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

Mai/Juni 2023

I. Never leave a running system. Oder: Wie man sich vor Phishing auf Ebay Kleinanzeigen schützt

Ebay Kleinanzeigen bilden das mit Abstand beliebteste und meistgenutzte Portal für private Käufe und Verkäufe. Und wo immer sich viele Menschen mit guten Absichten im Netz finden, sind auch die mit den bösen Absichten nicht weit. So veröffentlichte die Polizei im baden-württembergischen Konstanz das Beispiel eines jungen Mannes, den der Verkauf eines Buchs mehrere tausend Euro gekostet hat. Auch er war auf die fast schon klassische Phishing-Nummer auf Ebay (und anderen Auktions- oder Kleinanzeigen-Portalen) hereingefallen. Und die läuft folgendermassen ab:

Auf ein Angebot hin meldet sich eine interessierte Person, zeigt starkes Interesse am Artikel, gibt der verkaufenden Person aber zu verstehen, dass sie Ebays internen Messenger zur Kommunikation nicht nutzen will oder kann, oder dass die Zahlung via PayPal nicht funktioniert. Daher wird die verkaufende Person gebeten, manchmal auch aufgefordert, ihre privaten Kontakt- oder gar Bankverbindungsdaten preiszugeben. Im Fall des Konstanzer Buchverkäufers wurde der auf eine seriös aussehende Zahlungswebsite geführt

und dort aufgefordert, seine Bankdaten einzugeben. Kurze Zeit später entdeckte er dann statt des erwarteten Zahlungseingangs den Abfluss mehrerer tausend Euro von seinem Konto.

Bei einem ähnlich gelagerten Fall bemerkten die Personen, die techbook.de verfasst hatten, dass die Ebay-Konten der ausschliesslich weiblichen Interessentinnen nie länger als drei Tage bei Ebay existierten.

Es hat also weniger mit dem Eigennutz der Plattformbetreiber als mit dem Schutz der eigenen Daten und Kontostände zu tun, wenn diese ebenso wie die Polizei dazu auffordern, ausschliesslich die plattform-internen Systeme zur Kommunikation und zur Abwicklung der Zahlung zu nutzen. Hatte das Sprichwort der analogen Welt noch «Schuster, bleib bei deinem Leisten!» geheissen, heisst es in der virtuellen Welt von heute wohl: «Verkäufer, bleib bei deinen Plattform-Diensten!»

Nachzulesen unter:

https://www.techbook.de/shop-pay/shops-marktplaetze/ebay-kleinanzeigen-betrug-phishing
https://www.presseportal.de/blaulicht/pm/110973/5465001

II. Malware ab Werk: Viele Android-Geräte werden mit vorinstallierter Schadsoftware ausgeliefert

Kaum zu glauben, aber dennoch traurige Wahrheit: Es gibt tatsächlich Lohnfertiger (OEMs) vor allem von preiswerteren Android-Geräten, die sich von Cyberkriminellen dafür bezahlen lassen, Schadsoftware auf Android-Handys, -Tablets, -SmartWatches und -SmartTV-Geräte, werkseitig zu installieren. Das haben Sicherheitsforschende von TrendMicro auf der jüngst stattgefundenen Black Hat Asia Konferenz präsentiert.

Die böswilligen (Zweit-)Auftraggeber vermieten dann für einen begrenzten Zeitraum – die TrendMicro-Forscher berichten von 1'200 Sekunden – das kompromittierte Gerät, damit es andere Cyberkriminelle für ihre dunklen Machenschaften verwenden können. Und die sind vielfältiger Natur. Zum einen kann das Gerät als Botnet-Knoten verwendet werden. Zum anderen können die Cyberkriminellen Personen Daten, wie z.B. Ortungsdaten, IP-Adresse oder Tastenanschläge (etwa bei der Eingabe von Login-Daten) vom Gerät abziehen und missbrauchen.

Die kriminellen Zweitausrüster brüsten sich damit, mindestens 8.9 Millionen Geräte auf diesem Weg infiziert zu haben. Sie sollen zwar hauptsächlich in Osteuropa und Südostasien verkauft worden seien, doch bleibt das Thema «Bot-Netzwerke» auch in Europa und der Schweiz höchst relevant.

So berichtet Spamhaus in seinem Quartalsupdate 1/23 von 8'358 aktiven Botnet Command & Control (C&C) Servern, was einer Steigerung von 23% zum Quartal 4/22 entspricht. In der Spamhaus-Statistik führen nach wie vor die USA und China, was die Zahl der aktiven C&C Server angeht. Auffällig sei, so Spamhaus, das dramatische Quartalswachstum von 62% in Russland. Getoppt werden diese ohnehin unerfreulichen Zahlen aber im vierten Quartal 2022 von der Schweiz: Hier wurden 169% mehr bösartige C&C Server aktiviert als im Quartal zuvor. Inwieweit es Zusammenhänge zwischen dieser Steigerung und der zu beobachtenden Intensivierung von Cyberangriffen gegen die Schweiz (siehe Kapitel III und IV) gibt, kann derzeit nicht gesichert festgestellt werden. Fakt ist, dass die Alpenrepublik dadurch in die weltweiten Top Ten der Spamhaus Rangliste der installierten Botnet C&Cs katapultiert wurde.

Für die globale Android-Welt kommt es derzeit bedauerlicherweise noch schlimmer: Eine Virenanalyse des Security-Anbieters Doctor Web hat auf Google Play ein Android Softwaremodul entdeckt, das sein Unwesen in 101 Apps treibt, die insgesamt 421 Millionen Mal heruntergeladen wurden. Getarnt als SDK (Software Development Kit) zur einfachen Integration von Marketing-Tools in eine App, erweckt das «SpinOK»-Modul den Eindruck, es sei ein Hilfsmittel, um Userinnen und User in den befallenen Apps zu halten. Dazu liefert SpinOK Mini-Games sowie Token-belohnte Quests. In Tat und Wahrheit verbindet sich das Modul bei der Initialisierung mit einem C&C Server und lädt von dort SPAM und Werbebanner auf die befallenen Geräte. Zudem bezieht SpinOK Infos über verfügbare Sensoren und andere Geräteausstattungen, die die Malware zur Tarnung nutzen kann. Auf entgegengesetztem Weg liefert das böse Modul vertrauliche Infos und Daten an den Botnet-Server. Obwohl die Web-Doctors Google von ihren Entdeckungen unterrichtet haben, sind einige der Schadsoftware verbreitenden Apps immer noch auf Google Play erhältlich.

Daher sei hier die Liste der populärsten SpinOK-verseuchten Apps wiedergegeben. Die vollständige Auflistung findet sich im unten verlinkten Github Repository.

1) Noizz: video editor with music (über 100 Mio. Downloads),
2) Zapya - File Transfer, Share (mehr als 100 Mio. Downloads; Trojaner in Version 6.3.3 bis 6.4 enthalten, in 6.4.1 nicht mehr),
3) VFly: video editor & video maker (mehr als 50 Mio. Downloads),
4) MVBit - MV video status maker (über 50 Mio. Downloads),
5) Biugo - video maker & video editor (mehr als 50 Mio. Downloads),
6) Crazy Drop (über 10 Mio. Downloads),
7) Cashzine - Earn money reward (mehr als 10 Mio. Downloads),
8) Fizzo Novel - Reading Offline (mehr als 10 Mio. Downloads),
9) CashEM: Get Rewards (über 5 Mio. Downloads),
10) Tick: watch to earn (mehr als 5 Mio. Downloads).

Nachzulesen unter:

https://t3n.de/news/android-smartphones-schadsoftware-ausgeliefert-vorinstalliert-1552434
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://www.heise.de/news/Android-Spyware-SpinOk-kommt-auf-mehr-als-421-Millionen-Installationen-9069832.html
https://github.com/DoctorWebLtd/malware-iocs/blob/master/Android.Spy.SpinOk/README.adoc

III. Bildungssektor unter Attacke der Vice Society Ransomware Group – auch in der Schweiz

Dass die Cybercrime-Economy seit Jahren ähnlich organisiert, ökonomisch professionalisiert und spezialisiert ist wie die reale Wirtschaft auf der guten Seite, ist (leider) nichts Neues mehr. Jüngstes Beispiel ist die «Ransomware-as-a-Service-Company» Vice Society, die sich mit ihren kriminellen Machenschaften auf den Bildungssektor spezialisiert hat. Bereits im Januar hatte das amerikanische FBI davor gewarnt, dass die in Russland vermutete Gruppe 2022 die mit Abstand meisten Angriffe auf Bildungseinrichtungen durchgeführt hat.

Der Angriff läuft nach dem klassischen Muster aktueller Erpressungsattacken ab: Via erfolgreicher Phishing-Versuche oder Informationsdiebstahl gelangen die Angreifer an VPN-Anmeldedaten, die sie dazu nutzen, sich Zugang zum Netzwerk einer Bildungseinrichtung zu verschaffen. Einmal dort angelangt, stehlen sie die Daten, bevor sie sie verschlüsseln, um die Institution doppelt zu erpressen: Zum einen wird Lösegeld für die Entschlüsselung der Daten verlangt, für die zweite Erpressung wird mit der Veröffentlichung der gestohlenen Daten im Netz gedroht.

Als zweiten Angriffsvektor nutzen die vermeintlich russischen Cyberkriminellen klassische Exploits, wie die bereits 2021 entdeckte Print-Nightmare-Schwachstelle, die sich in der Drucker-Implementierung aller Windows- und Windows-Server-Versionen fand. Seit damals hat Microsoft zwar mehrere Sicherheitsupdates für den Drucker-Spooler veröffentlicht, doch zeigen die Erfahrungen mit der schleppenden Schliessung von Sicherheitslücken, dass die besten Patches nichts nützen, wenn sie nicht installiert werden. Gute Gründe, sich diese Mühe zu machen, gäbe es indes genug.

Denn Berichten der Malwarebyteslabs zufolge geht die Vice Society aktuell besonders fies vor, weil sie sich in vielfach genutzte und gebräuchliche IT-Tools einnistet und dort gut getarnt ihrem schädlichen Tun nachgeht. Für diese auch als Living off the Land (LOTL)-Attacke bekannte Angriffsversion nutzt Vice Society vor allem Windows Management Instrumentation, ein Tool, das in vielen Bildungseinrichtungen zur externen Wartung und Beobachtung von Computern im Netzwerk eingesetzt wird. Das Problem dabei: LOTL-Angriffe können fast nur mit einer Endpoint Detection Platform entdeckt werden.

SWITCH erkennt derzeit verstärkte Aktivitäten auch im Schweizer Hochschulsektor, die der Vice Society zugerechnet werden können. SWITCH-CERT beobachtet die Situation aktiv und alarmiert die Institutionen sofort, sobald Anzeichen eines Angriffs entdeckt werden. Zudem wird allen Institutionen DRINGEND empfohlen, für VPN-Anmeldungen die Multi-Faktor-Authentifizierung (MFA) umgehend zu aktivieren. Sie hat sich als entscheidende Sicherheitsmassnahme in der Abwehr solcher Attacken bewährt.

Dies umso mehr, als Palo Alto Networks Unit 42 im Frühjahr herausgefunden hat, dass Vice Society ein PowerShell-Skript entwickelt hat, um Daten aus kompromittierten Netzwerken abzuziehen. Bestens getarnt und voll automatisiert, gewährleistet es höchste Effizienz der Vice-Society-Angriffe und richtet schwere Schäden bei den Angegriffenen an. Für alle, die tiefer in diese Thematik einsteigen wollen, ist daher unten der Blogbeitrag auf bleepingcomputer.com verlinkt.

Nachzulesen unter:

https://www.malwarebytes.com/blog/business/2023/01/5-facts-about-vice-society-the-ransomware-group-wreaking-havoc-on-k-12-schools
https://www.heise.de/news/Windows-Vice-Society-Ransomware-schluepft-durch-PrintNightmare-Luecken-6165668.html
https://www.bleepingcomputer.com/news/security/vice-society-ransomware-uses-new-powershell-data-theft-tool-in-attacks

IV. «NoName057(16)»: Massive DDoS-Angriffe russischer Hacktivisten gegen die Schweiz

Der Angriffskrieg Russlands gegen die Ukraine hat neben offiziellen und Para-Militärs eine dritte Gruppe kriegführender Parteien ins Licht der Öffentlichkeit gerückt: Cybermilitante Gruppen, die die jeweilige Gegenpartei und ihre Unterstützer mit Cyberangriffswellen überziehen. Die derzeit aktivste ist ein russisches «Hacktivisten-Kollektiv» namens «NoName057(16)». Man könnte es als die «Wagner-Söldner» des Internets bezeichnen, auch wenn «NoName057(16) erste seit März 2022 – also unmittelbar nach dem Start des russischen Angriffs – öffentlich in Erscheinung trat. Und das in verblüffend schamloser Manier: Jede Attacke des Cyberterror-Kollektivs wird auf dessen Telegram-Kanal publiziert, so dass die italienische ThinkOpenGroup auf der Website ihrer BE42LATE-Geschäftseinheit einen Tracker mit den Aktivitäten und TelegramPosts von «NoName057(16)» eingerichtet hat (Link untenstehend).

Während Italien bereits in der Frühphase von Putins Angriffskrieg angegriffen worden war, und Anfang April «NoName057(16)» eine riesige DDoS-Angriffswelle gegen deutsche Behörden-Websites gestartet hatte, bekommt mittlerweile auch die Schweiz die zunehmende Wut der Hacktivisten zu spüren: So legte eine DDoS-Attacke zum Russischen Nationalfeiertag am 12. Juni mehrere Webseiten und Online-Dienste der Bundesver-

waltung und bundesnaher Betriebe – darunter auch die der SBB – lahm. In der Woche zuvor war die Website der eidgenössischen Räte angegriffen und teilweise ausser Betrieb gesetzt worden. Es ist davon auszugehen, dass diese Angriffe nicht die letzten ihrer Art gewesen sind, zumal der DECODEDavasat.io-Blog nach einer ausführlichen und detaillierten Analyse der Attacken (siehe Link unten) zum Schluss gelangt, dass «NoName057(16) intensiv daran arbeitet, die Effizienz der Angriffe deutlich zu steigern.

Darum verweisen wir an dieser Stelle auf die Website des Nationalen Zentrums für Cybersicherheit (NSCS) zum Thema «DDoS-Angriff – Was nun?» (Link unten). Die wichtigsten Tipps in aller Kürze:

1) Angriff vom frühestmöglichen Zeitpunkt an protokollieren.
2) Sicherstellen, dass minimale Infokanäle zu Kundschaft und Stakeholdern offengehalten werden können (z.B. mit einer statischen Website).
3) Angriff analysieren und Abwehrstrategie festlegen.
4) Agil auf Gegenmassnahmen des Angriffs und erneute DDoS-Attacke reagieren.
5) Vorfall ans NCSC melden und Anzeige erstatten.

In diesem Zusammenhang empfiehlt das NSCS zudem, auf Lösegeldforderungen nicht einzugehen und sich auf jeden Fall mit der Kantonspolizei kurzzuschliessen, falls eine Lösegeldzahlung dennoch erwogen wird.

Nachzulesen unter:

https://noname.be42late.co
https://www.watson.ch/digital/schweiz/909054730-noname-russische-hacker-attackieren-bund-webseiten-lahmgelegt
https://www.infosecurity-magazine.com/news/swiss-government-targeted-series/
https://www.srf.ch/news/schweiz/cyberangriff-aufs-parlament-bundesanwaltschaft-eroeffnet-strafverfahren
https://www.heise.de/news/Weitere-DDoS-Angriffe-auf-offizielle-Landes-Webseiten-8593741.html
https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks
https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ddos-angriff.html

V. Play ist alles andere als ein Spiel: Russlands Cyberterror gegen die Schweiz, Teil 2:

Neben «NoName057(16)» ist seit 2022 eine weitere in Russland vermutete Cybergang aktiv. Sie heisst «Play» und hat sich auf klassische Cybererpressung mit Datendiebstahl spezialisiert. Als erste prominente Opfer in der Schweiz waren die NZZ-, die CH Media-Gruppe und andere Medienhäuser von einem massiven Angriff betroffen. In dessen Verlauf konnten zum einen aktuelle Zeitungsausgaben nicht erscheinen, zum anderen veröffentlichten die Kriminellen aber auch sensible Daten jener Medienhäuser, die sich

geweigert hatten, Lösegeld zu zahlen.

Am 23. Mai setzte «Play» dann zum grossen Coup an und hackte den Berner IT-Dienstleister XPlain, auf dessen Kundenliste neben diversen Bundes- und Kantonsbehörden auch die Schweizer Armee, der Zoll, das Bundesamt für Polizei, die Landespolizei Liechtenstein und private Firmen stehen. In der Folge haben viele dieser Kunden zwar keine direkten Angriffe auf ihre Systeme erlebt, wohl aber feststellen müssen, dass Daten aus ihren Systemen im Darknet aufgetaucht sind. Einem Report von Le Temps am 18. Juni zufolge handelt es um die gigantische Datenmenge von 907 Gigabyte: «Darunter befanden sich beispielsweise Protokolldateien und Fehlerberichte des 2020 eingeführten neuen Systems des Bundes, das zur Erfassung biometrischer Daten wie Fingerabdrücke, Unterschriften und Gesichtsbilder verwendet wird, berichtete die NZZ, die einen Einblick in die Daten hatte. Es sind nicht nur Daten von Xplain online, sondern auch Daten von Kunden (Fedpol, Gerichte, SBB, Zoll, Polizei oder auch Gemeinden). Diese Daten sind hochsensibel, betreffen die Sicherheit der Schweiz und ihrer Bürger». Bestätigt wurde diese Einschätzung vier Tage zuvor durch das NCSC.

Nachzulesen unter:

https://www.swissinfo.ch/eng/business/more-swiss-media-groups-affected-by-ransomware-attack/48488756
https://www.netzwoche.ch/news/2023-06-05/ransomware-angriff-auf-it-dienstleister-trifft-auch-bundesstellen
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-95683.html
https://www.letemps.ch/economie/cyber/le-piratage-de-la-societe-xplain-une-veritable-bombe-a-retardement-pour-la-suisse

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

Der SWITCH 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.