Bundesamt für Verfassungsschutz

Köln, 26. Oktober 2015

BfV Cyber-Brief

Nr. 01/2015

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Referat 4D2/4D3
☎ 0221/792-3322

Aktuelle Angriffskampagne gegen Wirtschaftsunternehmen

Seit spätestens Juni 2015 ist eine Angreifergruppierung aktiv, die weltweit Wirtschaftskonzerne angreift. Dabei nutzt die Gruppierung ein hochprofessionelles Schadprogramm, welches oftmals von kommerziellen Antivirenprogrammen nicht erkannt wird. Das in der Angriffs-Mail verwendete Social-Engineering ist als besonders hochwertig zu bezeichnen, welches allerdings auch einen hohen Wiedererkennungswert hat.

Von dieser Angriffskampagne sind nach Erkenntnissen des Bundesamtes für Verfassungsschutz (BfV) bereits mehrere Unternehmen betroffen. Da davon auszugehen ist, dass auch andere deutsche Unternehmen die gleiche Angriffs-Mail erhalten haben bzw. erhalten werden, möchte das BfV als Nationale Spionageabwehrbehörde auf diesem Wege auf die aktuelle Bedrohung hinweisen.

A. Sachverhalt

Das BfV erhielt kürzlich einen Hinweis auf einen Cyber-Angriff gegen einen deutschen Großkonzern. Bei diesem Angriff ist es dem Täter gelungen, tief in das Netzwerk des Opfers zu gelangen. Das betroffene Unternehmen konnte die initiale Angriffs-Mail ausfindig machen:

Angriffs-Mail:

From: lh lx [mailto:hk.newskey@gmail.com]
Sent: Tuesday, June 09, 2015 4:20 AM
To:
Subject: Urgent: Confirmation needed regarding a tip-off video of your company staff

Weiter Letzter

Hello, I am a reporter of HNN. My name is akali We've recently received an anonymous tip-off video regarding a man having sex with a prostitute in Hong Kong. The video shows that after sex, he also committed sexual abuse on the girl who we think is underage. We also got an information that the hotel room is booked by your company. We failed to reach out to your HR, but fortunately we found your email address on the Internet. So we think we may stand a better chance to reach out to you to confirm its realness. The unverified video page is as below:

http://news.hnn.hk/2015/0526/news

We hope you can identify the man or just help to forward this email to someone who might. We will appreciate it very much. Thank you!

PS: We are going to make it official release in 3 days, so please give us confirmation ASAP!

Diese E-Mail wurde an die Abteilung für Öffentlichkeitsarbeit des betroffenen Unternehmens versandt und dort nach interner Weiterleitung mehrfach geöffnet. Durch das Aufrufen der „video page" über den Link hat sich das Schadprogramm PlugX auf den Rechnern installiert. Durch dieses Schadprogramm hat der Angreifer die Möglichkeit, auf die Rechner der Opfer zuzugreifen.

Das „social engineering" der Mail ist als besonders hochwertig zu qualifizieren. Die drohende Presseveröffentlichung eines kompromittierenden Videos könnte zu einem Imageverlust des Unternehmens führen, so dass sich insbesondere eine Abteilung für Öffentlichkeitsarbeit gezwungen sieht, einen solchen Link zu betätigen und das Video auf seine Echtheit zu überprüfen.

Aufgrund der vorliegenden Erkenntnisse geht das BfV von einem nachrichtendienstlichen Hintergrund der Angriffskampagne aus.

Durch die Analyse der Kampagne konnten weitere Opfer ermittelt werden, die durch eine inhaltsgleiche E-Mail angegriffen worden sind. Die technischen Parameter deuten ferner darauf hin, dass es weitere Opfer gibt, denen die Infektion bislang noch nicht aufgefallen ist.

B. Handlungsempfehlung

Um festzustellen, ob Ihr Unternehmen ebenfalls von dieser Angriffskampagne betroffen ist, empfehlen wir folgende Schritte:

- Suchen Sie in den E-Mail-Eingängen (auch der letzten Monate) nach dem oben in der Mail genannten Absender und Betreff.
- Überprüfen Sie, ob ähnliche Mails (z.B. Reporter droht mit Veröffentlichung) bei Ihnen eingegangen sind.
- Durchsicht der Netzwerk-Logs nach den in der Anlage aufgeführten Netzwerk-IOC[1].
- Suche nach den in der Anlage genannten Host-IOC (z.B. extrahierte Dateien).

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr der Infizierung Ihrer Rechner. In diesem Fall können wir Ihre Maßnahmen mit zuätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221-792-3322 oder

E-Mail: sensea@bfv.bund.de

Wir sichern Ihnen absolute Vertraulichkeit zu!

1 Indicators of compromise.

Anlage

Network based IOC

Domains

news.voanews.hk
web.voanews.hk
*.ns1.voanews.hk
blog.nhknews.hk
web12.nhknews.hk
news.nhknwes.hk
web.vancouversun.us
*.ns1.vancouversun.us
hxxps://plus.google.com/u/0/115747778649102578052/about
hxxps://plus.google.com/u/0/117498075882305449647/about
hxxps://twitter.com/linketelin
*.ns3.yomiuri.us

Infos

Die eingesetzte Schadsoftware kommuniziert zum Teil ausschließlich über DNS (UDP/53). Die Domains, welche durch die Schadsoftware abgefragt werden, bauen sich aus folgendem Muster auf:

```
(subdomain[ alphanum] .)subdomain[ alphanum] .ns[ 0-9] .domain.tld
```

Die alphanumerischen, kryptischen Subdomains enthalten wahrscheinlich kryptierte Informationen über das infizierte System.

Unikates, nicht standardisiertes Header-Feld

```
QtV1: [ Base64-encoded String]
```

in der C&C-Kommunikation via HTTP beziehungsweise HTTPS.

Host based IOC

MD5

f9e52f378d11d40f9abc554aa3a7794d – RAR Self Extractor
5b057113280e2a5ff9e8a8eb028ad7c3 – RAR Self Extractor
6a166303b5f94807ccc8b7744d00a5ce – RAR Self Extractor

71a2d4155d4e320a0435e5081f55f77a – legit PE for DLL-Sideloading
e26d04cecd6c7c71cfbb3f335875bc31 – legit PE for DLL-Sideloading
64ff0a8730472e36e62ce29a20f61529 – possibly legit PE for DLL-Sideloading
a61c72bdcce52c310362622b058eb6c1 – possibly legit PE for DLL-Sideloading
3a9cd20f84be1c919a6c8fb263e00a95 – possibly legit PE for DLL Sideloading

37aacb043222f814ef5013ab2bd6d820 – malicious DLL for Sideloading
551ad5248aca220ee2e9e87e4e4ccb66 – malicious DLL for Sideloading
9ab43753b6e47e5ef96ff3ddde8a4f15 – malicious DLL for Sideloading
2793c4ff43ab4cb453e104a3d38af326 – malicious DLL for Sideloading
cd394af558d05c49c21354c4d884243a – malicious DLL for Sideloading
37fb2c4ff5d89e3ed3af0a642cb6a508 – malicious DLL for Sideloading
b912bbdfa58fb1aab886f4f0b191625e – malicious DLL for Sideloading

a469b03daaaa5073f699bc0d152b313f – encrypted malicious Payload
047618a225812c9e554706cf42a327de – encrypted malicious Payload
02a175b81144b8fa22414e9cf281f71c – encrypted malicious Payload
32ab2c35d89e3d7f52d84869d010319f – encrypted malicious Payload
2e1d6cff4b52694c0905113d999587f9 – encrypted malicious Payload
6cb15b75cd54e414743e056e79315fa0 – encrypted malicious Payload
19148be7bf531f8c48dca2ec5405c29a – encrypted malicious Payload
d9af894d51ba61075c7cd329b0be52df – encrypted malicious Payload
9ef895b5892f6f1f917291812c110b31 – encrypted malicious Payload
5d067281d6c74b27d2e46c724c10df55 – encrypted malicious Payload

ca15eb5fe3d6c92517f759f672cedcfe – decrypted Payload in Memory
d13d2718b284879837f9467335ff490f – decrypted Payload in Memory
7cdb4b1f70019b32bdf2cfd4f94e9c2d – encrypted malicious Payload
471e2d354666e5e03bf62b72d3dc92c7 – decrypted Payload in Memory

Filesystem

```
%ProgramFiles%\Common Files\nahs
%ProgramFiles%\Common Files\nahs\AFLogVw.exe
%ProgramFiles%\Common Files\nahs\AhnI2.dll
%ProgramFiles%\Common Files\nahs\ovtbylawyvtmu
%TEMP%\RarSFX[ 0-9]*
%AUTO%\nahs\screen
C:\Documents and Settings\All Users\DRM\wsacs
C:\Documents and Settings\All Users\DRM\wsacs\AFLogVw.exe
C:\Documents and Settings\All Users\DRM\wsacs\AhnI2.dll
C:\ProgramData\wsacs\
%AUTO%\wsacs\screen
%Program Files%\Common Files\pras\
%Program Files%\Common Files\pras\AhnI2.dll
%Program Files%\Common Files\pras\AFLogVw.exe
%AUTO%\pras\screen
%ProgramFiles%\Common Files\svacs
%ProgramFiles%\Common Files\svacs\AFLogVw.exe
%ProgramFiles%\Common Files\svacs\AhnI2.dll
%AUTO%\whacs\screen
%ProgramFiles%\Common Files\whacs
%ProgramFiles%\Common Files\whacs\AFLogVw.exe
%ProgramFiles%\Common Files\whacs\AhnI2.dll
C:\programdata\wfaps\
C:\programdata\wfaps\AFLogVw.exe
C:\programdata\wfaps\\AhnI2.dll
%APPDATA%\Surge\ushata.exe
%APPDATA%\Surge\ushata.dll
%APPDATA%\Surge\sgkey.data
%APPDATA%\Surge\ushata
%APPDATA%\Surge\ushata.exe
%ProgramData%\Microsoft\Crypto\RSA\MachineKeys\ushata.exe (scheduled Job)
%CommonProgramFiles%\Surge\ushata.exe
%ProgramData%\Microsoft\Crypto\RSA\MachineKeys\ushata.exe (Scheduled Job)
C:\ProgramData\Microsoft\DeviceSync\
%USERTEMP%\RarSFX0\ARO.exe
%USERTEMP%\RarSFX0\aross.dll
%USERTEMP%\RarSFX0\aross.a
%Program Files%\Common Files\scvcs\ARO.exe
%AUTO%\scvcs\screen
```

```
%ProgramData%\moduu\ARO.exe
%ProgramData%\moduu\aross.dll
%AUTO%\moduu\screen
C:\Windows\Temp\RarSFX1\aross.dll
C:\ProgramData\wcuserv\aross.dll
C:\ProgramData\Microsoft\DeviceSync\XCrSvr.exe
C:\ProgramData\Microsoft\DeviceSync\XecureIO_v20.dll
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\sgkey.data
C:\Windows\mstisvc.dll
C:\Windows\Temp\%MACHINENAME%_p.ax
C:\ProgramData\Wupss\FSPMAPI.dll
C:\ProgramData\Wupss\FSPMAPI.dll.fsp
C:\ProgramData\Wupss\fsstm.exe
%AUTO%\wupss\screen
%AllUsersProfile%\DRM\SAENSS\fsstm.exe
%ProgramData%\SAENSS\fsstm.exe
%AUTO%\emproxy\screen
```

Registry

```
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_SAENSS
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_SAENSS\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_SAENSS\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_SAENSS
HKLM\SYSTEM\CurrentControlSet\Services\SAENSS
HKLM\SYSTEM\CurrentControlSet\Services\SAENSS\Enum
HKLM\SYSTEM\CurrentControlSet\Services\SAENSS\Security
HKLM\SOFTWARE\Classes\v1
HKLM\SYSTEM\CurrentControlSet\services\Wimgsvc0
HKLM\SYSTEM\CurrentControlSet\services\Wimgsvc0\Parameters\ServiceDll
HKLM\SOFTWARE\BINARY\AhnI2.dvd
HKCU\SOFTWARE\BINARY\AhnI2.dvd
HKLM\SYSTEM\ControlSet001\Services\nahs
HKLM\SYSTEM\CurrentControlSet\Services\nahs
HKLM\SYSTEM\CurrentControlSet\services\wfass
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\pras
HKLM\SYSTEM\CurrentControlSet\services\pras
HKLM\SYSTEM\CurrentControlSet\services\svacs
HKLM\SYSTEM\CurrentControlSet\services\whacs
HKLM\SYSTEM\CurrentControlSet\services\wfaps
HKLM\SYSTEM\CurrentControlSet\services\NetworkAutoCheck
```

```
HKLM\SYSTEM\ControlSet001\services\NetworkAutoCheck
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ntcs
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\java-secure
HKLM\SYSTEM\CurrentControlSet\services\DeviceSync
HKLM\SYSTEM\ControlSet001\services\DeviceSync
HKLM\SOFTWARE\BINARY\aross.a
HKCU\Software\BINARY\aross.a
HKLM\SYSTEM\CurrentControlSet\services\scvcs
HKLM\SYSTEM\ControlSet001\Services\moduu
HKLM\SYSTEM\CurrentControlSet\Services\moduu
HKLM\SYSTEM\CurrentControlSet\services\wcuserv
HKLM\SYSTEM\CurrentControlSet\services\wupss
```