independent, leadership-level communications channels exist where targets are coordinated. Once a proposed operation (as opposed to targets within that operation) is agreed on, a global message is sent to actors throughout the IRC network.

Some leaders overlapped between IRC channels, mostly to direct operations. Actors who appear to have leadership roles consist of AnonOps IRC network administrators, but are not limited to these administrators. Actor alcaparron, for example, was a coordinator of Operation Ley Sinde and an AnonOps IRC administrator.

Outlook and Implications

Whereas Operation Payback and many of Anonymous' previous operations focused on attacking corporate and other non-government websites, the operations of the last month, targeting and the associated rhetoric around Anonymous activity indicates a shift among the movement to focus on the political. It is unclear whether this trend will persist, but in comparison to Anonymous' actions during the Green Revolution in Iran ("Project Greenwave"), the rhetoric has adopted a decidedly more serious tone.

The effect events in Tunisia, which ultimately led to a change in government with the ouster of long-time dictator Ben Ali, appeared to act as a catalyzing agent in much of the IRC channel dialogue and on Anonymous' various websites. Revolutionary rhetoric appeared to legitimize and further motivate actors, many of whom are young and whose understanding of geopolitics is limited at best, to get involved in other events; from a review of commentary, many seemed to interpret correlation as causation in Tunisia's regime change.



Anonymous imagery highlights Tunisian regime change

In the higher-profile cases, such as OpTunisia, there was a concerted amount of conversation around the details of the revolution, especially violent events, and play-by-play accounts of what was happening on the ground. Many media outlets and commentators conflated the various influences and roles of social media, digital activism and Anonymous activities as evidence that web2.0 resources and concerned hacktivists were the decisive factors in the Tunisian regime's overthrow. This, no doubt, acted as a lightning rod for recruitment and further activism within a community that already identifies itself as part of an activist subculture looking out to fight for freedom.

Recent activities may indicate a shift to a more activist flavor, within at least part of Anonymous' leadership, expanding the group's interests beyond mere concerns on censorship. AnonOps' official twitter feed included a YouTube video of a demonstration in Koln, Germany of Tunisian diaspora "thanking" Anonymous for its role in overthrowing Ben Ali. The events in Egypt are likely to continue to reinforce these perceptions for Anonymous participants, regardless of the underlying drivers of regional discontent directed against authoritarian governments and stagnant economies.

Media attribution tends to lump Anonymous-attributed (or self-identifying members of the Anonymous movement), AnonOps and the various operations as one in the same. While doing so may be incorrect or may attribute a level of cohesion and agency that may be inaccurate, it has the effect of raising the groups' profile and mission statement. This publicity will likely galvanize further activists to become involved.

Anonspain Planning Attacks Against Spanish and US Government Sites

Originally published on Feb. 11, 2011

Key Points:

- Anonspain, the Spanish branch of Anonymous, has announced their intention to conduct distributed denial-of-service (DDoS) attacks against Spanish and US government websites, in addition to the site of the Spanish Academy of Motion Pictures and Sciences, on Feb. 13, 2011.

Overview

Anonspain has announced plans to conduct attacks against Spanish government websites and the website of the US Embassy in Spain on Feb. 13, 2011. Attacks are being conducted in response to the Ley Sinde copyright legislation, and the incident is timed to coincide with Premios Goya, the Spanish film community's annual awards celebration.

Anonspain Plans Attacks

Anonspain, the Spanish branch of Anonymous, has announced their intention to conduct DDoS attacks against Spanish and US government websites, in addition to the site of the Spanish Academy of Motion Pictures and Sciences, on Feb. 13, 2011. As in mid-January 2011, attacks are protests to proposed Ley Sinde laws, which would tighten copyright restrictions in the country (for more information, please see iSIGHT Partners *ThreatScape Network Conflict* "Anonymous Actors Conduct Successful DDoS Attacks on Embusa.es" Intel- 339646. Jan. 17, 2011). The incident is timed to correspond with XXV Premios Goya, the Spanish film community's annual awards celebration, and it may correspond with physical demonstrations by Anonymous.

Planned attacks will target websites associated with the Spanish government as well as embusa.es, which mirrors content from the official website of the US Embassy of Spain at madrid.usembassy.gov. Attacks are planned for the following sites:

Site	URL
US Embassy Spain	embusa.es
Spanish Senate	senado.es
Spanish People's Party	pp.es
Spanish Socialist Workers' Party	psoe.es
Spanish Academy of Motion Pictures and Sciences	academiacine.com

Implications

Anonymous attacks associated with the Ley Sinde legislation are likely to continue in the near term as the controversial laws remain under consideration by the Spanish legislature. Major events associated with the legislation are likely to correspond with additional attacks in the near term. Previous attacks have marshaled significant participation, and have successfully disrupted target websites; however, as time passes since the initial organizing events, participation may wane and reduce the effectiveness of attacks.

Anonymous Member's Media Statements Declaring "Cyberwar" on United States Interests Likely Not Credible

Originally published on March 10, 2011

Executive Summary

Key Points:

- Sensitive source reporting indicates that claims regarding future targeting of US government officials in retaliation for charges against a leak suspect are likely unsupported by the Anonymous hacker group's leadership figures, who appear unwilling to risk additional exposure to further law enforcement response to attacks against government entities.
- The self-appointed Anonymous "propagandist" appears to be excluded from the group's inner circle and has previously offered likely fabricated statements in discussions regarding his relationships, likely as part of efforts to pursue a book deal and associated financial compensation.
- The initial concept of operations is unlikely to have been introduced by the purported spokesman, but instead is believed to have originated as early as March 3, 2011 from a more experienced inner-circle member known as wintermute, aka q, likely with the encouragement of an unidentified third party, possibly outside of the Anonymous group. Wintermute was previously involved in other actions including intrusions against unclassified networks of a cleared defense contractor and possible eCrime activity targeting a US-based payment processor.
- Wintermute and like-minded supporters may execute independent retaliation on the planned date of action, March 20, 2011, despite the expressed disapproval of identified Anonops leadership figures. Any such action is likely to be uncoordinated and utilize less significant resources than those available to operators with the backing of the collective.

On March 7, 2011, a mainstream US media outlet interviewed a self-professed Anonymous group "propagandist." During this interview, the member, Barrett Brown, reportedly claimed that the group was planning an escalation of "guerilla cyberwar." This escalation reportedly planned to target unspecified government officials associated with the prosecution of the US military service-member, Bradley Manning, who has been charged with criminal offenses relating to his allegedly providing intelligence to the adversary and disclosing classified information. Brown stated that the Anonymous movement intended to retaliate against the US government based on its decision to bring charges against Manning. Sensitive source reporting indicates that a date of action for this operation was set for March 20, 2011. However, these statements are likely not credible, as the Anonymous group's inner circle, Anonops, does not appear to support operations. Brown remains a peripheral member, tolerated to date due to his utility for the group's media communications activities, but isolated from senior leadership's decision-making. Absent this support, it is unlikely that the proposed operation will leverage sufficient resources for substantive effects on target. Individual Anonymous members, including Brown, may pursue independent action. However, any operation is likely to be uncoordinated and will likely focus on generating media attention rather than degrading or destroying government networks.



Barrett Brown, self-professed Anonymous member, during MSNBC interview

Origin of Operational Concept

The concept of operations for retaliation following charges against Manning likely originated in part with an individual identified as wintermute, also known as q. Planning began as early as March 3, 2011 and appears to have been initiated by an unidentified third party, possibly external to the Anonymous group. Prior to this contact with the unidentified third party, Anonymous members had largely not reacted to news of additional charges against Manning.

Despite Brown's claims he functions as a "strategist" for the group's operations, it does not appear that he was involved in the development of the initial operational concepts. Brown is not a member of the Anonymous leadership's inner circle (Anonops) and is therefore excluded from the most authoritative discussions organizing future coordinated attacks.

Operational Evolution and Early Termination

Initial efforts to develop support within the distributed Anonymous collective for this operation faced immediate fragmentation. Early activities were branded Operation Bradley and attracted only limited participation. Discussions also continued under an earlier operational brand, Operation Eternal Ruin, utilized after initial intrusion operations against the unclassified networks of a cleared defense contractor in February 2011 (for additional detail on this incident, see iSIGHT Partners. *ThreatScape Network Conflict*, "Contractor Firm Network Compromised by Anonops, Likely Disclosing Cyber Security Contracting and Intelligence Liaison Relationships." Intel-349133. Feb. 8, 2011). Subsequently, the current action was rebranded Operation Manning, but still failed to inspire meaningful support. Operational planning and development ceased by March 4, 2011 without specific targets having been nominated and no other future courses of action discussed. Targeting discussions did focus on a geographic area of operations, Quantico, Virginia, where Manning is held. However, the group's stated goal of targeting specific government officials does not appear to have been realized.

Sensitive source reporting indicates that wintermute abandoned the nascent effort due to pressure from "higher levels." This included direct intervention by an Anonops leadership figure known as Nerdo, also known as Patrick (LNU). Nerdo is believed to have been acting out of concern that the operation would attract additional law enforcement pressure from US federal authorities. Nerdo is believed to have been among subjects served with search warrants by the United Kingdom's Metropolitan Police Service in early 2011, and this experience may have had a deterrent effect on Nerdo's willingness to condone future action against government targets. Wintermute reportedly claimed that he would respect this decision and no longer pursue action through Anonops. However, he and likeminded individuals appear to have contemplated possible independent action in support of Manning, separate

from the Anonymous collective. These actions may include communications outside of core Anonymous channels intended to evade oversight by leadership figures within the Anonops command structure.

Potential participants may include individuals associated with Op Eternal Ruin activities or earlier Op Manning plans. Identified individuals active during the window of discussion were AfterDeath, amd, AnonGuest46441, AnonGuy3, anonpanda, Anonymous9, antweasel, antivigilante, Budlighty, Chuck, DeMan, Effexor, EverGr33n, esc, ferminter, guttergutter, H3rM3s, jiffies, josie, KYTV, lenard, matthi, meekwarrior, msme, Noah, p0ng, rawksolid976, sasquatch, sepr, syo, ShoopadoowopBrown, shift, tb, trelane, TOX1CAT3D, The_Vole, zoidburger and zorch. However, none of these aliases has been confirmed to support independent action.

Barrett Brown has also been observed communicating outside of core Anonymous channels with other Anonymous members. These actors may also pursue uncoordinated action on or around the declared operational date of March 20, 2011. However, Brown's communications in these channels have included a number of likely fabricated statements, further raising questions regarding his credibility. These likely fabricated statements have included attempts to highlight Brown's alleged relationships with unspecified individuals employed by the Central Intelligence Agency (CIA). Brown is believed to be pursuing a book deal with an unidentified publisher. The book is purportedly based on his experiences in Anonymous, and Brown likely has financial incentive to manufacture high-profile media incidents in support of this objective.

Indications of Possible Involvement by Wintermute (aka q) in Fraud Operations

Wintermute has been active in the loosely constituted leadership cell Anonops. Sensitive source reporting indicates that he was likely one of the five core members directly involved in intrusion actions against the unclassified networks of the cleared defense contractor, HBGary, in early February 2011. Wintermute's exact role in that operation remains unclear. Wintermute utilizes an anonymization infrastructure to obscure attribution indicators. His most recent connections originate from IP 92.241.190.37, which is provided by Heihachi, a hosting services reseller frequently utilized within the eCrime underground since at least early 2009 to acquire bulletproof hosting infrastructure that is resistant to law enforcement or security industry takedown attempts. Heihachi servers are typically provisioned through Russian datacenters, including the Wahome facility in Moscow.

It is unclear how long wintermute had access to the server utilizing the specific IP address 92.241.190.37 prior to observed access in early March 2011. According to unconfirmed victim reporting during late February 2011, this address was identified in association with a DNS redirection incident targeting PayPal users, in which login attempts to the popular payment platform were hijacked through modification of users' HOSTS files to remap the PayPal domain name to point to the 92.241.190.37 address. The mechanism by which the HOST file modification was accomplished remains unclear, but likely involved malware infection, which is commonly observed in these types of incidents.

PayPal has been repeatedly targeted by Anonymous members since Operation Payback in December 2010 due to the service's refusal to process payments for entities associated with the WikiLeaks organization. To date, Anonymous members have not been linked to fraud operations against the PayPal platform. Such targeting might represent a natural evolution of ongoing hostilities toward the payment service, particularly following takedown efforts directed against key infrastructure used to sustain Anonops communication and centralized DDoS-targeting command and control (C&C). However, due to the widespread abuse of Heihachi servers in a variety of eCrime activities, including other phishing and malware operations that frequently involve multiple actors rotating access on a very short-term basis,

no conclusive assessment of this scenario is possible based on the limited information available regarding the suspected incident.

Implications and Outlook

The distributed and self-affiliating nature of Anonymous membership, based entirely around individual participation, frequently leads to nominated operations that fail to garner collective support or lose momentum in the face of disapproval from members of the leadership's inner circle. While this does not preclude individual action, it does limit the ability to coordinate DDoS targeting through centralized C&C mechanisms and likely means that more sophisticated members may choose not to participate due to fear of censure by the leadership. Such censure would cost more highly skilled participants often hard-won social capital within a fractious organization and removes much of the incentive structure provided by peer-level recognition that drives commitment to the organization. While personal ideologies may win out for other participants, the lack of social reinforcement tends to sap energy and enthusiasm for wildcat attacks.

A likely more experienced operator such as wintermute who is capable of leveraging independent resources acquired through the eCrime underground may indeed successfully attract other supporters and execute an unsanctioned and uncoordinated action despite these identified constraints. However, such actions would likely focus on capturing media attention and generating press coverage rather than sustained intrusion or attack intended to degrade or destroy government networks.

Anonymous Targeting of Koch Industries

Originally published on March 15, 2011

Executive Summary

Key Points:

- Sensitive source reporting indicates the Anonymous hacker group could not reach consensus regarding action against Koch Industries, and as a result, coordinated attacks remain unlikely to emerge.
- The Anonymous group's loose leadership structure does not appear to have supported these attacks, despite vocal advocacy by some membership elements. This sapped resources and momentum from the proposed operation.
- Actions were also hampered by lack of cohesion, ideological disorganization and a general lack of sophistication among interested actors; and these dynamics will likely continued to degrade proposed Anonymous-related attacks against Koch Industries in the near term.

The following annotated review of sensitive source reporting provides insight into Anonymous member discussions regarding potential action against Koch Industries due to prevalent media coverage of alleged involvement in Wisconsin political issues. These discussions took place against the backdrop of the group's ongoing consensus-targeting activities, which nominate new targets for future attacks and decide on the group's strategic communications posture should attacks be carried out. This process is highly variable between Anonymous operations, but consensus formation remains an important dynamic to coordinate resources for action against a target. Approval from the Anonymous group's loosely constituted leadership cell—Anonops—remains important in determining which attacks will receive organizational support. Lack of support does not indicate attacks may not proceed independently, as individual members execute "wildcat" actions using their own resources. However, such attacks tend to be uncoordinated and often fail to generate significant effects.

During this period, Koch Industries was only one of a large number of other potential targets nominated and discussed. There was little observed support for action, and despite vocal advocacy by a small subset of Anonymous members, no real consensus was reached. This severely limited attack options for proponents advocating action against Koch industries, forcing the consideration of alternative tactics. These alternatives also failed to generate significant support.

Discussions of Targeting Koch Industries

Anti-Koch Discussions

Targeting of Koch Industries has been repeatedly suggested in IRC channels associated with Anonymous and its core organization, Anonops. While these suggestions are widely made in several channels, substantive discussion of this activity is predominately limited to Operation Wisconsin and Operation kochblock channels.

01:15 < katapult> how bout an #opkoch - i hate those fucks so much
01:15 < crimethinker> katapult, go start it.

04:09 < Ratfucking> Koch Brothers would be the ultimate jewell in the crown though. They basically run all of the government, especially those on the conservative side of the aisle

23:26 < AnonNews842> it's a shame anonymous doesn't seem interested in taking on Walker or the Koch brothers

23:26 < AnonNews842> I think it should

23:26 < Fauxsheux> there's a lot going on in the world

23:27 < AnonNews842> very true, and the current focus is a noble cause

Calls to Action

On several occasions, actors primarily associated with efforts to target the Koch Industries made off-channel attempts to draw aid from fellow Anonymous members. Often these actors attempted to recruit members for distributed denial-of-service (DDoS) attacks using the Low Orbit Ion Cannon (LOIC) tool, but most recruitment efforts focused on securing help in conducting intrusion operations or in the collection of compromising documents.

1:39 < TheMiNd> the koch plan trolls the koch bros, it trolls the feds

21:39 < TheMiNd> it helps wisconsin

21:39 < gr3n4d4> ohio needs help too --

21:39 < TheMiNd> and it starts a social movement in the US

21:39 < rev> yeah lets help wisconsin

02:56 < wevz> twitt, fb, email, etc. we can not destroy by ddos, and intel is working hard, but without leakable shit, we are at a wall

00:58 < OmegaC> if none of you have anything better to do, there is a channel where you can ddos. go to channel #OpKochBlock and get bwraep program while you're at it. The rest will be explained there.

06:40 < TheMiNd> we haven't pwned anyone hard in like weeks

06:40 < AntiVenom> some kiddy told me about how he was the leader of anonymous then I crashed his game server then he told me how his dad was in the mafia and I just lol'd

06:40 < xor> TheMiNd: isnt that evil against the noobs?

06:40 < man> own me bitch

06:41 < &no> man, behave

06:41 < TheMiNd> its illegal to own another man

06:41 < AntiVenom> lol

06:41 < xor> be nice to the noobs, they are the building materials for intertubes & all larger ops

06:41 < TheMiNd> well

06:41 < TheMiNd> then

06:41 < TheMiNd> lets pwn something big

06:41 < ditto> *newbs

06:41 < TheMiNd> koch bros

02:53 < wevz> anyone want to help dstroy koch indusries?

02:53 < %p0ke> Tony is a service bot u know

02:53 < MBM> me

02:53 < wevz> industries

02:53 < MBM> **raises hand**
02:53 < anon18237> *How many are firing away?*
02:53 < wevz> *not a ddos.*
02:53 < MBM> *not a ddos*
02:53 < Divine_Mob> *i want to know hivenumber to...*
02:53 < MBM> *lets destory them*
02:53 < wevz> *need social engineer.*

Opposition to Focus on Koch

Mainstream Anonymous membership has repeatedly demonstrated an unwillingness to target Koch Industries. Reluctance is largely due to ideological implications of such an operation, concerns for the splintering of the Anonymous mission and concern for a heightened likelihood of repercussions. Membership has indicated that such attacks would violate stated principles of political neutrality and distract from ongoing focus. Furthermore, membership has voiced concern that attacks against US sites would substantially increase the likelihood of law enforcement repercussions.

21:39 < CiKey> *and.. just curiosity.... what relation is between assange/wikileaks/any and koch?*
21:39 < operationpayback594> *nunz*
21:40 < operationpayback426> *More attention needs to be brought to the koch situation and a ddos could help that*
21:40 < operationpayback325> *hmmm*
21:40 < operationpayback132> *no Wisconsin ppl arent fn dying being shot at!*

12:13 < Explorer93> *i recommend against cyber attacks against domestic US targets. it's a good way to get the FBI to climb up your ass with spikey boots, and set up a permanent base camp. <<*

05:01 < riot> *how koch is any worse for buying politicians than unions or soros. this has already been covered and long done with*

00:26 <@locust> *i just don't want us to start ddosing afp and c4g again*

DDoS Attacks

Initial DDoS Failures Recognized

Initial efforts to conduct DDoS attacks against sites associate with Koch Industries were widely regarded as a failure.

07:24 <+Still_anon> *wooo more press coverage on the koch attack*
07:24 <+Still_anon> *even if it only lasted an hour :<*

06:42 <~locust> *th3j35t3r we failed at keeping angelsoft down (koch toilet paper site)*

06:43 < puddie> *we don;t have the resources for ddos, but a good infor war could be fun*

20:56 < TheMiNd> *We have a plan to hit the Koch bros*
20:56 < hello> *Mi5/6 will have. A say if you Ddos direct*
20:56 < TheMiNd> *with a DDoS*

20:56 < anonvish17> that's why during opegypyt we called off DDoS attacks on the american arms dealer that developed tear gas and shot guns used by Mubarak's men

20:56 < anonvish17> we'd get fucked over

20:56 < TheMiNd> and if the feds come after the attack

20:56 < TheMiNd> They look like fools

21:39 < TheMiNd> the koch plan trolls the koch bros, it trolls the feds

21:39 < TheMiNd> it helps wisconsin

20:48 < TheMiNd> can we get enough anons together for a short-term DDoS

20:48 < TheMiNd> just to hit Koch a bit?



<--- 52 website domain hosted,+1

It is the general consensus to NOT DDOS in this op.

unless you feel like doing it privately and at your own risk/pace bro.

will need people with expertise to find vulnerable areas. also they are very aware that we are looking for exploits. (you can blame the PR storm for that one)

.yeah its almost gauranteed to be a honeypot <--- also true we dont need to go for big sites when we can get press and our message out thre by ddosing related weaker sites IMO-

just be wary of being viewed as attacking quote unquote free speech (even if corporate sponsored :() how to avoid that iyo? debate needs to occur, not my place to say, there are many opinions on what is considered media. (which we don't "attack"/ddos btw+1)

GOLD- <http://www.robtex.com/dns/kochind.com.html#shared>

Nessus report- <http://tinyurl.com/4pgc5ft>

<http://www.quiltednorthern.com/>

<http://www.angelsoft.com>

<http://www.colhogar.com/>

<http://www.kochpipeline.com/>

<http://www.ksandt.com/>

<http://www.fhr.com/>

<http://www.gp.com/>

<http://www.kochfertilizer.com/>

<http://www.kochservices.com/>

<http://www.kochcareers.com/>

<http://www.invista.com>

<http://www.brawnytowels.com>

<http://www.dixie.com>

<https://www.ewoodorder.com/> <---Georgia Pacific site for lumber auctions

<https://mygp.gp.com/> <--- GP employee login

(needs to not happen)

OmegaC: for those who are going to use bwraep, here is the list of urls to use. just put them in your urls.txt:

http://www.kochind.com/site_map.aspx

<http://www.kochind.com/Viewpoint/>

<http://www.kochind.com/Perspectives/>

<http://www.kochind.com/About/default.aspx>

<http://www.kochind.com/about/history.aspx>

<http://www.kochind.com/about/culture.aspx>

<http://www.kochind.com/about/locations.aspx>

<http://www.kochind.com/about/honors.aspx>

<http://www.kochind.com/IndustryAreas/default.aspx>

<http://www.kochind.com/IndustryAreas/refining.aspx>

<http://www.kochind.com/IndustryAreas/process.aspx>

<http://www.kochind.com/IndustryAreas/process.aspx>

<http://www.kochind.com/IndustryAreas/minerals.aspx>

<http://www.kochind.com/IndustryAreas/fertilizers.aspx>

<http://www.kochind.com/IndustryAreas/fibers.aspx>

<http://www.kochind.com/IndustryAreas/commodity.aspx>

Pirate Pad entry regarding DDos of Koch sites (Part A)

<http://www.kochind.com/IndustryAreas/Community.aspx>
<http://www.kochind.com/IndustryAreas/forestry.aspx>
<http://www.kochind.com/IndustryAreas/ranching.aspx>
<http://www.kochind.com/about/businessDevelopment.aspx>
<http://www.kochind.com/MBM/default.aspx>
http://www.kochind.com/MBM/five_dimensions.aspx
http://www.kochind.com/MBM/guiding_principles.aspx
http://www.kochind.com/MBM/science_of_success.aspx
<http://www.kochind.com/Community/default.aspx>
<http://www.kochind.com/Community/education.aspx>
http://www.kochind.com/Community/human_service.aspx
<http://www.kochind.com/Community/environment.aspx>
<http://www.kochind.com/EHS/default.aspx>
<http://www.kochind.com/EHS/Environment.aspx>
<http://www.kochind.com/EHS/HealthandSafety.aspx>
<http://www.kochind.com/newsroom/KochandtheEnvironment.aspx>
<http://www.kochind.com/EHS/default.aspx>
<http://www.kochind.com/files/KochEHSFacts.pdf>
<http://www.kochind.com/newsroom/publications.aspx>
<http://www.kochind.com/Careers/default.aspx>
<http://www.kochcareers.com/>
<http://www.kochind.com/Newsroom/default.aspx>
http://www.kochind.com/newsroom/news_releases.aspx
http://www.kochind.com/newsroom/news_stories.aspx
<http://www.kochind.com/FactsSheets/default.aspx>
<http://www.kochind.com/newsroom/publications.aspx>
<http://www.kochind.com/newsroom/bios.aspx>

DDoS Wisconsin State Government Websites

A guaranteed honeypot, this is the way to go for those who want to get v& in the name of justice and liberty. Because such a large protest has erupted, you will surely have the backing of constitutional lawyers and your actions will be judged as civil disobedience which is protected free speech.

Find owner of misinformation, fake Democratic site "widemocrats.com" Exposure of outside agent, possible financial incentives will result in more negative PR for Governor and Koch Bros. Also operating twitter account "widemocrats". DDoS attack last resort

"Drake Karl Schwichtenberg" is name offered by twitter user 3/14/2011, no confirmation of authenticity

Pirate Pad entry regarding DDoS of Koch sites (Part B)

Attempts were made on several occasions to organize membership for additional DDoS attacks, despite repeated failures. Actor 'TheMiNd' has repeatedly encouraged membership to join in attacks, though reaction was mixed to negative. TheMiNd has made several references to a plan for DDoS attacks that would eventually embarrass any investigating "Feds," though he did not explain it.

Target lists were eventually posted by membership for those interested in carrying out attacks alone, but this activity was discouraged.

Avoiding DDoS

DDoS attacks were specifically maligned by membership due to insufficient interest in the activity and subsequent inability to gather sufficient participation to conduct a worthwhile attack. Furthermore, many actors have actively discouraged political sites, given implications to free speech and possible conflict with central Anonymous principles.

08:38 < wevz> im in support of basically anything we choose except ddos (unless we have serious #s)

08:38 <+anarchacker> mib: agreed

08:39 < wevz> but i am very into the idea of effectively choosing something fast with the group and GOGOGO

21:38 < gr3n4d4> are we ddosing any of the koch sites?
21:38 < operationpayback325> and why
21:38 < TheMiNd> gr3n4d4: no because there's no support for it
21:38 < gr3n4d4> ah
21:38 < operationpayback132> and it's stupid and a waste of time to attack impotently
21:38 < operationpayback594> simply ddos'ing any of the suggested targets will do nothing
21:39 < rev> i like the plan to ddos the Kosh sites

Intrusion Operations and Collecting "Dox"

Focus on Intrusions and "Dox"

Membership have shifted primary focus on searching for and conducting intrusion operations with the express purpose of identifying, stealing and eventually publishing "Dox"—correspondence they believe would ultimately encourage public relations issues for Koch Industries. To that end, membership has made repeated references to attempts to scan networks associated with Koch industries in order to discover vulnerabilities such as SQL injection vulnerabilities, which might be exploited to gain remote access to protected networks. However, conversations regarding well-known hacker methodologies belie the lack of sophistication among these actors, who have not demonstrated the capacity to successfully carry out activities of this magnitude.

00:38 < Index> Attn #Anonleaks, high expectations: "Wouldn't it be something if the Koch brothers were hacked and documents surfaced that detailed their conspiracy against the "average American" to advance their corporate/Christian Fascist agenda? I believe that most of us know that if anyone can get in and dig deep enough, these two fascist bastards would likely face criminal charges on several different
00:38 < Index> fronts. Everything that is happening is reminiscent of the Smedley Butler era."
14:17 < Anti>
<https://selfservice.kochind.com/servlets/iclientservlet/hrprod/?cmd=login&errorCode=106&languageCd=ENG> https://www.mybizportal.net/dana-na/auth/url_142/welcome.cgi
<http://www.kochind.com/AppErrors.aspx?aspxerrorpath=/form%20id=%22form1%22%20name=%22form1%22%20method=%22post%22%20action=%22searchresults.aspx>
14:17 <+Effexor> Title: SelfService Sign In (at selfservice.kochind.com)
14:19 <%stonedguise> i see what you did there
14:20 <&joepie91> yes, and so did the other 175 people in this channel
14:20 <&joepie91> lol
14:20 <&joepie91> feds inclus
14:20 < Anti> Just spreading the word
14:20 < Anti> first 2 sites are employee login ports for koch
14:20 <%stonedguise> just sayin'
14:20 < Anti> last one may be vulnerable to SQL injection

08:13 <@locust> air2air we have a couple people working on vulnerabilities of koch websites
08:14 <%slaxer> no i am ok with totalitarianism if it serves the good of humanity and does not violate civil liberties or general freedom of the people
08:14 < anon01> meant to ask you that locust, is the scan still running?
08:14 <@locust> as far as americans for prosperity and club 4 growth etc., i'm fairly certain we agreed not to target them.
08:14 < Air2air> Oh man is that all? I got a bunch locust

08:14 <@locust> we are not going to target astroturf movements
08:14 <%slaxer> anncurry, well the start is hostnames
08:14 <%slaxer> track hosting services
08:15 <The_Hatchet> I still say we should get into koch main website and shutdown all of the business on their network by DDoSing their primary work servers instead of their front servers
08:15 <%slaxer> then detect vulns in services
08:15 <@locust> so i mean if you have a good suggestion suggest it.
08:15 <%slaxer> DDoS is over
08:15 <@locust> ^
08:15 <%slaxer> its infiltrate or nothing
08:15 <@locust> and we still have someone personal e-mail as a headstart
08:16 <@locust> someone's*
08:16 <The_Hatchet> I haven't hacked in almost 4 years now, I have none of the modern tools anymore
08:16 <Air2air> I assume we are using DDos because it's safer right?
08:16 <Air2air> I prefer injection or xss
08:16 <The_Hatchet> It is temporary, sends a message
08:16 <@locust> erhm... well ddosing something that's out of your countries jurisdiction is pretty safe.
08:16 <@locust> ddosing it from within the country is not so safe... considering the difficulty of spoofing ips with loic.
08:16 <Air2air> Yeah I know guys who subcontract DDos .. don't know it myself.
08:17 <@locust> oh shi- brb
08:17 <%slaxer> air2air: no not at all, its just simpler for the majority of people
08:17 <%slaxer> it is also a good idea to DDoS while a team does scans for services
08:17 <Air2air> Ah ok
08:17 <Air2air> This is so cool
08:18 <%slaxer> ha
08:18 <TheMiNd> seems pretty pointless to DDoS anything
08:18 <Slider> haha
08:18 <Slider> why?
08:18 <TheMiNd> without wide support
08:18 <%slaxer> your time is better spent learning about 0day vulnz
08:18 <The_Hatchet> Sending a message is never pointless
08:18 <%slaxer> like apache vulnz
08:19 <Air2air> Thought Apache was harder.. sql easy even I can do that
08:19 <%slaxer> themind: any attention is good attention
08:19 <+anarchacker> try RFIs or SQL injectins first. easy shit
08:19 <%slaxer> it gets people talking
08:19 <The_Hatchet> We have plenty of support, plus DDoS puts us in the news, which brings us wide support (except on fox, but fox ain't news)
08:19 <anon01> I know this is the opwisc channel, but did anyone see the wbc/anon sign on cnn??
08:19 <TheMiNd> slaxer: I mean, people are trying to DDoS shit when they don't have the numbers
08:19 <Air2air> fox lol
08:19 <TheMiNd> just to DDoS
08:19 <cvzero> ^
08:20 <@Agamemnon> careful anons.... just saying....
08:20 <%slaxer> themind:yeah i know :-/

08:20 <@Agamemnon> be sure to obscure with vpn
08:20 <%slaxer> agreed

23:48 <mib_vy5xtc> We need to HBGary the Koch bro's emails
23:48 <@locust> well hopefully we have done that to some extent.
23:48 <@locust> probably not enough though...
23:48 <kongming> and that while you may disagree with their intentions to allow public employees to dis-associate with unions, you dislike the idea of no-bid contracts more
23:48 <mib_vy5xtc> If there's an ethical ban on doing that directly to Walker, so be it, but we can crack the people he's likely doing biz wiht
23:48 <@locust> and yes mib_vy5xtc
23:49 <@locust> that would be good

06:32 <pawprints> iamfromflorida: you need to be finding entrances to Koch Industries sites.

08:49 <TheMiNd> no, we have stuxnet

Intrusion Operations Failure

Conversations repeatedly indicate failures to successfully "Dox" Koch industries or carry out successful intrusion operations.

23:12 <shadow--> locust u cracked koch borthers web?
23:13 <@locust> no not yet :'(
23:13 <@locust> try back later maybe :P
23:13 <@locust> brb
23:13 <shadow--> :P
23:13 <shadow--> i wish u good luck

10:06 <~locust> any luck on finding dox on koch so far?
10:06 <wmirc> nah only good ones jk
10:06 <~locust> tbh i didn't have much luck finding anything
10:07 <wmirc> their too old

00:32 <locust> i tried to dox koch to no avail
00:32 <locust> i'm hoping someone else will have better luck
00:32 <locust> starting with close relatives is a good idea/lead though

Possible Intrusion Operations Success

On a single occasion, prominent actor 'locust' claimed to have discovered a Koch Industries file marked confidential. However, he offered no evidence to confirm his claims.

06:10 <kai> btw locust, i constantly have my browser crash from having too many tabs open
lulz
06:10 <@locust> lol it's not just me then :)
06:11 <@locust> also i think i have to run some virus scans
06:11 <@locust> i was trying to get dox on koch brothers last night and opened file from
kochind. with header confidential
06:11 <@locust> set off a bunch of weird shit

06:11 <kai> oh, thats not good
06:11 <Kate> in b4 FBI raid
06:11 <@locust> yeah be careful
06:11 <@locust> lol
06:11 <@semirrahge> hahah
06:11 <@locust> i've been waiting for it for so long now
06:11 <kai> heard that thme plus hbgary have pdfs out that can fu ur shit
06:11 <@semirrahge> V&, mate
06:12 * locust constantly has rickroll ready for when feds come
06:12 <mud> better install magnets in your doorframe
06:12 <Kate> @ kai, yeah they can embed all sorts of fun things in pdfs
06:12 <kai> i don't even know what that means mud
06:12 <@locust> ^
06:12 <@semirrahge> PDF is major security hole to any system.
06:12 <@locust> yeah fuck pdfs

Additional Attack Options

As part of "Operation Kochblock," Anonymous members allegedly sent letters to personnel associated with Koch Industries in order to encourage the willful leaking of harmful documents. This activity was carried out in conjunction with attempts to encourage a boycott of Koch industries associated consumer products, as an alternative to unpopular DDoS attacks. Statements by organizers did not indicate a favorable reaction, but members have alleged that the campaign resulted in enumeration of IP addresses.

Letter Imploring Employees to Leak

#hackers.log:22:50 <TheMiNd> they sent a letter (lol) asking koch employees to leak stuff
#hackers.log:22:51 <TheMiNd> well they e-mailed it to them
#hackers.log:22:52 <TheMiNd> and somehow they managed to gather the IPs of anyone who viewed the document
#hackers.log:22:52 <TheMiNd> at least if i'm understanding it right
#hackers.log:22:52 <TheMiNd> they may have actually succeeded in doing something competent, for once... I don't know

Indirect Targeting, Amazon Bombing and Forum Poisoning

Members suggested a number of methods to target Koch Industries. On two occasions, actors recommended indirectly targeting Koch Industries by exploiting customer relationships or family ties. In the former case, actors would identify major, institutional customers and place unspecified pressure on them to end business relationships with Koch industries. In the latter, the children of the Koch family would be indentified and pressured to assist Anonymous, possibly through extortion. Other methods suggested were attacks against Koch-associated consumer products on Amazon or other forums to undermine sales.

03:08 <decon> Has anyone considered finding out who the big purchasers of Koch Industries products are (e.g. institutions, large corporations, etc.)? If we could pressure them to publicly renounce Koch and join the boycott we could have a corporate mashup.

06:49 <@rakaris> find out where their kids go to college or work and show up

06:49 <@rakaris> make sure that we are everywhere in the Koch's lives
 06:49 <@rakaris> protesting
 06:49 <~CryptKper> get that imposter out of here
 06:49 <~locust> rakaris i tried to dox koch brothers and failed
 06:49 <seufhu> don't target the kids! that is stupid
 06:49 <Th3-5p3ctr3> ?
 06:49 <dabard> I take that back... 1h57m to Saturday.
 06:49 <~locust> if anyone doxs them then they get free cookies for a week
 06:49 <Th3-5p3ctr3> The fuck'd I say to get my bullshit card pulled?
 06:49 <@rakaris> seufhu, but it might also be a soft spot
 06:49 <dabard> *07
 06:49 <seufhu> well de, we now know what timezone YOU are in... lulz
 06:49 <~locust> lol
 06:49 <seufhu> *debard
 06:50 <@X> done, and done
 06:50 <seufhu> rakaris... what would be a softspot?
 06:50 <~CryptKper> college kids dox can lead to big daddy dox
 06:50 <~CryptKper> but more importantly
 06:50 <seufhu> ooic
 06:50 <~CryptKper> don't dox kids

 02:53 <cvzero> hmmm, what sort of products does koch have other than tp ?
 02:53 <cvzero> have we considered amazon bombing koch products to drive down their popularity and sales ?

 05:52 <Th3-5p3ctr3> Is there a Koch Brothers website with a forum? :P
 05:52 <~locust> lol i dunno
 05:52 * dabard is listening to Welcome to the Working Week by Elvis Costello - My Aim is True (Remastered) (1:00/1:23)
 05:53 <dabard> Irony is a bitch.
 05:53 <~locust> i was so pissed i stumbled upon this article last night, and it was non-anon posting, so i created account whathaveyou, only to find out they have to preview your comments before you can post :(
 05:53 <@X> lol
 05:53 <Th3-5p3ctr3> I haven't even bothered to hit up the Koch subsidiary sites...but if any of those sites have like, product discussion forums, some well disguised propaganda posts could be very useful.

Disenfranchisement with Operation

As successful intrusion operations have failed to materialize, actors have voiced growing disenfranchisement with attempts to target Koch Industries. This attitude has pervaded the group's organizers and led to significant fractioning.

02:29 <wevz> ISNT ANYONE GIONG TO HACK THE FUCKING ACCOUNTS OF KOCH EMPLOYEES
 OR NOT

19:44 <ShadowMoo> So are we running an op against koch or was that a hoax?
 19:45 <Raiden> I was wondering the same thing

08:11 < pawprints> oh, well it's hard to do much damage by avoiding paper towels and toilet paper.

00:59 < wevzwevz> the mind why do you kick before discussion. youre a drag on this whol op

00:59 < wevzwevz> whenever you are ops on this channel, we fail

01:00 < wevzwevz> youre a fucking idiot

Actors

Anonymous leadership has not been associated with targeting of Koch Industries, and only prominent actor 'tflow' been associated at all with related channels. Conversations between locust and other actors indicate that tflow will not communicate with channel locust. tflow has not shown an interest in taking part in the attacks nor have any other members of Anonymous leadership.

Actors locust, TheMiNd and wevz are primary Anonymous figures encouraging/facilitating attacks against Koch industries. Locust is associated with a known Montana IP address, which corresponds with claims regarding the time during conversations. Actor TheMiNd is likely identified as a university student from an unknown area. Actor wevz is associated with a known California-based IP address.

07:31 < locust> joepie91 i don't think tflow likes me :(

07:31 <~joepie91> locust: howso?

07:31 < locust> he doesn't respond

10:28 < locust> it is 4:20 where i live

08:23 <@TheMiNd> 30 years ago at my university i'd have been doing lab work, hands on learning the entire time

08:23 <@TheMiNd> now i sit on my ass for lectures that I could just as easily watch on youtube

Implications

Attempts by Anonymous to attack or facilitate attacks against Koch Industries have been hampered by lack of cohesion, ideological disorganization and a general lack of sophistication among interested actors. Despite several efforts, actors have failed repeatedly to achieve notable results, discouraging participants and encouraging infighting amongst interested parties.

Anonymous leadership, which ultimately controls attack capability, has shown no interest in targeting Koch Industries and is likely to discourage such activity in the future. This is especially likely in the interim, as the organization focuses on a number of more popular targets. Though the organization is somewhat democratic in nature, Anonymous leadership has shown a willingness to cancel attacks, especially attacks against US targets.

Anonymous Using Secondary Botnet to Support DDoS Activities

Originally published on March 15, 2011

Key Points:

- Anonymous hacker group members are now operating an IRC-based distributed denial-of-service (DDoS) botnet. It is believed that this botnet is matching the targets nominated by consensus within Anonymous' general population.
- This botnet is not available to the general Anonymous population, and operators have taken some steps to ensure that the botnet is neither accessed by nor publicly discussed among general users.
- The botnet is likely intended to augment existing Low Orbit Ion Cannon (LOIC)-based capability, while maintaining the appearance of volunteer and crowd-based DDoS attacks.

Overview

Anonymous members have been observed operating an IRC botnet for the purposes of DDoS attacks. This secondary botnet appears to be operated by a select group of actors within Anonymous who have made notable efforts to keep the capability undisclosed to the general Anonymous membership, likely in order to make the group's attacks seem more effective and group-sourced than they really are. This infrastructure is likely being used in order to bolster attacks by the general Anonymous population, which has previously used crowd-sourced volunteer botnets to perform DDoS attacks, but has faced diminishing effectiveness over the past several months.

This botnet is believed to be built from bots donated by the operating actors. Varying claims have been made as to the size of these donations and the size of the whole infrastructure. One actor claims to have donated 10,000 to 20,000 bots, and that the infrastructure includes up to 100,000 bots. The botnet is believed to have contributed to DDoS attacks against Broadcast Music Inc's website, BMI.com and the anti-piracy group the Brein Foundation's anti-piracy.nl, both of which experienced significant downtime.

The DDoS infrastructure is using a version of malware known as "vibot," a basic Python script with flooding capabilities and an update functionality. While the malware is considered very basic, the most significant addition to this script is that the network does not get its targets through the channel topic, as is common with many IRC botnets, but instead checks in with another server for updates and targeting information. This may be an attempt by channel operators to keep their targeting information more secure.

Secondary Botnet Undisclosed to General "Anonymous" Population

Sensitive source reporting indicates that key members of Anonymous are operating an IRC DDoS infrastructure in addition to relying on volunteer DDoS tools such as the LOIC, High Orbit Ion Cannon (HOIC) and Geosynchronous Orbital Ion Canon. This IRC botnet has likely been set up in order to make the organization's DDoS attacks seem more effective to victims, the media covering the attacks and Anonymous' own members. It is highly likely that use of this DDoS botnet will lead to more significant Anonymous DDoS attacks in the future.

As the botnet is likely intended to support general Anonymous activities, it is likely that Anonymous administrators will use this botnet to attack the same targets as Anonymous' general population. The

appearance of more effective attacks will likely improve the morale of the general Anonymous population, and group members will likely continue to believe the group's support is greater and more effective than it truly is. This perception will likely also be reflected in public reporting surrounding potential future DDoS attacks. Likely to maintain this myth, the Anonymous administrators have taken steps to ensure that this infrastructure remains secret from the general Anonymous population.

In addition to any ideological or group-oriented motivations the operating members of this botnet may have, they have the opportunity to operate the IRC botnet with less risk, as culpability for the attacks continues to be spread amongst the group as a whole, rather than focused on these select actors. However, it is unclear exactly how much influence the administrators may have in target selection.

Botnet Uses Simple Python Script "vibot"

The botnet appears to be using a basic and poorly written Python script known as "vibot" (MD5: ea1259997a9b6845621298bae84b40e0), can provide basic flooding activities and includes a function to perform updates. The script also has a named group of white listed actors who have permission to issue IRC commands. This exclusivity reinforces the idea that the botnet is intended to be used by a select group of actors and likely provides a control measure to prevent the infrastructure from being turned against internal targets associated with specific Anonymous factional interests.

The malware does not get its targeting through the channel topic, as is common with many IRC botnets, but instead checks in with a server for updates and targeting information. It is likely that the malware is able to receive commands either from the IRC channel or the command and control (C&C) server. The use of a separate, non-IRC C&C servers is likely part of a continued effort by adversary operators to conceal their targeting practices from security researchers and the general Anonymous population.

Infrastructure May Be Responsible for Recent Attacks

While Anonymous has a history of using of a large-scale volunteer botnet through participants' voluntary download of the LOIC and subsequent tools, the IRC DDoS botnet is believed to be the product of existing botnet infrastructures that may have been donated by the operating actors in order to further Anonymous' ambitions. It is unclear how many bots may be in this botnet. One actor has claimed to have donated between 10,000 and 20,000 bots, and that the botnet numbers close to 100,000 bots, but it is difficult to verify these claims. These statements may be an individual posturing for respect among the community for their donation, or the numbers may have been inflated in order to encourage additional bot donations. iSIGHT Partners can confirm up to approximately 3700 of these bots, but it is highly likely that the network utilizes a significantly greater number of bots.

This infrastructure is believed to have been involved in Anonymous' DDoS attacks against BMI.com, the website for Broadcast Music Inc., and anti-piracy.nl, the website of anti-piracy group the Brein Foundation—both of these sites experienced significant downtime as a result of DDoS attacks that may have included this infrastructure.

Previous Reporting on Anonymous

For additional reporting regarding Anonymous' use of DDoS attacks, see iSIGHT Partners. *Global MTR*, "Anonymous" Members' Calls to Action Against Politicians Affiliated with Recent Website Shutdowns." Intel-323355. Dec. 6, 2010; "Situational Awareness Report: Update on "Anonymous"-Related DDoS

Activity." Intel-325539. Dec. 9, 2010; "Situational Awareness Report: Overview of 'Anonymous' Attacks Against Websites Associated with Anti-WikiLeaks Activity." Intel-324978. Dec. 8, 2010.

For reporting on the diversification of Anonymous, see iSIGHT Partners. *Global MTR*, "Situational Awareness Report: Anonymous DDoS Attacks Wane." Intel-328177. Dec. 13, 2010; "Situational Awareness Report: Anonymous Movement Disorganized and Less Effective." Intel-327103. Dec. 10, 2010; "Situational Awareness Report: "Anonymous"-Related DDoS Attacks; Techniques, Actors Diversifying." Intel-325772. Dec. 9, 2010.

For discussion surrounding several group dynamics of Anonymous, including target selection, see iSIGHT Partners. *Network Conflict*, "Anonymous Movement Increasingly Focused on Government Targets and Geopolitical Rhetoric Through January 2011." Intel-344994. Jan. 28, 2010.

Outlook

It is likely that the group of controlling actors behind this covert botnet will continue to maintain and operate the infrastructure to further the group's ambitions, reinforce members' morale and maintain a media presence. The botnet is large and significantly increases Anonymous' DDoS abilities, but is neither complex nor advanced in its structure.

Anonymous' Planned 'Operation Metal Gear' Ineffectively Targeting Government Contractors

Originally published on March 18, 2011

Key Points:

- On March 16, 2011, members of Anonymous announced their intention to launch an investigation into specialized persona management software they allege is actively used by contractor Booz Allen Hamilton.
- The investigation, called Operation Metal Gear, has received moderate interest by Anonymous rank and file and several leadership figures, though it has yet to uncover compromising information per its stated purpose.
- Participation is likely to wane as the operation continues to return marginal results, but focus may shift to attempted network intrusions to gather targeted information in an attempt to achieve operational objectives and associated media effects.

Overview

Operation Metal Gear, an effort by the Anonymous hacker group to investigate activities related to specialized persona management software, began on March 16, 2011. The operation is specifically engaged in attempts to uncover information regarding use of the software by federal contractor Booz Allen Hamilton, which the group accuses of actively using the software to conduct operations in Azerbaijan, Iraq and Tunisia. Information-collection efforts have been sporadic and disorganized, betraying unfamiliarity with government activities and focusing on random government and government contractor personnel. While Operation Metal Gear has established a moderate following, including interest by identified Anonymous leadership figures, the operation's continued failure to effectively produce results is likely to cause participant interest to wane. As in other attempts by Anonymous to gather information, there will likely be a growing impetus to conduct intrusions against target networks. However, intrusion capabilities are controlled by a small contingent of Anonymous members, significantly reducing the likelihood that such an operation would be conducted successfully.

Operation Metal Gear

On March 16, 2011, members of the loosely knit organization Anonymous announced their intention to launch an investigation into the procurement and use of specialized persona management software by the US military, likely in reaction to open-source media reporting regarding the issue. The investigation, called Operation Metal Gear by Anonymous members, seeks to uncover information surrounding the procurement of a specialized computer program created to facilitate the use of several unique personas for use in online engagements within social media channels.

According to a solicitation notice filed by the Air Force and obtained by Anonymous, the persona management software in question is intended to create multiple, fictitious profiles for use by single operators. A single user would be able to control up to 10 separate personas without fear of discovery by adversary actors. Though they did not indicate how they came to be interested in the persona-management software or the Air Force solicitation notice, both were highlighted in mainstream media shortly after the mid-February data breach of security contractor HB Gary and again in early March 2011.

On March 16, 2011, Anonymous members made an open call for aid in investigating the persona management software and its ties to federal contractor Booz Allen Hamilton. The group has assigned this software package a cryptonym, "Metal Gear," for reference in internal conversations. According to statements by the Anonymous members based on HB Gary-associated e-mail conversations, Booz Allen Hamilton has obtained the software contract. Furthermore, the group alleges that Booz Allen Hamilton is actively using the software to conduct information operations and suppress dissident voices in Azerbaijan, Iraq and Tunisia.

The group has also alleged IBM developed the software in question and provided a link to a site detailing an IBM patent for a persona management system. The patent holders have been identified, and members have been directed to uncover available information on these individuals.

Thus far, the investigation has been limited to readily available open-source information, which appears to have been gathered using common commercial search engines. Furthermore, the information gathered by participants has only a limited degree of association with the subject of the investigation, exposing the group's clear unfamiliarity with government activities and inability to understand complex and often unrelated bureaucratic activities. An e-mail from HB Gary regarding a malware analysis class that included representatives from Booz Allen, USAF, IBM and other government agencies and government contractors has received particular scrutiny, regardless of its context. Members were encouraged to gather information on these identified personnel, which has thus far included personal phone numbers and addresses, social networking profiles and professional contact information.

Actor Involvement

Operation Metal Gear has obtained moderate interest, and within one day, more than 70 Anonymous members were observed participating in discussions regarding these activities. A number of leadership figures have also been observed in these discussions. Sensitive single-source reporting indicates that participants included the following figures, who were also involved in earlier Anonymous operations:

Actor	Previous Activities
Esc	Operation Freedom coordinator
BarretBrown	Anonops media personality
Anonmyous9	Operation Freedom and Operation Payback coordinator
Alca	Operation Payback coordinator
Evilworks	Operation Freedom and Operation Payback coordinator and Anonops IRC network administrator
Avunit	Operation Freedom, Operation Payback, and Anonleaks coordinator
Shift	Operation Payback coordinator
Topiary	Operation Freedom, Operation Payback, and Anonleaks
Nessuno	Operation Freedom, Operation Payback, and Anonleaks
Sean aka FK	Operation Freedom and Operation Payback coordinator and Anonops IRC network administrator
Cody aka Neo	Operation Freedom coordinator and Anonops IRC network administrator
joepie91	Admin for Anonnews and involved with Anonleaks

Implications

Despite moderate buy in from leadership figures, Operation Metal Gear has ultimately failed to uncover information confirming suspicions that the software in question is in wide use in morally ambiguous contexts, as the hacker group has claimed. On the contrary, members have aggregated a disorganized collection of open-source data with little to no relevance to their ultimate objective. If this feckless process continues, as in previously observed campaigns, enthusiastic followers and resources are likely to falter and drop off entirely.

Previous Anonymous operations focused on information gathering have encouraged membership to conduct active intrusions against targeted organizations. Though there is no evidence to suggest these measures have been undertaken as of yet, frustration with open-source information collection may spur members to alter their approach. Any such operation is likely to target personnel already identified by the operation. Though Anonymous has previously demonstrated the sophistication necessary to conduct such an operation, these capabilities are scarce and controlled by a small contingent of Anonymous members, significantly reducing the likelihood that such an operation would be conducted successfully.

Alleged Anonymous Actor Posts Communiqué Discussing Targeting Global Financial Institutions Dubbed "Operation Empire State"

Originally published on March 22, 2011

Key Points:

- Anonymous-affiliated "Operation Empire State" may be an attempt by minority anarchist-leaning Anonymous members to target global financial institutions via cyber and/or physical attacks and protests.
- This minority group is likely attempting to hijack Anonymous communications infrastructure and media profile for their own means.
- At this time, it is unlikely Operations Empire State will pose a significant threat to the identified targets.

Overview

On March 12, 2011, an unknown actor posted an Anonymous-branded video discussing Anonymous' intentions to begin targeting the US Federal Reserve, International Monetary Fund, World Bank and Bank of International Settlement. The video was quickly picked up by the press and spread across the Internet. The video dubbed the upcoming attacks "Operation Empire State," referring to the location of the US Federal Reserve in New York, NY. The group is currently organizing attacks under the "opOES" banner. A sensitive source with direct access to Anonymous communications questioned the opOES organizers' affiliations with Anonymous. It is likely the group behind opOES does not represent the core of Anonymous supporters or ideology and is likely an anarchist offshoot not directly affiliated with Anonymous attacks.

In December 2010, Anonymous targeted the MasterCard, Visa and PayPal websites, dubbing the attacks "Operation Payback." These attacks were high-profile retaliatory attacks in response to the sites closing payment processing to WikiLeaks. The shutdown halted donations to the WikiLeaks site, potentially crippling it. Intense discussions surrounding these attacks were observed in multiple Anonymous-affiliated IRC chat rooms. Similar discussions were not observed on the same communications channels or with the same intensity discussing opOES.

The Anonymous group's 2010 targeting of a financial institution via Low Orbit Ion Cannon (LOIC) sets a precedent for attacks against large-scale financial institutions. However, their attacks were politically motivated due to the pressure on WikiLeaks, and it is highly likely that Anonymous' core does not currently support opOES.

Two confirmed Anonymous leaders have been observed within the opOES-themed chat rooms planning the operation. Both actors have a relatively high level of access to Anonymous communications and direct access a large pool of Anonymous sympathizers. However, the opOES planning channel, which contains these Anonymous actors, has few other leadership figures present. This may indicate that the actors behind the operation are not supported by the larger Anonymous population. Given the targets chosen by the actors, it is likely that a small anarchist group with support from a small group of Anonymous sympathizers is attempting to hijack the Anonymous infrastructure and popularity to conduct their own ideologically motivated attacks against global financial institutions. It is unlikely that the opOES attacks will amount to any significant threat to the US Federal Reserve or other related global financial institutions.

Drone Attacking AnonOps Servers Identified

Originally published on April 21, 2011

Key Points:

- A source has observed distributed denial-of-service (DDoS) attacks targeting AnonOps, the unofficial central leadership cell of Anonymous, which began as early as March 14, 2010, and enumerated drones participating in the incident.
- The attacks have not been attributed, though they may be linked with splinter elements, such as Backtrace security or anti-Anonymous activist actors.

Overview

A sensitive source has observed drone systems carrying out DDoS attacks on servers used by AnonOps, the unofficial central leadership cell of Anonymous. Attacks began as early as March 14, 2010, and are ongoing, though they have not caused observable service disruption. Attacking drones, which are enumerated in this report, may be proxies, and there is no indication whether systems were voluntarily taking part in attack infrastructure or surreptitiously compromised and controlled by remote actors. Many of these addresses may also be spoofed by attackers to conceal true attack infrastructure.

Attacks against AnonOps infrastructure are frequent and remain definitively unattributed. According to the source, AnonOps leadership has posited numerous attribution scenarios of the incident, conjecturing that the attacks could be the work of anti-Anonymous activists, such as the widely known actor th3 j35t3r (for further details, please see iSIGHT Partners. *ThreatScape Network Conflict* "Disrupting the eJihad" Intel-199093. Jan. 21, 2010). Furthermore, membership has indicated that the attacks could be tied to rival splinter groups. Membership explicitly implicated Backtrace Security, a splinter group that has broken with Anonymous on ideological grounds, claiming that the group had become too involved in moral issues and lost touch with the chaotic principles that had previously defined its activities.

Other recent incidents, such as attacks against the Spanish financial sector, indicate that Anonymous elements are taking initiative and pursuing divergent objectives, possibly leading to greater fractionalization (for further details, please see iSIGHT Partners. *ThreatScape Network Conflict* "New Anonymous Operation Targeting Financial Institutions in Spanish-Speaking Countries." Intel- 389414. April 15, 2011). Additional possible attackers include past victims of Anonymous, though there is no precedent for such activity.

Attacks are likely to continue against AnonOps in the near term; however, there is no indication that they will significantly disrupt operations. Nevertheless, these incidents may signify a greater threat to the organization, as elements fraction to pursue objectives and wage internal conflicts.

Anonymous Members Demonstrating Increased Intent and Capability to Conduct Planned and Opportunistic High-Profile Intrusions

Originally published on April 27, 2011

Key Points:

- According to sensitive source reporting, throughout April 2011, actors affiliated with the Anonymous movement have engaged in a series of corporate network intrusions against multiple high-profile targets (including Sony and Fox), resulting in the procurement of a substantial amount of confidential information and network enumeration data.
- The Fox.com operation was likely more opportunistic than targeted, whereas the Sony intrusion may have been specifically planned and targeted as a retaliatory measure.
- The extent and exact nature of data that the malicious actors procured is currently unclear, but definitely includes extensive network enumeration data, database credentials, passwords and the likelihood of access to internal corporate communications.
- As password reuse is common, the procurement of such data could represent a serious threat not only to corporate network and operational integrity, but also to customer/subscriber data. The data could also be used to discredit the corporations as part of Anonleaks activity, which could have long-term brand impact.

Overview

Sensitive source reporting indicates that Anonops-affiliated actors have actively discussed and executed targeted intrusions against high-profile corporate entities to include Sony and Fox. The concept of operations for these intrusions varies in each case, although a source with direct access claims that discussions occurred within the last three weeks. The motivations behind these intrusions are likely varied. With Fox, actors appeared to be motivated by opportunism; the network was compromised by vulnerabilities found in the configuration of Fox.com, but the tactics, techniques and procedures (TTPs) behind other breaches are currently unclear. Concerning the high-profile Sony intrusion, a source with direct access characterized discussions as having a more targeted intent, possibly in regard to recent legal actions carried out by the company, but it is unclear whether the source of the intrusion was internal or external. The actors behind these recent intrusions are likely closely affiliated with the Anonymous movement's leadership figures, but these three intrusions do not appear to be part of a large-scale, coordinated effort with substantial support from the Anonymous collective. Rather, they were likely discussed and/or executed by a few highly coordinated, technically sophisticated individuals who identified the value of procuring such data. The adversary's accumulation of a massive amount of potentially high-value data could be used in various ways, but actors will likely seek out an opportunity to release the data itself or publicize their access in a well-timed and likely self-serving manner. This could include attempts at discrediting the companies in an Anonleaks or HBGary-like scenario, circulating captured credentials or propriety data for illicit financial or intelligence gain, or any other future exploitation that is deemed politically expedient when the time arises.

Attack on Sony

Sensitive source reporting indicates that Anonymous-affiliated actors began discussing targeting Sony on April 17, 2011. This effort is believed to have resulted in an active intrusion attempt, although the tactics used in the intrusion are currently unclear. A source with direct access claims that the Anonymous actors may have had prior communications with a Sony insider who facilitated the intrusion. It is

unknown whether the alleged insider approached Anonymous members him/herself or vice versa. The PlayStation Network/Qriocity service has been unavailable since April 20. Sony issued a press release on April 26 stating that unauthorized intrusions occurred from April 17-19, which corroborates sensitive source reporting. Sony announced it had experienced a significant data breach with the loss of more than 70 million subscribers' names, addresses (city, state, zip), countries, e-mail addresses, birthdates, PlayStation Network/Qriocity passwords and logins and handles/PSN online IDs. It remains unclear whether any credit card or other personal financial information was compromised.

The targeting of Sony may be related to perceived injustices regarding a recent lawsuit, given the emergence of Anonymous members' rhetoric over suppression of "free speech." In early January 2011, Sony filed suit against a hacker named George Hotz and other hackers for jailbreaking the PlayStation 3 (PS3) platform. Hotz posted information regarding the jailbreak on his website, along with a YouTube video of him conducting the hack. In reaction, Sony filed for a restraining order against Hotz and filed suit for damages. On April 11, 2011, Sony posted on its PlayStation blog that Sony and Hotz reached a settlement that included a permanent injunction banning Hotz from posting information about the hack, and that the settlement was reached in principal on March 31, 2011. On April 4, 2011, (before Sony's blog announcement, but apparently after the settlement was reached) Anonymous members warned Sony Anonymous was going to attack the company over this lawsuit. The warning was followed by an alleged distributed denial-of-service (DDoS) attack targeting Sony.com and Playstation.com.

It is unlikely the Hotz' jailbreaking of the PS3 platform would have led to, or given any advantage to, an intrusion launched against the PlayStation network, as his published hacks are only effective locally on an individual PS3 machines. The case against Hotz was brought under the Digital Millennium Copyright Act because Hotz published an encryption key and software tools that would allow someone to take control of their individual PS3 box and run software of their choosing. These capabilities would likely not allow for intrusion against the entire PlayStation network.

Fox.com

The Fox.com compromise was likely an opportunistic rather than a targeted attack. A source with direct access to information surrounding the Fox compromise indicated that actors placed a web shell on the Fox.com server and used it to conduct reconnaissance on internal Fox networks. Adversary actors then found database credentials in the source code of the website's PHP files. The result of this compromise reportedly involved exfiltration of a large amount of data, although the full nature of this dataset remains unknown. The attackers' intentions for future utilization of the data also remain unclear. The Anonymous hackers' alleged emphasis on the stealthy acquisition of this data suggests the actors may intend to use this data in the future for a still undetermined purpose. A source with direct access indicated that there were limited conversations pointing to political motivations for releasing Fox data (or proving that Fox's networks were compromised) because of perceptions of Fox's political persuasions. For example, actors could release internal communications from the company as part of an Anonleaks scenario, as actors' believe Fox's reporting on WikiLeaks or similar Anonymous-supported causes is biased. The same source indicates that other tactics such as defacements were briefly considered.

The tactics, techniques and procedures used by actors in the intrusion could be characterized as sophisticated and resourceful. Actors initially breached security by exploiting a local file include vulnerability; it is possible that a malicious actor randomly discovered this vulnerability and was not specifically targeting weaknesses in Fox.com's security. Once the initial vulnerability was identified, actors were then able to leverage it to procure more information about the network and identify further vulnerabilities.

Possible Motivations Behind the Attacks and Future Use of Data

The motivations behind these intrusions have not been clearly expressed by the actors and do not appear to be part of a specific coordinated campaign. The operators' procurement of data, information and access provide significant potential future leverage for a number of future outcomes. It is likely that any access will be leveraged for further information acquisition efforts, including reconnaissance and document exfiltration. Sensitive corporate information and documents may be used for future political posturing and influence operations. Sensitive personal information may be publicly released in an effort to damage consumer confidence in Sony. It remains unclear whether the attackers were able to compromise credit card information. If so, this information could be publicly released, privately exploited or sold. The group could also release fake credit card numbers in an effort to further discredit these companies' corporate images.

While neither the group nor its members have appeared to be motivated by financial gain of compromised credentials, Anonymous actors have previously sought to acquire credentials and create the illusion they had compromised credentials. According to sensitive source reporting, in the midst of Operation Payback during December 2010, Anonymous members suggested contacting a PayPal insider who could access data centers. PayPal was on a list of potential targets due to its corporate decision to block transfers to an account set up to accept donations for Bradley Manning's defense fund (Manning is accused of allegedly providing documents to the WikiLeaks organization). The source indicated that an actor with the moniker Deviant posted PayPal credentials that appeared to be legitimate and live as of late April 2011, and that actors had logged in to the accounts and changed the passwords to gain exclusive control over them. In the same vein, in December 2010 Anonymous claimed to have breached an unknown number of MasterCard credit card numbers and posted them on a Pastebin site. These numbers were later determined to be false, and it appears that Anonymous members sought to create the illusion that MasterCard's servers were breached in order to inflict reputational damage on the company.

Implications and Outlook

The actors who likely committed these intrusions have coordinated on operations in the past and are comprised of a core group of more sophisticated actors with specialized skill sets (e.g., some focus on SQL injections, others are skilled at remote file includes, etc.). It is possible that the actors involved in ongoing intrusions were also aware of—or were in some part responsible for—earlier corporate intrusions such as the operation against HBGary. In early February 2011, Anonymous successfully hacked HBGary's network and gained access to executive-level e-mail archives. The attack was motivated by claims of HBGary employee Aaron Barr that he had attribution information on Anonymous actors. In response, Anonymous leaked the compromised e-mails, which contained sensitive information on the company's government and private clients.

Actor behavior indicates the group may intend to use this data in the future for a still undetermined purpose at a time deemed to be reputationally or politically expedient in the eyes of the perpetrators. This opportunistic behavior, strongly influenced by political beliefs and specific ideologies regarding perceived injustices around free speech and/or corporate malfeasance, appears to be escalating in seriousness and is likely to be reinforced by press coverage and increased publicity.

New Anonymous Operation Targeting Financial Institutions in Spanish-Speaking Countries

Originally published on April 29, 2011

Key Points:

- On April 14, 2011, Anonymous began a new operation dubbed "Operacion Hipoteca," targeted against financial institutions in Spanish-speaking countries, primarily Spain—but it could also include targets in South America.
- The alleged motivation for the attacks is governments' and financial institutions' failure to help the people who have been hit by the economic crisis or other personal tragedy, landing them into financially untenable situations while these entities have only increased their own bonuses and other benefits.
- The first target of the operation was the Spanish bank BBVA, who was hit with a distributed denial-of-service (DDoS) attack that made its website inaccessible for approximately 12 hours. Other potential targets included in Anonymous' communication are Banco Santander, La Caixa and Bankia, though none of these banks have yet been attacked.

Anonymous Announces Operation "Hipoteca"

On April 14, 2011, the Spanish branch of Anonymous announced a new campaign dubbed "Operacion Hipoteca" (Operation Mortgage). The operation plans to target financial institutions in Spanish-speaking countries, who Anonymous is accusing of repossessing homes due to nonpayment of mortgages. The manifesto—published as part of the launch of the operation—states that the government has not protected its people from abuse by big corporations, but has rather conspired with them so that while the common people are suffering from the economic crisis, the big business stakeholders and politicians are only seeing increased profits.



Part Anonymous' communication concerning the motivation and justification for Operation Hipoteca (iSIGHT Partners)

The case of José Luis Burgos, who has been fighting Banco Santander for two years over a mortgage, is given as an example of corporate mistreatment of its customers. Burgos was diagnosed with scoliosis in 2005 and forced to leave his job; however, his insurance did not cover payments for the mortgage that he had taken three years earlier with Santander to renovate his house. In April 2010, Burgos received a notice from Santander threatening to take his home due to nonpayment.

The operation, and its first target, BBVA, were announced on Anonymous' Twitter account on April 14, 2011. Following the announcement, BBVA's website was intermittently inaccessible for approximately 12 hours due to Anonymous' DDoS attack. Similar to previously observed attacks, the group used IRC DDoS infrastructure, which relies on tools such as the Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC) and Geosynchronous Orbital Ion Cannon to launch largely volunteer-based DDoS attacks, though iSIGHT Partners has previously reported that the group is highly likely also using a secondary botnet to bolster its attack capacity (for more information regarding Anonymous and its capabilities, see iSIGHT Partners. *Global Monthly Threat Report*, "Anonymous Using Secondary Botnet to Support DDoS Activities." Intel-376246, March 15, 2011).

Although the operation was announced on Anonymous' Twitter account, it was somewhat independent from the group's core operational group, and the participants were primarily Spanish-speaking actors, including the organizer who uses the handle "Renegado." Although several active actors, such as tflow (likely a Brazilian actor that has been connected to the HBGary attack), Mestri and Ryan (also known as "v") participated in the attack, the organizer and most of the actors are not the same as the core group that is responsible for Operation Freedom and Payback.

The communication published by Anonymous lists Banco Santander, La Caixa and Bankia as potential targets; however, their websites do not appear to have been attacked at this time. Several other banks, including Banesto, Cajamar, Cam Bank, Solbank and Bankinter could also be targeted as each of the banks seem to regularly conduct repossessions of property, which they resell to new customers, offering them 100 percent mortgage on these properties. In 2009, several large Spanish banks and investment banks had become Spain's biggest real estate companies due to large numbers of repossessions, and they now own between several hundred to thousands of residences throughout Spain.

Implications

Although the operation is currently only targeting financial institutions in Spanish-speaking countries, it could be expanded to cover financial institutions in the United States. In the US, the targets would highly likely include companies such as AIG that received government bailout money and were accused of fraud or other wrongdoing following the economic crisis.

Following the attack, on April 15, 2011, Anonymous websites anonymous-spain.es and anonspain.com were taken offline. Anonymous-spain.es was likely taken down by its web hosting service Strato. This action will likely exacerbate the situation, as several previous cases, such as the compromise of HBGary's servers, demonstrate that Anonymous is easily provoked by action against its infrastructure. The group frequently attempts to retaliate following disruption in order to show its resilience and to demonstrate its superiority compared to its adversaries. The takedowns were likely due to the attack against BBVA; however, other Anonymous websites and servers have also undergone several DDoS attacks recently, which are possible organized by a group calling themselves "Backtrace Security," which is comprised of ex-Anonymous members who have publicly vowed to bring an end to Anonymous, who they see as having moved too far from its roots.

AnonOps Attacked by Splinter Group; Adopts Web Server Attack Tool 'Slow Post' for New Campaigns

Originally published on May 9, 2011

Key Points:

- According to iSIGHT Partners' sources, AnonOps—the central IRC network of Anonymous—came under distributed denial-of-service (DDoS) attack throughout the end of April 2011 by actors formerly associated with the movement.
- These actors conducted the successful attacks by leveraging botnets that included compromised web servers.
- Anonymous has developed and began to field a tool for leveraging compromised web servers in denial-of-service (DoS) attacks and used this tool in attacks against websites of the New Zealand government.

Overview

DDoS attacks targeting AnonOps throughout the end of April 2011 were conducted by actors associated with the website 808chan.org. These actors were previously heavily involved in Anonymous activity, but have since separated from the group. These actors used botnets and compromised web servers to conduct the DDoS attacks, leveraging significant bandwidth in the process. Following the attacks, actor NewEraCracker disseminated the 'Slow Post' DoS tool, which acts on the same principle by harnessing the bandwidth of compromised web servers. Slow Post was used shortly thereafter to target New Zealand government websites. Employing tools such as Slow Post will significantly reduce the participation levels necessary to carry out disabling attacks, but it will require a threshold of sophistication for the user, creating a barrier to entry that may be insurmountable to the average Anonymous member.

Anonymous Splinter Group Successfully Attacks AnonOps

A series of DDoS attacks against AnonOps, the central IRC network of Anonymous, successfully disrupted the organization's activities throughout the end of April 2011. According to iSIGHT Partners' sources, attacks were conducted using a botnet of surreptitiously compromised drones rather than the participatory infrastructure more commonly and widely used by Anonymous. Additionally, the attacking botnet consisted of compromised web servers and leveraged significant bandwidth. Attacking drones are listed in this report.

According to iSIGHT Partners' sources, attacks against AnonOps were conducted by partially identified actors acting on personal rather than ideological motives. Actors implicated in the attacks are:

- xero
- nikon
- chippy1337
- zedkappa
- EvilHom3r

The actors are believed to be tied to 808chan.org, a forum similar in many regards to 4chan.org, the forum that most heavily influenced the creation of Anonymous. Like 4chan.org, 808chan.org is associated with relatively banal activity and socially deviant behavior. Actors associated with 808chan.org are believed to have taken an early role in organizing AnonOps and providing an unknown portion of the server infrastructure used to host the operation. However, after a falling-out with other Anonymous leadership figures in late 2010, the organization's role in maintaining the server infrastructure ended.

Despite their attacks on AnonOps, actors have formed strong ties to AnonOps administrator Ryan. Ryan is believed to have previously collaborated with xero and nikon to attack 4chon.net, when users of that site were found spamming links on encyclopediadramatica.ch, a website that categorizes lexicon specifically devoted to Anonymous and its associated activities. Since this collaboration and despite attacks on AnonOps servers, which Ryan administers, the actors appear to remain in contact and on agreeable terms.

AnonOps Recovers and Conducts Attacks Against New Zealand and Iran

After recovering from the late April attacks, Anonymous has principally focused on the New Zealand and Iranian governments. Operation Iran, which was timed to coincide with International Worker's Day on May 1, successfully shutdown Iranian state websites including the Office of the Supreme Leader and the Islamic Revolutionary Guard. The attacks are an offshoot of Operation Freedom, Anonymous' larger campaign in support of revolutionary activity in the Muslim world.

Attacks against the New Zealand government are motivated by that country's passage of stringent copyright legislation in April 2011. The new law will require Internet Service Providers (ISP) to notify customers suspected of copyright infringement three times before ultimately cancelling service. Additionally, the legislation grants a copyright tribunal power to grant significant damages to copyright holders in legal claims. Attacks against the New Zealand government, which successfully disrupted online access to New Zealand government services, are part of Operation Payback, the major Anonymous campaign that has principally focused on issues related to copyright and transparency.

New DoS Tool Adopted Following Attacks

Attacks against New Zealand were conducted in part by using a DoS tool created by NewEraCracker, the creator of the Low Orbit Ion Cannon (LOIC). The PHP tool, which is called Slow Post, can be surreptitiously dropped on a compromised web server. When directed to attack a target, the tool leverages the server's available bandwidth, which could be significantly greater than bandwidth available to workstations taking part in LOIC attacks. It is believed that NewEraCracker was inspired to create the tool following the successful attacks against AnonOps, which are believed to have been carried out in a similar manner.

```
root@server [/tmp]# php slowPOST.php

SLOW
POST

v0.5.3 Alpha by NewEraCracker

Please specify the target url: 
```

Screenshot from Slow Post DDoS tool

During the attacks against New Zealand government sites, Anonymous members claimed to have compromised the site watchdog.net.nz, the website of an ISP that purposely blocks significant content from users. The Slow Post tool was allegedly loaded to the site's web server, which was then directed to attack the website of New Zealand's Parliament, parliament.nz.

Implications

Attacks against AnonOps are the most recent expression of a longstanding schism within Anonymous between Anonymous' current politically motivated form and its more chaotic and socially deviant past. As Anonymous members take a greater interest in ideological issues, this schism is likely to deepen. Furthermore, incoherent ideology has led to the fragmentation of participants into single-issue splinter groups that have separated from mainstream membership as disagreements over the organization's ideological future materialize.

The propagation of new attack methodologies to Anonymous is significant. Server-based DoS is a powerful capability that could be leveraged to lower the participatory requirements of attack campaigns. However, this capability will require greater sophistication on the part of attackers and is unlikely to be widely used in the same manner as the LOIC.

Anonymous Likely to Remain Viable Despite Leadership Schism

Originally published on May 10, 2011

Key Points:

- A long-standing schism between Anonymous actor Ryan and other members came to a head when Ryan's IRC operator status was taken away in early May 2011.
- Ryan had been carrying out distributed denial-of-service (DDoS) attacks in conjunction with actors from an Anonymous splinter group and may have been attempting to wrest complete control of AnonOps from other administrators. Ryan, who was likely identified, has crippled AnonOps temporarily and is likely responsible for releasing a list of member IP addresses.
- Ryan's involvement in AnonOps had been largely detrimental and his departure may return some organizational cohesion, but Anonymous still suffers from the challenges of running a leaderless organization while members exercise disparate levels of influence.

Outlook

Continued pressures driving toward increased fragmentation of the loosely constituted AnonOps leadership structure within the Anonymous hacker movement created a crisis among the group's key members in early May 2011. AnonOps administrator Ryan's long-standing estrangement from other group leadership came to a head when his IRC operator status was taken away and he was accused of conducting attacks against AnonOps in collaboration with an Anonymous splinter cell. Ryan, who has been in conflict with several members of Anonymous, is believed to have been attempting to wrest control of AnonOps communications and command infrastructure. Ryan has since cut off portions of AnonOps under his control and carried out attacks on remaining infrastructure. Furthermore, he is believed to be responsible for publishing a list of IP addresses associated with Anonymous members. Despite the chaos surrounding his departure, Ryan's exit may be healthy for the organization, which has lost significant factions due to Ryan's personality conflicts. However, Anonymous faces undeniable structural challenges that are likely to lead to future conflicts between emergent leadership.

Ryan Breaks with Anonymous

The ongoing estrangement of Anonymous leadership figure and AnonOps administrator Ryan (aka v, aka viral) from core membership came to a head when his IRC operator status was revoked on May 6, 2011. Ryan has been accused by core Anonymous membership and AnonOps infrastructure administrators of carrying out the DDoS attacks that disrupted the service throughout the end of April.

Ryan is believed to have carried out attacks against AnonOps in collaboration with an Anonymous splinter group associated with related sites 808chan.org and skidsr.us (for further details, see iSIGHT Partners. *ThreatScape Network Conflict*, "AnonOps Attacked by Splinter Group; Adopts Web Server Attack Tool 'Slow Post' for New Campaigns." Intel-399485. May 9, 2011). It is possible the attacks were part of a broader attempt to wrest greater administrative control of the AnonOps server infrastructure.

Ryan has been a consistent source of personality conflict within AnonOps, particularly with other administrators who have control over the disparate servers that form the organization's infrastructure. Ryan and the actor Owen have been at the center of this conflict, and Owen has previously negotiated with Ryan over ownership of AnonOps infrastructure. Notably, other conflicts with Ryan have led to the estrangement of the Hispanic faction of AnonOps, which in turn led to the migration of these

participants to anonworld.net, a second IRC network. Altercations between Ryan and other members often reflect Ryan's immaturity and desire for greater control of the AnonOps network.

After having his IRC status revoked, Ryan redirected several key Anonymous-branded domains away from the AnonOps IRC network and launched DDoS attacks on servers connected to the remaining network. In response, the remainder of the AnonOps network administrator staff distributed a press release warning members to avoid redirected domains. As of this writing, core components of the group's communications infrastructure are still not functioning.

Dear Users of the AnonOps Network,

We regret to inform you today that our network has been compromised by a former IRC-operator and fellow helper named "Ryan". He decided that he didn't like the leaderless command structure that AnonOps Network Admins use. So he organised a coup d'etat, with his "friends" at skidsr.us. Using the networks service bot "Zalgo" he scavenged the IP's and passwords of all the network servers (including the hub) and then systematically aimed denial of service attacks at them (which is why the network has been unstable for the past week). Unfortunately he has control of the domain names AnonOps.ru (and possibly AnonOps.net, we don't know at this stage) so we are unable to continue using them. We however still have control over AnonOps.in, and will continue to publish news there.

We would **STRONGLY ADVISE** all users to **STAY AWAY** from AnonOps.net and AnonOps.ru, and they should be considered COMPROMISED. Using or connecting to any service on those addresses may put your computer, and by extension your person, at risk.

We will continue to update you on this story, as well as on how we proceed with the future of Anonops.

We are **profoundly sorry** for this drama, and we can't give you an estimate on when service will resume normally.

Alas, the IRC-network will probably remain down until we can sort this out.

We will try to keep you up to date you via our official channel (anonops.in).

Signed,

The "Old" AnonOps netstaff.
"shitstorm", "Nerdo", "owen", "blergh", and "Power2All"

P.S: Further notices on AnonOps.net/ru will probably be posted to dispell this one, and any unavailability of AnonOps.in will only prove this message is true. **THIS IS NOT A JOKE, THIS ISN'T A LIE, THIS IS THE TRUTH AND WE ARE SORRY FOR THAT.**

P.P.S: The person behind this attack is also involved in the "new" Encyclopedia Dramatica (encyclopediadramatica.ch). If you have previously signed up as a user with a legitimate email-address/password, you should take caution and consider that your account and password *might* be compromised.

tl;dr:

AnonOps.ru/net got hijacked by a rogue admin, and no longer has anything to do with AnonOps, this domain should **NOT** be used if you wish to connect to the legitimate AnonOps network. Please use anonops.in instead. Sorry!

An unknown actor released biographical data on Ryan following the split, identifying Ryan as a juvenile from Wickford, England. This data is confirmed by sensitive single-source reporting. Since the release, he has received numerous death threats and been subjected to physical harassment. During the same period, a list of Anonymous members and corresponding IP addresses were released. The list, which has been validated in part by a sensitive source with indirect access, is likely have to been released by Ryan, who could have leveraged his ownership of the AnonOps infrastructure to collect this data.

Implications

The fallout between Ryan and Anonymous leadership figures is not a major shock to the group, as Ryan's behavior had eroded his relationships well before the most recent events. Previously, Ryan's influence was primarily negative, resulting in divisions between the leadership influencers and major participant factions such as the Hispanic group, the core organizational element consisting of Spanish-speaking Anonymous actors. In the long term, Ryan's abrupt departure may in fact bring greater cohesion to the group, as detractors return to the AnonOps core.

However, this event illustrates the fundamental challenge faced by this "leaderless resistance" and non-hierarchically organized network. Despite its democratic ideals, the group does require leadership elements to coordinate and carry out many functions, such as network administration. Other capabilities, such as the use of botnets rather than the participatory Low Orbit Ion Cannon (LOIC) system, also skew individual perceived importance to the group as a whole, and allow for the aggregation and exercise of power within the group. These functions necessarily create members with greater influence than others, who may come into conflict.

Such conflicts are likely to arise in a system that does not recognize distinctions of leadership, though it clearly exists, and therefore does not possess a viable dispute resolution construct that does not involve the withdrawal of consent. It is a short step from the denial of continued participation to the attempt to forge alternative participation pathways, particularly for young and idealistic individuals whose sense of identity formation is increasingly intertwined with these activities—especially given the reinforcement of worldwide media coverage. Continued conflict between factions is likely to offer an equally robust sense of importance to involved individuals and may drive competitive efforts to sabotage other factions and to accomplish independent operational objectives against the movement's targets.

LulzSec Most Likely Anonymous Attribution Front

Originally published on May 10, 2011

Key Points:

- On May 7, 2011, a group calling itself LulzSec began to leak data obtained through a compromise of Fox.com.
- According to a sensitive source with direct access, LulzSec is the Anonymous faction responsible for an intrusion of Fox.com—previously reported by iSIGHT Partners—and intrusions targeting Sony, HBGary and the Westboro Baptist Church.
- LulzSec is likely to have been created as an attribution front due to the legal implications of the attacks it has carried out, especially given the fallout surrounding the Sony intrusion.

Overview

A group calling itself LulzSec began to release data obtained through a compromise of Fox.com on May 7, 2011. The group initially released a database containing personal information regarding the applicants for the television series the *X-Factor*. The group then released a database of credentials associated with the site two days later. Though the faction has publicly refuted claims that it is associated with Anonymous, sensitive source reporting indicates that LulzSec is the same Anonymous faction that carried out compromise operations against Fox.com, Sony, HBGary and the Westboro Baptist Church. The faction is likely an attribution front created due to the legal implications of its intrusion activities, which are often in conflict with the stated ideological boundaries of the Anonymous collective. The continued fallout from operations targeting Sony are likely a strong impetus for this front's fabrication, allowing key Anonymous leadership influencers to maintain a degree of rhetorical distance from hardcore intrusion operators in order to avoid potential abandonment by supporters unwilling to cross certain perceived legal or ethical bright lines.

LulzSec Emerges

On May 7, 2011, a group calling itself LulzSec released information from a compromised database of potential contestants applying to be part of the Fox network television series *X-Factor*, distributing the information through a popular peer-to-peer (P2P) torrent tracking service. The release coincided with the establishment of the Twitter account @LulzSec, which advertised the leak and promised further information releases.

X Factor Leaked Contestants Database

Type: Other > Other

Files: 2

Size: 32.58 MB (34160784 Bytes)

Quality: +0/-0 (0)

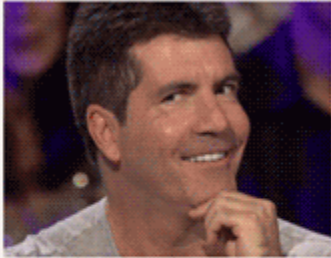
Uploaded: 2011-05-07 03:19:34 GMT

By: LulzSec

Seeders: 0

Leechers: 0

Comments: 0



Tweet

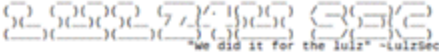
0

Download

Enjoy Movies, TV Shows, Music and Games on your browser!

[DOWNLOAD THIS TORRENT \(MAGNET LINK\)](#)

[DOWNLOAD THIS TORRENT \(TORRENT FILE\)](#)



we did it for the lulz -LulzSec

Hello, good day, and how are you? Splendid! We're LulzSec, a small team of lulzy individuals who feel the drabness of the cyber community is a burden on what matters: fun. Considering fun is now restricted to Friday, where we look forward to the weekend, weekend, we have now taken it upon ourselves to spread fun, fun, fun, throughout the entire calendar year.

As an introduction, please find below the X-Factor 2011 contestants' contact information. Expect more to come, and if you're like us and like seeing other people get mad, check out our Twitter!

Host settings:
MySQL version: (5.1.47-log) running on 10.90.57.192 (www.fox.com)
Date: 22.04.2011 15:50:02
Database: "xfactorreg"

Sample:

id	firstname	lastname	dob	phone	email	auditiontype	numberofperformers
10	Nathan	Flanagan-Frankl	3/26/1992	8479772322	nflanaganfrankl@gmail.com	solo	0
11	Rossana	Ordonez	6/28/1985	7023277358	youthful_youth@hotmail.com	solo	0
12	Andrew	Miller	7/24/1989	6199946389	aspeventservices@yahoo.com	solo	0

[DOWNLOAD THIS TORRENT \(MAGNET LINK\)](#)

[DOWNLOAD THIS TORRENT \(TORRENT FILE\)](#)

X-Factor database leak on The Pirate Bay

On May 9, 2011, LulzSec issued a series of announcements from @LulzSec revealing the details of a compromise of credentials associated with the Fox Network. These targets included a series of LinkedIn accounts tied to Fox Network employees, which had been defaced by faction members. Subsequently, Twitter accounts associated with Fox affiliates were revealed to be compromised when they were made to comment directly to @LulzSec. Finally, a record of 396 alleged compromised accounts and passwords was released on Pastebin with a note claiming that LulzSec doesn't like Fox, and encouraging followers to search for and "ravage" social media accounts that share the same credentials.

© 2011 All rights reserved. iSIGHT PartnersSM, Inc. Confidential & Proprietary Document.

Page 73

```
1. #####
2. ## OFFICIAL LULZSEC MEMO OF JUSTICE ##
3. #####
4.
5. tl;dr http://i.imgur.com/TkI54.png
6. password list below
7.
8.
9. Dear Fox.com,
10.
11. We don't like you very much. As such, we cordially invite you to kiss our hand-crafted crescent fresh
    asses.
12.
13. Remember that time we leaked all your X-Factor contestants?
    http://thepiratebay.org/torrent/6372763/X_Factor_Leaked_Contestants_Database
14.
15. Well now we're leaking some more of your junk. We invite the Internet to ravage the following list of
    emails and passwords (from a database within Fox.com) - Facebook, MySpace, PayPal, whatever you can get
    your hands on. Take from them everything. Remember to proxy up, or tunnel like a pro!
16.
17. Follow us on twitter; we're owning more things next week. Kisses!
18.
19. All the best,
20.
21. LulzSec
22. twitter.com/LulzSec
```

Pastebin letter accompanying database link

Relationship to Anonymous

LulzSec has openly expressed solidarity with AnonOps, recognizing the ongoing availability problems facing the Anonymous communications network and stating, "let's cheer you up." However, the faction has explicitly denied its relation to Anonymous, as illustrated by the group's Twitter tagline:

Taking you on a wondrous voyage through time and space. The (bad) press likes to call us Anonymous, we aren't Anonymous! Kittens!

Sensitive source reporting indicates that LulzSec is indeed an Anonymous faction acting as an attribution front. The faction has allegedly fabricated the front because it is aware of the legal implications of its ongoing intrusion operations against multiple targets, which conflicts with the political ideology that Anonymous has adopted.

The compromise of a Fox.com server by Anonymous members in April 2011 most likely facilitated this incident. As previously reported by iSIGHT Partners, it is believed that Anonymous-affiliated intrusion operators placed a web shell on the Fox.com server and used it to conduct reconnaissance on internal Fox networks. Adversary actors then found database credentials in the source code of the website's PHP files. The same actors also carried out attacks on Sony (for further details, please see iSIGHT Partners. *ThreatScape Network Conflict*, "Anonymous Members Demonstrating Increased Intent and Capability to Conduct Planned and Opportunistic High-Profile Intrusions." Intel-394912. April 27, 2011). This Anonymous faction is also believed to be responsible for attacks on HBGary, Gawker and Westboro Baptist Church.

Implications

LulzSec is most likely an Anonymous faction comprised of sophisticated actors capable of carrying out significant intrusion activity. Though the group does appear to have some ideological grounding, the attacks they have carried out appear to be in part opportunistic, leveraging access opportunities based on potential publicity effects. Furthermore, the group has previously demonstrated its willingness to ignore the group consensus within the wider Anonymous movement—and within the narrow circles of key leadership influencers—to carry out attacks in spite of widespread condemnation, as in the case of the Westboro Baptist Church.

The creation of the LulzSec front is likely to have been brought about by pressure exerted on Anonymous following the compromise of Sony, in which the same actors likely took part. The backlash against Anonymous since that incident has been substantial, forcing the group to take the difficult step of "proving" its innocence in the court of public opinion. While LulzSec does not share the ethical constraints espoused by the mainstream Anonymous movement, in the near term, it is likely to take action on behalf of the organization and carry out attacks in concert with Anonymous objectives when circumstances permit. However, in the long term, it is possible that the group will become more ideologically divergent and pursue objectives of its own choosing on a greater scale. These developments are consistent with observed pressures toward factionalization, which point toward increasing potential incentives for independent action by smaller elements of the Anonymous movement.