SWITCH Security Report on current trends in IT security and privacy

May/June 2023

SWITCH

I. Never leave a running system. Or: How to protect yourself from phishing on Ebay Classified Ads

Ebay Classified Ads is by far the most popular and most commonly used portal for private purchases and sales. But for every person with good intentions on the internet there are unfortunately those with bad ones too. For example, the police in Konstanz in Baden-Württemberg published the story of a young man whose book sale cost several thousand euros. He too had fallen for the almost classic phishing trick on Ebay (and other auction or classified ad portals). Here's how it works:

A potential buyer gets in touch about an item and seems very interested in it, but tells the seller that they do not want or cannot use Ebay's internal messenger for communication, or that payment via PayPal isn't working. It is therefore asked, sometimes even demanded that the seller reveals their private contact or even bank details. In the case of the Konstanz book seller, he was directed to a reputable-looking payment website and asked to enter his bank details there. A short time later, instead of the expected payment, he discovered that several thousand euros had been withdrawn from his account.

In a similar case, the people who put together techbook.de noticed that the Ebay accounts of the exclusively female interested parties had never existed on Ebay for more than three days.

It is therefore clear that platform operators, along with the police, ask users to only use the platform's internal systems for communication and payment processing primarily to protect their data and accounts rather than for their own self-interest. While the saying before the existence of the internet used to be 'Cobbler, stick to your last!,' in today's virtual world, the rule of thumb should be 'Seller, stick to your platform!'

Read more at:

https://www.techbook.de/shop-pay/shops-marktplaetze/ebay-kleinanzeigen-betrug-phishing
https://www.presseportal.de/blaulicht/pm/110973/5465001

II. Factory-installed Malware: Many Android devices come with pre-installed malware

Hard to believe, but it's a sad truth that there are indeed original equipment manufacturers (OEMs), especially of cheaper Android devices, who are paid by cybercriminals to install malware on Android phones, tablets, smartwatches and -SmartTV devices during their manufacture. This was presented by security researchers from TrendMicro at the recent Black Hat Asia Conference.

The malicious (secondary) clients then rent out the compromised device for a limited period of time – the TrendMicro researchers report that it took 1.200 seconds – so that other cybercriminals can use it for illegal activities. These activities are diverse in their nature. Firstly, the device can be used in a botnet. Secondly, cybercriminals can extract and misuse personal data such as location data, IP address or keystrokes (e.g., when entering login details) from the device.

Criminal secondary equipment manufacturers boast of having infected at least 8.9 million devices in this way. Although they are said to have been sold primarily in Eastern Europe and Southeast Asia, the issue of bot networks is very relevant in Europe and Switzerland too.

In its quarterly update 1/23, Spamhaus reported 8,358 active Botnet Command & Control (C&C) servers, which corresponds to an increase of 23% compared to quarter 4/22. In terms of the number of active C&C servers, the USA and China continue to lead in the spam house statistics. According to Spamhaus, the dramatic quarterly growth of 62% in Russia is striking. However, these unpleasant figures will be topped by Switzerland in the fourth quarter of 2022 - Here, there were 169% more malicious C&C servers activated than in the previous quarter. The extent to which there is a correlation between this increase and the observed escalation of cyber-attacks against Switzerland (see Chapters III and IV) cannot be determined with certainty at present. The fact is that the country has been catapulted into the worldwide top ten of the Spamhaus ranks of installed botnet C&Cs.

Unfortunately, things are taking a turn for the worse in the global Android world: A virus analysis by the security provider Doctor Web has discovered an Android software module on Google Play that is wreaking havoc in 101 apps, which have been downloaded a total of 421 million times. Disguised as an SDK (Software Development Kit) for easy integration of marketing tools into an app, the 'SpinOK' module masquerades as a tool for making users remain in infected apps. SpinOK also provides mini-games as well as token-rewarded quests. In fact, the module connects to a C&C server during initialisation and loads spam and advertising banners to the affected devices from there. SpinOK also obtains information about available sensors and other equipment that the malware can use as a camouflage. In the other direction, the infected module delivers confidential information and data to the botnet server. Although the web doctors have informed Google of their findings, some of the apps that have been responsible for spreading malware are still available on Google Play.

Therefore, we have compiled a list of the most popular SpinOK-infected apps. The complete listing can be found in the Github Repository linked below.

1) Noizz: video editor with music (over 100 million downloads),
2) Zapya – File Transfer, Share (more than 100 million downloads; Trojans included in versions 6.3.3 to 6.4, none in 6.4.1),
3) VFly: video editor & video maker (more than 50 million downloads),
4) MVBit – MV video status maker (over 50 million downloads),
5) Biugo – video maker & video editor (more than 50 million downloads),
6) Crazy Drop (over 10 million downloads),
7) Cashzine – Earn money reward (more than 10 million downloads),
8) Fizzo Novel – reading offline (more than 10 million downloads),
9) CashEM: Get Rewards (over 5 million downloads),
10) Tick: watch to earn (more than 5 million downloads).

Read more at:

https://t3n.de/news/android-smartphones-schadsoftware-ausgeliefert-vorinstalliert-1552434
https://info.spamhaus.com/hubfs/Botnet%20Reports/2023%20Q1%20Botnet%20Threat%20Update.pdf
https://www.heise.de/news/Android-Spyware-SpinOk-kommt-auf-mehr-als-421-Millionen-Installationen-9069832.html
https://github.com/DoctorWebLtd/malware-iocs/blob/master/Android.Spy.SpinOk/README.adoc

III. Education sector under attack by Vice Society Ransomware Group – including in Switzerland

The fact that the cybercrime economy has been organised, economically professionalised and specialised in a similar way to the good side of the real economy is (unfortunately) nothing new anymore. The most recent example is the "ransomware-as-a-service" company Vice Society, which specialises in the education sector with its criminal activities. Back in January, the American FBI warned that the group, suspected to be in Russia, carried out by far the most attacks on educational institutions in 2022.

These attacks follow the classic pattern of current blackmail attacks: Attackers gain access to VPN credentials through successful phishing attempts or information theft, which they use to gain access to an educational institution's network. Once there, they steal the data before encrypting it to blackmail the institution in two ways: Firstly, a ransom is demanded for the decryption of the data; secondly, the institution is blackmailed with threats that the stolen data will be published online.

As a second attack vector, the supposedly Russian cybercriminals are using classic exploits, such as the Print-Nightmare vulnerability discovered back in 2021, which was found in the printer implementation of all Windows and Windows server versions. Microsoft has released several security updates for the printer spooler since this time, but experience with the slow closure of security loopholes shows that even the best patches are useless if they are not installed. There are plenty of good reasons to go to the trouble of doing this.

According to reports by Malwarebytes Labs, the Vice Society is currently particularly malicious, because it is embedded in widely used and common IT tools and carries out its harmful activities there while being well-camouflaged. For this version of the attack, also known as the Living Off the Land (LOTL) attack, Vice Society mainly uses Windows Management Instrumentation, a tool used in many educational institutions for external maintenance and monitoring of computers in the network. The problem is that LOTL attacks can almost only be detected with an Endpoint Detection Platform.

Recently, SWITCH has noticed increased activities in the Swiss higher education sector that can be attributed to the Vice Society. SWITCH-CERT is actively monitoring the situation and immediately alerts the institutions as soon as there are signs of an attack. In addition, it is recommended that all institutions activate Multi-Factor Authentication (MFA) for VPN logins immediately and as a matter of urgency. This has proven to be a key security measure in defending against such attacks.

This was shown to be the case even more so when Palo Alto Networks Unit 42 discovered in spring that Vice Society had developed a PowerShell script to extract data from compromised networks. Optimally camouflaged and fully automated, it ensures maximum efficiency of Vice Society attacks and causes serious damage to its targets. For those wanting a more in-depth look at this topic, the blog post on bleepingcomputer.com is linked below.

Read more at:

https://www.malwarebytes.com/blog/business/2023/01/5-facts-about-vice-society-the-ransomware-group-wreaking-havoc-on-k-12-schools
https://www.heise.de/news/Windows-Vice-Society-Ransomware-schluepft-durch-PrintNightmare-Luecken-6165668.html
https://www.bleepingcomputer.com/news/security/vice-society-ransomware-uses-new-powershell-data-theft-tool-in-attacks

IV. 'NoName057(16)': Serious DDoS attacks by Russian hacktivists against Switzerland

In addition to official and para-military parties, Russia's war of aggression against Ukraine has turned the public spotlight onto a third group of belligerent parties: Cyber-militant groups that launch waves of cyber-attacks against the respective counterparty and its supporters. The most active currently is a Russian 'hacktivist collective' called 'NoName057(16)'. Its members could be referred to as the 'Wagner mercenaries' of the internet, even though 'NoName057(16)' made its first public appearance in March 2022 – i.e. immediately after the start of the Russian attack. This appearance was surprisingly shameless. Every attack by the cyber-terror collective is published on its Telegram channel, which has led to the Italian ThinkOpenGroup setting up a tracker on the website of its BE42LATE business unit with the activities and Telegram posts of 'NoName057(16)' (link below).

Italy had already been attacked in the early stages of Putin's war, and NoName057(16) also launched a huge wave of DDoS attacks against German government websites at the beginning of April. Now Switzerland is also beginning to feel the hacktivists' ever-increasing anger: For example, a DDoS attack on the Russian National Day on 12 June brought several websites and online services of the federal administration and businesses related to the federal government to a complete standstill – including those of the SBB. In the week before this, the website of the Swiss Federal Councils had been attacked and partly disabled. It can be assumed that these attacks were not the last of their kind, especially since the DECODEDavasat.io blog, following a comprehensive and detailed analysis of the attacks (see link below), concludes that 'NoName057(16) is putting serious work into significantly increasing the efficiency of the attacks.

It's because of things like this that we recommend a read of the National Cyber Security Centre (NSCS) website's article on this subject 'DDoS attack – what next?' (Link below). The most important tips in brief:

1) Make a record of the attack at the earliest possible point in time.

2) Ensure that low-level information channels to customers and stakeholders can be kept open (e.g. with a static website).

3) Analyse attack and define defence strategy.

4) Respond to attack countermeasures and renewed DDoS attacks flexibly.

5) Report the incident to the NCSC and report it.

The NSCS also recommends not responding to ransom demands and always contacting the cantonal police if you are considering paying a ransom.

Read more at:

https://noname.be42late.co
https://www.watson.ch/digital/schweiz/909054730-noname-russische-hacker-attackieren-bund-webseiten-lahmgelegt
https://www.infosecurity-magazine.com/news/swiss-government-targeted-series/
https://www.srf.ch/news/schweiz/cyberangriff-aufs-parlament-bundesanwaltschaft-eroeffnet-strafverfahren
https://www.heise.de/news/Weitere-DDoS-Angriffe-auf-offizielle-Landes-Webseiten-8593741.html
https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks
https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/vorfall-was-nun/ddos-angriff.html

V. Play is anything but a game: Russia's Cyber Terror Against Switzerland, Part 2:

In addition to 'NoName057(16)', another suspected cyber gang has been active in Russia since 2022. It's called Play and specialises in classic cyber blackmail involving data theft. The NZZ, CH Media Group and other media companies were the first prominent victims in Switzerland to be hit by a large-scale attack. In the course of the attack, the publication of current newspaper issues was prevented, and the criminals also published sensitive data from media companies that had refused to pay a ransom.

Then, on 23 May, 'Play' launched into a major coup, hacking the Bern-based IT service provider XPlain, whose customer list includes various federal and cantonal authorities, the Swiss army, customs, the Federal Office of Police, the Liechtenstein state police and private companies. Although many of these customers did not experience direct attacks on their systems as a result of this operation, they did discover that data from their systems had surfaced on the dark web. According to a report by Le Temps on 18 June, this was an enormous volume of data at 907 gigabytes: 'Included, for example, were log files and error reports for the federal government's new system introduced in 2020, which is used to collect biometric data such as fingerprints, signatures and facial images,' reported the NZZ, which has viewed the data. The attack didn't just compromise data from Xplain online, but also data from customers (Fedpol, courts, SBB, customs, police and municipalities).

This data is highly sensitive and has an impact on the security of Switzerland and its citizens.' This assessment of events was confirmed by the NCSC four days earlier.

Read more at:

https://www.swissinfo.ch/eng/business/more-swiss-media-groups-affected-by-ransomware-attack/48488756
https://www.netzwoche.ch/news/2023-06-05/ransomware-angriff-auf-it-dienstleister-trifft-auch-bundesstellen
https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-95683.html
https://www.letemps.ch/economie/cyber/le-piratage-de-la-societe-xplain-une-veritable-bombe-a-retardement-pour-la-suisse

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 or opinions set out in the security report or the accuracy of these.