SWITCH-CERT report on the latest IT security and privacy trends

September/October 2018

SWITCH

I. Turning Good instead of Breaking Bad? Hacking to fend off other hackers

Cryptominers infiltrating computers where they don't belong in order to mine cryptocurrencies is nothing new. But Chinese security experts from netlab360 have now discovered FBot, a well-intentioned (yet nonetheless illegal) piece of malware that infiltrates computers infected by the com.ufo.miner cryptominer and then eliminates it. Once its work is done, FBot removes itself. It still remains a complete mystery exactly just who and what are behind FBot. All that is clear is that the 'benevolent' trojan does not communicate with its masterminds via traditional DNS servers but, instead, uses the same blockchain-based DNS protocol EmerDNS used by the blockchain service provider Emercoin.

What we do know a lot more about today is Mirai – the Internet of Things botnet which deployed DDoS attacks and counterattacks in October 2016, paralysing the internet along the entire east coast of the United States before causing further internet outages, panic and serious damage all over the world. The goal of Mirai's three 18- to 20-year-old creators was apparently to disable the hosting provider for the video game Minecraft or extort money from it. At the same time, the three tricksters were also running what was basically a lucrative advertising click fraud business on the side. When the malware authors saw the wave of damage they had caused with Mirai, they panicked and released the code in order to escape imminent prosecution. But then other hackers began using the code to launch new attacks, causing devastating internet outages. Mirai is still the

underlying code for botnets like Satori and Reaper. And brand-new ones are using a more refined version of it to wreak havoc on Android and Linux systems.
Mirai's creators, who did end up getting caught after all, were recently sentenced before a court in Alaska. They did manage to get out of long prison sentences by striking a new sort of deal with the prosecuting authorities: the three men all walked away with suspended sentences contingent upon them helping in the fight against cybercrime. This meant that they would have to place their obviously profound knowledge and 2,500 hours of their time at the disposal of the FBI and security researchers over a five-year period.

Read more:

https://blog.netlab.360.com/threat-alert-a-new-worm-fbot-cleaning-adbminer-is-using-a-blockchain-based-dns-en
https://www.heise.de/security/meldung/FBot-Botnetz-entfernt-Krypto-Miner-Infektionen-4168434.html
https://sensorstechforum.com/fbot-bot-cleans-systems-infected-com-ufo-miner
https://www.zdnet.com/article/bizarre-botnet-infects-your-pc-to-scrub-away-malware
https://www.wired.com/story/mirai-botnet-creators-fbi-sentencing
https://www.heise.de/security/meldung/Mirai-Die-Entwickler-des-IoT-Botnetzes-arbeiten-jetzt-fuer-das-FBI-4169926.html
https://arstechnica.com/tech-policy/2018/09/mirai-botnet-creators-praised-for-helping-fbi-wont-serve-prison-time
... and sure to put a smile on your face:
http://littlefun.org/uploads/52420a24e691b26fb67d9285_736.jpg

II. What do a firefighter and Google Chrome 69 have in common?

In a cabaret by Emil Steinberger, a firefighter has a reason to celebrate: winning the lottery. After much vacillation, he decides to use the money for a down payment on a flat that, despite his large fortune, still greatly exceeds his winnings. So he conceals the purchase from his wife and remarks, 'Well, you don't have to mention everything right on the very first day!' Google, too, recently had a reason to celebrate: the search giant's Chrome web browser just turned 10 this year, so the company released a new version – Chrome 69 – to mark the occasion. But this joyous event had a shadowy side: after much protest by users, Google was forced to retract its new, partial URL display – something it had initially hailed as an innovation. And the Chrome 69 developers had apparently followed Emil's firefighter by deciding not to reveal everything right away. In the official announcement for the new browser, it was never mentioned that users with an active Google account would be automatically logged into Chrome, even if they had never linked the browser with a Google account. Bloggers and data privacy advocates suspected that user data was being synchronised automatically – in the same way as when users log in manually. This was cause for great alarm. But this synchronisation

apparently does not take place with the new forced login – even if it has been cast in this light in several publications on the topic.
So Google seemed puzzled by the extent and severity of the accusations, which ranged from a serious breach in trust to data protection violations because Google's privacy policy does not cover forced logins.

Read more:

https://www.cnbc.com/2018/09/24/google-chrome-69-automatic-login.html
https://blog.cryptographyengineering.com/2018/09/23/why-im-leaving-chrome
https://www.googlewatchblog.de/2018/09/kritik-google-chrome-neuerung
https://gadgets.ndtv.com/apps/features/google-chrome-69-sign-in-controversy-explained-1921359
https://techcrunch.com/2018/09/24/security-experts-say-chrome-69s-forced-login-feature-violates-user-privacy
https://gizmodo.com/google-chrome-is-now-quietly-forcing-you-to-log-in-here-1829265681

III. 15 months later: new attacks, same old vulnerability

WannaCry? Eternal Blue? We do recall hearing something about that... ah, yes: in May 2017, a piece of ransomware called WannaCry was spreading on Windows systems around the world at lightning speed, paralysing hundreds of thousands of unpatched systems. It represented the largest cyberattack in history at the time. To infiltrate systems, the malware exploited a vulnerability known as Eternal Blue (as we reported in our 5/6/2017 security report). After 15 months, all patches should be installed and the vulnerability eliminated. Or so you would think. Yet hackers continue to exploit Eternal Blue to attack Windows systems and smuggle in cryptotrojans, for example. Antivirus provider Avira warned in a blog post that antivirus software can, of course, detect the malware and disable it, but that a new infection is possible shortly thereafter using the SMB protocol, version 1.0. This is troubling because Microsoft did, in fact, close the security gap that was unleashed on the virtual world by the NSA, but hundreds of thousands Windows installations are (still) not updated and protected. This is why the security experts at Avira once again recommend disabling the obsolete SMB 1.0 protocol on unpatched Windows systems.

Read more:

https://www.switch.ch/export/sites/default/security/.galleries/files/security-reports/SWITCH_Security_Report_2017-3_de.pdf
https://blog.avira.com/nsa-eternalblue-exploits-live-on-with-an-endless-infection-loop
https://www.heise.de/security/meldung/EternalBlue-Hunderttausende-Rechner-ueber-alte-NSA-Schwachstelle-infizierbar-4167918.html
https://www.cybereason.com/blog/wannamine-cryptominer-eternalblue-wannacry
https://searchsecurity.techtarget.com/news/252448889/WannaMine-cryptojacker-targets-unpatched-EternalBlue-flaw

IV. Peekaboo exploits vulnerability in surveillance cameras in a major way

It's a common storyline in film and television: a good or evil heist to break into a room under video surveillance and elude detection, gain unauthorised access to cameras, use them to spy on targets or victims, delete recordings or replace the live feed. In the last scenario, surveillance personnel are tricked with images of a normal situation while the bank safe is being removed, thieves are making off with an item worth millions or an employee is being kidnapped or even killed.
Unfortunately, reality does not stray far from fiction in this case: in mid-September, researchers from the cybersecurity company Tenable discovered a zero-day vulnerability, which they christened "Peekaboo". It crops up in video management solutions made by NUUO. The company's systems are used in approximately 2,500 web-based camera models from more than 100 manufacturers. In the worst case scenario, not only the camera and its recordings could be hijacked, but cybercriminals could also use the camera as a gateway to access the very network that was supposed to provide extra security through video surveillance.
The large-scale access to surveillance cameras has recently been a topic of discussion within the newly formed Austrian Federal Government, which wants to use all images from surveillance cameras in public places – from hospitals to public buses. This is why it asked all of the relevant operators to provide the necessary interfaces and notify the national police stations how they can be accessed.

Read more:

https://www.zdnet.com/article/hackers-can-tamper-with-surveillance-camera-footage-due-to-new-zero-day-vulnerability
https://www.darkreading.com/iot/internet-connected-cctv-cameras-vulnerable-to-peekaboo-hack/d/d-id/1332841
https://derstandard.at/2000087605164/Innenministerium-verlangt-Zugriff-auf-Bilder-oeffentlicher-Kameras

This SWITCH-CERT security report was written by Dieter Brecheis and Frank Herberg.