Targeted Intrusions Exfiltrate Data from Pakistani Government Networks; Tied to Ongoing Strategic Campaign

Prepared for the U.S. Government

May 11, 2011

iSIGHTPARTNERS
Security beyond the edge

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 deposed 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.

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.

Contents

Executive Summary 4
Overview 4
Campaign Details 4
Victimology 5
Attribution 7
Links to Previous Campaigns 7
Outlook and Implications 8

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.

Originally published on April 26, 2011

Executive Summary

Key Points:

- Intrusion operations connected to an ongoing campaign targeting Pakistani government networks were observed on March 4, 2011, through April 7, 2011.
- These newly identified intrusions targeted the Embassy of Pakistan in the United States, the Pakistani Mission to the United Nations and the Pakistani Ministry of Interior's Federal Civil Defence.
- These intrusions are likely apart of an ongoing strategic campaign that will likely continue in the near to mid-term.

Overview

On March 4, 2011, a continuation of an ongoing series of intrusion operations targeting Pakistani government networks was identified. Intrusions observed from December 2009 through March 2010 are likely connected to these newly identified incidents. This new series of intrusion attempts targeted the Embassy of Pakistan in the United States, the Pakistani Mission to the United Nations and the Pakistani Ministry of Interior's Federal Civil Defence. These intrusion operations appeared to use common social engineering tactics and were likely enabled by targeted spear-phishing e-mails. The ongoing and apparently successful nature of these operations suggest that the operator responsible for these intrusions will execute additional operations in the near to mid-term.

Campaign Details

iSIGHT Partners observed a number of malicious payloads designed to perform document exfiltration connecting to two different drop zones. These malicious payloads have the following properties:

File: LATEST Indian and American Political people CARTOON.ppt
Size: 670294
MD5: ACDE02979B7B04A7645E00375F90F67D

File: Jihadism_is_Kufr__not_Islam_.doc.exe
Size: 349222
MD5: 12874BF21A56709451F2DF221C073F03

ACDE02979B7B04A7645E00375F90F67D was first observed on March 18, 2011, and 12874BF21A56709451F2DF221C073F03 was first observed on April 7, 2011.

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.

The payloads were likely delivered via a targeted spear-phishing campaign. Infected victims connected to and uploaded files to two FTP servers hosted at FTP.currentnewsstore[dot]com and FTP.alr3ady[dot]net.

FTP Server	FTP Account	IP
FTP.currentnewsstore[dot]com	down@currentnewsstore.com	96.44.189.184
FTP.alr3ady[dot]net	current@alr3ady.net	79.142.64.183
FTP.alr3ady[dot]net	dayteam@alr3ady.net	79.142.64.183

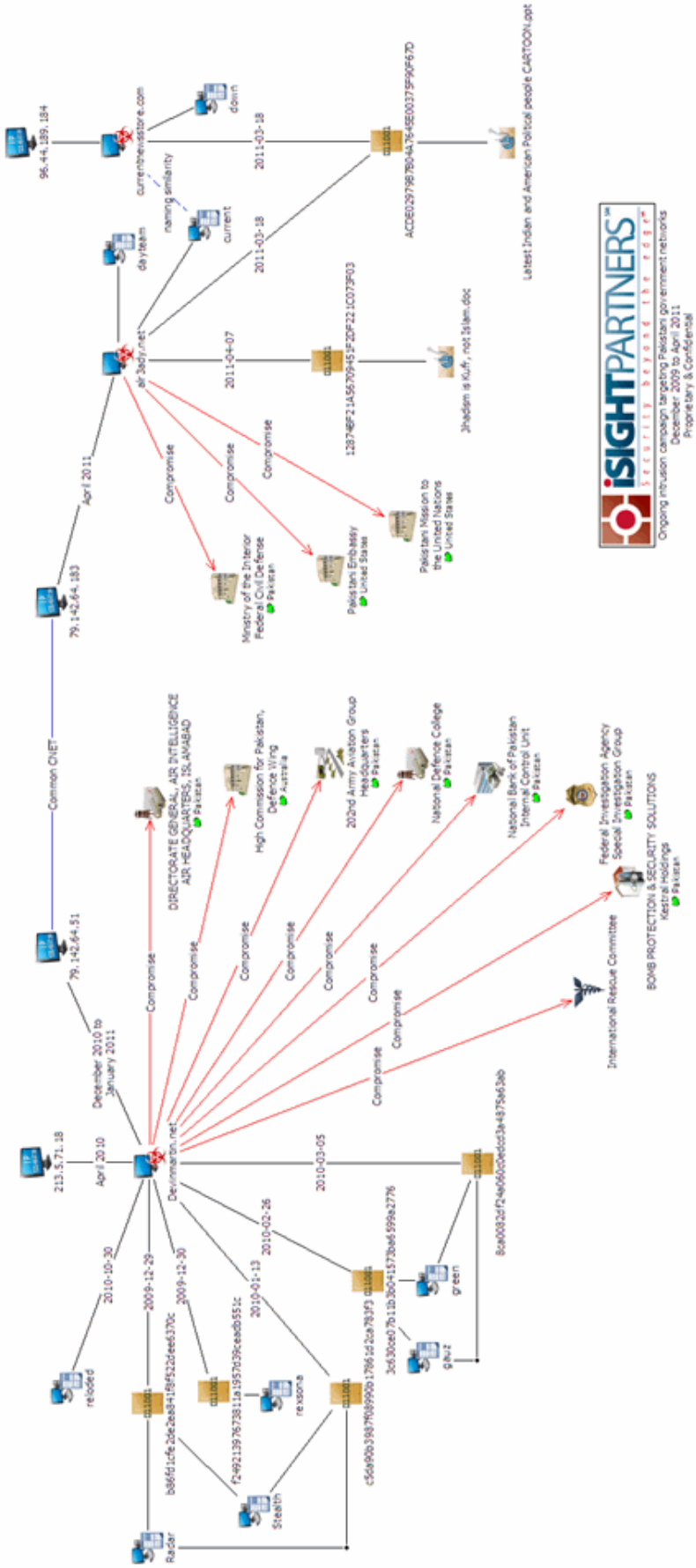
Drop zone details

The malicious payloads scanned victim hard drives for .pdf, .xls, .doc and .ppt files. Identified files were then exfiltrated to these drop zones. Previous identified malware payloads associated with this campaign had also targeted Keyhole Markup Language (.kmz) file types, but such targeting was not observed in this case. However, the functionality may have been presented by not observed.

Victimology

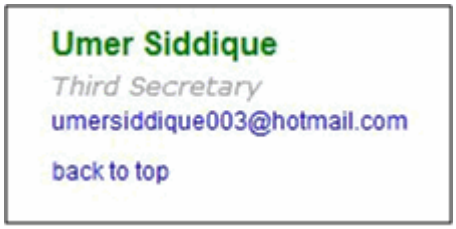
Targeted victims include the Pakistani Embassy to the United States of America, the Pakistani Mission to the United Nations and the government of Pakistan's Ministry of the Interior's Federal Civil Defense organization. Sensitive source reporting indicates compromised documents exfiltrated from victim networks included classified Pakistani diplomatic cables dating back to at least 2008, documents associated with the Pakistani High Commission, as well as details of bilateral meetings between the US and Pakistani governments. Additionally, documents related to military strategy and operations are believed to have been compromised, including schedules related to courses at the US Training Center, formerly known as Blackwater.

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.



© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.

This campaign likely utilized targeted spear-phishing e-mails as a propagation vector. The Pakistani Mission to the United Nations maintains a page on its website that includes e-mail addresses for its staff members.



E-mail address of indentified victim posted on pakun[dot]org

Sensitive source reporting identifies Umer Siddique as a likely victim of this intrusion campaign. It is therefore possible that Siddique's e-mail address, and the e-mail addresses' of other staffers found at the pakun[dot]org website, were used as a vector to target the Pakistani Mission to the United Nations.

Attribution

The currentnewsstore.com drop zone is currently hosted at 96.44.189.184. Between Nov. 21, 2010, and March 18, 2011, currentnewsstore.com resolved to 96.30.46.216. The 96.30.46.216 is maintained by an Internet service provider (ISP) known as Mantra Ventures. This provider maintains a domain at mantraventures.com. This domain is registered to:

> Mantra Tech Ventures Pvt Ltd.
> Arun Bansal (arun@arunbansal.com)
> #464, Neelkanth Apts, Sec-13,
> Delhi, 110085
> INDIA
> Tel. +91.01127550061

Although this identified relationship to an Indian company is of interest, it does not provide a definitive attribution to the operator responsible for these observed intrusions.

Links to Previous Campaigns

Between December 2009 and December 2010, iSIGHT Partners observed a similar malware-driven document exfiltration campaign targeting Pakistani defense networks. The malware variants used in this earlier campaign also exfiltrated sensitive documents to a remote FTP server hosted at the domain devinmartin.net.

Between Dec. 9, 2010, and Jan. 10, 2011, devinmartin.net resolved to the IP address 79.142.64.51. The alr3ady.net domain currently resolves to an IP address in the same C-NET at 79.142.64.183.

Additionally, the FTP accounts used to exfiltrate information to all of the identified drop zones were secured with the same six-character password (for more information on the earlier intrusion operations, please see iSIGHT Partners. *ThreatScape Network Conflict*, "Likely Indian Origin Malware Infection Targeting Pakistani Defense Networks." Intel-215836. March 12, 2010).

The newly observed malware payloads do not appear to include artifacts that previously were identified in earlier intrusion lures, which indicated authorship by an Indian defense contractor that offers services

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.

for the development of lawful intercept tools. However, the identified malware payload used to exfiltrate targeted documents does contain strings indicating that the malware tool may have originally been named "FTPBack," in a "new release," version 2. This bears a strong similarity to previously identified malware payload originally named FtpBackup, observed earlier in the campaign from December 2009. It is likely that the newly observed variant represents a progressive evolution of the malware payload utilized in the earlier campaign. The author or organizational entity responsible for development of this tool may be indicated by a further element of the string artifacts "BNaga." The tool was likely compiled using Visual C++ version 7, in a project directory named "kaam." This word can be translated as "work" in Urdu. In previously identified malware payloads, development was likely resourced through a freelance software programmer talent exchange. The services of this author or entity may have also been acquired through a similar pathway (for additional details on earlier attribution indications identifying developer and client in the 2009/2010 campaign series, please see iSIGHT Partners. *ThreatScape Network Conflict,* "Indian Defense Contractor Likely Developed Malware Utilized in Targeted Intrusions Against Pakistani Defense Networks." Intel-226199. April 8, 2010).

Personnel associated with the previously identified contractor were also identified in connection with attempted purchases of zero-day exploit code; however, it is unclear if any exploit code was used to deliver the identified malware in this case (for additional detail on these attempted purchases, please see iSIGHT Partners. *ThreatScape Network Conflict,* " Former Employee of Indian Government Contractor Attempts Purchase of Weaponized Adobe Exploit Code." Intel-245581. June 11, 2010).

Outlook and Implications

These campaigns were likely executed by the same operator and are part of an ongoing strategic espionage campaign aimed at the highest levels of the Pakistani government. The aggressive nature of this campaign—particularly the willingness to target communications from the Pakistani embassy—indicates that the operators responsible for this campaign are unlikely to discontinue operations.

Further, the individual intrusions that are a part of this campaign do not appear to rely on sophisticated techniques, tactics and procedures. Rather, the intrusions appear to be enabled via standard social engineering tactics as opposed to novel exploit code. Despite the use of common tactics, these operations appear to be successful and are therefore likely to continue.

While this continuing campaign appears to have connections to India, it remains unclear whether this intrusion operation is executed under official sanction, or as an independent action by individuals associated with the Indian defense contracting community.

© 2011 All rights reserved. iSIGHT Partners[SM], Inc. Confidential & Proprietary Document.