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

März/April 2023

I. Erst der Crash, dann der Betrug: Cyberbetrüger versuchen nach dem Zusammenbruch der Silicon Valley Bank, Daten und Geld der Opfer zu stehlen

Das Szenario mutet an wie ein schlechtes Klischee aus Wildwest-Filmen: Kaum ist der Protagonist am Boden, schon kommen Aasgeier, um zu sehen, wieviel Beute sie machen können. Jüngst zu beobachten nach dem Zusammenbruch der Silicon Valley Bank (SVB). Da verzeichneten Security-Forscher eine in Zahl und Vielfalt zunehmende Welle von Cyberangriffen auf die Opfer das Bankencrashs. Offensichtlicher Hintergedanke: Menschen in Panik klammern sich an jeden Hoffnungs-Strohhalm und verlieren die Skepsis gegenüber jenen, die ihn anbieten.

In der ersten Angriffswelle versuchten Cyberbetrüger, Geld und Daten jener SVB-Kunden zu ergaunern, die mit der Kryptowährung USD Coin (USDC) handeln. Dieser digitale Stablecoin ist an den US-Dollar geknüpft und war seinerseits vom SVB-Zusammenbruch tangiert. Die Masche in vereinfachter Darstellung: Die Betrüger imitierten Websites von Kryptowährungs-Häusern und forderten die Opfer auf, ihre USDC-Guthaben zu beanspruchen oder zu einem günstigen Kurs in US-Dollar zu tauschen. Konkret: Nach der

Installation der Fake-Websites verschickten die Gangster via bösartiger Send-Grid-Konten Mails an die Opfer, die einen Link auf die gefakte Seite enthielten. Dort wurden die Opfer zur Installation eines URL-Handlers, wie z.B. MetaMaskWallet verführt. Der forderte die Opfer auf, zur Sicherung ihres Krypto-Guthabens einen SmartContract zu installieren, der den Inhalt der digitalen Geldbörse der Opfer direkt auf die Konten der Betrüger leitete.

Auch wenn nicht alle Neuregistrierungen von Domains mit Bezug zur Silicon Valley Bank in betrügerischer Absicht erfolgt seien, so sah das Internet Storm Center ISC des renommierten SANS-Instituts in der beobachtbaren Rallye um die Registrierung dieser Adressen ein Zeichen dafür, dass Cyberbetrugswellen zu erwarten seien. Konkret warnte das ISC davor, dass Cyberkriminelle die Unsicherheiten nach dem SVB-Crash für sogenanntes Business-E-Mail Compromise nutzen könnten. Mit dieser auch als CEO-Fraud bekannten Masche versuchen Betrüger, Mitarbeiter von Unternehmen zu Zahlungen auf ihr Konto zu veranlassen. Diese Variante des Spear Phishings nutzt dabei täuschend echt aussehende, aber eben in den Kontodaten veränderte Mail- oder Rechnungsformulare von Geschäftspartnern der Opfer – oder die Cyberkriminellen geben selbst vor, Kunde zu sein bzw. werden zu wollen. Es braucht nicht viel Fantasie, sich vorzustellen, wie effektiv diese Masche funktioniert, wenn die Hausbank vieler Unternehmen eben zusammengebrochen ist und ein Mail ankommt, auf der ein Geschäftspartner ankündigt, dass er daher seine Kontodaten geändert habe. Zumal diese Methode bereits im üblichen Geschäftsalltag immer wieder funktioniert und derzeit vor allem in Deutschland und Österreich zu enormen Schäden führt. Während hier vor allem das CERT-AT zu Vorsicht und Gegenmassnahmen mahnt, ist im Fall des SVB-Crashs mittlerweile die US-amerikanische Cybersicherheitsagentur CISA aktiv geworden. In einem Blogpost vom 15. März warnte die Behörde vor Betrügereien im Zusammenhang mit Banken allgemein, den Zusammenbrüchen von SVB und der Signature Bank, New York, insbesondere und auch davor, dass sich Betrüger als FDIC, also als Federal Deposit Insurance Corporation ausgeben, um Daten abzufragen oder Zahlungen auf Ihre Konten einzufordern. Die FDIC ist in den USA eine Art «Konkursverwalter» gescheiterter Finanzhäuser.

Explizit fordert die CISA-Userinnen und User zur Vorsicht im Umgang mit E-Mails mit Bankbezug in der Betreffzeile, in Anhängen oder Links. Auch sollten Aufrufen in Social Media, Textmessages oder Besuchern an der Haustür kritisch begegnet werden. Zudem weist die CISA auch darauf hin, dass die FDIC niemals nach persönlichen Daten fragen würde.

Ergänzend dazu sei hier auch noch auf die Sicherheitstipps des CERT-AT verwiesen, das dazu rät, Mitarbeitende regelmässig in IT-Sicherheitsfragen zu sensibilisieren und zu schulen. Zudem sollten Kunden- und vor allem zahlungsrelevante oder generell sensible Daten nicht alleine aufgrund einer E-Mail, sondern immer erst nach Rücksprache mit dem

(echten) Absender geändert werden. Und schliesslich weist das CERT-AT darauf hin, dass auch technische Massnahmen, wie z.B. die Einführung digitaler Signaturen für E-Mails und Dokumente oder die verstärkte Absicherung von E-Mail-Systemen durch DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework) o.ä., helfen, vor derlei Attacken, Social Engineering oder E-Mail-Spoofing zu schützen.

Nachzulesen unter:

https://isc.sans.edu/diary/Incoming+Silicon+Valley+Bank+Related+Scams/29630/
https://www.heise.de/news/Betrueger-missbrauchen-Zusammenbruch-der-SVB-fuer-Geld-und-Datenklau-7546557.html
https://www.heise.de/news/Spear-Phishing-Oesterreichische-und-deutsche-Unternehmen-im-Visier-7538772.html
https://www.cisa.gov/news-events/alerts/2023/03/15/beware-bank-related-scams

II. Wiedersehen macht keine Freude – Emotet kommt (nicht nur) via OneNote E-Mail-Anhang zurück

In der Ausgabe Januar/Februar 2021 dieses Reports berichteten wir unter der Überschrift «Der König ist tot – Es lebe hoffentlich so schnell kein neuer!» darüber, dass es Sicherheitsbehörden gelungen sei, die Infrastruktur des Malware-Netzwerks hinter dem «König der Schadsoftware» (Zitat: Arne Schönbohm, Präsident des deutschen Bundesamts für Sicherheit in der Informationstechnik BSI) unter ihre Kontrolle zu bringen. Nun ist der extrem bösartige und gefährliche Trojaner, der vor allem in Malware-as-a-Service-Geschäftsmodellen von Cyberkriminellen genutzt wird, zurück. Gut getarnt nistet er sich tief in befallene Systeme ein und installiert dort ebenso gut getarnte Hintertüren, durch die neue Malware nachgeladen werden kann.

Am 7. März warnten Sicherheitsforscher der E-Mail-Security-Firma Cofense davor, dass Emotet nach mehrmonatiger Pause wieder aktiv sei. In sehr gut gemachten E-Mails, die vortäuschen, auf einen aktiven E-Mail-Verlauf zu antworten, werden Empfängerinnen und Empfänger aufgefordert, eine unverschlüsselte ZIP-Datei zu öffnen. Bisher zeigten sich nach dem Entpacken Office-Dokumente mit Finanzthemen oder Rechnungen voller bösartiger Makros, die die Aktivierung weitere Inhalte erforderlich machten. Mit deren Aktivierung wurde Emotet als .dll-Datei geladen und konnte sein verbrecherisches Treiben auf dem befallenen System starten.

Einem Bericht von bleepingcomputer.com zufolge wurden Mitte März auf diesem Weg amerikanische Steuerzahler mit Fakemails unter dem Faksimile der Steuerbehörde angeschrieben. Im unverschlüsselten, aber gezippten Anhang: ein Fake-Formular «W-9» als bösartiges Word-Dokument. Das ist auf mehr als 500 MB Dateigrösse aufgeblasen, um Sicherheitsvorkehrungen auszutricksen. Andere Cyberkriminelle, allen voran Meta Steeler (auch als redline bekannt) und IcedId (auch Bokbot), hatten es sich zunutze gemacht, dass

viele Sicherheitsprogramme Dateien ab gewissen Grössen nicht scannen oder nicht erlauben, sie in einer automatischen Sandbox zu öffnen. Deshalb hatte Microsoft seit letztem Sommer eine Initiative zur automatischen Blockade von Makros in heruntergeladenen Dokumenten gestartet. Nun haben die Verbrecher hinter Emotet offenbar ihre Strategie geändert.

Denn aktuell setzen die Finstermänner auf eine einfachere und elegantere Lösung: Der E-Mail wird eine einfache OneNote-Datei angehängt, auf der ein PopUp-Fenster anzeigt, dass die Datei geschützt sei und durch einen Doppelklick auf den View-Button entsperrt werden müsse. Dieser Doppelklick führt aber in Tat und Wahrheit ein verschleiertes Skript aus, das den fiesen Trojaner als .dll-Datei herunterlädt und mit «regsvr.32.exe» startet. Herausgefunden haben diese die Sicherheitsforscher von Malwarebytes Labs, die technische Details dazu auf ihrem Blog veröffentlicht haben. Der Beitrag ist unten verlinkt.

Nachzulesen unter:

https://www.switch.ch/permalink/af4cca41-7cfc-11eb-8217-5254009dc73c.pdf
https://cofense.com/blog/emotet-sending-malicious-emails-after-three-month-hiatus
https://www.bleepingcomputer.com/news/security/emotet-malware-distributed-as-fake-w-9-tax-forms-from-the-irs/
https://www.heise.de/news/Ransomware-Emotet-kehrt-zurueck-als-OneNote-E-Mail-Anhang-7551285.html
https://www.malwarebytes.com/blog/threat-intelligence/2023/03/emotet

III. Todsünde Trägheit: Immer noch sind MS Exchange Server in der Schweiz verwundbar

Trägheit ist nicht nur im katholischen Sündenregister als Todsünde aufgeführt, die mit strengsten Strafen sanktioniert wird. Auch in der IT-Sicherheit drohen all jenen ernste Konsequenzen, die zu träge sind, ihre Systeme mit den jeweils aktuellen Sicherheits-updates zu schützen. Darum warnte das National Center for Cyber Security (NSCS) im Februar (2023) zum wiederholten Mal davor, dass die seit September 2022 (!) bekannte Sicherheitslücke «ProxyNotShell» auf mehr als 650 Servern in der Schweiz noch immer nicht geschlossen sei, obwohl seit November 2022 ein Sicherheits-Update von Microsoft zur Verfügung stünde.

In diesem Zusammenhang empfiehlt das NSCS zudem, die richtigen und aktuellen Sicherheitskontakte aufzuschalten, um im Schadenfall die Betroffenen schnellstmöglich informieren zu können. Alle Details einschliesslich konkreter Handlungsempfehlungen im NSCS-Link unten.

Nachzulesen unter:

https://www.ncsc.admin.ch/23exchange-de

IV. Künstlich, intelligent, lückenhaft: ChatGPT nach Datenleck vorübergehend offline

In der letzten Ausgabe dieses Security Reports hatten wir darüber berichtet, dass u.a. die Sicherheitsexperten von McAfee in künstlichen Intelligenzen wir ChatGPT ein grosses Missbrauchspotenzial sehen. Zitat: «Zum einen könnten sie Malware sowohl quantitativ als auch qualitativ in neue Dimensionen führen, weil ChatGPT keine Pausen braucht, sondern 24/7 und rund um die Uhr Malware schreiben kann. Schlimmer noch: ChatGPT (und andere hochentwickelte AI) ist in der Lage, sogenannte polymorphe Malware zu entwickeln, die sich quasi selbstlernend ständig weiterentwickelt und so nahezu kaum mehr auffindbar, geschweige denn zu bekämpfen ist...»

Nicht erwähnt hatten die McAfee-Spezialisten ein Risiko, dessentwegen ChatGPT-Betreiber OpenAI seine Vorzeige-AI am 20. März 2023 offline nehmen musste: eine offenbar unsauber implementierte Cloud-Lösung. Wie im OpenAI-Blogbeitrag vom 24. März nachzulesen, hatte ein Bug in einer Open-Source-Library von Redis ein Datenleck geöffnet. Das ermöglichte es einigen Benutzern, Vor- und Nachnamen, E-Mail- und Zahlungsadresse sowie die letzten vier Ziffern und das Ablaufdatum der Kreditkarte eines anderen aktiven Nutzers einzusehen. Laut OpenAI seien davon etwa 1,2% aller ChatGPT Plus-Abonnenten betroffen gewesen. Inzwischen hat OpenAI nach eigenen Angaben in enger Zusammenarbeit mit Redis die Lücke geschlossen und das System wieder online gebracht.

Der Vorfall hat zwischenzeitlich die italienische Datenschutzbehörde «Garante per la protezione dei dati personali» auf den Plan gerufen, die OpenAI am 31. März mit sofortiger Wirkung untersagte, ihre äusserst erfolgreiche AI-Lösung anzubieten. Begründet hat die Behörde die Sperrung damit, dass OpenAI keine Rechtsgrundlage zur Sammlung personenbezogener Daten für das Training seiner Systeme hat, und darüber hinaus Nutzerinnen und Nutzer auch nicht darüber informiert, dass ihre Daten gesammelt und wie sie verwendet würden. Da ChatGPT zudem keinen Filter zur Überprüfung es Alters von Usern aufweise, verstosse OpenAI gegen den Jugendschutz. Die italienischen Datenschützer forderten OpenAI dazu auf, binnen 20 Tagen über ergriffene Massnahmen zu informieren. Um ihrer Forderung Nachdruck zu verleihen, drohten sie für den Fall, dass dies nicht geschehe, mit einer Geldbusse von bis zu 20 Millionen Euro oder bis zu 4% des Jahresumsatzes.

Nachzulesen unter:

https://www.heise.de/news/ChatGPT-Datenleck-ermoeglichte-Einsicht-in-Informationen-fremder-Benutzer-8042945.html
https://openai.com/blog/march-20-chatgpt-outage
https://www.faz.net/aktuell/wirtschaft/italien-sperrt-chatgpt-verstoss-gegen-datenschutz-18791222.html
https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/

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.