Switch Security Report

on the latest IT security and privacy trends

January/February 2024

I. The attack of the killer toothbrushes - probing is better than biting into sour (news) apples!

On 30 January, the Aargauer Zeitung reported, citing experts from the cybersecurity company Fortinet, that three million smart electronic toothbrushes had been infected with malware. This was to misuse them in a botnet for DDoS attacks on Swiss companies. A successful attack on the website of an unspecified company resulted in damage totalling several million Swiss francs. The report spread virally via IT-savvy portals around the globe. Other security experts pricked up their ears and sounded the fake news alarm. And this turned out to be justified. The Aargauer Zeitung and Fortinet blamed each other. Fortinet explained that it had wanted to use a hypothetical example scenario to show the Aargauer Zeitung the potential danger posed by every networked IoT device - from baby monitors and smart home cameras to smart toothbrushes. Apparently, this scenario was perceived as real and published due to translation errors. For its part, the Aargauer Zeitung pointed out that this had been presented differently by Fortinet before the article was published.

In the meantime, blogs and news platforms - including those that had spread the story - are endeavouring to provide counterstatements and corrections. Bleepingcomputer.com points out that the veracity of the story should have been questioned from the outset due to a lack of details

and technical inaccuracies. For example, many IoT devices (including smart toothbrushes) are not directly connected to the internet, but send their data via Bluetooth to an app, which then forwards it to a web server. A much more complex structure would therefore be required for an attack by killer toothbrushes.

Meanwhile, experts advise that reports of large-scale cyberattacks should be thoroughly scrutinised before they are published so that awareness and vigilance do not wane in the face of increasing cybercrime and cyber warfare worldwide. The 2024 edition of the Munich Security Conference, for example, addressed cyber security issues to a significant extent for the first time. And in his blog post linked below, cyber security expert Paul Ducklin provides sound tips on how to strike a balance between providing information quickly and making a threat clear on the one hand and virally spreading fake news on the other. His most important piece of advice: "Don't make much ado about nothing!"

Read more at:

https://www.aargauerzeitung.ch/wirtschaft/kriminalitaet-die-zahnbuersten-greifen-an-das-sind-die-aktuellen-cybergefahren-und-so-koennen-sie-sich-schuetzen-ld.2569480
https://www.aargauerzeitung.ch/wirtschaft/cyberangriff-die-gehackten-zahnbuersten-gehen-medial-um-die-welt-und-loesen-fragen-aus-wie-es-dazu-kam-ld.2577182
https://www.tomshardware.com/networking/three-million-malware-infected-smart-toothbrushes-used-in-swiss-ddos-attacks-botnet-causes-millions-of-euros-in-damages
https://www.golem.de/news/iot-hacker-missbrauchen-zahnbuersten-fuer-ddos-angriffe-2402-181921.html
https://www.independent.co.uk/tech/toothbrush-hack-cyber-attack-botnet-b2492018.html
https://www.bleepingcomputer.com/news/security/no-3-million-electric-toothbrushes-were-not-used-in-a-ddos-attack/
https://pducklin.com/2024/02/08/tall-toothbrush-tales-how-to-avoid-x-million-y-attacked-z-hype/

II. Any Information on AnyDesk?

We have repeatedly emphasised in these security reports that the threat situation remains tense. We have also pointed out that hackers and hacker groups, both private and state-affiliated, are increasingly attacking targets that promise to scale the damage. The most recent example: AnyDesk. The Stuttgart-based software company with branches in Tampa Bay, Shanghai and Hong Kong has systems for remote access and remote maintenance in use with 170,000 customers worldwide. On 31 January, heise.de reported that the remote maintenance software had only been working with faults for a week and that AnyDesk had offered maintenance windows and a software update, but no further information on the background, although thehackernews.com pointed out in an article dated 3 February 2024 that AnyDesk had already warned customers of faults and interruptions to system operation via the customer portal on 24 January 2024.

The fact that the company did not report the incident to the authorities until 1 February 2024 was met with criticism from security experts. For example, cybersecuritydive.com quoted SentinelOne's Chief Trust Officer as saying: "...they knew this on Jan.29 but didn't announce until the end of day

on Friday. Not cool!" (editorial note: that was 2 February)

On 2 February 2024, AnyDesk then announced in a separate press release that it had discovered a breach in various of the company's production systems. Together with the security experts from CrowdStrike, the company then checked all systems and, where necessary, reset them, renewed certificates, and forced a password reset on the customer side. According to AnyDesk, no outflow of customer data or compromised customer systems are currently recognisable. In contrast, heise.de reported on 4 February 2024 that the cybersecurity company Resecurity had discovered and verified an offer for 18,000 data records of AnyDesk customers in a forum for cybercriminals. However, it is currently unclear how up-to-date these data records are.

What is certain, however, is that it concerns login data for AnyDesk's customer portal, which has lost at least some of its value due to the fact that AnyDesk declared all logins invalid after the intrusion became known and asked all customers to set up new passwords or multi-factor authentication. Nevertheless, the data provided harbours a potential threat, as customer details such as the number of devices working with the software, software licence keys, login times, etc. made it possible to spy on the companies.

AnyDesk then confirmed in a further communication dated 5 February 2024 that there was no information about the outflow of customer data or the compromise of customer systems, but nevertheless recommended an update to versions 7.0.15 or 8.0.8 for security reasons. On the same day, the German Federal Office for Information Security BSI confirmed the incident and the company's statements.

As it cannot be ruled out that both source code and certificates have been leaked, there is a risk, according to the BSI, that AnyDesk customers could be attacked, especially as the software is often used with privileged rights - as described at the beginning: (Too) many cyber criminals know their business! In this context, there are warnings of man-in-the-middle and supply chain attacks in particular. The BSI recommends that all AnyDesk customers update to the latest software with the latest certificate. It also points out that updates should only be obtained via the software's update function or the manufacturer's support page. Employees should also be sensitised and passwords renewed.

Read more at:

https://www.heise.de/news/Fernwartungssoftware-Anydesk-kaempft-mit-Stoerungen-9614705.html
https://thehackernews.com/2024/02/anydesk-hacked-popular-remote-desktop.html
https://www.cybersecuritydive.com/news/anydesk-attack-credential-reset/706554/
https://AnyDesk.com/en/public-statement-2-2-2024
https://www.bleepingcomputer.com/news/security/anydesk-says-hackers-breached-its-production-servers-reset-passwords/#google_vignette
https://www.heise.de/news/IT-Sicherheitsvorfall-Anydesk-bestaetigt-Einbruch-in-Produktionssysteme-9617356.html
https://www.heise.de/news/Kundendaten-von-Anydesk-zum-Verkauf-angeboten-9617991.html
https://anydesk.com/en/public-statement
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-213655-1032.pdf?__blob=publicationFile&v=2

III. All the bees have flown the coop - US State Department offers million-dollar rewards for tips on cyber extortionists despite considerable successes

In 2023, there was good news alongside record damage caused by ransomware: Working together, the security authorities had managed to take over infrastructures of the notorious cyber extortion organisation HIVE (Beehive). Shortly afterwards, the websites of the ALPHV/Blackcat criminals competing with HIVE could no longer be found on the Darknet. There, various ransomware providers and cyber extortionists fought poaching battles for alleged former employees and affiliates of HIVE and ALPHV. At the beginning of February 2024, EUROPOL announced that it had succeeded in taking over the largest and most active network for ransomware as a service through international cooperation: LockBit. It remains to be seen how long and how sustainable these successes will be. For one thing, the ALPHV/Blackcat sites, for example, are now back online. And secondly, there is apparently no trace of the people behind HIVE.

But there is hope here too: given the high frequency with which these groups were/are travelling, every week without activity is a win. In November 2022, the US Federal Bureau of Investigation (FBI) announced that HIVE criminals had extorted over 100 million dollars in ransom money from more than 130,000 companies between July 2021 and October 2022.

And in the meantime, the US State Department has now put out bait for the HIVE hive bees that have flown the coop, motivating all criminals to carry out their nefarious activities: Money, lots of it. Now the US government is offering a reward of up to 10 million dollars for information leading to the criminals behind the HIVE network. And not just for citizens of the United States, but worldwide. They can hand in the clues at any US consulate or embassy.

The piquant irony of HIVE is that the CIA, another US intelligence agency, launched a suite of malware under the exact same name, HIVE, which enables state agents to access data from monitored devices or send new commands to them. This was reported by securityaffairs.com in January 2023, among others. It is therefore to be hoped that the offer or even payment of the multi-million ransom is not just an accounting trick to shift budget items, but that the US government is serious about draining the increasingly stifling swamp of cyber extortion.

That this is the case can be concluded from the fact that on 15 February 2024, the US State Department offered a $15 million reward package for locating or identifying the leadership of ALPHV/Blackcat and its partners. It would be the jackpot for the authorities, for the whistleblower and ultimately for all of us.

Read more at:

https://www.heise.de/news/AlphV-meldet-sich-zurueck-Verhaftungen-und-Betrug-bei-anderen-Gruppen-9574446.html

https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/#google_vignette
https://www.heise.de/news/Operation-Cronos-Internationalen-Behoerden-gelingt-Schlag-gegen-Lockbit-9632833.html
https://www.heise.de/news/Ransomware-Lockbit-durch-Ermittler-zerschlagen-zwei-Festnahmen-9633327.html
https://www.bleepingcomputer.com/news/security/fbi-hive-ransomware-extorted-100m-from-over-1-300-victims
https://gbhackers.com/hive-ransomware-10-million-reward
https://www.heise.de/news/Hive-10-Millionen-US-Dollar-Belohnung-fuer-Hinweise-zur-Ransomware-Gruppe-9623257.html
https://securityaffairs.com/140878/malware/cia-hive-malware-detected.html
https://www.state.gov/reward-for-information-alphv-blackcat-ransomware-as-a-service
https://www.heise.de/news/ALPHV-15-Millionen-US-Dollar-fuer-Tipps-zur-Ergreifung-der-Ransomware-Gruppe-9630351.html

IV. From Smallville to SkyNet - Artificial intelligences use nuclear weapons to bring about peace

Almost 40 years lie between Smallville and SkyNet - and the difference between peaceful coexistence and the downfall of humanity. While the ChatGPT-based simulation Smallville 2023 by researchers at Stanford University and Google gives a village of 25 inhabitants a rather peaceful existence, the further development of the artificial intelligence SkyNet brings death and destruction to humanity in the almost hopeless battle against the war machines and robots developed by the same AI - as "Terminator" fans know. Now, researchers from the Georgia Institute of Technology, Stanford University, Northeastern University and the Hoover Wargaming and Crisis Simulation Initiative have simulated what humanity could expect if the five technologically leading large language models were to make military and diplomatic decisions. Spoiler: It's not Smallville. In various crisis scenarios, in which the researchers pitted eight so-called nation agents with different goals against each other, all models showed "unpredictable escalation patterns", including the use of nuclear weapons.

The fact that artificial intelligence is already being used in both cyber and physical wars is no longer a simulation, but a bitter reality. This is also the case in the Ukraine war instigated by Russia, in which the NATO states want to deliver AI-controlled swarms of drones to Ukraine. Meanwhile, OpenAI and Microsoft have closed user accounts for their artificial intelligence systems that are attributed to so-called state threat actors. According to the two companies, the groups "Charcoal Typhoon" and "Salmon Typhoon" attributed to the Chinese state are said to have used OpenAI services to obtain information about cybersecurity tools, error-free coding, the creation of phishing campaigns and more. The "Forest Blizzard" group associated with Russia is said to have targeted satellite communications and radar technology. The "Emerald Street" group, attributed to North Korea, sought to identify experts and organisations involved in defence issues in the Asia-Pacific region. The "Crimson Sandstorm" group believed to be based in Iran was involved in malware detection and content creation as well as web and app development for spear phishing campaigns.

In an initial reaction, Microsoft and OpenAI have adopted principles for dealing with AI risks of this kind. At the same time, researchers from the universities of Cambridge, Harvard and Toronto as

well as OpenAI have recently called for various measures to limit the risks mentioned above - from the export ban on high-performance chips and other hardware and software required for AI applications to real and virtual kill switches. At the same time, however, they also point to new dangers arising from the installation of such kill switches. For example, cyber criminals could switch off or "turn around" AI at an unfavourable time by activating and using such kill switches. All in all, it is clear that the discussion about opportunities and risks, and even more so any kind of functioning regulation of AI, is currently lagging far behind the pace of development of AI itself. The Terminators of this world will be pleased.

Read more at:

https://www.br.de/nachrichten/netzwelt/smallville-ein-dorf-mit-25-ki-bewohnern-auf-basis-von-chatgpt,TbVH5PS
https://www.heise.de/news/Fuer-den-Frieden-KI-setzt-in-Kriegssimulation-Atomwaffen-ein-9628928.html
https://www.heise.de/news/Ukraine-Krieg-NATO-Staaten-wollen-wohl-tausende-Drohnen-mit-KI-Technik-liefern-9631963.html
https://www.heise.de/news/KI-OpenAI-und-Microsoft-schliessen-Konten-staatlicher-Bedrohungsakteure-9631899.html
https://www.heise.de/news/Gegen-die-Apokalypse-Wissenschaftler-fordern-Kill-Switch-fuer-KI-9631689.html

V. Major damage even without AI - NoName057(16) continues to massively attack targets in Europe

The pro-Russian hacker group NoName057/16 proves that it doesn't take AI to take out infrastructure facilities or companies of dissident states. Since March 2022, over 1,500 (in words: one thousand five hundred!) DDoS attacks on what the attackers consider to be anti-Russian targets have been attributed to this group. Many of these were also in Switzerland, as we reported in the May/June 2023 issue of this report. The group referred to there as the "Wagner mercenaries of the internet" has since further developed its own malware called DDoSia, which is now coded in Golang instead of Python. The unusual approach of announcing all activities via the Russian messenger Telegram has also been further developed so that the recruiting and onboarding process for new hacktivists is extremely low threshold via Telegram. The gamification approach, in which attackers can use DDoSia to attack targets in the West and collect points, is almost cynical. The group has even developed its own cryptocurrency for this purpose. And the endeavours are bearing fruit. Cybersecurity provider Netscout reports that the number of BotNet servers involved has grown from 400 to just under 10,000 in just one year.

While at the beginning of the war in Ukraine, the Baltic states in particular were exposed to massive DDoSia attacks alongside Ukraine, the Czech Republic, Poland and Spain are currently the main targets, even though Ukraine, the USA, Canada and other Western countries have to endure DDoSia attacks time and again. In all countries, the waves of NoName057(16) attacks primarily affect public administration, the transport and logistics sector and the finance and banking industry. This means that Switzerland is once again being targeted by cyber criminals. And it is to be feared

that the attacks will increase following the imposition of new sanctions against the Russian warmongers.

Read more at:

https://www.netscout.com/blog/asert/noname057-16
https://de.wikipedia.org/wiki/NoName057(16)
https://thecyberexpress.com/noname-ransomware-attack-on-ukraine
https://securityaffairs.com/151149/hacking/noname-ddos-attack-canadian-airports.html
https://www.inside-it.ch/ddos-angreifer-noname-gehen-wieder-auf-die-schweiz-los-20230908

This Switch Security Report was written in German by Dieter Brecheis and Frank Herberg and translated into English using Deepl Pro.

The Switch Security Report does not reflect the opinion of Switch but is a compilation of various reports published in the media. Switch assumes no liability whatsoever for the content, opinions or correctness of the information presented in the Security Report.