SWITCH security report on the latest IT security and privacy trends

January/February 2021

SWITCH

I. Dependency confusion – when trust is too good to be true

Imagine the following scenario: anyone can leave groceries on publicly accessible tables in the city centre and anyone can help themselves from these tables. A fresh lasagne al forno is on one of the tables. Nobody knows where it came from or what's in it. But it looks great, smells fantastic, and would be just the thing right now because you happen to be hungry. Would you take the lasagne home, put it in your oven, and pass it around at work without checking what's in it? Even though 30 highly trained and highly paid chefs work there?

Sounds absurd, right? Maybe even crazy? It is. Yet this is exactly what happens every day in the world of IT – except the tables are 'open source repositories', and instead of lasagne, they contain every kind of software you can imagine. Even though people don't always know where the code they are – roughly speaking – integrating into their own software and running on servers, terminal devices or networks has come from, everyone digs in. Even tech giants like PayPal, Shopify, Netflix, Yelp, Tesla, Uber, Apple, Microsoft and more besides. All of them became 'victims' of security researcher Alex Birsan, who earned USD 130,000

through bug bounty programs and other means by investigating whether and how malware had gotten into his clients' systems through dependencies from open source repositories. Mr Birsan discovered that the question wasn't 'whether?' but actually 'how?'.

The security researcher exploited the fact that many programming languages make it relatively easy to check whether a dependency is available locally or online. Since it's usually the dependency with the higher version number (i.e. the more recent version) that's downloaded, he only had to copy the names of the dependencies used up until then, assign them a higher version number and upload his own code to publicly accessible repositories under these names and version numbers. The code was readily accepted and got him access to tech companies' internal systems. Mr Birsan used the DNS protocol to read out data from the hacked systems and prove how deeply he could infiltrate them.

The companies, all of which were informed in advance – Mr Birsan places great emphasis on this fact in his report – then changed their practices regarding the use of scripts from repositories so that hacks like this will no longer be possible in the future.

Read more:

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
https://www.heise.de/news/Sicherheitsforscher-bricht-ueber-Open-Source-Repositories-bei-PayPal-Co-ein-5051635.html
https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/amp

II. Water hacking – not a new trendy sport, but a serious threat

While a malware script from a repository led to a (fictional) Europe-wide power outage with devastating consequences in Marc Elsberg's 2012 thriller 'Blackout', on 5 February Florida experienced a very real attack on one of its OT systems: the city of Oldsmar's water supply. A hacker obtained access to the water treatment plant's controls and tried to increase the admixture of sodium hydroxide by a factor of 111, turning 15,000 people's drinking water into a deadly cocktail. Fortunately, the tampering was detected in time, although according to unconfirmed reports the attackers had slipped into the system through a remote maintenance software also used by many external partners of the water treatment plant.

This close shave shows that attacks on critical infrastructures through OT (operational technology), ICS (industrial control systems) and SCADA (supervisory control and data acquisition) systems must increasingly be recognised and treated as serious threats. SWITCH has been staying abreast of this development for years by building its own OT/ICS/SCADA security unit.

Read more:

https://www.welivesecurity.com/2021/02/09/hacker-attempts-poison-florida-city-water-supply
https://www.faz.net/aktuell/gesellschaft/kriminalitaet/florida-hacker-manipulieren-wasser-in-aufbereitungsanlage-17188261.html
https://www.computerworld.ch/security/hacking/hacker-brunnenvergifter-2630786.html
https://edition.cnn.com/2021/02/08/us/oldsmar-florida-hack-water-poison/index.html?utm_source=twCNN&utm_term=link&utm_medium=social&utm_content=2021-02-09T02%3A55%3A27
https://www.databreachtoday.com/5-critical-questions-raised-by-water-treatment-facility-hack-a-15955

III. Emotet: the king is dead – let there be no successor!

In 2019, Arne Schönbohm (President of Germany's Federal Office for Information Security (BSI)) called Emotet the 'king of malware'. In mid-January 2021, Europol and eight European states' cyber task forces ended its reign by bringing the infrastructure of this globally feared malware network under their control after a concerted two-year campaign.

Emotet made its first unwelcome appearance in 2014 as a bank trojan, but mutated over time into a licensed skeleton key for other cyber criminals, becoming the favourite tool of organised crime. Using the simple trick of compromising computers with malware by means of fake Word documents (such as invoices, delivery notices and COVID-19 support grant applications), the Emotet hackers installed a well-camouflaged, reusable access gateway to systems and networks. They resold this access to other criminals, who were then able to install and use their own worms, ransomware or data grabbers. The massive impact that Emotet had is confirmed by the fact that, in no less than five security reports since the 1/2019 issue, we have reported on, proposed security measures against and advocated increased awareness of the risks associated with e.g. the malware trio made up of Emotet, Trickbot and Ryuk.

The Emotet threat seems to be vanquished for now, but to everyone seriously involved in cybersecurity, a great and important battle may have been fought and won – but the war will go on. Especially since – and this is extremely important to know – only Emotet's infrastructure has been smashed. All the other downloaded malware programs, like ransomware and other viruses, remain active and highly dangerous.

Read more:

https://www.tagesschau.de/wirtschaft/emotet-bka-101.html
https://www.golem.de/news/europol-ermittler-legen-koenig-der-schadsoftware-lahm-2101-153723.html
https://www.swisscybersecurity.net/cybersecurity/2021-01-28/europol-legt-banking-trojaner-emotet-lahm
https://www.heise.de/news/Emotet-Strafverfolger-zerschlagen-Malware-Infrastruktur-5038233.html
https://www.nzz.ch/technologie/die-ermittler-machen-fortschritte-im-kampf-gegen-cyberkriminelle-doch-das-alleine-reicht-nicht-ld.1599047?reduced=true
https://www.heise.de/news/Emotet-Was-passiert-mit-den-Opfern-5039808.html

IV. Rumours of its death are greatly exaggerated: how phishing mailers trick cutting-edge security filters with good old Morse code

We shouldn't write Emotet off quite yet, despite its destruction. That much is shown by another recent example: in early February, Bleepingcomputer.com reported that hackers have found a new way to circumvent the security filters of 21st century email programs using an almost 200-year-old system of signs. They use Morse code. In 1837, Samuel Morse worked together with Alfred Vail to develop the set of symbols named after him, which encodes letters as a series of dots and dashes or short and long signals of all kinds (lights, sounds, electrical pulses).

In 2021, cyber criminals first sent an email with an ostensibly important Excel file attached. In reality, it's an HTML document containing JavaScript, where the letters have been replaced by Morse code so security filters don't recognise the script as malicious.

If the document is opened, the Morse code automatically turns into a hexadecimal character string that leads to a fake Office 365 login page being displayed. If the user follows the prompt to enter their credentials, the username and password are sent directly to the cyber criminals. According to Bleepingcomputer, the hackers have so far succeeded in phishing credentials from at least eleven companies.

The malicious attachment is recognisable due to the fact that it ends in a double file name extension as follows: '.xlsx.html'. This can be viewed if the file name extension display is activated in the operating system settings (it seems that only Windows systems are affected at present). If the file name extension display is not activated, be sure to exercise caution if an email attachment is still displayed with the extension '.xlsx'.

Read more:

https://www.com-magazin.de/news/hacker/hacker-nutzen-morsecode-verbreitung-malware-2631419.html
https://www.bleepingcomputer.com/news/security/new-phishing-attack-uses-morse-code-to-hide-malicious-urls/
https://www.reddit.com/r/cybersecurity/comments/le2q3v/first_time_ive_seen_this_a_malware_attachement_in

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