# PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs

NOVEMBER 9, 2016

*by Steven Adair*

In the wake of the 2016 United States Presidential Election, not even six hours after Donald Trump became the nation's President-Elect, an advanced persistent threat (APT) group launched a series of coordinated and well-planned spear phishing campaigns. Volexity observed five different attack waves with a heavy focus on U.S.-based think tanks and non-governmental organizations (NGOs). These e-mails came from a mix of attacker created Google Gmail accounts and what appears to be compromised e-mail accounts at Harvard's Faculty of Arts and Sciences (FAS). These e-mails were sent in large quantities to different individuals across many organizations and individuals focusing in **national security**, **defense**, **international affairs**, **public policy**, and **European and Asian studies**. Two of the attacks purported to be messages forwarded on from the **Clinton Foundation** giving insight and perhaps a postmortem analysis into the elections. Two of the other attacks purported to be eFax links or documents pertaining to the election's outcome being revised or rigged. The last attack claimed to be a link to a PDF download on "*Why American Elections Are Flawed*." Volexity believes a group it refers to as **The Dukes** (also known as APT29 or Cozy Bear) is responsible for post-election attack activity.

## Background

Since August of this year, Volexity has been actively involved in investigating and tracking several attack campaigns from the Dukes. Most notably the Dukes have previously been tied to the breach of the Democratic National Committee (DNC) and intrusions into multiple high-profile United States Government organizations. In July 2015, the Dukes started heavily targeting think tanks and NGOs. This represented a fairly significant shift in the group's previous operations and one that continued in the lead up to and immediately after the 2016 United States Presidential election.

On August 10, 2016 and August 25, 2016, the Dukes launched several waves of highly targeted spear phishing attacks against several U.S.-based think tanks and NGOs. These spear phishing messages were spoofed and made to appear to have been sent from real individuals at well-known think tanks in the United States and Europe. These August waves of attacks purported to be from individuals at Transparency International, the Center for a New American Security (CNAS), the International Institute for Strategic Studies (IISS), Eurasia Group, and the Council on Foreign Relations (CFR).

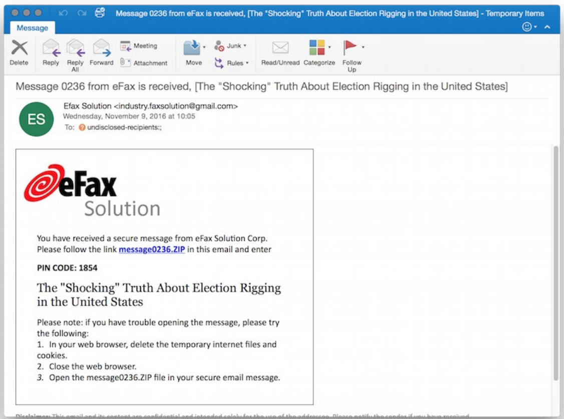
The Dukes are known for launching their attacks by sending links to ZIP files, that contain malicious executables, hosted on legitimate compromised web servers. However, each of the e-mail messages from the August attacks contained a Microsoft Office Word (.doc) or Excel (.xls) attachment. These attachments, when viewed, contained legitimate report content from each of the organizations they appeared to have been sent from. However, the attackers inserted macros into the documents designed to install a malware downloader on the system. Successful exploitation would result in the download of a PNG image file from a compromised webserver. These attack campaigns leveraged steganography in the PNG files by hiding components of a backdoor that would exist only in memory after being loaded into rundll32.exe. Volexity has dubbed this backdoor **PowerDuke**. Similar attack campaigns using documents with macros dropping PowerDuke were further observed through October, where Universities, and not think tanks appear to have been the primary targets. Details of these attacks have been provided to Volexity customers. Concerned NGO's and Universities that may have been targeted by these attacks campaigns are welcome to reach out for additional details.

## November 9 – Post-Election Spear Phishing Waves

The post-election attacks launched by the Dukes on November 9 were very similar to previous attacks seen from the Dukes in both 2015 and 2016. The PowerDuke malware, first seen in August 2016, was once again used in these most recent attacks. Three of the five attack waves contained links to download files from domains that the attackers appear to have control over. The other two attacks contained documents with malicious macros embedded within them. Each of these different attack waves were slightly different from one another and are detailed below.

### Attack Wave 1: eFax – The "Shocking" Truth About Election Rigging

The first attack wave is similar to much older attacks from the Dukes that purport to be an electronic Fax. This message claims to have been sent from Secure Fax Corp. and has a link to a ZIP file that contains a Microsoft shortcut file (.LNK). This shortcut file contains PowerShell commands that conduct anti-VM checks, drop a backdoor, and launch a clean decoy document. The e-mail message was sent from the attacker controlled e-mail account **industry.faxsolution@gmail.com**. The screen shot below shows the e-mail that was sent.


Message 0236 from eFax is received, [The "Shocking" Truth About Election Rigging in the United States] - Temporary Items
Message
Delete
Reply
Reply All
Forward
Meeting
Attachment
Move
Junk
Rules
Read/Unread
Categorize
Follow Up
ES
eFax
Solution

Message 0236 from eFax is received, [The "Shocking" Truth About Election Rigging in the United States]

Efax Solution <industry.faxsolution@gmail.com>
Wednesday, November 9, 2016 at 10:05
To: undisclosed-recipients:;

You have received a secure message from eFax Solution Corp.
Please follow the link message0236.ZIP in this email and enter

**PIN CODE: 1854**

The "Shocking" Truth About Election Rigging in the United States

Please note: if you have trouble opening the message, please try the following:

1. In your web browser, delete the temporary internet files and cookies.
2. Close the web browser.
3. Open the message0236.ZIP file in your secure email message.

Disclaimer: This email and its content are confidential and intended solely for the use of the addressee. Please notify the sender if you have received

SEARCH

RECENT POSTS

Microsoft Exchange Control Panel (ECP) Vulnerability CVE-2020-0688 Exploited

Vulnerable Private Networks: Corporate VPNs Exploited in the Wild

Digital Crackdown: Large-Scale Surveillance and Exploitation of Uyghurs

Active Exploitation of Newly Patched ColdFusion Vulnerability (CVE-2018-15961)

Magecart Strikes Again: Newegg in the Crosshairs

ARCHIVES

March 2020
September 2019
November 2018
September 2018
August 2018
July 2018
June 2018
April 2018
November 2017
July 2017
March 2017
November 2016
October 2015
July 2015
June 2015
April 2015
October 2014
September 2014

TAGS

digital surveillance crimeware APT Dukes Japan VPN Scanbox elections java vulnerabilities exploits Scanning spear phishing Drupal Afghanistan Gh0st Cisco Hong Kong China Adobe Flash

The e-mail contained links pointing to the following URL:

hxxp://efax.pfdweek[.]com/eFax/message0236.ZIP

Inside of this password (1854) protected ZIP file is a Microsoft shortcut file named:

**37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk**

Note that **pfdweek[.]com** appears to be under the control of the attackers but may be a hijacked domain.

Details on each of the files are included below.

**Filename:** message0236.ZIP
**File size:** 643843 bytes
**MD5 hash:** bea0a6f069bd547db685698bc9f9d25a
**SHA1 hash:** ee09bec09388338134d47fa993d5e0f86efe5bd4
**Notes:** Password protected ZIP file containing malicious Microsoft shortcut file (37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk)

**Filename:** 37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk
**File size:** 724003 bytes
**MD5 hash:** c272aebc661c54cc960ba9a4a3578952
**SHA1 hash:** 52d62213c66a603e33dab326bf4fa29d6ac681c4
**Notes:** Microsoft shortcut file with embedded PowerShell, PowerDuke backdoor (hqwhbr.lck), and clean decoy document.

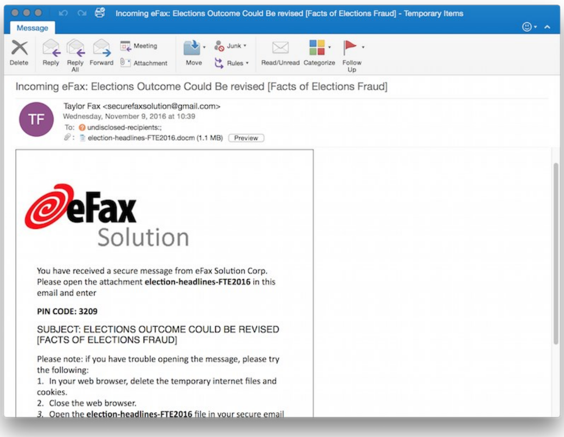
**Filename:** kxwn.lock
**File size:** 10752 bytes
**MD5 hash:** 28b95a2c399e60ee535c32e73860fbea
**SHA1 hash:** bf4ce67b6e745e26fcf3a2d41938a9dff1395076
**Notes:** Primary PowerDuke backdoor (DLL) loader (leverages kxwn.lock:schemas) dropped to "%APPDATA\Roaming\Microsoft\" with persistence via HKCU Run Key "WebCache" (rundll32.exe %APPDATA\Roaming\Microsoft\kxwn.lock , #2). Connects directly to **173.243.80.6:443** for command and control.

**Filename:** kxwn.lock:schemas
**File size:** 609853 bytes
**MD5 hash:** 4e1dec16d58ba5f4196f6a76a0bca75c
**SHA1 hash:** a7c43d7895ecef2b6306fb00972c321060753361
**Notes:** Alternate data stream (ADS) PNG file with the PowerDuke backdoor component hidden and encrypted within using Tiny Encryption Algorithm (TEA).

## Attack Wave 2: eFax – Elections Outcome Could Be revised [Facts of Elections Fraud]

The second attack wave that Volexity observed leveraged a Microsoft Word document with a malicious embedded macro. This appears to be consistent with several previous Dukes attack campaigns, such as those on August 25, 2016. The Macros contain several anti-VM checks designed to avoid executing in virtualized environments. The e-mail message was sent from the attacker controlled e-mail account **securefaxsolution@gmail.com**.

The screen shot below shows the e-mail that was sent.



Incoming eFax: Elections Outcome Could Be revised [Facts of Elections Fraud]

Taylor Fax <securefaxsolution@gmail.com>
Wednesday, November 9, 2016 at 10:39
To: undisclosed-recipients:;
: election-headlines-FTE2016.docm (1.1 MB) Preview

You have received a secure message from eFax Solution Corp. Please open the attachment **election-headlines-FTE2016** in this email and enter

**PIN CODE: 3209**

SUBJECT: ELECTIONS OUTCOME COULD BE REVISED [FACTS OF ELECTIONS FRAUD]

Please note: if you have trouble opening the message, please try the following:
1. In your web browser, delete the temporary internet files and cookies.
2. Close the web browser.
3. Open the **election-headlines-FTE2016** file in your secure email

Details on the malware components of this attack wave are included below.

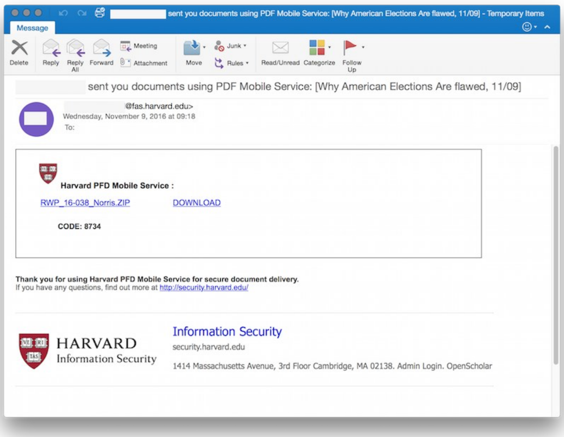
**Filename:** election-headlines-FTE2016.docm
**File size:** 835072 bytes
**MD5 hash:** a8e700492e113f73558131d94bc9ae2f
**SHA1 hash:** b5684384c8028f0324ed7119f6abf379f2789970
**Notes:** Document containing malicious macro that drops

**Filename:** fywhx.dll
**File size:** 10752 bytes
**MD5 hash:** ad6723f61e10aefd9688b29b474a9323
**SHA1 hash:** dd766876b3be5022bfb062f454f878abfbc670b8
**Notes:** PowerDuke backdoor file dropped to "%APPDATA\Roaming\HP\" with persistence via HKCU Run Key "ToolboxFX" (rundll32.exe %APPDATA\Roaming\HP\fywhx.dll #2). Connects directly to **185.132.124.43:443** for command and control.

**Filename:** fywhx.dll:schemas
**File size:** 608854 bytes
**MD5 hash:** 8c53ee9137a7d540fcff0d523f7d0822
**SHA1 hash:** ab32c09c46e0c9dbc576fefee68e5a2f57e0482e
**Notes:** Alternate data stream (ADS) PNG file with the PowerDuke backdoor component hidden and encrypted within using Tiny Encryption Algorithm (TEA).

## Attack Wave 3: Why American Elections Are Flawed

Volexity believes the following e-mail received the widest distribution among the targeted organizations. The e-mail purports to have been sent from Harvard's "PDF Mobile Service" or "PFD Mobile Service". The spelling of this non-existent service is inconsistent in the e-mail. The latter spelling appears to be a typographical error that is consistent with the domain names registered by the attackers. The screen shot below shows the e-mail that was sent.



[redacted] sent you documents using PDF Mobile Service: [Why American Elections Are flawed, 11/09] - Temporary Items

[redacted] sent you documents using PDF Mobile Service: [Why American Elections Are flawed, 11/09]

[redacted]@fas.harvard.edu>
Wednesday, November 9, 2016 at 09:18
To:

Harvard PFD Mobile Service :

RWP_16-038_Norris.ZIP DOWNLOAD

CODE: 8734

Thank you for using Harvard PFD Mobile Service for secure document delivery.
If you have any questions, find out more at http://security.harvard.edu/

HARVARD
Information Security

Information Security
security.harvard.edu
1414 Massachusetts Avenue, 3rd Floor Cambridge, MA 02138. Admin Login. OpenScholar

The e-mail contained links pointing to the following URL:

hxxp://efax.pfdresearch[.]org/eFax/RWP_16-038_Norris.ZIP

Inside of this password (8734) protected ZIP file is an executable named:

**RWP16-038_Norris.exe**

Note that **pfdresearch[.]org** appears to be under the control of the attackers but may be a hijacked domain.

Details on the malware components of this attack wave are included below.

**Filename:** RWP_16-038_Norris.ZIP
**File size:** 854996 bytes
**MD5 hash:** 8b3050a95e3ce00424b85f6e9cc3ccec
**SHA1 hash:** d5dcf445830c54af145c0dfeaebf28f8ec780eb5
**Notes:** Password protected ZIP file with malicious executable inside (RWP16-038_Norris.exe).

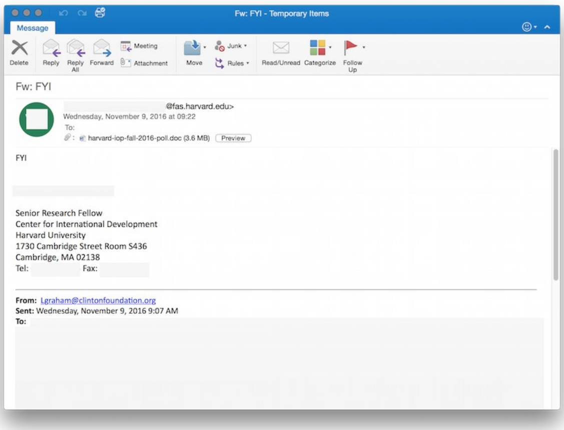
**Filename:** RWP16-038_Norris.exe
**File size:** 1144832 bytes
**MD5 hash:** 3335f0461e5472803f4b19b706eaf4b5
**SHA1 hash:** 5cc807f80f14bc4a1d6036865e50d576200dfd2e
**Notes:** Dropper for PowerDuke backdoor and clean decoy document

**Filename:** gwV46ilc.idx
**File size:** 10752 bytes
**MD5 hash:** ae997d2047705ff46a0c228f7b5d7052
**SHA1 hash:** 1067ddd5615518e0cbac7389a024b32f119a3229
**Notes:** Primary PowerDuke backdoor (DLL) loader (leverages gwV46ilc.idx:schemas) dropped to "%APPDATA\Roaming\Apple\" with persistence via HKCU Run Key "ConnectionCenter" (rundll32.exe %APPDATA\Roaming\Apple\gwV46ilc.idx, #2). Connects directly to **185.124.86.121:443** for command and control.

**Filename:** gwV46ilc.idx:schemas
**File size:** 580968 bytes
**MD5 hash:** 7b9b51cb44cd6a7af1cd28faeeda04a7
**SHA1 hash:** e3bd7bdfe0026cf4ee39fd75a771eac52ffea095
**Notes:** Alternate data stream (ADS) PNG file with the PowerDuke backdoor component hidden and encrypted within using Tiny Encryption Algorithm (TEA).

## Attack Wave 4: Clinton Foundation FYI #1

The fourth attack wave that Volexity observed leveraged a Microsoft Word document with a malicious embedded macro. This appears to be consistent with several previous Dukes attack campaigns, such as those on August 25, 2016. The Macros contain several anti-VM checks designed to avoid executing in virtualized environments. The screen shot below shows the e-mail that was sent.



Fw: FYI - Temporary Items

Fw: FYI

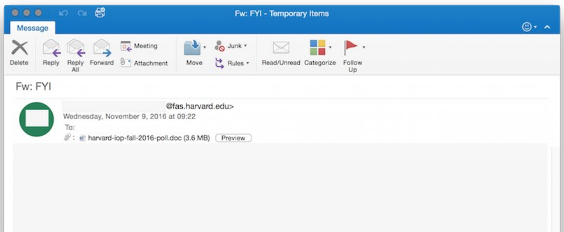
[redacted]@fas.harvard.edu>
Wednesday, November 9, 2016 at 09:22
To:
harvard-iop-fall-2016-poll.doc (3.6 MB)

FYI

[redacted]

Senior Research Fellow
Center for International Development
Harvard University
1730 Cambridge Street Room S436
Cambridge, MA 02138
Tel: [redacted] Fax: [redacted]

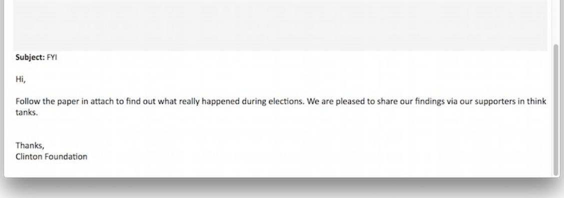
**From:** Lgraham@clintonfoundation.org
**Sent:** Wednesday, November 9, 2016 9:07 AM
**To:** [redacted]



Fw: FYI - Temporary Items

Fw: FYI

[redacted]@fas.harvard.edu>
Wednesday, November 9, 2016 at 09:22
To:
harvard-iop-fall-2016-poll.doc (3.6 MB)



**Subject:** FYI

Hi,

Follow the paper in attach to find out what really happened during elections. We are pleased to share our findings via our supporters in think tanks.

Thanks,
Clinton Foundation

Details on the malware components of this attack wave are included below.

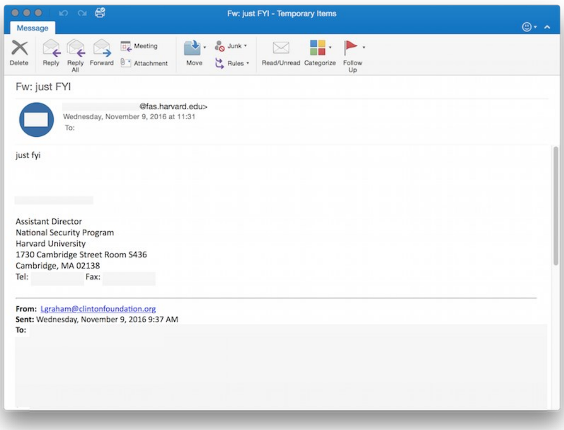
**Filename:** harvard-iop-fall-2016-poll.doc
**File size:** 2808832 bytes
**MD5 hash:** ead48f15ebc088384a4bd6190c2343fa
**SHA1 hash:** 0b9dccfcb2cc8bced343b9d930e475f1d0e5d966
**Notes:** Document containing malicious macro that drops impku.dat and impku.dat:shemas.

**Filename:**  impku.dat
**File size:** 10752 bytes
**MD5 hash:** 9f420779c90e118a0b5fd904380878a1
**SHA1 hash:** 11523d859e9a818c2628d7954502cbdb5eeb2199
**Notes:** PowerDuke backdoor file dropped to "%APPDATA\Roaming\Dell\" with persistence via HKCU Run Key "Communicator" (rundll32.exe %APPDATA\Roaming\Dell\impku.idat, #2). Connects directly to **185.26.144.109:443** for command and control.

**Filename:** impku.dat:schemas
**File size:**  608854 bytes
**MD5 hash:** b774f39d31c32da0f6a5fb5d0e6d2892
**SHA1 hash:** ae3ff39c2a7266132e0af016a48b97d565463d90
**Notes:** Alternate data stream (ADS) PNG  file with the PowerDuke backdoor component hidden and encrypted within using Tiny Encryption Algorithm (TEA).

## Attack Wave 5: Clinton Foundation FYI #2

The fifth attack wave that Volexity observed once against leveraged a download link and a new domain that appears to be under control of the attackers. The link in the e-mail points to a ZIP file that has a Microsoft shortcut file (.LNK) inside of it. This shortcut file contains PowerShell commands that conduct anti-VM checks, drop a backdoor, and launch a clean decoy document. Like Attack Wave #3, this e-mail message also purported to be forwarded from Laura Graham at the Clinton Foundation. The message body contained dozens of e-mail addresses to which the message originally claims to have been sent, with organizations similar to Attack Wave #3. The e-mail message from this attack wave, with identifying information removed, is shown below.



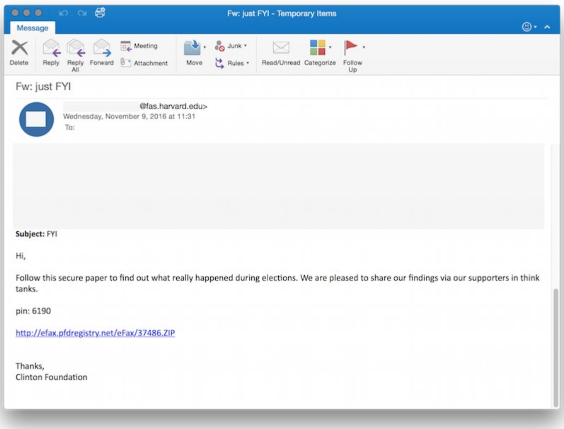
Fw: just FYI

@fas.harvard.edu>
Wednesday, November 9, 2016 at 11:31
To:

just fyi

Assistant Director
National Security Program
Harvard University
1730 Cambridge Street Room S436
Cambridge, MA 02138
Tel:  Fax:

**From:** Lgraham@clintonfoundation.org
**Sent:** Wednesday, November 9, 2016 9:37 AM
**To:**



Fw: just FYI

@fas.harvard.edu>
Wednesday, November 9, 2016 at 11:31
To:

**Subject:** FYI

Hi,

Follow this secure paper to find out what really happened during elections. We are pleased to share our findings via our supporters in think tanks.

pin: 6190

http://efax.pfdregistry.net/eFax/37486.ZIP

Thanks,
Clinton Foundation

As seen in the screen shot above, the e-mail contained links pointing to the following URL:

hxxp://efax.pfdregistry[.]net/eFax/37486.ZIP

Inside of this password (6190) protected ZIP file a Microsoft Shortcut file named:

**37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk**

Note that **pfdregistry[.]net** appears to be under the control of the attackers but may be a hijacked domain.

Details on the malware components of this attack wave are included below.

**Filename:** 37486.ZIP
**File size:** 580688 bytes
**MD5 hash:** f79caf27a99c091e6c1775b306993341
**SHA1 hash:** a76c02c067eae26d78f4b494274dfa6aedc6fa7a

**Notes:** Password protected ZIP file containing malicious Microsoft shortcut file 37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk.

**Filename:** 37486-the-shocking-truth-about-election-rigging-in-america.rtf.lnk
**File size:** 661782 bytes
**MD5 hash:** f713d5df826c6051e65f995e57d6817d
**SHA1 hash:** 68ce4c0324f03976247ff48803a7d988f9f9f43f
**Notes:** Microsoft shortcut file with embedded PowerShell, PowerDuke backdoor (hqwhbr.lck), and clean decoy document.

**Filename:** hqwhbr.lck
**File size:** 10752 bytes
**MD5 hash:** 57c627d68e156676d08bfc0829b94331
**SHA1 hash:** 4bcbf078a78ba0e842f78963ba9dd71240ab6a6d
**Notes:** PowerDuke backdoor file dropped to "%APPDATA\Roaming\Skype\" with persistence via HKCU Run Key "IAStorIcon" (rundll32.exe %APPDATA\Roaming\Apple\hqwhbr.lck, #2).  Connects directly to **177.10.96.30:443** for command and control.

**Filename:** hqwhbr.lck:schemas
**File size:** 547636 bytes
**MD5 hash:** cbf96820dc74a50a91b2b8b94376682a
**SHA1 hash:** 5f105801a1abb398dadc756480713f9bd7a4aa73
**Notes:** Alternate data stream (ADS) PNG  file with the PowerDuke backdoor component hidden and encrypted within using Tiny Encryption Algorithm (TEA).

## The PowerDuke Backdoor

The PowerDuke backdoor boasts a pretty extensive list of features that allow the Dukes to examine and control a system. Volexity suspects the feature set that has been built into PowerDuke is an extension of their anti-VM capabilities in the initial dropper files. Several commands supported by PowerDuke facilitate getting information about the system.

A previous analysis of PowerDuke showed it supported the following commands.

| | |
|---|---|
| comp | get the NetBIOS name via GetComputerNameEx |
| domain | get the computer's domain via NetWkstaGetInfo |
| drives | get logical drives, drive type, free space, serial number, etc. |
| fsize | get the size of a file via GetFileAttributesExW or failing that, by mapping the file and getting the size |
| kill | stop a process via TerminateProcess |
| memstat | get memory usage status via GlobalMemoryStatusEx, total RAM, percent used, etc. |
| osdate | get the time the machine was built (via InstallDate registry key) |
| osver | get OS info via registry, such as ProductName, CurrentBuild, CurrentVersion, CSDBuildNumber, etc. |
| pslist | list processes via CreateToolhelp32Snapshot |
| pwd | get current directory via GetCurrentDirectoryW |
| run | start a process via CreateProcessW |
| # | runs cmd.exe /c and gets the output via Named Pipe and sends the data back |
| siduser | gets the current user's SID via GetTokenInformation and LookupAccountSidW |
| time | the time + timezone (GetLocalTime and GetTimeZoneInformation) |
| uptime | number of seconds since the last boot |
| user | the user's name via GetUserNameExW |
| wipe | writes random data across a file, then deletes the file |
| wnd | gets the text of the current foreground window |
| fgetp | download file |
| fputp | upload file |
| power | reboot or shutdown (via previously loaded PowrProf.dll) |
| cdt | change to temporary directory |
| reqdelay | sleep for specified time |

Volexity has not fully examined the PowerDuke instances from these campaigns but has noted the malware appears to support the following additional commands not described above:

- sidcomp
- buzy
- exit
- copy
- detectav
- mkdir
- software
- shlist
- shinfo
- shdel
- shadd
- setpng
- conn
- setsrv

Volexity may update this post following further PowerDuke analysis.

## Network Indicators

Below are network indicators associated with download URLs for the aforementioned Dukes attack campaigns.

| Hostname | IP Address | ASN Information |
|---|---|---|
| efax.pfdresearch.org | 81.82.196.162 | 6848 \| 81.82.0.0/15 \| TELENET \| BE \| telenet.be \| Telenet Operaties N.V. |
| efax.pfdregistry.net | 65.15.88.243 | 7018 \| 65.15.64.0/19 \| ATT-INTERNET4 \| US \| bellsouth.net \| Bellsouth.net Inc. |
| efax.pfdweek.com | 84.206.44.194 | 31581 \| 84.206.0.0/16 \| KOPINT \| HU \| ekg.kopdat.hu \| National Infocommunications Service Company Limited by Shares |

Below are network indicators associated with command and control servers for the aforementioned Dukes attack campaigns.

| IP Address | ASN Information |
|---|---|
| 185.124.86.121 | 43260 \| 185.124.86.0/24 \| DGN \| TR \| – \| – |
| 185.132.124.43 | 43260 \| 185.132.124.0/24 \| DGN \| TR \| – \| – |
| 185.26.144.109 | 60721 \| 185.26.144.0/24 \| BURSABIL \| TR \| bursabil.com.tr \| Bursabil Konfeksiyon Tekstil Bilisim Teknoloji insaat Sanayi ve Ticaret Limited Sirketi |
| 173.243.80.6 | 14979 \| 173.243.80.0/24 \| AERONET-WIRELESS \| PR \| aeronetpr.com \| Aeronet Wireless |
| 177.10.96.30 | 262848 \| 177.10.96.0/21 \| Naja \| BR \| najatel.com.br \| Naja Telecomunicacoes Ltda. |

## Conclusion

The Dukes continue to launch well-crafted and clever attack campaigns. They have had tremendous success evading anti-virus and anti-malware solutions at both the desktop and mail gateway levels. The group's anti-VM macros and PowerShell scripts appear to have drastically reduced the number of sandboxes and bots that the group has to deal with on their command and control infrastructure. This combined with their use of steganography to hide their backdoor within PNG files that are downloaded remotely and loaded in memory only or via alternate data streams (ADS) is quite novel in its approach. Volexity believes that the Dukes are likely working to gain long-term access into think tanks and NGOs and will continue to launch new attacks for the foreseeable future.

Follow us on Twitter: @Volexity, @stevenadair, @5ck, @imhlv2, @attrc

APT, Dukes, elections, spear phishing