SWITCH Security Report on current trends in IT security and privacy

March/April 2023

SWITCH

I. First the crash, then the fraud: cyber crooks attempted to steal data and money from victims following the collapse of Silicon Valley Bank

The scenario sounds like a bad cliché from an old Western: no sooner is the protagonist on the ground than vultures swoop in to pick the carcass clean. The scene played out most recently following the collapse of Silicon Valley Bank (SVB). Security researchers recorded an increasing number and variety of cyber-attacks on the victims of the bank crashes. The obvious motive: people in a state of panic grasp at every last straw of hope and lose their usual wariness toward those who offer it.

In the first wave of attacks, cyber fraudsters attempted to steal money and data from SVB customers trading in the cryptocurrency USD Coin (USDC). This digital stablecoin is pegged to the US dollar and was itself affected by the SVB collapse. The scam in a nutshell: the scammers imitated the websites of cryptocurrency companies and asked the victims to claim their USDC balance or exchange it for US dollars at a favourable rate. In specific terms, after installing the fake websites, the scammers sent emails to the victims via malicious send-grid accounts containing a link to the fake website. There the victims were induced to install a URL handler, such as MetaMaskWallet. The handler then asked the victims to install a SmartContract in order to secure their crypto assets, which would forward the contents of the victims' digital wallets directly to the scammers' accounts.

Even if not all new registrations of domains related to Silicon Valley Bank were fraudulent, the Internet Storm Center (ISC) of the renowned SANS Institute saw the observable uptick in the registration of these addresses as a sign that waves of cyber fraud were in the offing. Specifically, the ISC warned that cybercriminals could use the uncertainties following the SVB crash for business email compromise attacks. This scam, also known as CEO fraud, is used by fraudsters to get employees of companies to make payments into their accounts. This variant of spear-phishing uses deceptively real-looking email or invoice forms from the victims' business partners that have been modified in the account details – or the cybercriminals themselves pretend to be or want to become a customer. It doesn't take much imagination to surmise how effective this scam can be when the bank of many companies has just collapsed and an email arrives in which a business partner announces that they have changed their account details. Not least since this method already works with some regularity in normal business life and is currently wreaking enormous damage, particularly in Germany and Austria. While CERT-AT in particular is urging caution and countermeasures, the US cybersecurity agency CISA has now taken action in the aftermath of the SVB crash. In a March 15 blog post, the agency warned of bank fraud in general, the collapse of SVB and Signature Bank, New York, in particular, and of fraudsters posing as the FDIC, or Federal Deposit Insurance Corporation, to retrieve data or demand payments to their accounts. In the US, the FDIC is a kind of 'bankruptcy administrator' for failed financial institutions.

CISA explicitly urges users to be cautious when handling emails with bank references in the subject line, attachments or links. Solicitations on social media, in text messages or by visitors at the front door should also be viewed with caution. In addition, CISA also points out that the FDIC would never ask for personal information.

Also useful in this regard are the security tips from CERT-AT, which recommends regularly raising employees' awareness of IT security issues and training them. Moreover, customer data and payment-related or generally sensitive data in particular should not be changed solely on the basis of an email, but always after consultation with the (real) sender. Finally, CERT-AT points out that technical measures, such as the introduction of digital signatures for emails and documents or increased security for email systems using DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework) or the like, also help to protect against such attacks, social engineering or email spoofing.

Read more at:

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. Unpleasant reunion – Emotet returns (not just) via OneNote email attachment

In the January/February 2021 issue of this report, we reported that security authorities had succeeded in removing the infrastructure of the malware network behind the 'King of malware' (quote: Arne Schönbohm, President of the German Federal Office for Information Security (BSI). Now the extremely malicious and dangerous Trojan, which is mainly used in malware-as-a-service business models by cyber criminals, is back. Well camouflaged, it enters deep into infected systems and installs equally well-camouflaged back doors through which new malware can be reloaded.

On 7 March, security researchers from the email security company Cofense warned that Emotet would be active again after a break of several months. In highly crafted emails that pretend to be responding to an active email history, recipients are asked to open an unencrypted ZIP file. Previously, after unpacking, Office documents with financial topics or invoices full of malicious macros would open that required activation of additional content. With their activation, Emotet was loaded as a .dll file and could start its criminal activity on the infected system.

According to a report by bleepingcomputer.com, in mid-March American taxpayers were contacted with fake emails under the tax office's facsimile letterhead. In the unencrypted but zipped attachment: a fake 'W-9' form in the form of a malicious Word document. The file size is inflated to more than 500 MB in order to circumvent security precautions. Other cybercriminals, and particularly Meta Steeler (also known as redline) and IcedId (also known as Bokbot), took advantage of the fact that many security programs do not scan files above a certain size or allow them to be opened in an automatic sandbox. This is why Microsoft launched an initiative last summer to automatically block macros in downloaded documents. Now the criminals behind Emotet have apparently changed their strategy.

The shady characters are now using a simpler and more elegant solution: attached to the email is a simple OneNote file for which a pop-up window indicates that the file is protected and needs to be unlocked by double-clicking the View button. However, this double-click actually executes a veiled script that downloads the nasty Trojan as a .dll file and starts with 'regsvr.32.exe'. This was discovered by security researchers at Malwarebytes Labs, who published technical details on their blog. The article is linked below.

Read more at:

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. Deadly sin of sloth: MS Exchange servers in Switzerland still vulnerable

Sloth is not just a deadly sin according to Catholic doctrine, subject to the severest of penalties. In IT security, too, there are serious consequences for those who are too sluggish to protect their systems with the latest security updates. That’s why the National Center for Cyber Security (NSCS) issued a warning in February (2023) that the ‘ProxyNotShell’ security vulnerability on more than 650 servers in Switzerland, which had been known since September 2022 (!), was still not closed, even though a security update from Microsoft had been available since November 2022.

In this context, the NSCS also recommends activating the correct and up-to-date security contacts in order to be able to inform those affected as quickly as possible in the event of damage. All details, including specific recommendations for action, can be found in the NSCS link below.

Read more at:

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

IV. Artificial, intelligent, riddled with holes: ChatGPT temporarily offline after data leak

In the last issue of this Security Report, we reported that McAfee’s security experts, among others, see great potential for abuse in artificial intelligence, such as ChatGPT. Quote: ‘On the one hand, they could take malware to new dimensions, both quantitatively and qualitatively, because ChatGPT doesn’t need any breaks. Instead, it can write malware 24/7. Worse still, ChatGPT (and other highly developed AI) is capable of developing what is known as polymorphic malware, which is constantly evolving in a quasi-self-learning way, making it virtually impossible to find, let alone fight…’

McAfee specialists did not mention a risk that forced ChatGPT operator OpenAI to take its flagship AI offline on 20 March 2023: a cloud solution that appears to be poorly implemented. As reported in the OpenAI blog post from 24 March, a bug in an open-source library from Redis had opened a data leak. This allowed some users to see the first and last names, email and payment addresses, as well as the last four digits and the expiry date of another active user's credit card. According to OpenAI, about 1.2% of all ChatGPT Plus subscribers were affected. In the meantime, OpenAI, in close collaboration with Redis, has closed the gap and brought the system back online.

The incident spurred the Italian data protection authority 'Garante per la protezione dei dati personali' to block OpenAI from offering its highly successful AI solution with immediate effect on 31 March. The authority justified the blocking on the grounds that OpenAI does not have a legal basis for collecting personal data for the training of its systems, nor does it inform users that their data is being collected and how it is being used. Since ChatGPT does not have a filter to check the age of users, OpenAI also violates the protection of minors, the order stated. The Italian data protection authorities asked OpenAI to inform them within 20 days of implemented remedial measures. To underscore their demand, they threatened fines of up to EUR 20 million or up to 4% of annual turnover if they failed to do so.

Read more at:

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/

This SWITCH Security Report was written by Dieter Brecheis and Michael Fuchs.

The SWITCH Security Report does not reflect the opinion of SWITCH. Rather, it is a compilation of various media reports. SWITCH assumes no liability whatsoever for the content, opinions or their accuracy in the Security Report.