Bundesamt für
Verfassungsschutz

Köln, 22. März 2017

BfV Cyber-Brief

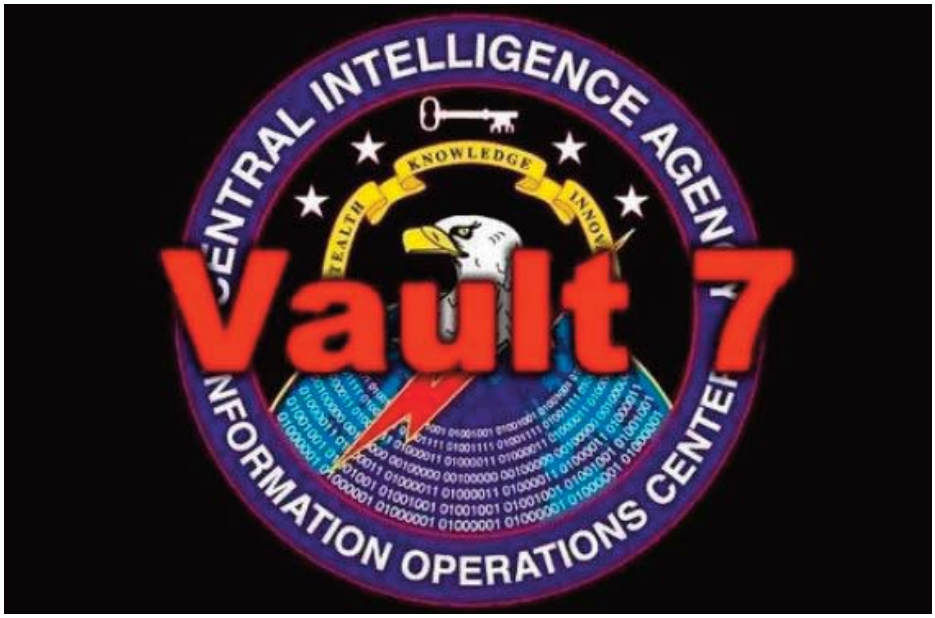
Nr. 01/2017

- WikiLeaks-Veröffentlichung „Vault7“ -

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

Aktuelle WikiLeaks-Veröffentlichung „Vault7“

Auf der Plattform WikiLeaks wurden am 7. März 2017 umfangreiche Daten veröffentlicht, die nach Aussage von WikiLeaks von einer internen Datenbank der CIA stammen sollen. Die veröffentlichten Daten beinhalten u.a. zahlreiche Informationen zu möglichen Cyberangriffswerkzeugen und dem Vorgehen bei Cyberangriffen.



Quelle: www.betanews.com

WikiLeaks hat die technischen Parameter der beschriebenen Angriffswerkzeuge nicht umfassend veröffentlicht, sondern in weiten Teilen eine Anonymisierung vorgenommen. Trotz dieser Anonymisierung finden sich einige technische Parameter, die als Indikator für eine Infektion dienen können. Diese werden mit diesem Cyber-Brief an Behörden sowie Unternehmen verteilt, um die eigenen Systeme auf eine mögliche Infektion untersuchen zu können.

Sachverhalt

Auf der Plattform WikiLeaks wurden am 7. März 2017 umfangreiche Daten unter der Bezeichnung „Vault 7“ veröffentlicht, die nach Aussage von WikiLeaks von einer internen Datenbank der CIA stammen und den Beginn einer Serie von Veröffentlichungen markieren sollen.

Die erste Veröffentlichungsreihe mit der Bezeichnung „Year Zero“ beinhaltet 8.761 Dokumente, die aus dem Netzwerk des „Center for Cyber Intelligence“ der CIA stammen sollen.

Die Dokumente umfassen einen Zeitraum von 2013 bis März 2016. Aus den veröffentlichten Daten ergeben sich u.a. zahlreiche Informationen zu möglichen Cyberangriffswerkzeugen und dem Vorgehen bei Cyberangriffen.

Laut den Unterlagen soll die CIA beispielsweise über eine Datenbank mit ausländischer Schadsoftware verfügen. Diese soll die Möglichkeit bieten, technische Merkmale und Indikatoren fremder Nachrichtendienste zu imitieren und für eigene Cyberangriffe zu verwenden („False Flag-Operationen“). Dies unterstreicht den Ansatz des Bundesamtes für Verfassungsschutz, dass bei der Attribution von Cyberangriffen allein technische Merkmale nicht ausreichen können.

Die in den Veröffentlichungen dargestellte Schadsoftware dient auch der Kompromittierung von Smartphones (Apple Betriebssystem iOS sowie Google Betriebssystem Android), Windows Betriebssystemen und Fernsehern (sogenannten Smart-TVs). Viele der in den WikiLeaks-Dokumenten aufgedeckten Schwachstellen und Sicherheitslücken sind allerdings bereits von den Herstellern beseitigt worden.

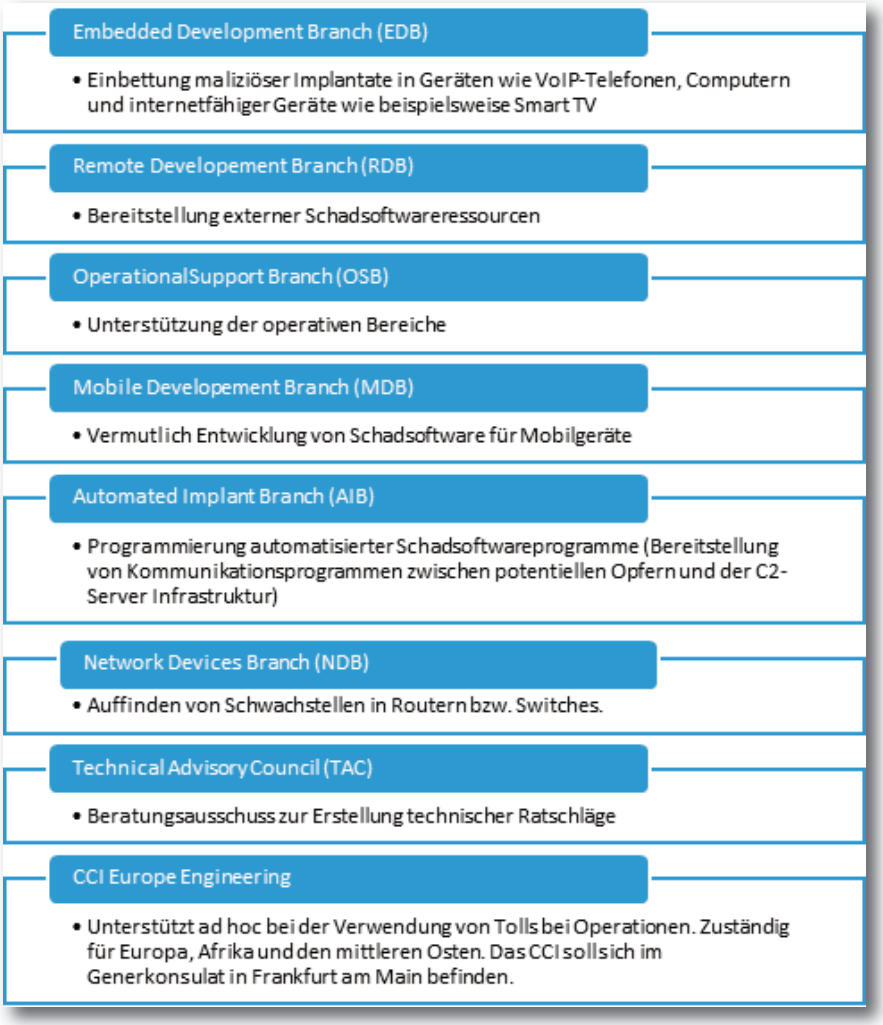
Darüber hinaus sind einige der benannten Schwachstellen, zum Beispiel für das Apple-Betriebssystem iOS oder Smart-TVs, lediglich ausnutzbar, wenn ein physischer Zugriff auf das Gerät möglich ist.

Aus den Dokumenten geht bislang keine direkte deutsche Betroffenheit hervor. Weder werden vergangene Angriffe, noch geplante Cyberangriffe gegen deutsche Unternehmen oder Behörden thematisiert.

Insgesamt ist die Veröffentlichung bei WikiLeakswie folgt gegliedert:

I. Departments/Branches/Groups

In diesem Kapitel finden sich insbesondere Informationen zu den einzelnen Arbeitsbereichen innerhalb der CIA, die sich mit Cyberangriffen und deren Vorbereitung befassen. Zu den nachfolgenden Einheiten finden sich dabei Informationen:



II. Projects

Innerhalb dieses Abschnitts werden einzelne Projekte beschrieben. Besonders erwähnenswert ist das Project „Marble Framework“. Hier wird bei der finalen Kompilierung von Schadsoftware eine automatisierte Verschleierung durchgeführt, um die Attribution von Cyberangriffen zu erschweren.

III. Operating Systems/Platforms

In diesem Abschnitt finden sich u.a. Hilfestellungen für Anwendungs- und Toolentwicklung hinsichtlich unterschiedlicher Betriebssysteme (wie z.B. IOS oder Android).

IV. Development/Tools

Innerhalb dieses Abschnitts werden diverse Tools vorgestellt, die von der CIA regelmäßig für Angriffe verwendet werden sollen.

V. Users

Hier sind Beiträge von einzelnen (anonymisierten) Personen veröffentlicht worden, die sich mit zahlreichen Cyberthemen auseinandersetzen. Es finden sich hier beispielsweise Hilfestellungen für andere Mitarbeiter, aber auch Auflistungen von aktuellen Projekten einzelner User.

Das Bundesamt für Verfassungsschutz als nationale Spionageabwehrbehörde möchte deutsche Stellen auf diesem Wege auf die aktuelle Bedrohungslage aufmerksam machen und mit den vorhandenen technischen Informationen versehen, um die eigenen Systeme auf eine Infektion hin untersuchen zu können.

Handlungsempfehlung

Um festzustellen, ob Ihr Unternehmen betroffen ist, empfehlen wir folgende Schritte:

- Durchsicht der Netzwerk-Logs nach den in der Anlage aufgeführten netzwerkbasierten IoC[1].
- Suche nach den in der Anlage aufgeführten hostbasierten-IoC.

Sollten Sie entsprechende Anhaltspunkte feststellen, besteht die Gefahr der Infizierung Ihrer Rechner. 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 sichern Ihnen absolute Vertraulichkeit zu!

1 Indicators of Compromise

Anlage: Indicators of Compromise (IOC)

Hashes

md5: 82684128dfd4a027fddb33711bd2a8ec

sha-256: f0d422222b6b39b4a141b6916cb4c844aeb6173fe185fe1030497d273f4e1377

md5: d85e26868162eefef20ca6f4aeca3a99

sha-256: ea042bd3a7df11273e233c423e9740e6b51001911139855ef39501472a1e5fb0

md5: d6eade9176d7e19454cf5e60c67574fc

sha-256: 7bb70ab14ad6003d77529f9edf9fa89dfde7656526f2393c07ae9d03455522f2

md5: d01606c6b6ee92475fa5bd4c87a8dfd0

sha-256: 172e496fc433592c3c7760fb97451106b5188189987477e5a33b13b5eee685e9

Domains and IP-Adressen

148.251.160[.]129

38.86.48[.]163

46.45.182[.]227

buglyter[.]net

charmore[.]net

delafrone[.]com

equivatec[.]com

feduptonec[.]net

flowhyper[.]net

lifeinsureadv[.]com

ns1.trickmel[.]com

ns1.vesselwatcher[.]net

ns1.winterfall[.]net

ns2.flowhyper[.]net

ns2.vesselwatcher[.]net

ronket[.]com

sightlinked[.]com

trickmel[.]com

vesselwatcher[.]net

winterfall[.]net

wisemip[.]net

www.vesselwatcher[.]net

zabbix-tech[.]com

win32-srv8.zabbix-tech[.]com