# SWITCH security report on the latest IT security and privacy trends

November/December 2020

## I. Choose your team carefully – hackers use fake MS Teams updates to attack networks, especially those of educational institutions

SARS-CoV-2 isn't the only highly infectious virus best avoided during the COVID-19 pandemic. More and more cybercriminals are exploiting the COVID-19 pandemic and the measures being taken to curb it to spread digital viruses in ever more innovative ways. Microsoft recently issued a warning stating that search engine searches for Microsoft Teams have been turning up first-page results and ads linking to download pages created by hackers. Taking advantage of the sharp increase in MS Teams use while so many are working from home, video conferencing and collaborating virtually, these pages trick users into downloading fake versions of the software that come with malware attached. The ZeroLogon vulnerability provided (and continues to provide) hackers with an avenue for gaining administrator access to the entire network and then downloading additional malware. They usually start off by stealing sensitive data, such as access codes and payment information. Next, they install a backdoor like Bladabindi to gain constant access to the network and remain undiscovered. The backdoor is then used to download Cobalt

Strike beacons to inconspicuously snoop around the entire network and smuggle in further malware. Many of these attacks ultimately succeeded in infecting the devices with ransomware and encrypting the data stored on them. No-one has said yet whether any of the data has been restored after the payment of ransoms.

The recent wave of attacks was doubly insidious. Firstly, the hackers not only managed to game search engine results, landing their pages' top rankings in the generic results; they also purchased ads with prime positioning. Secondly, the criminals have increasingly been targeting educational institutions that have been using MS Teams much more frequently during the pandemic to continue with their school, teaching and research activities wherever possible.

Microsoft recommends taking six precautions:

1) Use web browsers capable of recognising and blocking malicious websites.
2) Use strong passwords and change them regularly, especially for administrators.
3) Restrict administrator privileges to the most essential users.
4) Avoid creating service accounts for the entire network domain, particularly when they have administrator-like access privileges.
5) Keep a regularly updated list of criteria that allow/block the running of .exe files and implement them as official rules.
6) Disable the downloading of .exe files for JavaScript and VBScript.

Read more:

https://www.bleepingcomputer.com/news/security/fake-microsoft-teams-updates-lead-to-cobalt-strike-deployment
https://www.infocyte.com/blog/2020/09/02/cobalt-strike-the-new-favorite-among-thieves
https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike
https://www.krone.at/2274182

## II. Audacious coronavirus relief phishing delivers an extra malware 'bonus' on request and creates a challenge for BEC

Yet another brazen case in which fraudsters have exploited these tough times for businesses during the continuing coronavirus crisis: phishing with fake coronavirus emergency relief applications. In September, Germany's Federal Criminal Police Office (BKA) released its 'Special assessment of cybercrime during the coronavirus pandemic' (in German), which describes these phishing attempts as one of the most pressing IT threats for businesses and organisations.

Cybercriminals have been targeting their victims, sending emails with attachments and fake application forms for the second round of stopgap pandemic relief that started in late October. Those tricked into filling out the fake applications will suffer a double blow: not only are criminals plucking out their sensitive data, but the requested relief money never arrives either – not to mention the recently promised (and naturally non-existent) 'Christmas bonus' for small businesses, sole proprietorships and freelancers.

It appears that T-Online customers have been targeted most frequently. The European Commission's representation in Germany stated quite plainly that 'T-Online's recipient infrastructure does perform any verification to identify the origin of fraudulent emails'. The magenta-emblazoned communication giant then announced that it had 'taken action and was communicating' regarding the matter.

This same European Commission representation has since issued its fourth warning and advises recipients of such emails to simply disregard them and immediately and permanently delete them. This is also due to the fact that business email compromise (BEC) attacks are a specific type of cybercrime that is becoming increasingly harmful. BEC attacks usually start with a single email that tricks employees (or entrepreneurs) into paying fake invoices or transferring money to a fake account belonging to the cybercriminals. According to the *Phishing Activity Trend Report* published in September 2020 by the Anti-Phishing Working Group (APWG), the average amount of money stolen through phishing scams has increased from USD 54,000 per case to USD 80,000 per case. Since 2019, the Russian BEC gang known as 'Cosmic Lynx' has launched more than 200 waves of attacks on 46 companies or organisations and managed to make off with an average of USD 1.27 million.

In late November, the FBI also warned that BEC gangsters have also been sending their emails by implementing new auto-forwarding rules in the web client of a given email account. This enables them to send their phishing emails even faster and then directly enter the stream of emails pertaining to payments and financial transactions. According to the FBI, this method resulted in damages of USD 1.7 billion in 2019.

Read more:

https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2020/pm200930_BLBCybercrime.html
https://www.hwk-hannover.de/artikel/vorsicht-fake-mails-zu-corona-hilfspaket-23,0,5730.html
https://zac-niedersachsen.de/artikel/52
https://www.heise.de/news/Corona-Phishing-Betrueger-locken-mit-angeblichem-Weihnachtsbonus-fuer-Unternehmen-4974601.html
https://ec.europa.eu/germany/news/20201123-betrugsversuche-phishing_de
https://securityboulevard.com/2020/12/email-attackers-using-auto-forwarding-rules-to-perpetrate-bec-scams
https://www.zdnet.de/88382400/bec-wird-gefaehrlicher/

## III. Stopping the attempt to stop online hate speech?

We are all well aware of the disgraceful fact that the internet is rife with unbridled hatred. This is why Germany and France have already enacted (controversial) laws to combat online hate speech. In response to the French law, the European Commission asked its member states to refrain from any unilateral approach and to instead implement the EU's Digital Services Act, which the Commission had hoped to publish on 9 December of this year.

It appears that the Austrian government was unwilling to wait this long after it proposed its own set of laws in mid-November to curb online hate speech. This includes the 'Communication Platforms Act' (Kommunikationsplattformen-Gesetz – KoPl-G), which imposes hefty penalties on platforms that fail to promptly remove posts containing hate speech and any other obviously criminal content. The European Commission must give it the green light before it can go into effect. Now, big service providers are not the only ones pushing back against this; representatives of the European Parliament are too. While in the former case, it must be assumed that companies are shying away from the requirements and constraints associated with the law, the range of arguments put forth by the representatives from the various parties and countries is broader. Objections include fears that countries taking measures into their own hands will undermine the Digital Services Act and get in the way of uniform EU-wide reporting systems that would otherwise result in the prompt removal of hate speech, or even the expectation that companies might delete too much content in the future out of caution.

Read more:

https://www.zeit.de/digital/datenschutz/2020-06/hass-im-internet-gesetz-bundestag-hasskommentare-datenschutz
https://netzpolitik.org/2020/netzwerkdurchsetzungsgesetz-justizministerin-lobt-gesetz-gegen-hass-im-netz
https://digitalservicesact.eu
https://futurezone.at/netzpolitik/neues-gesetz-zu-hass-im-netz-was-sich-aendert/401019845
https://futurezone.at/netzpolitik/abgeordnete-eu-soll-hass-im-netz-gesetz-blockieren/401114265

## IV. Close the gates before it's too late: what *Sneakers* and the Internet of Things have in common

No, we're not talking about smart footwear, but rather a 1992 film, the Internet of Things (IoT), a new procurement law in the United States, and LidarPhone – a research project reported on in November 2020 that involved the transformation of a networked hoovering robot into a household spy. This is where the story circles back to the film: in one scene, a rather smart (in the conventional sense) Robert Redford and his squad of 'sneakers' find themselves sifting through the real-world rubbish of the CIO of a mafia-controlled company to identify his proclivities and ultimately get their hands on the access codes to the company's supercomputer. Had LidarPhone been available to them at the time, they might have accomplished their mission in a more graceful, not to mention less conspicuous and malodorous, fashion.

In November 2020, the computer scientists Sriram Sami, Yimin Dai, Sean Rui Xiang Tan, Nirupam Roy and Jun Han published the results of a research project in which they converted a household robotic vacuum cleaner (which also happens to be sold in Switzerland) into an eavesdropping spy. How? Robotic vacuum cleaners use a laser-guided motion and measuring system to navigate their way through spaces without damaging anything: LIDAR (light detection and ranging). Researchers managed to hack the smart hoovering robot and convert it into a sort of microphone that can, for example, record voice signals in the room and store them on their computers. Because more and more people are working from home and making video calls these days due to the pandemic, criminals and spies have found an interesting way to gain access to sensitive information (without any need to go dumpster diving). What's particularly striking here, however, is that IoT devices don't even need to have a built-in microphone to act as bugging devices.

It certainly does require a great deal of IT and sensor technology expertise, not to mention that the targeted IoT device still has to be hacked first. But in the case of most IoT devices, this is probably the easy part. We have reported on many occasions how carelessly many IoT devices – especially peripheral devices like surveillance cameras or smart home appliances – encrypt data (if at all). Using security codes like '1234', '9' or '0', hackers can charge straight through network gateways much like the mythical wooden Trojan horse used by the besiegers in ancient Greece.

Lawmakers in the United States have recognised this as well: the White House is set to sign off on a law passed by both chambers of the United States Congress to improve IT security in federal government agencies. The 'IoT Cybersecurity Amendment Act of 2020' requires them to use these types of networked devices only if they meet security standards that are eventually to be defined by the National Institute of Standards and Technology (NIST). Otherwise, they are to be removed or replaced. The annual 'Unit 42 IoT Threat Report' released by the cybersecurity research team from Palo Alto Networks, Unit 42 was a big wakeup call for US legislators. The March 2020 publication dramatically illustrated the seriousness of the cybersecurity threat posed by IoT devices. This is because operating systems and protocols are often either obsolete or have not been properly updated, and 98% of all data transferred between IoT devices and networks is unencrypted. To ensure that solutions to don’t go the same way as our new year’s resolutions, the budget authority OMB will be monitoring the implementation of the legal regulations soon after the law goes into effect. If a supplier and its subsidiaries intend to work for a federal authority, they will also be required to provide information about security vulnerabilities and how they have been closed.

Hopefully, as many manufacturers, service providers and users as possible will finally begin paying more attention the security of IoT devices.

Read more:

https://dl.acm.org/doi/10.1145/3384419.3430781
https://www.tagesanzeiger.ch/vorsicht-der-staubsauger-hoert-mit-234979732541
https://www.heise.de/news/IoT-Gesetz-zwingt-US-Behoerden-zu-mehr-IT-Sicherheit-4972510.html
https://start.paloaltonetworks.com/unit-42-iot-threat-report

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

The SWITCH security report discusses current topics in the field of cybersecurity. It is aimed at interested internet users and seeks to make them aware of current threats. Despite careful review, SWITCH accepts no liability for accuracy.