BSI/ANSSI
Deutsch-französisches IT-Sicherheitslagebild

Vol. 1 – Juli 2018

Bundesamt
für Sicherheit in der
Informationstechnik

1 Vorworte

Guillaume Poupard
Generaldirektor der ANSSI

Arne Schönbohm
Präsident des BSI

Das BSI ist für die ANSSI ein langjähriger und strategischer Partner Dank der vertrauensvollen, professionellen Zusammenarbeit, die sich über Jahre durch den regelmäßigen Austausch aufgebaut hat.

Dadurch stehen wir gemeinsam vor wichtigen technischen Herausforderungen, wie die Zertifizierung, die Stärkung der operationellen Kooperation, die Erarbeitung technischer Richtlinien, das Aufkommen und die Diversifizierung der Bedrohungslage.

Die Weiterentwicklung der Leistungsstärke auf rein nationaler Ebene, in Frankreich und Deutschland, reicht langfristig nicht aus, um ein Gegengewicht zur aktuellen Bedrohung zu bilden, die erfordert, dass wir unsere Kräfte vereinen.

Ich möchte die langjährige fruchtbare Zusammenarbeit und das große Potential auf diesem Feld betonen. Dieser erste gemeinsame Bericht ist ein Ausdruck der Intensivierung der deutsch-französischen Zusammenarbeit in der IT-Sicherheit, die ein Treiber für die Entwicklungen auf europäischer Ebene sein wird.

55 Jahre nach Unterzeichnung des Elysée-Vertrags wird die deutsch-französische Freundschaft und Kooperation auf europäischer Ebene durch eine Neuauflage im Jahre 2018 gestärkt und die deutsch-französische Zusammenarbeit auf wirtschaftlicher, politischer und gesellschaftlicher Ebene umso deutlicher.

Die durch diese Veröffentlichung hervorgehobene Kooperation von BSI und ANSSI stellt eine weitere Facette dieser starken Partnerschaft dar. Die Zusammenarbeit erstreckt sich auf alle relevanten Bereiche, die die digitale Sicherheit in Gegenwart und Zukunft gewährleisten: Cyber-Sicherheit, Kryptografie, Forschung, Zertifizierung und Standardisierung.

Dieser Bericht ist das Resultat gemeinsamer Analysen von Langzeitrisiken für die Cyber-Sicherheit. Die Auswertungen bilden das Fundament für weitergehende strategische Entscheidungen, um den wachsenden Herausforderungen zu begegnen.

Weiterhin drückt diese Veröffentlichung die Bedeutung der gemeinsamen Arbeit von BSI und ANSSI aus, welche neue Perspektiven eröffnet und eine Bereicherung für beide Parteien darstellt.

2 Allgemeine Bedrohungslage

Sowohl Frankreich als auch Deutschland stehen vor wachsenden Herausforderungen, welche in Folge der zunehmenden Vernetzung und Digitalisierung auftreten. Technischer Fortschritt eröffnet neue Möglichkeiten mit allen Vor- und Nachteilen.

Hochmoderne leistungsstarke und sichere Informationstechnologien sind grundlegend für den wirtschaftlichen Fortschritt und eröffnen der Gesellschaft des 21. Jahrhunderts neue Chancen. Technologien beeinflussen die Entwicklung im Bereich der Kommunikation, des Handels und Transports. Die Arbeitswelt muss sich den Fragen der Industrie 4.0 stellen, was z.B. auch die Etablierung einer sicheren digitalen kritischen Infrastruktur betreffen kann.

Auf der anderen Seite ermöglicht der Fortschritt genauso neue Möglichkeiten für Kriminalität, Spionage und Sabotage. Seit der sprunghaften Erhöhung der Bedrohung durch Ransomware im Jahr 2016 ist die allgemeine Bedrohungslage auf einem besorgniserregenden Level, welches durch eine höhere Intensität und vielfältigere Verbreitungswege noch erhöht wurde. Im nationalen Kontext reagierten ANSSI und BSI angemessen auf Vorfälle und stellen auf diese Weise die IT-Sicherheit bspw. der nationalen kritischen Infrastruktur sicher. Beide haben operationale und strategische Prozesse entwickelt, um maßgeschneidert Lösungen für Betroffene bereit zu stellen.

Während manche der beobachteten Vorfälle mit ungekannter Anzahl, Intensität oder der Verwendung neuer Methoden einhergehen, stechen andere durch hohe Medienresonanz heraus, da sie globale politische, wirtschaftliche oder strategische Entwicklungen tangieren. Versuche, in demokratische Prozesse oder wirtschaftliche Kontexte einzugreifen, fallen in die zweite Kategorie, wobei in wenigen Fällen bereits der Einsatz geringer Ressourcen eine ungleich hohe Resonanz hervorrufen kann. Das frühzeitige und kontinuierliche Sammeln valider Informationen über vergangene und aktuelle Vorfälle ist die Grundlage für eine fundierte Auswertung der aktuellen Bedrohungslage. Die folgende qualifizierte Evaluation trägt ihren Teil zu der Entwicklung angemessener Gegenmaßnahmen durch den Nutzer bei. Drei Hauptaspekte von Cyber-Bedrohungen werden in den folgenden Abschnitten näher erläutert.

1.1 Kriminalität: Verbreitung hoch entwickelter Angriffswerkzeuge

Die Veröffentlichung fortgeschrittener Angriffswerkzeuge wie Exploit-kits ermöglicht ihre zunehmende Verbreitung, die in manchen Fällen zu einer Angriffskampagne führt,

deren Konsequenzen desaströs sein können. Tatsächlich können derartige Werkzeuge unbegrenzt vervielfältigt und modifiziert werden. Angriffswerkzeuge, die im Internet veröffentlicht werden, werden von anderen kriminellen Gruppen aufgenommen und ergänzen die Palette ihrer Werkzeuge. Eine Zunahme von Angeboten bei Angriffswerkzeugen konnte beobachtetet werden. Der Hauptangriffsweg sind maliziöse Mails, die etwa eine Makro-Word-Datei, js-Datei oder einen Download-Link im Anhang enthält. Zuletzt wurden 86% des Gesamtmailverkehrs als potentiell unerwünscht und maliziös eingestuft. Maliziöse Mails werden durch große Botnetze wie etwa Necurs und Mirai verbreitet. Die Vielfalt der Angriffswerkzeuge, Vorgehensweisen und Akteuren verkompliziert die Lage und erschwert die Identifikation des Epizentrums einer Attacke.

1.2 Sabotage: Zunahme destruktiver Attacken

ANSSI stellt einen Anstieg von Angriffen mit destruktiven Effekten fest, um wirtschaftliche oder physische Sabotage zu betreiben. Unter anderem beobachtete die französische Behörde seit 2014 einen konstanten Anstieg in Ransomware-Attacken mit unterschiedlich hohem Verbreitungsgrad. Diese Art Schadcode entzieht Daten dem Zugriff durch das infizierte System bis das Opfer das Lösegeld bezahlt, üblicherweise geschieht dies mittels einer Kryptowährung wie dem Bitcoin.

Das BSI bestätigt diese Zunahme der Bedrohung durch Ransomware. Es ist definitiv möglich, dass die Intention der Sabotage manchen Ransomware-Angriffen im Jahr 2017 zu Grunde liegt. Ein Indikator hierzu könnte das implementierte lateral movement darstellen, welches den Effekt der Infektion auf die im lokalen Netz verbundenen Systeme ausweitet. In der Praxis infizierte NotPetya eine ukrainische Software, die im Finanzverwaltungsumfeld genutzt wurde, und verursachte Vorfälle im Bereich der kritischen Infrastrukturen, wie etwa bei Elektrizitätsherstellern, Flughäfen und im Zugbetrieb in der Ukraine.

1.3 Spionage: Kompromittierung von IT-Service-Dienstleistern und -Nutzern

Weltweit nimmt das ANSSI die Verbreitung von Aktionen im Bereich der Computerspionage wahr. Diese Operationen, teilweise im Bereich der organisierten Kriminalität, bestehen daraus, vertrauliche Informationen über Personen, ihren Wettbewerb, einen bestimmten Wirtschaftsbereich, und nicht-staatliche Organisationen zu sammeln. Ziel dieser Attacken ist es, einen strategischen Vorteil zu gewinnen ohne Kenntnis des Betroffenen, indem Techniken und Vorgehensweisen entsprechend dem Vertraulichkeitsniveau genutzt werden. 2017 wurden derartige Aktionen in besondere Weise ausgeführt, indem das avisierte Ziel nicht direkt

angegriffen wurde, sondern die Versorgungskette.

Doch nicht nur die hohe Zahl und Intensität der Angriffe ist alarmierend. Ein besonderes Risiko stellen konzeptionelle Schwachstellen dar. So wurde der Fall Meltdown/Spectre in den Medien stark wahrgenommen. Dabei wurde öffentlich bekannt, dass Prozessoren von Intel, ARM und AMD Seitenkanalangriffe auf Speicherbereiche nicht verhindern, welche bspw. wichtige Passwörter enthalten können. Eine weitere kritische Schwachstelle, die im Oktober 2017 bekannt wurde, stellt die Sicherheit von im WLAN übertragenen Daten in Frage. KRACK ist die Abkürzung von Key Reinstallation AttaCK und betrifft Sitzungsschlüssel, welche die Übertragung von WPA- und WPA2-geschützten Daten im WLAN sichern. Folglich können vertrauliche Datenpakete entschlüsselt werden und die Vertraulichkeit des Kommunikationstransfers ist verletzt.

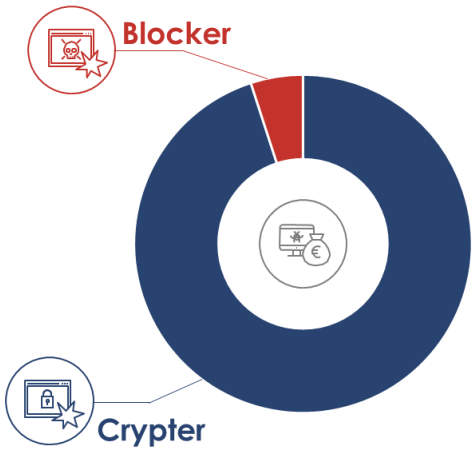
Daher sind effektive Strategien zum Schutz notwendig. Einige Mitigationsmaßnahmen sorgen für eine solide Grundlage hierzu:

- Gutes Patch-Management: Regelmäßiges, häufiges und bedarfsbedingtes sowie anlassbezogenes Einpflegen von Updates
- Hohe Achtsamkeit beim Öffnen von Mails
- Regelmäßiges und häufiges Erstellen von Backups, um Datenverluste bspw. durch Ransomware zu minimieren
    - Testen der Konsistenz und der Vollständigkeit der Daten, Testen des Einspielens
    - Decryption-Tools für Ransomware
- Aktuelle Antivirus-Software und persönliche Einstellung der Firewall
- Benutzeraccount mit eingeschränkten Rechten bei Internetzugang des Systems
- Unterschiedliche, starke und regelmäßig veränderte Passwörter
- Im Falle einer Detektion von Schadsoftware: Unverzügliche und adäquate Maßnahmenergreifung, d.h. Abbruch der Verbindung zu weiteren Hardware-Komponenten, um den Schaden zu minimieren, und Information der zuständigen Behörden

3 Ransomware

Definition: Ransomware ist eine Schadsoftware, die den Zugang zu Daten einschränkt oder unterbindet und zur erneuten Freigabe ein Lösegeld verlangt. Ransomware-Angriffe sind eine Form digitaler Erpressung.

3.1 Kategorien



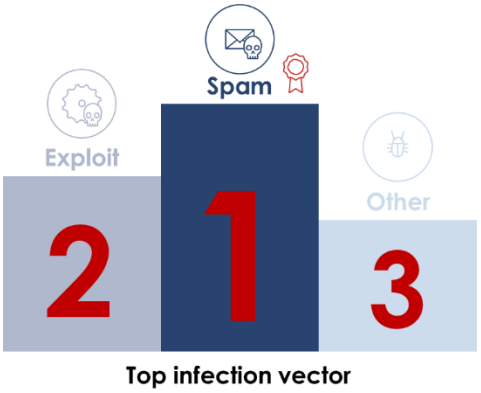
Es können zwei Kategorien von Ransomware unterschieden werden. Erstens: Ransomware, die den Zugang zu Daten blockiert, das Betriebssystem infiziert und nach einem Neustart geladen wird, um den Desktop mit einem Bild oder einer Webseite zu überlagern. 2015 erlangte ein Trojaner weite Verbreitung, der im Namen von Behörden nach Bußgeldern verlangte. Im Verlauf von 2016 trat Blocker Ransomware kaum noch auf.

Zweitens: 95% der bekannten Ransomware-Angriffe waren Verschlüsselungstools (Crypter) und verwendeten eine Kombination symmetrischer und asymmetrischer Verschlüsselung wie AES und RSA/ECC. Der Angreifer stellt dem Betroffenen in Aussicht, ein Entschlüsselungstool nach der Vornahme der Zahlung bereit zu stellen.[1] Die Ransomware vergleicht die Dateien auf den lokalen Verzeichnissen, wie Festplatten, USB-Sticks und Netzwerkkomponenten mit einer Liste von Dateiformaten und verschlüsselt nur diese. Dies stellt die Funktionalität des Betriebssystems sicher, sodass die Vornahme der Transaktion ermöglicht wird. [2]

.123 .3dm .3ds .3g2 .3gp .602 .7z .aes .arc .asc .asf .asm .asp .avi .bak .bat .bmp .brd .cgm .class .cmd .cpp .crt .cs .csr .csv .db .dbf .dch .dif .dip .djv .djvu .doc .docb .docm docx .dot .dotm .dotx .fla .flv .frm .gif .gpg .gz .hwp .ibd .jar .java .jpeg .jpg .js .key .lay .lay6 .ldf .m3u .m4u .max .mdb .mdf .mid .mkv .mml .mov .mp3 .mp4 .mpeg .mpg .ms11 .myd .myi .nef .odb .odg .odp .ods .odt .otg .otp .ots .ott .p12 .paq .pas .pdf .pem .php .pl .png .pot .potm .potx .ppam .pps .ppsm .ppsx .ppt .pptm .pptx .psd .qcow2 .rar .raw .rb .RTF .sch .sh .sldm .sldx .slk .sql .sqlite3 .Liedtitel .stc .std .sti .stw .svg .swf .sxc .sxd .sxi .sxm .sxw .tar .tar.bz2 .tbk .tgz .tif .tiff .txt .uop .uot .vb .vbs .vdi .vmdk .vmx .vob .wav .wb2 .wk1 .wks .wma .wmv .xlc .xlm .xls .xlsb .xlsm .xlsx .xlt .xltm .xltx .xlw .xml .zip

Liste von Dateiformaten, die von der Ransomware Locky verschlüsselt werden[2]

3.2 Angriffswege



- Spam: Die meisten Ransomware-Angriffe sind weit gestreute Spam-Mail-Kampagnen. Die Mails sind vorgebliche Rechnungen, Buchungsbestätigungen, Lieferscheine, Bewerbungen, gescannte Dokumente, Fax-Mails oder Bilder. Auf diese Weise wird der Empfänger getäuscht und zum Öffnen der Mail verleitet. Typischerweise enthält die maliziöse Mail ein Word-Dokument, das ein Makro ausführt, eine zip-, Skript- oder Programmdatei oder eine Kombination daraus, sodass ein Powershell-Skript ausgeführt wird.
- Exploit-Kits: Ein Exploit-Kit nutzt z.B. unterschiedliche Drive-by-Exploits, um Schwachstellen auf dem System eines Opfers zu finden, während die Aufmerksamkeit des Nutzers von etwas anderem eingenommen ist.
- Sonstiges: Serverseitige Softwareschwachstellen werden zur Infektion von Clients ausgenutzt. In wenigen Fällen wurde ein gezielter Brute-Force-Angriff durchgeführt, um an Administratorrechte zu gelangen. [2]

Die folgenden Angriffsstrategien erhöhen die Erfolgsrate des Angreifers:

- Die Höhe des Lösegelds wird nicht zu hoch angesetzt, sodass eine höhere Anzahl von Betroffenen in der Lage und Willens zu zahlen ist.
- Vorgeben einer Zahlungs-Deadline, bis zu der die Wiederherstellung der Daten möglich ist. Dies kann durch die Androhung begleitet werden, dass die Lösegeldforderung mit der Zeit erhöht wird.

Das Opfer kann zusätzlich unter Druck gesetzt werden, indem angedroht wird, ein Teil der Daten zu löschen, je länger die Zahlung des Lösegeldes sich verzögert. [2]

3.3 Maßnahmen

Da der Hauptangriffsweg von Ransomware Spam Mails sind, werden angemessene Mitigationsmaßnahmen gegen mailiziöse Mails das Risiko von Ransomware-Attacken

minimieren:

- Ablehnen von Skript-Dateiausführungen, wie JavaScript, VisualBasic und Poweshell
- Texteditor als Standardeinstellung für die Ausführung von Skriptdateien
- Ablehnen der Ausführung von Makros in Office Dokumenten
- Sichere Identifizierung des Dateiformats
- Erhöhung der Achtsamkeit des Nutzers beim Öffnen von Mails

Regelmäßiges, häufiges und anlassbezogenes Patchen von Anwendungen ist eine der Basismaßnahmen für IT-Sicherheit. So können Schwachstellen geschlossen werden, die von Exploit-Kits für eine Ransomware Infektion genutzt werden. Insbesondere Webbrowser, Plug-Ins, E-Mail-Software, PDF-Applikationen und Office-Programme sind bedroht und müssen regelmäßig aktualisiert werden. Allgemein sollte die Nutzung von Browser-Plugins so stark wie möglich eingeschränkt werden, ein Browser mit Sandbox-Technologie ist empfehlenswert, genauso wie eine aktuelle Antivirensoftware. [2]

Im Oktober 2017 reagierte Microsoft auf die zunehmende Bedrohung durch Ransomware, indem ein kontrollierter Dateizugriff bei Windows 10 implementiert wurde, um die Änderung wichtiger Dateien durch Schadcode effektiv zu verhindern. [3] Insgesamt werden Schutzmaßnahmen fortschrittlicher.

Der bedeutungsvollste Faktor ist die interne Achtsamkeit beim Öffnen von E-Mails und dem Besuchen von Webseiten. Das Prüfen der Authentizität des Senders und der Plausibilität der Betreffzeile der Mail sollten selbstverständlich sein. Nutzer sollten keine Rechte und Berechtigungen erhalten, die nicht zwingend notwendig für die Erfüllung ihrer Aufgaben sind, da dies ein unnötiges Risiko im Falle der Infektion des Systems darstellt. Ein Fernzugriff auf ein System sollte ausschließlich über VPN und eine 2-Faktor-Authentifizierung realisiert werden. Das Testen der Verwundbarkeit eines Systems durch externe Zugänge wird mit Durchführung eines Penetrationstests sicher gestellt. Alles in allem minimiert ein fehlerfrei implementierter Backup-Prozess zur regelmäßigen und häufigen Erstellung von Dateikopien das Risiko eines Datenverlusts.[2]

Sollte dennoch eine Ransomware-Infektion erfolgreich gewesen sein, ist das Vornehmen der Lösegeldtransaktion keine nachhaltige Handlungsoption. Denn die fehlerfreie Wiederherstellung der Daten ist nicht garantiert. Was jedoch garantiert ist, ist die Unterstützung der Entwicklung weiterer Angriffstools. Im Fall einer Ransomware-Infektion ist eine Strafanzeige anzuraten.

Nicht in jedem Fall sind die verschlüsselten Dateien verloren. Die hauptsächlich verwendeten Verschlüsselungsalgorithmen sind bekannt: RSA (Schlüssellänge 1024-4096 Bit), ECDH (Schlüssellänge 192 Bit), AES (Schlüssellänge 128-256 Bit), RC4 und Salsa20. Daher stehen zahlreiche Entschlüsselungstools Open Source zur Verfügung. Manche werden gar von Angreifern angeboten, die auf diese Weise Konkurrenz bei Ransomware-Angriffen ausschalten wollen.[1]

Harasom	18.08.2013	https://decrypter.emsisoft.com/harasom
CryptoDefense	02.04.2014	https://decrypter.emsisoft.com/cryptodefense
TorLocker / Scraper	08.04.2015	https://securelist.com/blog/research/69481/a-flawed-ransomware-encryptor/
PCLock	29.04.2015	https://decrypter.emsisoft.com/pclock
TeslaCrypt 1.0 / AlphaCrypt	13.05.2015	http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#decrypt
CoinVault / Bitcryptor	28.10.2015	https://noransom.kaspersky.com/
Linux Encoder	10.11.2015	https://labs.bitdefender.com/2015/11/linux-ransomware-debut-fails-on-predictable-encryption-key/
CryptInfinite	22.11.2015	https://decrypter.emsisoft.com/cryptinfinite
Rakhni	11.12.2015	http://support.kaspersky.com/de/viruses/disinfection/10556
Radamant	02.01.2016	https://decrypter.emsisoft.com/radamant
TeslaCrypt 2.0	20.01.2016	https://up2sha.re/GGTSPU-fw1.bsi.bund.de-32760-6546225-xMh9MxnlcLkeofgD-DAT/file?l=C5ag0MrQNqAb.pdf
KeyBTC	24.01.2016	https://decrypter.emsisoft.com/keybtc
LeChiffre	25.01.2016	https://decrypter.emsisoft.com/lechiffre
Gomasom	25.01.2016	https://decrypter.emsisoft.com/gomasom
CrypBoss	30.01.2016	https://decrypter.emsisoft.com/crypboss
DMALocker	06.02.2016	https://decrypter.emsisoft.com/dmalocker
HydraCrypt	12.02.2016	https://decrypter.emsisoft.com/hydracrypt
DMALocker2	18.02.2016	https://decrypter.emsisoft.com/dmalocker2
Nemucod	22.03.2016	https://decrypter.emsisoft.com/nemucod
Petya	09.04.2016	https://github.com/leo-stone/hack-petya/blob/master/README.md
Jigsaw/CryptoHitman	11.04.2016 11.05.2016	http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/ http://www.bleepingcomputer.com/news/security/jigsaw-ransomware-becomes-cryptohitman-with-porno-extension/
AutoLocky (nicht die in DE verbreitete Familie Locky)	16.04.2016	https://decrypter.emsisoft.com/autolocky

Beispiel verfügbarer Entschlüsselungstools im Mai 2016[2]

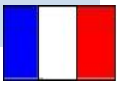
3.4 Entwicklung von Ransomware-Vorfällen

Eine aktuelle Sophos Studie unter Befragung von 2.100 Organisationen stellt fest, dass 54% der Firmen von Ransomware betroffen waren mit einem durchschnittlichen Schaden von 133 US-Dollar. 74% der Betroffenen verwendeten aktuelle Antivirensoftware. Demnach sind Ransomware-Vorfälle weiterhin zu beobachten.[4]

2015

Februar 2015 – CTB-Locker-Kampagne

Französische Bürger, KMUs und kommunale Behörden waren durch diese Kampagne betroffen. Die beobachtete Technik war die Versendung von Mails, die eine Fax-Nachricht im zip-Format im Anhang enthielten, zusammen mit der Malware CTB-Locker. Diese Ransomware war unter anderem beachtenswert auf Grund ihrer Verschlüsselung und Kommunikation über Tor.



- Weltweit führen 150.000 WordPress-Webseiten zu einem CryptoWall-download. [5]

Februar 2016 - Lukaskrankenhaus

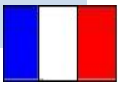
10.02. um 09:00: Die IT-Abteilung des Lukaskrankenhaus in Neuss registriert eine Alarmmeldung. Grund hierfür war eine Ransomware ähnlich zu TeslaCrypt 2.0 im Anhang einer Mail, die im internen Netz Dateien -notwendig für die Patientenversorgung- verschlüsselte. Doch das Lösegeld wurde nicht gezahlt und durch das Einspielen eines Backups beschränkte sich der Datenverlust auf 24 Std. Der Effekt war der Aufbau einer sicheren IT-Infrastruktur und die Schulung der Mitarbeiter im Bereich IT-Sicherheit.[6]

2016

- Ransomware war im Frühjahr die häufigste Angriffsart auf die IT-Infrastruktur von Firmen. Laut BSI-Umfrage hatten 33% der befragten Unternehmen Ransomware-Infektionen zu verzeichnen und in 75% dieser Fälle war der Angriffsweg eine Mail mit Schadcode-Anhang. In 70% der Vorfälle waren nur einzelne Systeme betroffen, in 22% war jedoch relevante IT-Infrastruktur betroffen.
- Bekannte Ransomware-Familien sind:
- Locky, TeslaCrypt, Nemucod, CTB-Locker, Petya, WannaCry, NotPetya, matsun, nymaim und Cerber
- Exploit-Kits werden Open Source und kommerziell angeboten: Angler, Neutrino, Magnitude, …
- Das ehemalige dridex-Netzwerk, das einen Online-Banking Trojaner verteilt hatte, wurde zur Verteilung von Ransomware umgenutzt.[7]
- SamSam ist eine gezielte Ransomware-Kampagne. Der anfängliche Zugang wurde durch eine Schwachstelle im JBoss-Applikationsserver geschaffen, sodass die Zugangsdaten für angebundene Windows Systeme abgegriffen, Nutzerdaten verschlüsselt und Backup-Dateien gelöscht wurden. [7]

September 2016 – ANSSI-Empfehlungen gegen Ransomware

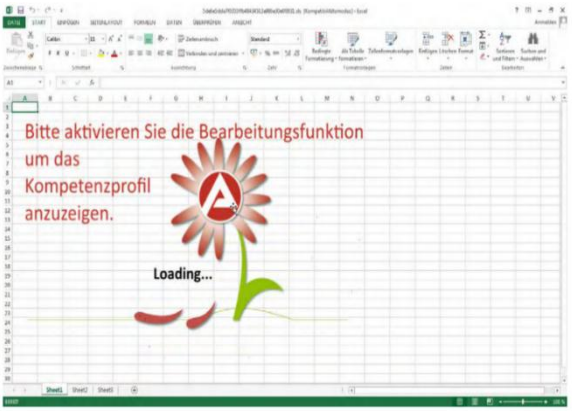
Um der Bedrohung zu begegnen veröffentlichte das ANSSI eine Darstellung der Best-Practice-Lösungen.



2017

Dezember 2016 – Bewerbungs-mailkampagne

Die Mails wurden gezielt an Personaler versendet und verlangten eine Makro-Ausführung bei einer Tabellen-kalkulationssoftware. Das VBSkript startete im Anschluss eine exe-Datei, verschlüsselte Daten und verhinderte den Neustart des Systems.[1]



- Blocker Ransomware für Mobilfunk-Geräte wird zunehmend beobachtet.
- Bekannte Ransomware-Familien sind: Locky, Cerber, CryptXXX, Crysis, WannaCry, NotPetya, matsun, nymaim und Petya/GoldenEye
- Jaff wurde durch das Necurs-Botnetz über Spam-Mails verteilt. Sie enthielten ein Word-Dokument mit Makro. Schon einen Monat später war jedoch ein Entschlüsselungstool verfügbar.
- NotPetya/ExPetr trat erstmals in der ukrainischen Finanzsoftware MEDoc auf. Die Webseite des Providers wurde kompromittiert und der automatische Update-Prozess führte zur Infektion. Die Schadsoftware suchte nach Zugangsdaten und nutzte die bekannte Microsoft Windows SMB-Schwachstelle für die lokale Ausbreitung. [8]
- Bad Rabbit war eine Drive-by-Ransomware-Massenattacke, die hauptsächlich Betroffene in Russland und der Ukraine hatte.[9]
- Verschiedene Angebote für Ransomware als Dienstleistung (Ransomware as a Service – RaaS) sind ab einem Preis von 35 US-Dollar verfügbar.[3]

Mai 2017 – WannaCry-Erklärung des ANSSI-Präsidenten

Einige Unternehmen sind in gewissem Maße betroffen, manche minimal, manche mit einem hohen Ausbreitungsgrad. Über die Betroffenheit der meisten Firmen, insbesondere kleinere mittelständische Unternehmen und Bürger, sind keine exakten Zahlen verfügbar.

Das Eingreifen eines britischen Forschers entschleunigte die Verbreitung, doch das Infektionsrisiko bestand weiterhin und manche Angreifergruppen wurden hierdurch ermutigt.

Mai/Juni 2017 – NotPetya und WannaCry

NotPetya traf die Systeme eines Konsumentengüterkonzerns durch einen manipulierten Patch und verbreitete sich intern. Die Schadsoftware verursachte einen 4,5 Tage währenden Produktionsstopp in 17 Fabriken und ein Herunterfahren des Kommunikationssystems. Nach offizieller Aussage sei der Schaden verhältnismäßig gering.[11]

Die WannaCry-Infektion des Systems eines Transportunternehmens wurde medienwirksam wahrgenommen. Die Anzeigetafeln wurden mit der roten Box für die Zahlungsaufforderung überlagert. Überwachungskameras und Automaten waren außer Betrieb, doch der Transportbetrieb war zu jedem Zeitpunkt sicher gestellt.[8]

3.5 Weitere Implikationen

Während die Medien sich stark auf den WannaCry-Vorfall konzentrierten, kam es kurze Zeit zuvor zu einem ähnlichen Angriff, der jenen in der Tat an Anzahl und Intensität des Schadens übertraf. Der Kryptominer Adylkuzz wurde in der gleichen Weise verteilt über den EternalBlue-Exploit und nutzte die SMB-Schwachstelle 445 aus. Anschließend installierte die Backdoor DoublePulsar, die ebenfalls im Zuge des „ShadowBroker-Leaks" veröffentlicht wurde, die Mining-Software. Adylkuzz schloss zusätzlich den SMB-Netzwerkverkehr, was möglicherweise die Verbreitung von WannaCry limitierte. Damit gab es eine belegbare Verbindung zwischen diesen Vorfällen, die allerdings einen Wettbewerb vermuten lässt.[12]

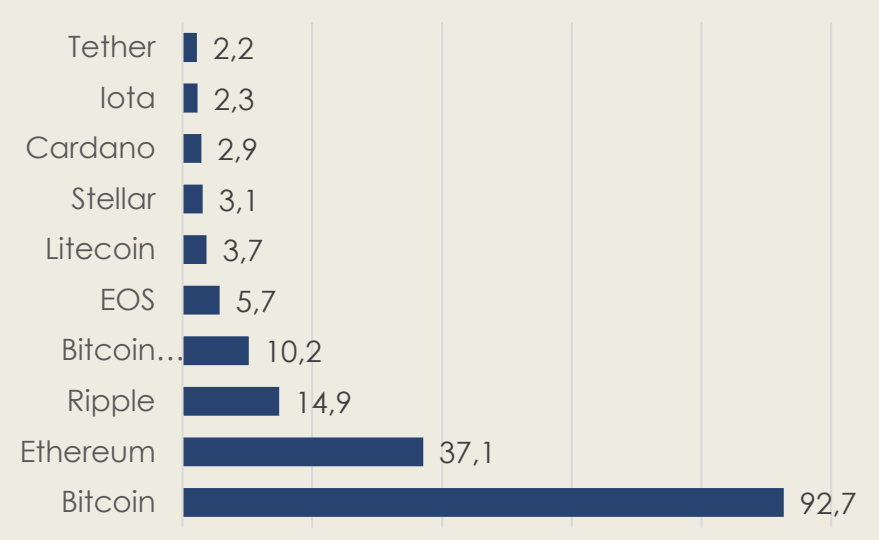
Ein weiteres Beispiel für die gleiche Nutzung von Distributionskanälen bei Cryptocurrency-Malware ist die aktuelle Kampagne RedisWannaMine vom März 2018. Schon der Name suggeriert einen inhaltlichen Zusammenhang mit WannaCry. RedisWannaMine nutzt den EternalBlue-Exploit, um die Windows SMB-Schwachstelle auszunutzen und lädt im Anschluss eine Mining-Software herunter.[13]

Der Quant Trojaner war ein ehemaliger Verteiler der Ransomware Locky und Schadsoftware der Pony-Familie, aber wurde auch als modifizierte Version beobachtet, um Kryptowährungswallets anzugreifen. Quant war kommerziell zu erwerben auf einem russischen Untergrundforum für einen Betrag von 275 US-Dollar. Die Schadsoftware scannt das Verzeichnis der Anwendungsdateien von bestimmten Währungen wie Bitcoin, Terracoin, Peercoin und Primecoin. Eine weitere Funktion ist das Stehlen von Zugangsdaten für Anwendungen und das Betriebssystem.[14]

Es existieren mehrere Berichte, die vermuten lassen, dass die Angreifer der Lazarus[15]-Gruppe und die Gruppe hinter der Ransomware VenusLocker[16] ihre Aktivitäten vom Angriffsfeld Ransomware auf Kriminalität im Bereich Kryptowährungen (Cryptocurrency Crime) verlagert haben und dass dies keine Einzelfälle sind.[17]

Dies könnte zur Schlussfolgerung führen, dass Ransomware als Bedrohung dem Feld des Cryptocurrency Crime weicht. Daher wird im folgenden Abschnitt der Hintergrund dieses Trendthemas erläutert.

4 Cryptocurrency Crime



Die zehn Kryptowährungen mit der höchsten Marktkapitalisierung[18]

Cryptocurrency Crime umfasst alle Aktionen mit der Intention, digitale Währungen zu erbeuten. Dies beinhaltet sowohl den Diebstahl digitaler Währungen als auch das illegale Kryptomining, auch als Cryptojacking bezeichnet, die Nutzung eines kompromittierten Systems zum „Schürfen“ von Kryptowährungen gegen eine Belohnung in Form der geschürften Währung. Bitcoin war die erste Kryptowährung, deren Konzept 2009 veröffentlicht wurde. Heute beläuft sich die Gesamtzahl der Kryptowährungen auf über 1800, aber nur wenige (ca. 30) sind als technologische und wirtschaftliche Projekte mit Langzeitperspektive einzuschätzen.

4.1 Blockchain und Kryptowährungen

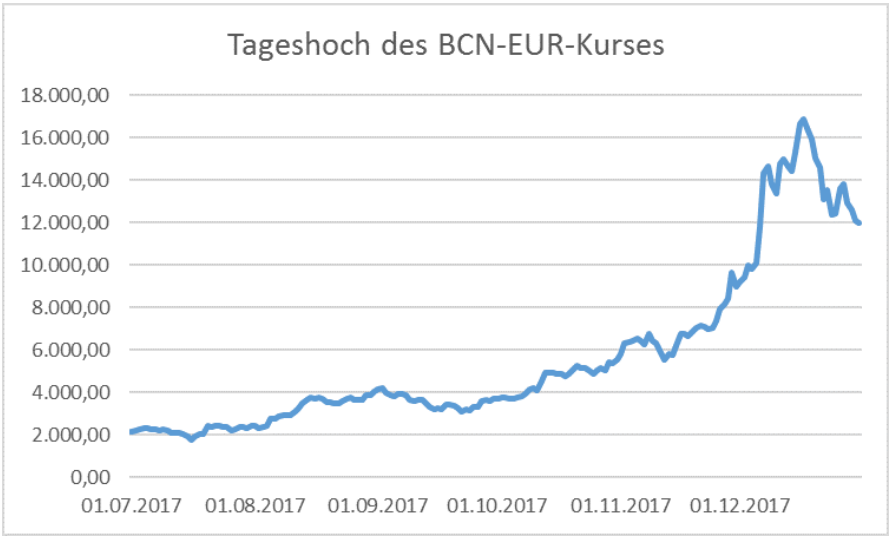
Eine Kryptowährung ist ein digitales Zahlungsmittel, das zur sicheren Übertragung von Transaktionen Techniken der Kryptografie nutzt, um die Erstellung neuer Einheiten zu kontrollieren und Zahlungstransfers zu verifizieren. Kryptowährungen basieren auf einer dezentralen Verwaltung, im Gegensatz zur zentralen Arbeitsweise beim herkömmlichen Online-Banking. Das dezentrale System wird als Blockchain bezeichnet, welches alle Informationen dezentral bereit stellt, diese regelmäßig prüft und in Blöcken verkettet zusammen stellt. Die Blockchain ist eine Form der Distributed Ledger Technology (DLT), bei der in der Regel ihre Nutzer nicht durch die Rechtevergabe von Lese-, Schreib- und Speicherberechtigung unterschieden wird. Jeder Eintrag der Datenbank muss einen Validierungsprozess durchlaufen und wird anschließend zu jeder Kopie eines jeden Netzwerkteilnehmers hinzugefügt. [19]

4.2 Erstellungsprozess von Kryptowährungen

Bei den meisten Kryptowährungen sieht der Prozess der Blockchain vor, dass jeder neue Block durch die Ausführung komplexer Rechenoperationen validiert werden muss. Diese Operationen erfordern (dezentrale) Rechenleistungen, die von Netzwerkteilnehmern erbracht werden. Um die Nutzer zur Aufwendung ihrer Ressourcen zu motivieren, bietet der Blockchain-Algorithmus den Teilnehmern eine Aufwandskompensation in Form der neu erstellten Währungseinheit.

4.3 Börsenkurs von Kryptowährungen und kriminelle Energie

Cryptocurrency crime war ein aufkommendes Thema im Jahr 2017 in Folge des starken Anstiegs in den Börsenkursen des hoch volatilen Bitcoins, der zur Zeit die höchste Marktkapitalisierung besitzt. Von Januar 2017 bis Januar 2018, stieg der Kurs von 900 auf 13.000 EUR (+1440%). Andere Kryptowährungen verzeichneten ähnliche Entwicklungen. (Monero: +2300%; Ethereum: +1980%; Ripple: +738%).



Entwicklung des Bitcoin-Euro-Kurses vom 01.07.-31.12.2017 [18]

4.4 Was ist Cryptojacking, die neue Cyber-Bedrohung?

Cryptocurrency Crime ist ein neuer Trend im Bedrohungsfeld „Cyber-Kriminalität". Kriminelle lenken ihre Aufmerksamkeit auf diesen Bereich aus zwei Gründen: Die steigenden Kurse und die (relative) Anonymität des Geldtransfers.

Seit Cryptomining ein spezielles Equipment mit hoher Rechenleistung und hohen Energiekosten erfordert, versuchen Angreifer dafür Ressourcen Dritter zu missbrauchen. Dabei werden unterschiedliche Vorgehensweisen verwendet:

- Botnet-Cryptojacking: Die Erstellung oder Nutzung eines (bestehenden) Botnetzes zum Minen einer Kryptowährung unter Nutzung der Rechenleistung der einzelnen

"Zombie"-Maschinen

Bsp.: PyCryptoMiner-Botnetz, identifiziert durch das F5 Network Labs. Das Botnetz nutzt die Schwachstelle CVE-2017-12149 und das SSH Protokoll zur Verbreitung

- Web-Cryptojacking: Technik, die legitime und viel besuchte Webseiten kompromittiert. Der Angreifer fügt eine JavaScrpit-Datei hinzu, sodass der Browser des Webseiten-Besuchers im Hintergrund schürft.

Bsp.: Im Januar 2017 wurde die Blackberry-Webseite für mobile Endgeräte mit einem CoinHive-Skript infiziert, sodass die Besucher der Webseite die Kryptowährung Monero (XMR) schürften.

- Direktes Cryptojacking: Der Angreifer fasst ein spezifisches Opfer ins Auge, das im Hinblick auf hohe Rechenleistung der Hardware ausgewählt wird, meist Unternehmen und Forschungseinrichtungen. Ist der Server mittels eines Exploit zugänglich gemacht worden, installiert der Angreifer die Mining-Software.

Bsp.: Nach Aussage des SANS Institute wurden Oracle Server der Firmen DIGITAL OCEAN, GODADDY, VERIZON BUSINESS SERVICE und ATHENIX durch diese Methode angegriffen. Global ist durch diese Angriffe ein Schaden von 190.000 EUR verursacht worden.

- Mobiles Cryptojacking: Verbreitung maliziöser Apps: Auch wenn die Rechenleistung mobiler Endgeräte deutlich geringer ist, wird vereinzelt die Nutzung mobiler Geräte beobachtet.

4.5 Entwicklung von Cryptomining-Vorfällen

Cryptojacking ist für sich genommen kein neues Phänomen. Zahlreiche Vorfälle sind seit dem Jahr 2011 beobachtet worden. Die Lage der IT-Sicherheit in Deutschland erwähnte das Mining jedoch erstmals im Jahr 2016, da zu diesem Zeitpunkt 15% der Botnetz-Infrastruktur illegales Cryptomining betrieben.[7] Doch im Jahr 2017 nahm Anzahl und Intensität der Vorfälle sprunghaft zu.

2017:

- Mehrere Arten von Mining-Malware nutzen bekannte Schwachstellen des Windows Betriebssystems, um ungepatchte Systeme zu infizieren. Unter anderem nutzte die Mining-Malware Zealot den EternalBlue-Exploit, was nicht den einzigen Fall darstellt, bei dem ehemalige Vorgehensweisen zur Verteilung von Ransomware adaptiert wurden. Das Kaspersky Lab detektierte eine Mining-Malware, die Kryptowährungen in einem Gegenwert von 5,5 Mio. EUR innerhalb von 6 Monaten generierte.[20]
- Der Trojaner Loapi infizierte mehr als 1 Mio. Smartphones. Die Schadsoftware verbreitete sich als Download über nicht offizielle App-Stores und über Werbung für Pornos und Antivirus-Software. Loapi ist der erste Kryptotrojaner, der einen physikalischen Schaden des infizierten Systems verursachte und ist ein Beispiel für die Ausweitung der Bedrohung des Cryptominings auf mobile Endgeräte.[21]
- Im Dezember wurde ein neuer Angriffsweg über soziale Netzwerke beobachtet. Die Schadsoftware Digmine befiel die Windows Registrierungsdatenbank der Clients und fügte dem Chrome-Browser eine Erweiterung hinzu. Ziel war das Ausspähen von Zugangsdaten beim automatischen facebook-Login, um die Malware anschließend an die facebook-Freunde der Opfer zu versenden.[22]

2018:

- Angreifer kompromittieren einen ungepatchten Oracle Server, um Monero in einem Wert von 190.000 EUR zu erbeuten.[23]
- RubyMiner infiltriert Web Server, welche bekannte Schwachstellen aufweisen, um auf diesen Monero zu minen. Diese Angriffskampagne erlaubte es den Akteuren auf insgesamt 700 Server in den Vereinigten Staaten, Deutschland, Großbritannien, Norwegen und Schweden zu arbeiten.[24]
- Der Monero-Miner JenkinsMiner nutzte eine Schwachstelle des Jenkins Servers und schüfte Moneros in einem Gegenwert von 2,5 Mio. EUR.[25]

4.6 Entwicklung von Kryptowährungsdiebstahl-Vorfällen

Hervorgehoben werden die drei herausragendsten Vorfälle aus 2017.

- In der Zeit vom 18.-20.07.2017 wurden Kryptowährungen in einer Höhe von 85 Mio. EUR gestohlen. Die Angreifer zielten auf konventionelle Banken und Handelsbörsen für Kryptowährungen ab. Dabei können zwei Strategien unterschieden werden: Austauschen von legitimen Wallet-Adressen, die online publiziert wurden, und das Ausnutzen von Schwachstellen bei Wallet-Anbietern zur Abschöpfung der Gesamtguthaben.[26]
- Am 07.12.2017 wurde eine Schwachstelle der Wallet-Software Nicehash ausgenutzt, um Kryptowährungen in einem Gegenwert von 50 Mio. EUR zu erbeuten. [27] Am 19.11.2017 geschah dies auch bei der Handelsplattform Tether. Der Schaden belief sich auf 25 Mio. EUR.[28]
- Nach Wochen der Inaktivität begann das Satori-Botnetz einen Code zu verteilen, der dem Diebstahl von Ethereum diente. Dieser löste den Claymore-Mining-Code ab, der öffentliche Adressen legitimer Miner veränderte, um die Kompensationszahlungen umzuleiten.[29]

4.7 Folgerungen

Die Bedrohung durch Cryptomining hat im zweiten Halbjahr des Jahres 2017 stark zugenommen. Ein Grund für diese Erhöhung ist die finanzielle Attraktivität, Kryptowährungen zu erwerben. Darüber hinaus garantiert ein installierter Miner ein regelmäßiges, wenn auch geringeres Einkommen und die Infektion wird in wenigen Fällen bemerkt, insbesondere wenn die CPU-Auslastung nicht die volle Kapazität ausnutzt. Die Vorfälle im Bereich des illegalen Cryptominings konzentrieren sich auf das Monero-Mining, das weniger rechenaufwendig als das Bitcoin-Mining ist und eine höhere Anonymität der Netzwerkteilnehmer bei der Nachverfolgung der Zahlungsströme garantiert. Monero-Mining wurde bei mobilen Endgeräten beobachtet und erstmals über die sozialen Netzwerke verbreitet. Insgesamt konnte eine Bedrohungserweiterung von der Verteilung von Ransomware hin zu illegalen Aktivitäten im Zusammenhang mit Kryptowährungen beobachtet werden.

Bzgl. des Diebstahls von Kryptowährungen sind hauptsächlich Bitcoin und Ethereum von Interesse, da sie am weitesten verbreitet sind. Die Vorgehensweisen sind die Kompromittierung von Webseiten, die Ausnutzung von Wallet-Schwachstellen, und das Ausspähen von Wallet-Credentials.

Quellen:

[1] „Cybercrime | Bundeslagebild 2016“ – Bundeskriminalamt; Wiesbaden 2016
[2] „Lagedossier Ransomware“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2016
[3] https://threatpost.com/crooks-switch-from-ransomware-to-cryptocurrency-mining/129229/; Stand: 23.03.2018
[4] “How to stay proteccted against ransomware” – Sophos Ltd.; February 2018
[5] „Die Lage der IT-Sicherheit in Deutschland 2015“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2015
[6] https://www.heise.de/newsticker/meldung/Trojaner-im-OP-wie-ein-Krankenhaus-mit-den-Folgen-lebt-3617880.html; Stand: 28.03.2018
[7] „Die Lage der IT-Sicherheit in Deutschland 2016“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2016
[8] „Die Lage der IT-Sicherheit in Deutschland 2017“ – Bundesamt für Sicherheit in der Informationstechnik; Bonn 2017
[9] https://securelist.com/bad-rabbit-ransomware/82851/; Stand: 23.03.2018
[10] https://www.cnbc.com/2017/05/17/wannacry-cyberattack-worldwide-sophos.html; Stand: 22.03.2017
[11] […]; Stand: 28.03.2018
[12] https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar; Stand: 23.03.2018
[13] http://securityaffairs.co/wordpress/70117/malware/cryptocurrency-mining-operations.html; Stand: 23.03.2018
[14] http://www.zdnet.com/article/quant-trojan-upgrade-targets-cryptocurrency-user-wallets/#ftag=RSSbaffb68; Stand: 23.03.2018
[15] https://www.zdnet.de/88321291/lazarus-gruppe-angeblich-fuer-bitcoin-stehlenden-trojaner-verantwortlich/?utm_source=rss&utm_medium=rss&utm_campaign=rss; Stand: 23.03.2018
[16] https://threatpost.com/crooks-switch-from-ransomware-to-cryptocurrency-mining/129229/; Stand: 23.03.2018
[17] https://securelist.com/mining-is-the-new-black/84232/; Stand: 23.03.2018
[18] Source of data: SIX Financial Information via https://www.finanzen.net Stand: 10.07.2018
[19] „Distributed-Ledger-Technologien im Zahlungsverkehr und in der Wertpapierabwicklung: Potenziale und Risiken“ - Deutsche Bundesbank, Monatsbericht September 2017, S. 36-38
[20] https://securelist.com/mining-is-the-new-black/84232/ ; Stand: 08.03.2018
[21] https://www.bleepingcomputer.com/news/security/android-malware-will-destroy-your-phone-no-ifs-and-buts-about-it/ ; Stand: 07.03.2018
[22] http://www.silicon.co.uk/workspace/malware-spreads-cryptocurrency-miner-facebook-messenger-226463 ; Stand: 16.03.2018
[23] https://www.heise.de/security/meldung/Angreifer-attackieren-ungepatchte-Server-Apps-von-Oracle-3938626.html; Stand: 10/04/2018
[24] https://research.checkpoint.com/rubyminer-cryptominer-affects-30-ww-networks/; Stand: 10/04/2018
[25] http://newsroom.trendmicro.com/blog/security-intelligence/cryptocurrency-mining-malware-2018s-new-menace; Stand: 08.03.2018
[26] https://www.darkreading.com/vulnerabilities---threats/uptick-in-malware-targets-the-banking-community/a/d-id/1329541 ; Stand: 08.03.2018

[27]https://www.theregister.co.uk/2017/12/06/nicehash_diced_up_by_hackers_thousands_of_bitcoin_pilfered/ ; Stand: 08.03.2018
[28] https://thehackernews.com/2017/11/tether-bitcoin-hacked.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Security+Blog%29 ; Stand: 08.03.2018
[29] https://www.helpnetsecurity.com/2018/01/17/satori-eth-mining-malware/; Stand: 10/04/2018