Bundesamt für
Verfassungsschutz

Köln, 11. Mai 2016

BfV Cyber-Brief

Nr. 02/2016

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Referat 4D2/4D3
☎ 0221/792-2600

Russische Cyberangriffskampagne Snake/Uroburos unvermindert aktiv

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse vor, nach denen deutsche Rüstungsunternehmen ins Visier der elektronischen Spionagekampagne Snake geraten sein könnten. Das BfV als nationale Spionageabwehrbehörde möchte deutsche Unternehmen auf diesem Wege auf die aktuelle Bedrohungslage aufmerksam machen. Bei dieser Angriffskampagne handelt sich um eine in Umfang und Qualität herausragende, über lange Zeit gezielt durchgeführte Cyberspionageoperation mit internationalem Ausmaß. Sie ist bis ins Jahr 2005 zurückverfolgbar.

IT-Sicherheitsunternehmen beschreiben neue Schadsoftware

Öffentlich bekannt wurde die Operation Anfang 2014 durch entsprechende Reports der IT-Sicherheitsunternehmen *BAE Systems Applied Intelligence* [1] und *G Data Security Labs* [2]. Danach handelt es sich bei dem Schadprogramm namens *Uroburos* (auch *Snake* [*BAE Systems*] bzw. *Turla* [*Kaspersky*] genannt) um eine hoch komplexe sowie hoch qualifizierte Software für Spionageoperationen mit internationalem Opferkreis. *Uroburos* ist darauf ausgelegt, in großen Netzen von Firmen, Behörden, Organisationen und Forschungseinrichtungen zu agieren.

Uroburos-Symbol (G Data-Report)

Die Schadsoftware wurde von G Data in Anspielung auf im Quellcode vorhandene Zeichenfolgen auf den Namen *Uroburos* getauft, angelehnt an ein altes griechisches Symbol einer Schlange oder eines Drachen, welcher seinen eigenen Schwanz frisst. Im nationalen und internationalen Sprachgebrauch setzte sich jedoch eher die Bezeichnung Snake durch.

```
80FA FFFF E0C9 B909 80FA FFFF 30CE B909 80FA FFFF 2C62 B909  €úÿÿÄÈ¹.€úÿÿàÉ¹.€úÿÿ0Î¹.€úÿÿ,b¹.
80FA FFFF 2CEE B909 80FA FFFF D4CB B909 80FA FFFF 54C6 B909  €úÿÿ`Ä¹.€úÿÿ,î¹.€úÿÿÔË¹.€úÿÿTÆ¹.
5572 3062 5572 2829 7347 6F54 794F 7523 0000 0000 0000 0000  €úÿÿ....Ur0bUr()sGoTy0u#.........
80FA FFFF 2C41 B509 80FA FFFF 34CC B909 80FA FFFF FCCC B909  "... X¹.€úÿÿ,Au.€úÿÿ4Ì¹.€úÿÿüÌ¹.
80FA FFFF 08CD B909 80FA FFFF 94CD B909 80FA FFFF D0EF B909  €úÿÿÐÐ¹.€úÿÿ.Í¹.€úÿÿ"Í¹.€úÿÿÐï¹.
80FA FFFF 58D3 B909 80FA FFFF 38D8 B909 80FA FFFF C4DD B909  €úÿÿ Î¹.€úÿÿXÓ¹.€úÿÿ8Ø¹.€úÿÿÄÝ¹.
```

Quelltext mit der Zeichenfolge Ur0bUr()sGoTy0u# (G Data-Report)

Das BfV geht davon aus, dass es sich bei dieser Kampagne um staatlich gelenkte Angriffe handelt. So sind unter den bisher bekannt gewordenen Zielen Supranationale Organisationen, Regierungsnetze, Schulen und Hochschulen sowie Unternehmen. Diese Zielauswahl zeigt ein staatliches Aufklärungsinteresse. Die Hochwertigkeit der eingesetzten Schadprogramme und der lange Zeitraum der Angriffsoperation, in denen dieses und verwandte Schadprogramme eingesetzt wurden, deuten zudem auf einen hohen Ressourcenaufwand mit entsprechender IT- und Analysekompetenz des Angreifers hin.

Aufklärungsinteresse und Angriffsmethoden

Neben dem Aufklärungsschwerpunkt Regierungseinrichtungen zeigt sich anhand der Zielauswahl ein Interesse des Angreifers an Entwicklungen in Wirtschaft und Forschung im Bereich Energietechnik, Röntgen- und Nukleartechnologie, Messtechnologie, Luft- und Raumfahrt sowie Rüstung.

1 Vgl. Report von BAE Systems Applied Intelligence, 2014: „Snake Campaign & Cyber Espionage Toolkit"; http://www.baesystems.com.
2 Vgl. Report von G Data SecurityLabs, Februar 2014: „Uroburos. Highly complex espionage software with Russian roots"; https://public.gdata-software.com.

Angriffsinfrastruktur

Der Angreifer bedient sich für seine Angriffe einer umfangreichen IT-Infrastruktur. Mindestens zwei Ebenen von Proxy-Servern sind der Kommunikation zwischen Opfersystem und Command-and-Control-Server zwischengeschaltet. Diese mehrstufige Kommunikation unter Verwendung eines Netzwerks von Proxy-Servern dient den Angreifern zur Wahrung der Anonymität.

Eine weitere, sehr ausgefeilte Methode zur Verwaltung der Rückmeldestrukturen besteht in der Nutzung satellitengestützter Kommunikation. Dieses vom IT-Sicherheitsunternehmen Kaspersky in einem ausführlichen Report von September 2015 [3] beschriebene Vorgehen hat den großen Vorteil, dass der physikalische Standort der C&C-Serverinfrastruktur nicht ohne weiteres bestimmt und blockiert, überwacht oder beschlagnahmt werden kann. Satellitengestützte Internetreceiver können überall innerhalb des vom Satelliten abgedeckten Bereichs lokalisiert sein.

Die von der Angreifer-Gruppe verwendete Methode ist hochgradig anonym und macht kein gültiges Satelliten-Internet-Abo erforderlich. Die Technik hinter dieser Methode basiert auf dem Kapern von Downstream-Bandbreite (DVB-S-Verbindungen) von verschiedenen ISPs und auf dem Fälschen von Daten-Paketen. Diese Methode ist technisch einfach zu realisieren, kostengünstig und bietet ein höheres Maß an Anonymität als andere konventionelle Methoden. Die von Kaspersky beobachteten Verbindungen waren – wohl aus Sicherheitsgründen – meist nur für mehrere Monate aktiv. Der Angreifer nutzt bevorzugt Provider von Satelliten-Internetverbindungen mit Sitz im Mittleren Osten, Afrika und den Vereinigten Arabischen Emiraten. Satellitenübertragungen aus diesen Ländern erreichen gewöhnlich keine europäischen oder nordamerikanischen Gebiete; dies erschwert die Aufklärung dieser Infrastrukturen zusätzlich.

Dem hohen Maß an Anonymität und den geringen Kosten stehen allerdings Einbußen in Sachen Zuverlässigkeit sowie eine vergleichbar geringe Bandbreite gegenüber, sodass dieses Verfahren traditionellere Methoden wie die Nutzung multipler Proxy-Levels oder gehackter Webseiten derzeit (noch) nicht ersetzen kann. Die satellitengestützte Kommunikation wird bislang eher selten und nur von wenigen APT-Gruppen genutzt, obwohl die Methodik bereits seit 2007 im Einsatz ist.

Infektionsweg

Die innerhalb der Snake-Kampagne am häufigsten festgestellte Angriffsmethode ist die des Watering-Hole-Angriffs (auch Strategic-Web-Compromise [SWC]). Hierfür identifiziert der Angreifer in einem ersten Schritt Webseiten, die für die Opfer von Interesse sind, und präpariert diese mit einem sog. iFrame [4]. Die IP-Adressen der Opfer werden vom Angreifer auf einer sog. Whitelist hinterlegt. Im Falle eines Kontaktes werden dann diese IP-Adressen gezielt auf Exploit-Server umgeleitet, über die der Schadcode ausgeliefert wird.

3 Vgl. Bericht von Securelist (Kaspersky), September 2015: „Turla in the Sky: Satelliten-C&C“;
https://de.securelist.com/blog/analysen/65255/satellite-turla-apt-command-and-control-in-the-sky

4 Verweis auf eine weitere Webseite im Quellcode der Webseite (nicht per se bösartig!).

Schadsoftware

Bei *Uroburos* handelt es sich um eine hochentwickelte und komplexe Schadsoftware. Das Design und der hohe Komplexitätsgrad lassen auf eine sehr aufwändige personal- und kostenintensive Entwicklung schließen. Die Entwicklung von *Uroburos* setzt eine gute Ausbildung und sehr tiefe Systemkenntnis der Entwickler voraus. Bei der Entwicklung wurden Anti-Forensik- und Anti-Analyse-Funktionalitäten berücksichtigt. Mit Hilfe dieses Schadprogramms kann der Angreifer die Kontrolle über den infizierten PC erlangen, beliebige Programmcodes auf dem Computer ausführen und dabei seine Systemaktivitäten verstecken. Die Schadsoftware ist außerdem in der Lage, Daten zu stehlen und den Netzwerkdatenverkehr mitzuschneiden. Durch den modularen Aufbau der Schadsoftware kann der Angreifer zum einen die Schadsoftware um weitere Funktionen erweitern, zum anderen wird dadurch die Detektionsgefahr verringert.

Es handelt sich um eine auf Dauer angelegte, systematisch durchgeführte und stetig fortentwickelte Angriffsoperation. So stammen die von *BAE Systems* analysierten und vermutlich demselben Urheber zuzurechnenden Schadprogramme aus den Jahren 2006 bis 2014.

Bisherige Erkenntnisse zu Aufbau, Komplexität und Funktionsweise der eingesetzten Schadsoftware(varianten) und zum Modus operandi bieten Anhaltspunkte für einen russischen Hintergrund.

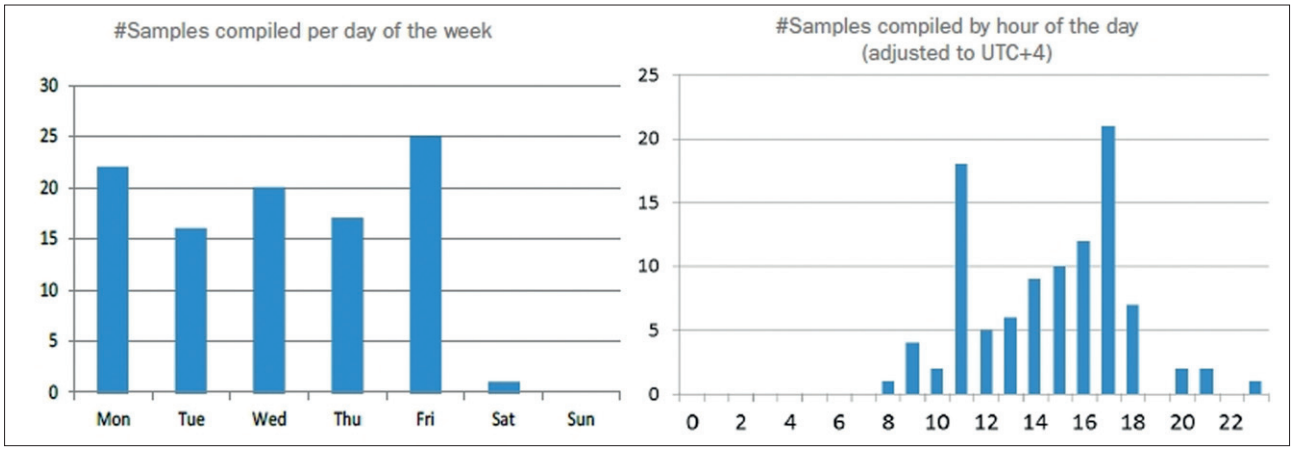
So fanden beispielsweise *G Data* und *Kaspersky* bei ihren Analysen Hinweise darauf, dass die Entwickler der Software russisch sprechen – ein weiteres Indiz für einen russischen Hintergrund der Angreifer. Der folgende Eintrag in den Spracheinstellungen zeigt den *Code 1251*; dieser dient der Darstellung kyrillischer Zeichen.

Russische Spracheinstellungen (Kaspersky-Report)

```
<center><span style='background-color:red;padding:1px;'>Password it's
wrong!</span></center><br><br><html><head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-
1251">
</head>
<body><center>
      <b>Admin panel</b><br><br>
      <font size="-3" face='Verdana, Arial, Helvetica, sans-serif'>Enter
password!</font>
```

Fehler im englischen Sprachgebrauch (wie oben *„Password it's wrong!"* oder auch *„File is not exists"*, *„File is exists for edit"*) sollen ferner darauf hindeuten, dass die Entwickler keine englischen Muttersprachler sind.

Auch zeigen die sog. Kompilierungszeiten [5], dass ein Großteil der Malware zu den üblichen Arbeitszeiten (Montag bis Freitag, 08:00 bis 18:00 Uhr) in den Großräumen Moskau und St. Petersburg geschrieben wurde.



Der weit überwiegende Teil der erkannten Malware-Samples wurde an Arbeitstagen zu „üblichen" Bürozeiten (dargestellt in UTC+4 [6]) programmiert. (Report von BAE Systems)

Bewertung

Die festgestellten Angriffe erfolgen technisch sehr versiert, zielgerichtet und passgenau. Von einem entsprechend hohen Schadpotenzial ist auszugehen. Es handelt sich um eine fortdauernde Angriffsoperation, von der nach wie vor eine hohe Gefahr für deutsche Stellen in Regierung und Verwaltung, Wirtschaft, Wissenschaft und Forschung ausgeht.

Für weitere Hintergrundinformationen und zur Überprüfung Ihrer Systeme wird auf die nachfolgenden Links und die IOCs verwiesen.

Aufgrund der schnell wechselnden Infrastruktur sowie Anpassung der Schadsoftware nachrichtendienstlicher Angreifer muss es sich bei jedem einzelnen technischen Parameter der IOC-Liste nicht unbedingt um ein speziell der Snake Kampagne zuzurechnendes Merkmal handeln. Sollten IOCs anschlagen, ist dies ein Indiz, nicht jedoch bereits der Beweis für eine Infektion. BfV empfiehlt in einem solchem Falle jedoch dringend, diesem ersten Anhaltspunkt nachzugehen, da die Gefahr besteht, dass Ihr Netzwerk infiziert ist. In diesem Fall können wir Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gern zur Verfügung:

Tel.: 0221 - 792 - 2600 oder
E-Mail: poststelle@bfv.bund.de
Referat 4D2

Wir sichern Ihnen absolute Vertraulichkeit zu!

5 Der Zeitpunkt, zu dem ein in einer bestimmten Programmiersprache geschriebenes Programm (z.B. eine Malware) in eine von einem Computer ausführbare Maschinensprache umgewandelt („kompiliert") worden ist. Dieser Zeitpunkt wird in der umgewandelten Datei mittels Zeitstempel festgehalten.

6 Die Zeitzone UTC+4 für den Westen Russlands (mit Moskau und St. Petersburg) galt - wegen reduzierter Anzahl der Zeitzonen und ganzjährig geltender Sommerzeit - zwischen März 2010 und Oktober 2014; seitdem gilt - wie bereits zuvor - dort wieder UTC+3. Die dargestellten „Bürozeiten" entsprechen dann 07:00 bis 17:00 Uhr.

Links

- Report von BAE Systems Applied Intelligence, 2014: „Snake Campaign & Cyber Espionage Toolkit“; http://www.baesystems.com
- Report von G Data SecurityLabs, Februar 2014: „Uroburos. Highly complex espionage software with Russian roots“; https://public.gdatasoftware.com
- Analyse von Securelist (Kaspersky), September 2015: „Turla in the Sky: Satelliten-C&C“; https://de.securelist.com/blog/analysen/65255/satellite-turla-apt-command-and-control-in-the-sky
- Report von Symantec, 26. Januar 2015: „The Waterbug attack group“, Version 1.01; https://www.symantec.com
- G Data SecurityBlog, 28. Februar 2014: „Uroburos - hochkomplexe Spionagesoftware mit russischen Wurzeln“; https://blog.gdata.de/artikel/uroburos-hochkomplexe-spionagesoftware-mit-russischen-wurzeln
- Report von Securelist (Kaspersky), 7. August 2014: „The Epic Turla Operation“; http://securelist.com/analysis/publications/65545/the-epic-turla-opera

IOCs

File (MD5)

AE23B358DAFA13F51582B05760EF0840

255118AC14A9E66124F7110ACD16F2CD

F4230728BA98FDC02835EDDBE5D678AF

EC7E3CFAEAAC0401316D66E964BE684E

EA23D67E41D1F0A7F7E7A8B59E7CB60F

B407B6E5B4046DA226D6E189A67F62CA

B1DB5128A47728005A2C628060DA5764

6F1DBB8BF33638FC0EAF371FDAD182AA

9D481769DE63789D571805009CBF709A

0AE421691579FF6B27F65F49E79E88F6

D8D9CB742D815EEEA769CCDF81C448E4

81D82A7FAFD58A542669F25AFDE265B7

Host

adobe.faqserv.com

spaces.ddns.us

googlemail.dynssl.com

www.googlemail.dynssl.com

iphone.mrface.com

consilium.faqserv.com

www1.proxydns.com

www.dnslook.isasecret.com

www.easybuy.sellclassics.com

majoor.no-ip.org

bills.yourtrap.com

dnslook.isasecret.com

mobile.lflinkup.com

tickets.trickip.net

easybuy.sellclassics.com

ftp.dnslook.isasecret.com

ftp.easybuy.sellclassics.com

ftp.iphone.mrface.com

ftp.topvkantivir.dnset.com

topvkantivir.dnset.com

www.iphone.mrface.com

www.topvkantivir.dnset.com

www3.topvkantivir.dnset.com

webonline.mefound.com

sportacademy.my03.com

easport-news.publicvm.com

new-book.linkpc.net

newgame.2waky.com

newsweek.servehttp.com

easycounter.sytes.net

cnews.serveblog.net

radioazerbaijan.ca

cqcount.servehttp.com

laboutiquemayorista.es

legalsilencer.com

image.servepics.com
candybagonsale.com
avg-update.sytes.net
newsforum.servehttp.com
bgl.serveftp.net
adobes3.sytes.et
newsweek.serveblog.net
pressforum.serveblog.net
stockholm-blog.hopto.org
north-area.bbsindex.com
pockerroom.servebeer.com
arctic-zone.bbsindex.com
cars-online.zapto.org
eunews-online.zapto.org
fifa-rules.25u.com
forum.sytes.net
franceonline.systes.net
freeutils.3utilities.com
health-everyday.faqserver.com
nhl-blog.servegame.com
olympik-blog.4dq.com
pockerroom.serveblog.net
scandinavia-facts.systes.net
sportmusic.servemp3.com
supernews.systes.net
sweeden-history.zapto.org
tiger.got-game.org
top-facts.sytes.net
weather-online.hopto.org
wintersport.sytes.net
x-files.zapto.org
forum.4dq.com
forum.acmetoy.com
marketplace.servehttp.com
music-world.servemp3.com
newutils.3utilities.com

interesting-news.zapto.org

academyawards.effers.com

cheapflights.etowns.net

toolsthemxp3.biz

softprog.freeoda.com

euassociate.6te.net

euland.freevar.com

communityeuxp3.biz

swim.onlinewebshop.net

july.mypressonline.com

winter.sit11.com

eu-sciffi.99k.org

www.spaces.ddns.us