SWITCHcert Security Report

May/June 2017

SWITCH

I. Plenty of tears as WannaCry encrypts unpatched systems

If some media reports are to be believed, this was the biggest cyberattack the world has ever seen. The story has all the makings of a bestseller featuring the usual suspects, including the US National Security Agency and North Korea, a malware blogger turned accidental hero and real lives placed in real danger.

It all started on 12 May 2017 with WannaCrypt (also known as WannaCry, WCry and WanaCrypt0r) spreading across the globe like wildfire, infecting unpatched Windows computers, encrypting their files and demanding payment of USD 300 in bitcoins within three days to unlock them. After three days, the cybercriminals said, the ransom amount would double. After six days without payment, they would delete all the files. Unlike other ransomware, WannaCrypt spread in the form of a worm. It did so by exploiting a weakness in the outdated Version 1 of the Microsoft Server Message Block protocol (SMBv1), which had been revealed when a hacker group called The Shadow Brokers published several exploits – including the one known as EternalBlue – developed by Equation Group, which is linked with the NSA. Microsoft provided patches for the most recent operating system versions at the time, but systems that had not been updated obviously remained unprotected.

On Monday, 15 May, it was claimed that over 200,000 computers in more than 100 countries had already been infected. The final figure is thought to be around 300,000 – relatively few of them being in Switzerland. WannaCrypt hit the UK's National Health Service especially hard, leading to media reports of utter chaos breaking out in the country's hospitals. German rail operator Deutsche Bahn also had highly visible problems with its station display boards.

Marcus Hutchins, the 22-year-old author of a blog called MalwareTech, stopped the worm in its tracks when he discovered a domain name in its code, which may have been intended as a potential «kill switch», and promptly registered it.

Taking stock of the WannaCry attack three weeks later, there are plenty of grounds for tears in a number of respects.

It is clear that, in addition to large numbers of private individuals and companies, some organisations with life-and-death significance and critical infrastructures are taking such a lax approach to IT security that they are not keeping their protection up to date or allocating a sufficient budget to maintenance, updates, upgrades and security in general.

It would also appear that intelligence services are more interested in finding exploits and back doors into the computers of the people they are supposed to be protecting than they are in security.

Rob VandenBrink's article in the SANS blog on what we can learn from the WannaCry attack is well worth a read. He comes to the conclusion that we are just not very good at learning from our mistakes. «Oh wait, we already knew that!» he asserts, sadly hitting the nail on the head. While we might not have been able to prevent WannaCry, we could have massively restricted its impact if we had all simply heeded the security advice we have been hearing for years.

Read more here:

https://www.heise.de/suche/?q=wannacry&search_submit.x=0&search_submit.y=0&rm=search
https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack
https://www.golem.de/news/ransomware-entschluesselungstool-fuer-wanna-cry-veroeffentlicht-1705-127942.html
https://www.golem.de/news/wanna-cry-mehrere-tor-server-in-frankreich-beschlagnahmt-1705-127905.html
https://venturebeat.com/2017/05/19/ransomware-wannacry-causes-fewer-tears-than-feared
https://www.wired.com/2017/05/wannacry-ransomware-ddos-attack
https://isc.sans.edu/diary/What+did+we+Learn+from+WannaCry%3F+-+Oh+Wait%2C+We+Already+Knew+That%21/22444

II. WannaCry's siblings from the NSA toolbox

Most accounts attribute the demise of WannaCry to 22-year-old security blogger Marcus Hutchins finding a mysterious domain name in the ransomware worm's code, officially registering it and thus preventing the worm from spreading further. However, there is mounting evidence that WannaCry may have been halted sooner by an equally malicious sibling called Adylkuzz. Just like a third family member, EternalRocks, Adylkuzz uses the same exploits from the NSA's EternalBlue toolbox. Adylkuzz and EternalRocks are by no means copycat versions of WannaCry. In fact, they are completely separate, extremely dangerous forms of malware that attack computers via SMB vulnerabilities. For example, bleepingcomputer.com reports that EternalRocks was constructed from seven NSA tools, whereas WannaCry only uses two. Armed with a Trojan to hold users to ransom or steal login, e-banking and identity information, EternalRocks could pose a very severe threat indeed. Adylkuzz demonstrates just how severe this threat might be: it has probably crept, undetected, onto more computers than WannaCry since the spring purportedly earned its criminal authors more than USD 1 million. It does not make money from ransoms but from mining Monero – one of the top ten cryptocurrencies along with Bitcoin. Security researchers at the US company Proofpoint published technical details of the Adylkuzz attack and information on its scope. Since mining software, by its very nature, demands very high computing power and lots of electricity, the Adylkuzz attackers decided to shift the related costs onto the owners of infected machines. However, they could do without any rival malware clogging up these compromised systems, so they close the SMB loophole on TCP port 455, and this appears to have blocked the WannaCry worm in many instances. You might say that the early Trojan catches the worm.

Read more here:

https://www.bleepingcomputer.com/news/security/new-smb-worm-uses-seven-nsa-hacking-tools-wannacry-used-just-two
http://www.trojaner-info.de/daten-sichern-verschluesseln/aktuelles/adylkuzz-attacke-erbrachte-hackern-1-million-us-dollar.html
https://nzzas.nzz.ch/notizen/adylkuzz-dieser-neue-cyber-parasit-will-mit-unseren-computern-geld-scheffeln-

ld.1295250
https://bitcoin-live.de/ethereum-mining-deutsch
https://www.proofpoint.com/us/threat-insight/post/adylkuzz-cryptocurrency-mining-malware-spreading-for-weeks-via-eternalblue-doublepulsar
https://arstechnica.com/security/2017/05/massive-cryptocurrency-botnet-used-leaked-nsa-exploits-weeks-before-wcry
http://blogs.flexerasoftware.com/vulnerability-management/2017/05/chasing-wannacry-what-about-adylkuzz.html

III. Keyloggers fitted as standard – HP notebooks snooping on users

In our last Security Report, we explained how many factory-fresh Android smartphones from a variety of manufacturers had malware installed on them. It was revealed at the start of May that spyware also comes as standard with several laptops in HP's EliteBook, ProBook, Elite X2 and ZBook ranges, albeit not with any malicious intent. The audio driver on these notebook models includes a keylogger that records every key press in a publicly readable log file. It is not currently known how many machines from other manufacturers have this Conexant Systems package installed. HP has now admitted the mistake, which has been around since 2015, but is yet to offer a solution.

Read more here:

https://www.golem.de/news/hp-notebooks-audiotreiber-mit-keylogger-funktion-1705-127769.html
https://www.heise.de/security/meldung/HP-Notebooks-Audio-Treiber-belauscht-Tastatur-3710250.html
http://www.zdnet.com/article/keylogger-found-on-several-hp-laptops
https://www.heise.de/security/meldung/Keylogger-auf-HP-Notebooks-Hersteller-gesteht-Fehler-ein-3712567.html
https://www.netzwelt.de/news/160887-keylogger-hp-notebook-hersteller-veroeffentlicht-statement.html

IV. Hakuna Metadata – the browsing goldmine

In the African language of Swahili, «hakuna matata» means «no worries!». Two IT researchers asking what metadata and browser histories reveal about us have thus appropriated the phrase with more than a hint of cynicism in their title «Hakuna Metadata – let's have some fun with Sid's browsing history». We might indeed wonder what there is to be worried about. These data are a real goldmine for Internet service providers because they make user profiling possible, which is extremely valuable for advertising networks and the key to success for automatically delivered «programmatic advertising». The European Digital Rights (EDRi) researcher and blogger who co-authored the aforementioned article goes so far as to quote former NSA General Counsel Stewart Baker: «Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content.»

Nothing underlines the fact that metadata are a matter of life and death better than this statement from Michael Hayden, former Director of the NSA and the CIA: «We kill people based on metadata.»

With this in mind, we should perhaps be thankful that marketing firms like Admeira – a Swiss joint venture between broadcaster SRG, telecom provider Swisscom and the Ringier publishing house – are only seeking to take our metadata for advertising purposes rather than our lives. On top of this and in contrast to the intelligence services, they also allow users to opt out of allowing their metadata to be collected and used (see last source quoted below).

Read more here:

https://netzpolitik.org/2017/hakuna-metadata-warum-metadaten-und-browserverlaeufe-mehr-ueber-uns-verraten-als-oft-vermutet
https://edri.org/hakuna-metadata-lets-have-some-fun-with-sids-browsing-history
http://www.privacypies.org/blog/metadata/2017/02/28/hakuna-metadata-1.html
https://www.nzz.ch/feuilleton/medien/admeira-swisscom-nutzerdaten-fuer-werbevermarktung-ld.150067
https://www.konsumentenschutz.ch/themen/datenschutz/swisscom-so-kontrollieren-sie-ihre-daten
http://www.admeira.ch/optout

V. Unboxed and hacked – new Samsung Galaxy S8 iris scanner

We have already written a lot in the Security Report about the sense and effectiveness of biometric identification functions. From Apple's TouchID to Samsung's iris scanner in its new «Unbox Your Phone» flagship Galaxy S8 model, they all seem to have one thing in common: they are not entirely secure. Less than four weeks after its launch, a PhD student at TU Berlin has brought the Galaxy scanner down to earth with a bump by tricking it with the aid of a photo of his eye and a contact lens. As explained in connection with the TouchID hack on Apple's iPhone, however, we must reiterate the caveat that many users do not use biometric or any other functions to lock their smartphone for sheer convenience. Matthias Schindler, who works for European Parliament member Julia Reda, tweeted sarcastically, «Remember: Always change your iris pattern every 3 months to prevent ID theft and unauthorized access to your phone and accounts!»

Read more here:

http://www.zeit.de/digital/datenschutz/2017-05/samsung-galaxy-s8-biometrie-auge-gehackt
https://www.theguardian.com/technology/2017/may/23/samsung-galaxy-s8-iris-scanner-german-hackers-biometric-security
http://www.zeit.de/digital/datenschutz/2014-12/fingerabdruck-merkel-leyen-hack-ccc-31c3
https://twitter.com/presroi/status/866946445550784515

New SWITCH-CERT Security Blog entries

Why the most successful Retefe spam campaign never paid off
https://securityblog.switch.ch/2017/05/18/why-the-most-successful-retefe-spam-campaign-never-paid-off/

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.

It does not reflect the opinions of SWITCH but is instead a summary of articles published in various media. SWITCH accepts no liability for the content or opinions contained in the Security Report or for its correctness.