Untersuchungsbericht zu den Angriffen auf die IT der Fraktion DIE LINKE im Bundestag

von Claudio Guarnieri

05.06.2015

Übersetzung: netzpolitik.org

Claudio Guarnieri ist IT-Sicherheitsforscher. Er konnte sich kompromittierte Server im Bundestag ansehen und macht die Ergebnisse nun der Öffentlichkeit zugänglich. Guarnieri beschäftigt sich intensiv mit Malware, er hat unter anderem den Anti-Viren-Scanner „Detek“„ für Staatstrojaner entwickelt sowie eine Übersicht über die von NSA und den Five Eyes eingesetzte Malware erstellt.

Zusammenfassung der Ergebnisse

Auf zwei separaten Servern der Linken im Bundestag wurden zwei verdächtige Artefakte gefunden. Eines ist ein Open-Source-Tool, mit dem man durch Remote-Zugriff von einem Linux-Host aus Befehle auf einem Windows-Host ausführen kann. Das andere ist ein spezielles Tool, das trotz seiner großen Dateigröße nur sehr begrenzte Funktionalitäten hat. Es verhält sich wie ein Tunnel, den die Angreifer wahrscheinlich nutzten, um sich in dem angegriffenen Netzwerk festzusetzen.

Die Kombination der beiden Werkzeuge hat den Angreifern ermöglicht, einen ständigen Zugang zum Netzwerk zu haben und alle Informationen zu sammeln und auszuleiten, die sie interessant fanden. Es ist außerdem nicht auszuschließen, dass außer den zwei erkannten Schadprogrammen noch andere bösartige Artefakte installiert, aber noch nicht gefunden wurden.

Die Eigenschaften eines der Artefakte und die Erkenntnisse über die Infrastruktur der Angreifer legen nahe, dass der Angriff von einer staatlich unterstützten Gruppe namens **Sofacy** (oder **APT28**) stammt. In Sicherheitskreisen besteht Einigkeit darüber, dass die Gruppe aus Russland stammt.

Artefakte

Das erste Artefakt – im Weiteren **Artefakt #1** genannt – hat die folgenden Eigenschaften:

Name	winexesvc.exe
Größe	23552
MD5	77e7fb6b56c3ece4ef4e93b6dc608be0
SHA1	f46f84e53263a33e266aae520cb2c1bd0a73354e
SHA256	5130f600cd9a9cdc82d4bad938b20cbd2f699aadb76e7f3f1a93602330d9997d

Das zweite Artefakt – im Weiteren **Artefakt #2** genannt – hat die folgenden Eigenschaften:

Name	svchost.exe.exe
Size	1062912
MD5	5e70a5c47c6b59dae7faf0f2d62b28b3
SHA1	cdeea936331fcdd8158c876e9d23539f8976c305
SHA256	730a0e3daf0b54f065bdd2ca427fbe10e8d4e28646a5dc40cbcfb15e1702ed9a
Compile-Zeit	20150422 10:49:54

Analyse von Artefakt #1

Artefakt #1 wurde auf einem Fileserver gefunden, der von der Linken betrieben wird. Die Binärdatei ist eine 64bit-kompatibel kompilierte Binärdatei für das Open-Source-Tool[1] **Winexe**. Winexe ist eine ähnliche Software wie das populärere **PSExec** und es erlaubt Systemadministratoren, Remote-Befehle auf angegebenen Servern auszuführen. Kommerzielle Lösungen wie Symantecs pcAnywhere haben mehr Funktionen, aber Winexe ist leichtgewichtig und muss weder installiert noch konfiguriert werden. Einer der Gründe, warum Winexe PSExec vorgezogen wird ist, dass Winexe auch für Linuxrechner verfügbar ist.

Angreifer nutzen immer häufiger Tools wie Winexe und PSExec, um sich in infizierten Netzwerken zu bewegen. Es lassen sich nicht nur sämtliche Befehle auf dem Zielsystem ausführen, die Tools ziehen auch in der Regel keinen Verdacht auf sich, da sie meist auf einer Unbedenklichkeitsliste für Antiviren- und andere kommerzielle Sicherheitssoftware stehen.

[1] https://github.com/skalkoto/winexe/

Winexe ist ein Windowsdienst, der so konfiguriert werden kann, dass er beim Hochfahren des Rechners automatisch startet und dann auf Befehle über eine „Named Pipe“ wartet. Named Pipes sind eine bei Windows genutzte Methode zur Kommunikation zwischen Prozessen. Durch sie können Prozesse kommunizieren und Daten austauschen, sogar über ein Netzwerk. Bei Artefakt #1 heißt der Kommunikationskanal „**ahexec**“. Rechner im Netzwerk können darauf zugreifen, indem sie ein ein Datei-Handle auf „**Servername\pipe\ahexec**“ öffnen.

Sobald er mit der Pipe verbunden ist, kann ein Nutzer oder ein Programm dem Handle die Informationen zum Ausführen eines Programms übermitteln (so wie man es sonst über die Kommandozeile tun würde). Die Information wird dann an den Aufruf von *CreateProcessAsUserA* übergeben und der spezifizierte Befehl wird ausgeführt.

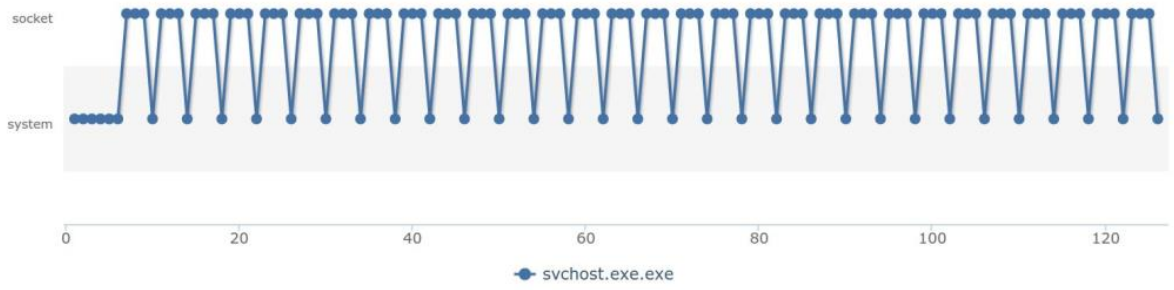
Sobald Artefakt #1 sich im Netzwerk befindet, kann der Angreifer zusätzliche Skripte herunterladen oder erzeugen, Befehle ausführen und Daten ausleiten (zum Beispiel einfach durch das FTP-Protokoll). Es ist plausibel, dass sich Artefakt #1 unter anderem Namen auch auf anderen Servern befinden könnte, obwohl wahrscheinlich ist, dass der Angreifer es nur auf Servern platziert hat, bei denen er Interesse an einem dauerhaften Zugriff hat.

Es ist wichtig, dass alle Vorkommen des Programms gefunden und beseitigt werden, denn sie arbeiten autark und bieten die Möglichkeit, einfach und offen Befehle auf dem Zielrechner auszuführen, möglicherweise sogar mit Administrator-Rechten.

Analyse von Artefakt #2

Artefakt #2 wurde vom Admin Controller gefunden, der von der Linken betrieben wird. Es ist zugeschnittene Malware, die trotz ihrer erheblichen Größe (1,1 MB) nur sehr begrenzte Funktionalitäten zur Verfügung stellt. Artefakt #2 dient dem Angreifer als Rückkanal, um seinen Zugriff auf das infizierte Netz zu behalten. Die Eigenschaften des Artefakts zeigen, dass die Urheber der Malware sie **Xtunnel** genannt haben. Wie der Name andeutet, scheint das Artefakt wirklich als Tunnel zu fungieren, damit der Angreifer aus der Ferne auf das interne Netzwerk zugreifen kann und dabei die Persistenz wahren kann.

Das Artefakt benötigt eine intakte Netzwerk-Verbindung, um einwandfrei zu funktionieren. Wenn eine solche Verbindung nicht hergestellt werden kann, verfängt sich der Prozess in einer Endlos-Schleife, wie das folgende Schema zeigt:



Wie man sieht, versucht das Artefakt nach dem ersten Starten eine Verbindung aufzubauen, indem es einen Netzwerk-Socket erstellt. Wenn das schief geht, wartet es drei Sekunden und versucht es erneut. Die Autoren der Malware scheinen keinen Aufwand betrieben zu haben, Hinweise zu verstecken oder den Code zu verschleiern. Die IP-Adresse, zu der eine Verbindung versucht wird, steht fest programmiert und im Klartext in der Binärdatei. Wir können den in der folgenden Abbildung gezeigten Ablauf beobachten, mit dem das Artefakt versucht, eine Verbindung zu der IP-Adresse **176.31.112.10** aufzubauen.

Diese bestimmte IP-Adresse ist eine wichtige Information, die uns später ermöglichen wird, den Angriff mit einer Serie früherer gezielter Angriffe in Verbindung zu bringen. Die Details

der Zuordnung werden später in einem gesonderten Abschnitt erklärt. Im weiteren Verlauf werden wir diese IP-Adresse **Command & Control (C&C)** nennen.

Das Artefakt kann mehrere Parameter empfangen, einschließlich -Si, -Sp, -Up, -Pp, -Pi und -SSL. Folgende Signalpakete werden von dem Artefakt an Command & Control gesendet:

-Si

```
000000002a 00 00 00                                    *…
00000004b2 23 16 85 ee 59 52 a6 79 3a 2a e2 da 11 c0 1b.#…YR. y:*…..
00000014de 77 ea 47 35 11 de 8a 76 1a ee 16 d9 fd 28 0d .w.G5… v…..(.
```

-Sp

```
0000000022 00 00 00                                    "…
0000000490 ac c6 39 09 b6 23 72 9d 36 a6 3b 2e b7 02 ce…9..#r .6.;….
00000014dd 09 d4 e4 d3 e6 01 5f 6a 37 b2 39 01 b4 0a af …….._ j7.9….
```

-Up

```
0000000007 00 00 00                                    ….
000000047e e2 82 05 74 be 3f 9b 8e 6a dc 5c d1 fe 85 f7~…t.?. .j.\….
000000145f 33 26 6e 5e 62 c1 0e c0 da a3 b3 6c f9 ca 88_3&n^b.. ….l…
```

Falls der Parameter -SSL per Kommandozeile an das Artefakt übergeben wurde, werden Signale in eine SSL-Verbindung gepackt und ein Handshake mit C&C wird initiiert.

Interessanterweise kommt das Artefakt gebündelt mit einer Kopie von OpenSSL 1.0.1e aus dem Februar 2013, die auch für die ungewöhnliche Größe der Binärdatei verantwortlich ist. Der Command & Control-Server scheint auch eine veraltete Version von OpenSSL zu nutzen und anfällig gegenüber Heartbleed-Angriffen[2] zu sein. Auch wenn es unwahrscheinlich ist, muss in Betracht gezogen werden, dass der C&C-Server durch diese Sicherheitslücke selbst Opfer von Angriffen Dritter geworden sein könnte.

[2] http://www.zoomeye.org/lab/heartbleed/2015?port=&code=FR&p=6

Wenn die Verbindungen zu C&C von einer Firewall blockiert oder beendet werden, wird das Artefakt funktionsunfähig, da es keine Ausweichlösung bereithält. Da es außerdem nicht selbstständig andere Funktionalitäten ausführt, würde es dann keine direkte Gefahr mehr darstellen.

Eine Yara-Signatur um das Artefakt aufzuspüren befindet sich im Anhang.

Analyse der Auswirkungen

Obwohl die Werkzeuge, die in dem infizierten Netzwerk gefunden wurden, vergleichsweise simpel sind, darf man die Auswirkungen des Angriffs und die Fähigkeiten der Angreifer nicht unterschätzen. In funktioneller Hinsicht reicht die Kombination eines Tunnels und der Ausführung von Befehlen völlig aus, damit sich ein Angreifer mit ausreichenden Privilegien ungestört in einem Netzwerk bewegen kann.

Es ist bemerkenswert, dass Artefakt #2 von den Urhebern am **22. April 2015**kompiliert wurde. Das legt die Vermutung nahe, dass der Angriff nur wenige Wochen angedauert hat. Doch da die Angreifer sich nicht bemüht zu haben scheinen, ihre Spuren zu verstecken oder einen langfristigeren Zugriff zu sichern (beispielsweise wirkt es, als hätten sie nicht versucht, zusätzliche Administratoren-Accounts anzulegen), ist wahrscheinlich, dass die Durchführung der Aktion schnell stattfinden sollte, um bei dieser Gelegenheit so viele Daten wie möglich zu sammeln und auszuleiten.

Diese Vermutung wird von einer rekonstruierten Batch-Datei mit dem folgenden Inhalt unterstützt:

```
for %%G in (.pdf, .xls, .xlsx, .doc, .docx)
do (forfiles /P F:\[REDACTED] /m *%%G /s /d +01.05.2015 /c "cmd /c copy @path
C:\ProgramData\[REDACTED]\d\@file" )
```

Dieses Skript identifiziert alle PDFs und Office-Dokumente, die nach dem **1. Mai** (spezifiziert in einem Datumsformat, das von Microsoft Windows in deutscher Sprache unterstützt wird) datiert sind und sammelt sie in einem Ordner, mit dem Ziel, sie dann auszuleiten. In keinem der Artefakte fand sich eine spezielle Datenübertragungsfunktionalität,

daher kann es sein, dass der Angreifer die Dokumente über ein gewöhnliches Werkzeug wie FTP hochgeladen hat. Es ist möglich, dass eine vorherige Version des Skripts genutzt wurde, um Daten vor dem 1. Mai 2015 zu sammeln und auszuleiten.

Durch das Wesen des Angreifers und seiner Arbeitsweise (die wir im nächsten Abschnitt beschreiben werden) kann jedoch nicht ausgeschlossen werden, dass noch zusätzliche, anspruchsvolle Artefakte platziert wurden, die entweder bisher noch nicht gefunden oder aber nach der Entdeckung und der öffentlichen Enthüllung des Vorfalls wieder entfernt wurden.

Diese Überlegungen lassen darauf schließen, dass die Infizierung durch einen erfahrenen Angreifer stattgefunden hat.

Zuordnung

Die Zuordnung von Malware-Angriffen ist niemals leicht, aber im Laufe der Untersuchung habe ich Hinweise darauf gefunden, dass der Angreifer mit einer staatlich unterstützen Gruppe namens **Sofacy Group**, auch bekannt als**APT28** oder **Operation Pawn Storm** zusammenhängt. Diese Gruppen werden von der Sicherheitsindustrie in Russland verortet.[3] Es gibt jedoch keine Beweise, die es ermöglichen, die Angriffe bestimmten Regierungen oder Staaten zuzuordnen.

Sofacy ist eine Gruppe, die sich darauf spezialisiert hat, weitbekannte Ziele anzugreifen und vertrauliche Informationen zu stehlen. Sie sind seit etwa 2006 in dieser Hinsicht aktiv. Es wird angenommen, dass die Gruppe erfolgreich Außen- und Innenministerien von Ex-Sowjet-Staaten, osteuropäische Regierungen und Militäreinrichtungen sowie die NATO und das Weiße Haus[4] angegriffen hat.

Sofacy ist dafür bekannt, dass häufig Phishing-Angriffe genutzt werden, um die Ziele dazu zu bringen, ihre Anmeldedaten in einen realisitschen Nachbau interner Systeme wie Webmailer einzugeben. Das wurde beispielsweise in den berühmten Attacken gegen das georgische Innenministerium eingesetzt, die der Invasion von Georgien im Kaukasuskrieg vorangingen.

[3] https://www.fireeye.com/resources/pdfs/apt28.pdf
[4] http://blog.trendmicro.com/trendlabs-security-intelligence/operation-pawn-storm-ramps-up-its-activities-targets-nato-white-house/

Um die Phishing-Angriffe glaubhafter erscheinen zu lassen, nutzt die Sofacy Group *Typesquatting*, das heißt, sie nutzen absichtliche Rechtschreibfehler (beispielsweise wird der Buchstabe “i” mit “l” und “g” mit “q” ersetzt oder es werden Satzzeichen eingefügt) und registrieren Domains, die dem Original stark ähneln:

Quelle: PWC[5]

Sofacy ist ebenso dafür bekannt, auf den Angriff zugeschnittene Exploit-Frameworks und Spearfishing-Angriffe zu nutzen. Im vorliegenden Fall ist es jedoch möglich, dass sie es geschafft haben, durch einen Phishingangriff Zugriff auf Zugangsdaten von Netzwerkadministratoren im Bundestag zu erhalten, was ihnen dann ermöglicht hat, sich durch das Netzwerk zu bewegen und Zugriff auf weitere Daten zu erhalten. Kurz vor dem

[5] http://pwc.blogs.com/cyber_security_updates/2014/10/phresh-phishing-against-government-defence-and-energy.html

Angriff auf den Bundestag haben Sicherheitsunternehmen über die Ausnutzung von Zero-Day-Exploits im Flash Player und Windows durch den selben Angreifer[6] berichtet.

Geteilte Command & Control-Infrastruktur

Die Artefakte selbst enthalten keine nützlichen Hinweise auf eine Zuordnung der Urheberschaft, doch die Netzwerkinfrastruktur, die während des Angriffs genutzt wurde, bringt einige bemerkenswerte Erkenntnisse hervor. Während wir den Command & Control-Server mit der IP-Adresse **176.31.112.10** untersuchten, dessen Adresse fest in Artefakt #2 programmiert ist, konnten wir einige Fehler finden, die die Angreifer gemacht haben. Das hat es uns ermöglicht, den Angriff mit früheren bekannten Angriffen der Sofacy Group in Verbindung zu bringen.

Die IP-Adressen 176.31.112.10 ist ein der französischen Hostingfirma OHV zugeordneter Server, aber offensichtlich wird er von einer sicheren Offshore-Hosting-Firma namens CrookServers.com betrieben und befindet sich anscheinend in Pakistan:[7]

Company Address: MUAnetworks U ashraf Village Kakra Town Mirpur AJK Pakistan

Es ist bei Angreifern üblich, dass sie auf Offshore-Hosting zurückgreifen, da diese seltener mit Strafverfolgungsbehörden kooperieren, wenn es um Takedown-Requests oder die Identifizierung ihrer Kunden geht.

CrookServers scheint auf mehrere Datencenter verteilte Server zu haben, sowie Hosting-Anbieter auf der ganzen Welt.

Bei der Analyse vergangener Daten in Verbindung mit C&C 176.31.112.10 haben wir entdeckt, dass der Server am 16. Februar 2015 ein Zertifikat mit einer anderen IP-Adresse

[6] https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html
[7] http://www.crookservers.com/support-information.php

geteilt hat, die ebenso CrookServers zuzuordnen ist und die ebenso bei OHV gehostet wird: **213.251.187.145**.

Das rekonstruierte geteilte SSL-Zertifikat, das von einer öffentlichen Internet-weiten Scanning-Initiative[8] ermittelt wurde, hatte zu dieser Zeit folgende Attribute:

MD5	b84b66bcdecd4b4529014619ed649d76
SHA1	fef1725ad72e4ef0432f8cb0cb73bf7ead339a7c
Algorithm	sha1WithRSAEncryption
Self-Signed	No
Subject	**C**: GB **L**: Salford **ST**: Greater Manchester **CN**: mail.mfa.gov.ua **O**: COMODO CA Limited **all**: C=GB/ST=Greater Manchester/L=Salford/O=COMODO CA Limited/CN=mail.mfa.gov.ua
Serial	16474505314457171426
Not before	20140414083521Z
Not after	20410830083521Z

Wie dargestellt nutzt das Zertifikat **mail.mfa.gov.ua** als Common Name. Das suggeriert, dass das Zertifikat vorher bei einem ähnlichen Angriff auf das ukrainische Außenministerium oder verwandte Ziele genutzt wurde, auch wenn es keine öffentliche Dokumentierung eines solchen Angriffs gibt.

[8] https://scans.io

Wichtiger ist jedoch die IP-Adresse, mit der dieses Zertifikats geteilt wurde – 213.251.187.145. Sie wurde zuvor mit der Sofacy Group im Rahmen von Phishing-Angriffen auf albanische Regierungsorganisationen in Verbindung gebracht. Die Gruppe registrierte die Domain **qov.al** (der Buchstabe "q" hat das "g" ersetzt) und erstellte realistische Subdomains, um die Opfer beim Besuch der Seite in eine Falle zu locken. Die Domain war unter der IP-Adresse 213.251.187.145 von Juli 2014 bis März 2015 aktiv.

Die Angriffe der Sofacy Group auf albanische Regierungsinstitutionen wurden im Dezember 2014[9] von der Beratungsfirma PwC dokumentiert und gemeldet. Bemerkenswert ist, dass dieser Server auch von CrookServers betrieben wird, da unter anderem *454-reverse.crookservers.net* zur selben IP-Adresse aufgelöst wird.

Ähnliche Artefakte und der root9B-Bericht

Die Hinweise aus den vorangegangenen Absätzen legen eine Verbindung mit der Sofacy Group deutlich nahe, doch die Artefakte (insbesondere #2) waren noch nicht als Teil des Arsenals der Angreifer bekannt.

Wie dem auch sei, am 12. Mai 2015 (einige Wochen, nachdem der Angriff auf den Bundestag vermutlich begonnen hat), veröffentlichte die amerikanische Sicherheitsfirma root9B[10] einen Bericht, der Details zu Malware-Auszügen enthielt, die Artefakt #2 sehr ähneln. Dieser Bericht erwähnt auch die IP-Adresse, die als Command & Control-Server für den Angriff auf den Bundestag genutzt wurde (176.31.112.10).
Der Bericht ist zu großen Teilen fehlerhaft[11], dennoch sind einige der Indikatoren für eine Kompromittierung des Systems berechtigt und scheinen Sofacy korrekt zugeordnet worden zu sein.

Die folgenden Hashes für Malware-Artefakte ähneln stark denen von Artefakt #2:

5f6b2a0d1d966fc4f1ed292b46240767f4acb06c13512b0061b434ae2a692fa1
566ab945f61be016bfd9e83cc1b64f783b9b8deb891e6d504d3442bc8281b092

[9] http://pwc.blogs.com/cyber_security_updates/2014/12/apt28-sofacy-so-funny.html
[10] http://www.prnewswire.com/news-releases/root9b-uncovers-planned-sofacy-cyber-attack-targeting-several-international-and-domestic-financial-institutions-300081634.html
[11] http://krebsonsecurity.com/2015/05/security-firm-redefines-apt-african-phishing-threat/

Anhang: Signaturen zur Erkennung

```
rule apt_sofacy_xtunnel
{
  meta:
    author = "Claudio Guarnieri"
  strings:
    $xaps = ":\\PROJECT\\XAPS_"

    $variant11 = "XAPS_OBJECTIVE.dll"
    $variant12 = "start"

    $variant21 = "UserAgent: Mozilla/5.0 (Windows NT 6.3;
WOW64; rv:28.0) Gecko/20100101 Firefox/28.0"
    $variant22 = "is you live?"

    $mix1 = "176.31.112.10"
    $mix2 = "error in select, errno %d"
    $mix3 = "no msg"
    $mix4 = "is you live?"
    $mix5 = "127.0.0.1"
    $mix6 = "err %d"
    $mix7 = "i`m wait"
    $mix8 = "hello"
    $mix9 = "OpenSSL 1.0.1e 11 Feb 2013"
    $mix10 = "Xtunnel.exe"

  condition:
    ((uint16(0) == 0x5A4D) or (uint16(0) == 0xCFD0)) and
    (($xaps) or (all of ($variant1*)) or (all of ($variant2*))
or (6 of ($mix*)))
}
```