SWITCH-CERT Report zu aktuellen Trends im Bereich IT-Security und Privacy

September / Oktober 2018

SWITCH

I. Turning Good statt Breaking Bad? Wenn Hacker hacken, um Hacker zu vertreiben

Dass Kryptominer in fremde Rechner eindringen, um digitale Währungen zu schürfen, ist nicht neu. Nun aber haben chinesische Sicherheitsforscher von netlab360 Fbot entdeckt. FBot dringt – bei aller vermeintlich guten Absicht dennoch illegalerweise – in Rechner ein, die vom Kryptominer com.ufo.miner befallen sind, und macht diesen unschädlich. Ist das Werk vollbracht, löscht sich FBot selbst. Wer hinter FBot steckt und mit welchen Motiven FBot aktiviert wurde, ist völlig unklar. Bekannt ist einzig, dass der «gute» Trojaner nicht über klassische DNS-Server mit seinen Hintermännern kommuniziert, sondern dazu das Blockchain-basierte DNS-Protokoll EmerDNS nutzt, das vom Blockchain-Diensteanbieter Emercoin eingesetzt wird.

Weit mehr Details weiss man heute über Mirai – jenes Botnet im Internet of Things, das mittels DDoS-Angriffen und Gegenangriffen im Oktober 2016 das Internet der gesamten Ostküste der USA lahmgelegt und dann weltweit für Internetausfälle, Panik und hohe Schäden gesorgt hatte. Mirai sollte nach dem Willen seiner drei seinerzeit 18- bis 20-jährigen Schöpfer nämlich Hoster des Videospiels Minecraft ausschalten oder Lösegeld von ihnen erpressen. Quasi nebenbei betrieben die drei damit auch ein offenbar gut laufendes Ad-Fraud-Business, also Klickbetrug an Werbetreibenden. Als die Malware-Schreiber aber erkannten, welche Zerstörungswelle Mirai anrichtete, gerieten sie in Panik und veröffentlichten den Code, um einer drohenden Verfolgung zu entgehen. Den wiederum nutzten andere Hacker zu neuen Angriffen, die dann die

verheerenden Internetausfälle zur Folge hatten. Auch aktuell ist der Mirai-Code Basis für Botnetze, wie z.B. Satori oder Reaper. Und brandaktuell treibt eine verfeinerte Mirai-Version ihr Unwesen auf Android- und Linux-Systemen.
Die Mirai-Schöpfer, die der Strafverfolgung dann doch nicht entkommen waren, wurden indes vor kurzem von einem Gericht in Alaska verurteilt. Den angedrohten langen Haftstrafen entgingen sie mit einem neuartigen Deal mit den Strafverfolgungsbehörden. Alle drei kamen mit Bewährungsstrafen davon, die unter der Auflage erlassen wurden, dass sie während 5 Jahren und 2.500 Arbeitsstunden FBI und Security-Forscher mit ihrem offenbar sehr profunden Fähigkeiten im Kampf gegen Cyberkriminelle unterstützen.

Nachzulesen unter:

https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en
https://www.heise.de/security/meldung/FBot-Botnetz-entfernt-Krypto-Miner-Infektionen-4168434.html
https://sensorstechforum.com/fbot-bot-cleans-systems-infected-com-ufo-miner
https://www.zdnet.com/article/bizarre-botnet-infects-your-pc-to-scrub-away-malware
https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing
https://www.heise.de/security/meldung/Mirai-Die-Entwickler-des-IoT-Botnetzes-arbeiten-jetzt-fuer-das-FBI-4169926.html
https://arstechnica.com/tech-policy/2018/09/mirai-botnet-creators-praised-for-helping-fbi-wont-serve-prison-time
...und zum Schmunzeln:
http://littlefun.org/uploads/52420a24e691b26fb67d9285_736.jpg

II. Was haben ein Feuerwehrmann und Googles Chrome 69 gemeinsam?

In einem Kabarettstück hat Emil Steinbergers Feuerwehrmann etwas zu feiern: einen Lottogewinn. Den nutzt er nach langem Hin und Her als Anzahlung für eine Eigentumswohnung, deren Preis seine Vermögenverhältnisse trotz des Gewinns deutlich übersteigt. Deshalb verschweigt er den Kauf gegenüber seiner Frau und kommentiert dies mit den Worten: «Man muss ja nicht alles gleich am ersten Tag erzählen!» Auch Google hatte Grund zum Feiern: Chrome, der Browser des Suchmaschinengiganten, wurde 10 Jahre alt. Zum Geburtstag gab´s eine neue Version – Chrome 69. Aber auch dieses freudige Ereignis hatte dunkle Seiten: denn zum einen musste Goggle die als Innovation angekündigte neue – unvollständige – URL-Anzeige nach Protesten vieler User wieder zurücknehmen. Und zum anderen hatten sich die Chrome 69-Entwickler offenbar Emils Feuerwehrmann-Kommentar zu Herzen genommen, nicht alles gleich am ersten Tag erzählen zu wollen. Denn in der offiziellen Ankündigung des neuen Browsers verloren sie kein Wort darüber, dass User mit einem aktiven Google-Konto automatisch in Chrome eingeloggt werden, auch wenn sie Browser und Google-Account nie verknüpft haben. Blogger und Datenschützer

vermuteten daraufhin eine automatisierte Synchronisation von Userdaten – wie beim manuellen Login üblich - und zeigten sich alarmiert. Beim neuen erzwungenen Login findet diese Synchronisation aber offenbar nicht statt, auch wenn dies in einigen Veröffentlichungen zum Thema so dargestellt ist.
Deshalb gibt man sich bei Google verwundert über Ausmass und Heftigkeit der Vorwürfe, die vom schweren Vertrauensbruch bis zur Verletzung des Datenschutzes reichen, weil Googles Datenschutzerklärung den «Zwangs-Login» nicht abdecke.

Nachzulesen unter:

https://www.cnbc.com/2018/09/24/google-chrome-69-automatic-login.html
https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome
https://www.googlewatchblog.de/2018/09/kritik-google-chrome-neuerung
https://gadgets.ndtv.com/apps/features/google-chrome-69-sign-in-controversy-explained-1921359
https://techcrunch.com/2018/09/24/security-experts-say-chrome-69s-forced-login-feature-violates-user-privacy
https://gizmodo.com/google-chrome-is-now-quietly-forcing-you-to-log-in-here-1829265681

III. 15 Monate später: Neue Angriffe über alte Schwachstelle

WannaCry? Eternal Blue? Da war doch was ... richtig: Im Mai 2017 verbreitete sich der Erpressungstrojaner WannaCry in rasender Geschwindigkeit über den Windows-Globus und legte hunderttausende ungepatchte Systeme lahm – seinerzeit der grösste Cyberangriff der Geschichte. Als Einfallstor nutzte die Malware eine Schwachstelle namens Eternal Blue (wir berichteten im Security Report 05/06 2017). Nach nunmehr 15 Monaten sollte man eigentlich glauben dürfen, dass alle Patches installiert und die Schwachstelle geschlossen ist. Eigentlich. Denn nach wie vor wird Eternal Blue dazu genutzt, Windows-Systeme anzugreifen und z.B. Kryptotrojaner auf Rechner einzuschleusen. Der Virenscanner-Anbieter Avira warnt in einem Blogpost davor, dass Virenscanner die Malware zwar finden und unschädlich machen können, kurze Zeit später aber eine Neuinfektion via dem SMB-Protokoll, Version 1.0 stattfindet. Problematisch ist dies deshalb, weil Microsoft die von der NSA in die virtuelle Welt gebrachte Schwachstelle zwar geschlossen hat, viele Installationen aber eben nicht mit Sicherheitsupdates von Microsoft versorgt und gesichert. Die Sicherheitsforscher von Avira empfehlen einmal mehr, das veraltete Protokoll SMB-1.0 auf den ungepatchen Windows-Systemen abzuschalten.

Nachzulesen unter:

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2017-3_de.pdf
https://blog.avira.com/nsa-eternalblue-exploits-live-on-with-an-endless-infection-loop

https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry
https://searchsecurity.techtarget.com/news/252448889/WannaMine-cryptojacker-targets-unpatched-EternalBlue-flaw

IV. Peekaboo macht Überwachungskameras im grossen Stil angreifbar

Das Vorgehen ist bekannt aus Film und Fernsehen: Wollen Gute oder Böse dabei unentdeckt bleiben, wie sie in Räume vordringen, die von Überwachungskameras gesichert werden, verschaffen sie sich unerlaubten Zugang zu den Kameras, spionieren mit deren Hilfe ihr Angriffsziel oder ihre Opfer aus, löschen Aufzeichnungen oder tauschen den Live-Feed aus. Letzteres, um den Überwachern Bilder der Normalität vorzugaukeln, obwohl gerade der Banksafe ausgenommen, das millionenteuer versicherte Exponat gestohlen, das Personal entführt oder gar eliminiert wird. Die Realität sieht leider nicht besser aus: Mitte September fanden Forscher der Cybersecurityfirma Tenable eine Zero-Day-Schwachstelle, die sie «Peekaboo» tauften. Zu finden ist sie in Videomanagement-Lösungen der Firma NUUO. NUUO-Systeme finden sich in ca. 2.500 webbasierten Kameramodellen von mehr als 100 Herstellern. Und das führt im schlimmsten Szenario zur Konsequenz, dass nicht nur die Kamera und deren Aufnahmen übernommen werden können, sondern Cyberkriminelle die Kamera auch als Einfallstor ins Netzwerk dessen nutzen können, der mit dem Einsatz der Kameras eigentlich ein Plus an Sicherheit intendiert hatte.
Mit einem grossflächigen Zugriff auf Überwachungskameras macht dieser Tage auch die neue österreichische Bundesregierung von sich reden. Denn diese möchte alle Bilder von Überwachungskameras aller öffentlichen Stellen – vom Krankenhaus bis zum öffentlichen Linienbus – nutzen und hat daher alle relevanten Betreiber aufgefordert, entsprechende Schnittstellen bereitzustellen und den Landespolizeistellen mitzuteilen, wie der Zugriff darüber erfolgen kann.

Nachzulesen unter:

https://www.zdnet.com/article/hackers-can-tamper-with-surveillance-camera-footage-due-to-new-zero-day-vulnerability
https://www.darkreading.com/iot/internet-connected-cctv-cameras-vulnerable-to-peekaboo-hack/d/d-id/1332841
https://derstandard.at/2000087605164/Innenministerium-verlangt-Zugriff-auf-Bilder-oeffentlicher-Kameras

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Frank Herberg verfasst.