

BfV Cyber-Brief


Nr. 02/2018

- Hinweis auf aktuelle Angriffskampagne -



Kontakt:

Bundesamt für Verfassungsschutz
Referat 4D2/4D3

 0221/792-2600

Hochwertige Cyberangriffe gegen deutsche Medienunternehmen und Organisationen im Bereich der Chemiewaffenforschung

Dem Bundesamt für Verfassungsschutz (BfV) liegen Erkenntnisse zu einer Spear-Phishing Angriffswelle mit mutmaßlich nachrichtendienstlichem Hintergrund vor. Diese Angriffe richteten sich aktuell gegen deutsche Medienunternehmen und Organisationen im Bereich der Chemiewaffenforschung. Es bestehen Indizien für eine Zuordnung der Angriffe zur APT¹-Gruppierung SANDWORM.

Sachverhalt

Eine besonders hochwertige Spear-Phishing Angriffswelle richtet sich aktuell gegen deutsche Medienunternehmen und Organisationen im Bereich der Chemiewaffenforschung. Die Angriffe fanden vermutlich zwischen August 2017 und Juni 2018 statt und dauern vermutlich noch an. Die in der Angriffswelle versandten Spear-Phishing Mails enthalten ein maliziöses Worddokument als Anhang. Beim Öffnen dieses Dokumentes wird dem Opfer empfohlen die Ausführung von Makros zuzulassen. Hierdurch kommt es z. B. zur Ausführung eines VBA Skripts, welches das Logging der PowerShell deaktiviert, PowerShell-Befehle ausführt und eine weitere Datei mit zusätzlichem Code herunterlädt. Letztendlich wird ein PowerShell Empire Agent heruntergeladen, welcher es den Angreifern erlaubt beliebige PowerShell-Befehle auf den kompromittierten Systemen auszuführen.

Das IT-Sicherheitsunternehmen Kaspersky hat zu diesen Angriffen ebenfalls am 19.06.2018 einen Report veröffentlicht².

Dem BfV sind im Zusammenhang mit dieser Angriffswelle bislang zwei deutschsprachige Schaddokumente mit den Namen

- „E-Mail-Adressliste_2018.doc“ und
- „Wichtig! Neue Anforderungen an die Informationssicherheit. Konten bearbeite.doc“ (sic!)

bekannt geworden. Beide Schaddokumente wurden ebenfalls von mutmaßlich deutschen Opfern auf die Plattform Virustotal (<https://virustotal.com>) hochgeladen:

1 Advanced Persistent Threat

2 <https://securelist.com/olympic-destroyer-is-still-alive/86169/>

SHA256: 2497d4da90863b916074116775eb76b983040468f2ab4e4327993639bd263787

Dateiname: Wichtig! Neue Anforderungen an die Informationssicherheit. Konten...

Erkennungsrate: 12 / 61

Analyse-Datum: 2017-11-08 07:38:50 UTC (vor 7 Monate, 1 Woche)

Antivirus Ergebnis Aktualisierung

| Antivirus | Ergebnis | Aktualisierung |
|--------------------------|------------------------------|----------------|
| AegisLab | Troj.Script.Agent.tc | 2017 1108 |
| Avast | VBA-Downloader-DXY [Trj] | 2017 1108 |
| AVG | VBA-Downloader-DXY [Trj] | 2017 1108 |
| Cyren | Trojan.TFBN-7 | 2017 1108 |
| Fortinet | WM/DocDLJWY!tr | 2017 1108 |
| Kaspersky | HEUR:Trojan.Script.Agent.gen | 2017 1108 |
| Qihoo-360 | Wix32/Trojan.Downloader.dbf | 2017 1108 |
| Sophos AV | Troj/DocDI-JWY | 2017 1108 |
| Symantec | Trojan.Gen.2 | 2017 1108 |
| TrendMicro-HouseCall | Suspicious_GEN.F47V0810 | 2017 1108 |
| ViRobot | DOC.Z.Agent.632832.A | 2017 1108 |
| ZoneAlarm by Check Point | HEUR:Trojan.Script.Agent.gen | 2017 1108 |

SHA256: 09fa321c109450dba8b97f8be268e9a9e996b3f6bcf02127927a8a3d314269

Dateiname: E-Mail-Adressliste_2018.doc

Erkennungsrate: 3 / 59

Analyse-Datum: 2018-06-05 14:42:10 UTC (vor 1 Woche) Zeige Neueste (/de/file/09fa321c109450dba8b97f8be268e9a9e996b3f6bcf02127927a8a3d314269/analysis/)

The file being studied follows the Compound Document File format! More specifically, it is a MS Word Document file.

Commonly abused properties

- The studied file makes use of macros, a macro is a series of commands and instructions that you group together as a single command to accomplish a task automatically. Macros are often abused to perform malicious tasks when working with a document.
- May create OLE objects.
- Seems to contain deobfuscation code.

Summary

last_author AV

creation_datetime 2018-06-05 13:28:00

Nach Erkenntnissen des BfV kam es bereits zu Spear-Phishing Angriffen mit diesen Schaddokumenten gegen deutsche Medienunternehmen. Darüber hinaus gibt es Hinweise, dass sich die Angriffe auch gegen eine Organisation im Bereich der Chemiewaffenforschung gerichtet haben. Betroffenheiten weiterer, hier noch nicht bekannter, Unternehmen in Deutschland sind wahrscheinlich.

Laut Kaspersky bestehen technische Überschneidungen zur Kampagne „Olympic Destroyer“, die für die versuchten Cybersabotageangriffe gegen die Olympischen Winterspiele in Südkorea 2018 verantwortlich ist.



Nach Einschätzung des BfV liegen bei den hier beschriebenen Spear-Phishing Angriffen Anhaltspunkte für eine Attribution zur nachrichtendienstlichen Gruppierung SANDWORM vor.

Die technisch hoch versierte und äußerst aggressive APT-Gruppierung SANDWORM, die auch unter den Bezeichnungen Quedagh und BlackEnergy bekannt ist, ist seit mindestens 2013 aktiv. Zu Beginn der Aktivitäten führte die Gruppierung laut öffentlichen IT-Sicherheitsreports u.a. Cyberspionageoperationen gegen die NATO, westliche Regierungsstellen, Telekommunikationsunternehmen sowie akademische Einrichtungen durch.

Seit 2015 wurden jedoch vermehrt Cybersabotageangriffe von SANDWORM, insbesondere gegen Ziele in der Ukraine, bekannt. So bestehen Indizien für eine Urheberschaft von SANDWORM bei den erfolgreichen Cybersabotageangriffen gegen ukrainische Energieversorger im Dezember 2015 und Dezember 2016. SANDWORM stellt eine der derzeit gefährlichsten APT-Gruppierungen weltweit dar.

Ziel der Angriffe könnte daher nicht nur das Ausspähen von Daten, sondern auch die Sabotage von IT-Systemen sein.

Handlungsempfehlung

Die Ausführung von Makros sollte generell stark eingeschränkt werden, um die Ausführung von malignem Code zu unterbinden.

Ein längerfristiges Logging sollte zumindest für Internet Proxy-Server umgesetzt werden.

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

- Suchen Sie in den E-Mail Eingängen (auch der letzten Monate) nach den oben genannten E-Mail Anhängen.
- Prüfen Sie ihre Logdateien anhand der dem Cyber-Brief beigefügten IP-Adressen von C2-Servern.

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr, dass Ihre IT-Systeme infiziert sind. In diesem Fall können wir Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen und weitere Hinweise geben. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221-792-2600 oder

E-Mail: poststelle@bfv.bund.de

Wir weisen darauf hin, dass die Durchführung der in diesem Schreiben genannten Maßnahmen nicht die Meldung gemäß § 8b Abs. 4 BSI-Gesetz bzw. § 109 Abs. 5 TKG gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) ersetzt.

IOCs³:

| SHA1 Hash | SHA256 Hash | MD5 Hash | Titel des Dokuments | Erstelldatum |
|--|--|--|---|--------------|
| 79a66 07a34 ed859 24152 c1e44 a9b4e 78cbf8 9777 | 2497d4 da9086 3b9f607 411677 5eb76b 983040 468f2ab 4e4327 993639 bd2637 87 | a0bd94 1fbcc16 388ce7 4ce10c8 df3c75 | Wichtig! Neue Anforderungen an die Informationssicherheit. Konten bearbeite.doc | 09.08.2017 |
| c5cb46 a524fd 13436 0d857 38d0fe e0898 96be8 2c | b85027 de6871 e2ed1a 2154ed b645fd0 168079 89b441 07fc280 4eb6e9 acce3b9 d | e2e102 291d25 9f05462 5cc8531 8b7ef5 | E-Mail-Adressliste_2018.doc | 05.06.2018 |

Genutzte C2-Server:

200.122.181.63

185.148.145.141

79.142.76.40

130.185.250.77

185.128.42.194

200.122.181.64

185.94.193.203

86.96.193.134

159.148.186.116

5.133.12.224

3 Indicators of Compromise