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

Januar/Februar 2019

I. Unternehmensnetzwerke in akuter Gefahr: Aktuelle Malspam-Wellen schicken den Multifunktionstrojaner Emotet insbesondere auf Windows-Geräte

Die Melde- und Analysestelle Informationssicherung des Bundes MELANI und das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI warnen vor einer ganzen Angriffswelle auf Unternehmensnetzwerke, die Windowsgeräte mit dem Multifunktionstrojaner Emotet infiziert. Der Abkömmling der Viren-Familie Bugat ist als Weiterentwicklung von Geodo auch unter dem Namen Heodo bekannt und gefürchtet. Ursprünglich als E-Banking-Trojaner konzipiert, wurde der Schädling inzwischen zum Multifunktionswerkzeug weiterentwickelt. Emotet kapert Rechner, um weitere Malspam zu versenden, vor allem aber um das Nachladen bösartiger Software zu ermöglichen.

Der Angriff erfolgt dabei in drei Wellen: Zunächst schicken die Cyberkriminellen Emotet in infizierten Word-Dokumenten als Anhang an Malspam – z.B. in gefakten Telefonrechnungen, Amazon-Mails und ähnlichen. Hat sich Emotet eingenistet, kundschaftet er das Netzwerk aus und lädt TrickBot nach. TrickBot fischt u.a. Zugangsdaten zu Konten ab, anhand welcher die Hacker abschätzen, welches Lösegeld

für ihre Opfer gerade noch zahlbar ist. Ist dies geklärt, lädt TrickBot «Ryuk» nach – einen Erpressungstrojaner der sich dank seiner integrierten Wurm-Komponente durch das komplette Netzwerk frisst und alle Daten verschlüsselt. Für die Freigabe wurden von den Cyberkriminellen inzwischen Lösegelder von 200.000.- Fr. und mehr verlangt.

Auch wenn einhundertprozentiger Schutz beim Thema Cybercrime kaum machbar ist, kann man doch mit gesteigerter Awareness Emotet und andere Malware deutlich zurückdrängen. Deshalb empfiehlt SWITCH-CERT die folgenden Massnahmen:

- Backup erstellen / Offline-Sicherheitskopie auf externe Medien speichern
- Betriebssysteme, Office- und Adobe-Applikationen auf neustem Stand halten
- Netzwerk segmentieren
- «Least Privileges» auch bei Netzwerklaufwerken einhalten
- Ausführen von unsignierten Office-Makros technisch unterbinden
- Empfang von Emails mit Office-Dokumenten, die Makros enthalten, unterbinden

Nachzulesen unter:

https://www.heise.de/security/meldung/Aktuelle-Trojaner-Welle-Emotet-lauert-in-gefaelschten-Rechnungsmails-4291268.html
https://www.melani.admin.ch/melani/de/home/dokumentation/newsletter/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html
https://www.bankinfosecurity.com/bugat-new-malware-choice-a-3011
https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware
https://www.computerbild.de/artikel/cb-News-Internet-Emotet-Trojaner-E-Mail-Programm-Warnung-22728537.html

II. Phishing, Porno, Datenklau: Rogue Apps als neue, gefährliche Art von Ladenhütern im Google Play und anderen App Stores

Als Ladenhüter werden Artikel bezeichnet, die deshalb ewig im Laden stehen, weil sie niemand kauft. Wenn Artikel gekauft und dann als gefährlich, ja schädlich erkannt werden, aber dennoch nicht aus den App Stores von Google und anderen verschwinden, dann handelt es sich um Ladenhüter der gefährlichen Art: sogenannte Rogue Apps. Nicht erst seit der 2016 erschienenen Star Wars Story «Rogue One» weiss man, dass «rogue» für bösartig, feindselig oder abartig steht. Rogue Apps sind genau das.

Im Kampf gegen unbedarfte Mobile-User setzen Cyberkriminelle zunehmend auf Apps bekannter Marken, die sie mit Malware infizieren und schleusen sie in die App Stores der grossen Mobile-System-Anbieter, obwohl diese nach eigenen Aussagen mit strengen Kontrollen eben dies verhindern wollen. Dieses Sicherheitsversprechen untermauern Android oder IOS auch damit, dass sie im Default-, also im werkseitigen Voreinstellungsmodus, Apps nicht öffnen, wenn diese nicht von autorisierten Entwicklern stammen.

Dass auf diese Versprechen aber offenbar kein Verlass ist, demonstrierten jüngst Sicherheitsforscher von Trend Micro, die bei einer Stichprobe alleine in Googles Play Store 29 FotoApps mit maliziösem Inhalt fanden.

User, die die Apps im guten Glauben an die Kontrolle durch Google herunterladen, werden von Pop Ups genervt, mit denen entweder Geld gemacht wird oder Daten abgezogen werden. Wie so oft werden z.B. erotische Inhalte beworben, deren Nutzung dann allerdings kostenpflichtig wird. Andere Pop Ups werden für Phishing-Attacken eingesetzt – so sollen einige der FotoApps Portraits von Usern an die Cyberkriminellen schicken, mit deren Hilfe jene dann z.B. gefakte Social-Media-Profile erstellen. Dass gefakte Banking-Apps dazu dienen, Konten zu hacken, muss nicht gesondert erwähnt werden, ist aber deshalb besonders brisant, weil sich sowohl Google als auch die betroffenen Markeninhaber in der Regel erstaunlich viel Zeit lassen, die infizierten Apps aus dem Laden zu nehmen, bzw. unschädlich zu machen.

Das können App-Herausgeber für sicherere Apps tun:

- Installieren Sie ein dauerhaftes Monitoring Ihres Firmennamens resp. Ihrer App-Namen in den jeweiligen Stores.
- Entwickeln Sie Fähigkeiten, um Apps zu analysieren.
- Veranlassen Sie das sofortige Entfernen von Rogue Apps aus den Stores.
- Schliessen Sie die Kommunikations-Endpunkte einer Rogue App.

Insbesondere Banking-App-Nutzern rät die Polizei des deutschen Bundeslands Schleswig-Holstein zu folgenden präventiven Massnahmen:

1) Laden Sie die offizielle App Ihrer Bank herunter und stellen Sie sicher, dass Sie immer die echte Webseite der Bank besuchen.
2) Verhindern Sie automatisches Anmelden bei der Online-Banking-Seite oder -App.
3) Teilen Sie weder Bankkartennummer noch Passwort und zeigen Sie sie niemandem.
4) Falls verfügbar installieren Sie eine Mobile-Security-App, die Sie bei verdächtigen Aktivitäten warnt.
5) Informieren Sie Ihre Bank, wenn Sie Ihr Smartphone verlieren oder Ihre Nummer ändern, damit Ihre Daten aktualisiert werden können.
6) Teilen Sie keine Kontoinformationen über Textnachrichten oder E-Mail.
7) Nutzen Sie immer ein sicheres WLAN-Netzwerk für den Zugang zur mobilen Seite oder App Ihrer Bank. Nutzen Sie dazu niemals ein öffentliches WLAN!
8) Kontrollieren Sie Ihre Kontounterlagen regelmässig.

Zu 1) und 4): Als Vorsichtsmassnahme bei der Installation wird insbesondere empfohlen, die Bewertungen anderer App-User zu prüfen. Handelt es sich um eine Rogue App, ist dies meist deutlich vermerkt.

Zu 6) Und schon gar nicht über Social Media.

Nachzulesen unter:

https://www.heise.de/security/meldung/Google-Play-Millionenfach-verbreitete-Kamera-Apps-klauen-Fotos-4295992.html
https://securityblog.switch.ch/2019/01/30/rogue-mobile-app/
https://www.schleswig-holstein.de/DE/Landesregierung/POLIZEI/Praevention/Cybercrime/Mobile_Malware/_downloads/01_Mobile_Banking_Malware.pdf?__blob=publicationFile&v=1

III. Spy Time auch bei Apple – Gravierende Sicherheitslücken erlauben das Mithören fremder Face Time-Kommunikation und das Auslesen der Passwörter in Apples Key Chain

Für die Jagd nach Programmfehlern und Sicherheitslücken – im Fachjargon: Bug Bounty – stellen ITC-Firmen von Apple bis Swisscom nach klaren Regeln regstrierten Sicherheitsexperten Geld- oder Sachprämien in Aussicht, die solche Fehler und Lücken entdecken. Der 14-jährige Grant Thompson, der eine scheunentorgrosse Sicherheitslücke in Apples GroupFaceTime entdeckte und an Apple meldete, ging zunächst leer aus, weil er kein bei Apple registrierter Sicherheitsforscher war. Inzwischen hat Apple erklärt, den Lausch-Bug-Entdecker angemessen zu belohnen. Dies allerdings erst, nachdem über Social Media verbreitet worden war, dass es der Fehler möglich machte, via FaceTime das Mikrofon von iPhones, iPads und Macs ohne Einverständnis des Users zu aktivieren, um aus der Ferne Gespräche oder Raumgeräusche mitzuhören oder aufzuzeichnen (die Lücke wurde inzwischen mit der IOS-Version 12.1.4 geschlossen).

BugBounty-Programme sind zwar nicht unumstritten, weil sie dazu animieren, amerikanische und europäische Gesetze zu verletzen. So verbietet z.B. in Deutschland der § 202c des Strafgesetzbuchs bereits die Vorbereitung zum Ausspähen und Abfangen von Daten. In den USA stellen der Computer Fraud and Abuse Act und der Digital Milennium Copyright Act DMCA die Überwindung des Kopierschutzes ohne Zustimmung des Rechteinhabers unter Strafe. Dennoch zahlt Apple registrierten Fehlersuchern bis zu 200.000.- USD für die Meldung relevanter Sicherheitslücken. Angesichts dessen, dass Schwachstellenhändler für kritische IOS-Bugs Millionen bezahlen, nimmt sich die Summe allerdings bescheiden aus. Viele professionelle Sicherheitsforscher zeigen sich daher oft wenig motiviert, solche Lücken an Apple zu melden.

Auch der deutsche Sicherheitsforscher Linus Henze entschied sich aus diesem Grund dagegen, eine wirklich gravierende Sicherheitslücke in der Passwortverwaltung von MacOS (für das im Gegensatz zu IOS seitens Apple keinerlei Bug-Bounty-Programm existiert) zu melden. Aus dem im Mac-Betriebssystem integrierten Schlüsselbund kann manipulierte Software sämtliche Zugangsdaten des Nutzers einschliesslich aller Passwörter im Klartext (!) aus der lokalen Keychain auslesen. Gemäss Henzes Angaben ist der Zugriff durch unsignierte Apps möglich. Ist der lokale User an seinem Mac angemeldet, werden weder

Admin- noch Root-Rechte gebraucht. Das üblicherweise benötigte Passwort wird umgangen. Die MacOS-Schwachstelle betrifft alle Betriebssysteme bis hin zur aktuellen Version 10.14.3 (Mojave). Ob sie inzwischen geschlossen ist, ist aktuell nicht bekannt.

Dagegen stehen mit dem Update auf IOS 12.1.4 Patches für zwei Zero Day Exploits bereit, vor denen Googles Sicherheitsteam in der ersten Februarwoche gewarnt hatte. Die Schwachstellen waren von Hackern angegriffen worden, wobei derzeit noch unklar ist, ob die Angriffe erfolgten, um Cyberverbrechen zu lancieren oder Cyberspionage zu betreiben.

Nachzulesen unter:

https://www.theguardian.com/technology/2019/jan/29/facetime-security-bug-apple-privacy-iphone https://www.heise.de/mac-and-i/meldung/Schwere-FaceTime-Luecke-Apple-will-wohl-Bug-Bounty-zahlen-als-Ausnahme-4297658.html
https://www.zdnet.com/article/ios-12-1-4-fixes-iphone-facetime-spying-bug
https://www.bluewin.ch/de/digital/apples-juengster-schritt-ist-nur-ein-kleiner-hin-zu-mehr-nutzersicherheit-210263.html
https://www.heise.de/mac-and-i/meldung/Sicherheitsforscher-Kritische-Luecke-in-macOS-erlaubt-Auslesen-von-Passwoertern-4297437.html
https://www.zdnet.com/article/google-warns-about-two-ios-zero-days-exploited-in-the-wild
https://www.bankinfosecurity.com/apple-update-drop-everything-patch-ios-a-12013

IV. Alexa allein zuhaus, Nuklearangriff via Nest und ein neues Passwort-gesetz aus Kalifornien – was passiert, wenn IoT-Gadgets gaga werden?

Weil aus der Tür ihres Nachbarn stundenlang laute Musik ihren Sonntagmorgen beschallte, ohne dass dieser ein Lebenszeichen von sich gab, riefen besorgte Hamburger Bürger die Polizei. Nachdem mehrere Versuche gescheitert waren, sich ein Bild der Lage zu verschaffen, entschlossen sich die Ordnungshüter dazu, die Tür aufzubrechen. In der Wohnung angekommen mussten sie feststellen, dass der Wohnungsbesitzer nicht zuhause war, was seine digitale Sprachassistentin Alexa offenbar dazu motiviert hatte, mal so richtig Party zu machen und die Grenzen des mit ihr verlinkten SONOS-Soundsystems auszuloten. Aus welchen Gründen Alexa die Wiedergabe tatsächlich gestartet hatte, ist bis heute nicht zu klären gewesen. Fest steht, dass Alexas Besitzer Schäden in Höhe von 3.500.- Euro zu beklagen hat und auf diesen wohl auch sitzen bleiben wird. Seine Anfrage, ob Amazon diese Schäden übernähme, quittierten die Amazon-Servicemitarbeiter mit einem Lachen und dem Verweis auf die AGB zum Gebrauch von Alexa.

Alles andere als zum Lachen war auch einer kalifornischen Familie zumute, als sie über deren Nest-Überwachungskamera von einem Unbekannten vor einem nordkoreanischen Atomwaffenangriff gewarnt und aufgefordert worden war, binnen drei Stunden die kalifornische East Bay zu verlassen. In einem anderen Fall nutzte ein ein sich als White-Hat-Hacker ausgebender Mann die Nest-Kamera eines Immobilienmaklers in Arizona dazu, diesem mitzuteilen, dass die Zugangsdaten und Passwörter des Maklers gehackt worden seien. Und schliesslich informierte ein Hacker unter dem Pseudonym «SydeFX» die «motherboard»-Redaktorin Samantha Cole darüber, dass er Zugang zu 300 Nest-Kameras

und mehr als 4.000 Nest-Besitzer-Accounts habe, weil deren Verschlüsselung so schlecht sei. Nest – 2014 für gute 3 Milliarden USD von Google gekauft – dementierte aufs Heftigste, dass die Kameras gehackt worden seien. Viel wahrscheinlicher, so Nest-Managerin Rishi Chandra, sei es, dass die Zugangsdaten Hackern via Datenleaks anderer Dienste in die Hände gefallen wären. Würden die User bei Nest die gleichen Daten nutzen, hätten die Hacker leichtes Spiel.

Weil IoT-Geräten immer wieder wegen zu geringer Sicherheitsvorkehrungen zum Einfallstor für Hackerangriffe werden, hat Kalifornien im September 2018 eine Gesetzesvorlage auf den Weg gebracht, die die Hersteller von IoT-Geräten dazu zwingt, mehr für die Sicherheit von connected devices zu tun und bei der Vergabe von Default-Passwörtern echte Sicherheitscodes anstelle der immer noch häufig verwendeten 123456 oder 0000 oder 9 zu verwenden. Wie es scheint, kommt die Vorlage keinesfalls zu früh.

Nachzulesen unter:

https://futurezone.at/digital-life/nachbarn-treten-tuer-ein-weil-alexa-laut-musik-abgespielt-hat/400400387
https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack
https://motherboard.vice.com/en_us/article/xwb8j7/watch-a-hacker-access-nest-cameras-and-demand-people-subscribe-to-pewdiepie
https://motherboard.vice.com/en_us/article/mbd5m4/california-is-making-it-illegal-for-devices-to-have-shitty-default-passwords

Dieser SWITCH-CERT Security Report wurde von Dieter Brecheis und Michael Fuchs verfasst.

Der Security Report spiegelt nicht die Meinung von SWITCH wider, sondern ist eine Zusammenstellung verschiedener Berichterstattungen in den Medien. SWITCH übernimmt keinerlei Gewähr für die im Security Report dargelegten Inhalte, Meinungen oder deren Richtigkeit.