I. Ransomware – the new normal of digital extortion

Kidnapping someone and holding them hostage in order to demand a ransom in return for not injuring or killing them – this reprehensible extortion method has been a favourite among violent criminals since time immemorial. Although the act of holding data hostage with the help of ransomware may seem less brutal – even if only at first glance – it is becoming the biggest threat to the ICT infrastructures of companies, organisations and, sadly, hospitals too. Hence, ‘at first glance’.

In a recent case, a ransomware attack on the University Hospital Düsseldorf led to the death of a patient. Because of the disruption to the IT systems, she had to be taken to a hospital further away instead of the university hospital’s A&E department, and later died. The public prosecutor’s office is therefore investigating not only the cyber attack itself but also the possibility of a manslaughter charge for the woman’s death.

The gang behind the attack, apparently based in Russia, operates with the same level of professionalism and brutality as the Emotet criminals we reported on in the last Security Newsletter. It vigorously attacks companies and institutions with ransomware called
‘DoppelPaymer’ and demands a ransom based on the victim’s importance and financial status. And like the Emotet data kidnappers, the DoppelPaymer gangsters also adopt a time-based, double-pronged attack strategy. In the case of the University Hospital Düsseldorf, they appear to have placed a backdoor immediately after the Citrix vulnerability known as ‘Shitrix’ was discovered at the start of the year. This backdoor also went unnoticed when the University Hospital had all of its systems checked after the patch. The cyber criminals then reloaded Paymer at the start of September and encrypted the systems.

The irony of it all is that the perpetrators had actually intended to attack the University of Düsseldorf, not the University Hospital. They had even sent a digital extortion letter to the university. As soon as they were made aware of their mistake, they gave the police a digital key. Nevertheless, the University Hospital’s systems were still not fully functional at the end of September.

According to statistics from Temple University in Philadelphia (itself the victim of a hack in August 2019), ransomware attacks are at an all-time high, with the number of reported cases rising from just two in 2013 to 241 in the first three quarters of 2020. Similarly, data collected by the security specialist Acronis shows that the number of cyber attacks in the first quarter of 2020 was up by around one-third compared to the fourth quarter of 2019. Acronis also reported a huge increase in ransomware attacks by the groups Emotet, DoppelPaymer, Maze and Sodinokibi.

Even more worryingly, it was found that data is no longer just being encrypted and then released after the demanded funds have been paid, as is the case with a ransom attack. Data breaches are becoming more common too. With this form of attack, the perpetrators steal sensitive data (e.g. patient records, calculations, security codes) and demand hush money for not publishing it. Recent victims of data breaches include the Swiss train manufacturer Stadler, which was targeted in May 2020. The cyber extortionists also use the stolen data to blackmail customers and suppliers of their immediate victims.

But those on the wrong end of an attack don’t just suffer at the hands of the hackers – anyone tempted to pay the ransom in order to quickly regain control of their systems might also find themselves in hot water with the US government. This is because payments of any kind and for any reason to countries on the sanctions list of the Office of Foreign Assets Control (OFAC) are seen as sanction violations and subject to heavy fines.

So, what can be done? The security platform digitalguardian.com has compiled a compact list of measures, the most important of which are listed here. It all starts with the 3A! strategy that we recommend time and again: Awareness! Awareness! Awareness! In addition to being more aware ourselves, we also need to raise awareness of hacking, phishing and smishing (see topic III) among employees. digitalguardian has created a helpful infographic for this purpose, which
can be viewed via the penultimate link below. The full list of protective measures is as follows:

- **Back-ups:** regular, frequent, careful and physically separated from your network.
- **Principle of least privilege:** configure employee accounts with only the access privileges required for their job roles.
- **Updates:** regular, preferably automated.
- **Disable any features that aren’t needed in software applications.**
- **Ransom payments:** only if absolutely necessary, and always in consultation with the authorities.

Hardware and software protection solutions should be considered in addition. Note here that your Active Directory also needs special protection, as it gives hackers direct access to network resources, user accounts and access privileges – the promised land and a real goldmine for cyber attackers. And let’s face it: if you kept any treasure at home, you’d also protect it extremely well, wouldn’t you?

Read more:

https://www.securityweek.com/university-project-tracks-ransomware-attacks-critical-infrastructure
https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001
https://digitalguardian.com/blog/dont-get-hooked-how-recognize-and-avoid-phishing-attacks-infographic
https://www.heise.de/select/n/2020/10/2007210021036488235

II. A murky supply chain – how hackers profited from Cumulus data

A multi-tier supply chain might start with the manufacturer, extend to wholesalers and retailers, and end with the customer. This concept is nothing new and is widespread in the real economy. In May, it was revealed that customer data from the Cumulus loyalty points programme of Swiss retail giant Migros had been stolen and misused by hackers. The attack revealed a very different kind of multi-tier supply chain, extending from highly skilled and technically sophisticated ‘premium hackers’ to less well-equipped groups of cyber criminals.

With a targeted cyber attack, a group of Polish cyber criminals called ‘InfinityBlack’ hacked into the accounts of Cumulus customers, then sold the customer IDs to other criminals via an online platform. These criminals then redeemed the Cumulus loyalty points for electrical goods, resulting in total losses of CHF 53,000. If not for the rapid and successful intervention of the Vaud cantonal police in cooperation with Europol, the total damage would have been much
higher. This is because, during the course of arresting the InfinityBlack hackers, the investigators discovered more than 170 million records from other Swiss loyalty programmes in their databases. According to the investigators, the potential damage would have amounted to around CHF 642,000 if full use had been made of the stolen data.

Read more:
https://www.tagesanzeiger.ch/hacker-pluendern-schweizer-cumulus-kunden-68857470648

III. Smisherman’s Friends – a new wave of smishing attacks is washing over Europe and Switzerland

‘Mobile first’ has established itself as a priority-based development strategy for operators of social media platforms and websites. Cyber criminals now appear to be jumping on the bandwagon too. Back in March 2020, ComputerWeekly.de warned of the serious threat to IT security posed by smishing, as both company-managed and personal mobile devices are far more vulnerable to smishing attacks than classic IT devices are to phishing emails.

The direct, instant and often casual nature of SMS messages on mobile phones and tablets makes it much harder for users to tell if they have fallen victim to a hack by fulfilling a request in the message to click on a link, reset their password or authenticate a login. According to a study by Gartner, almost half of all text messages are answered. Considering the fact that text messages are seen as much more important than emails (with an open rate as high as 98%, according to Gartner), it is clear why hackers are increasingly targeting mobile devices. The number and variety of attacks has risen sharply, as described in Computerwoche’s informative article (link below). An excellent technical overview is provided in the trustedsec.com incident walkthrough, available via the link below.

The security experts at Kaspersky had already warned of ‘Roaming Mantis’ back in 2018. The group of hackers behind the malware, which specialises in smishing, phishing and DNS hijacking, had originally only targeted the mobile devices of Asian users, but they are now causing trouble worldwide with a whole series of Android malware: MoqHao, FunkyBot, FakeSpy and FakeCop. In an update, securelist.com reports that Roaming Mantis has since become much more sophisticated. In particular, the malware is now considerably better at disguising itself and eluding tracking and discovery measures.

In Switzerland, smishers mainly rely on the postal service to carry out their cyber-criminal activities. For example, users are prompted to install a (fake) postal service app to track the delivery status of a parcel. The fake app then loads Android malware that steals SMS content
and contact details and uses the compromised mobile device as a spambot for further smishing campaigns. Another common modus operandi involves notifying people by SMS that a parcel delivery has been blocked and can only be completed if customs or delivery charges are paid. The corresponding link then takes the victim directly to a phishing page, where they are asked to enter their credit card details. If the SWITCH registry or other registrars become aware of such cases, they generally deactivate the domains involved within two to three days, as was done with hXXps://post-ch.[.]club, hXXps://my-post[.]top, hXXps://www.my-post[.]top, hXXps://m-post[.]top and hXXps://a-post[.]top, for example.

Read more:
https://www.computerwoche.de/a/wie-phishing-per-sms-funktioniert,3548969
https://www.trustedsec.com/blog/sms-phish-an-incident-walkthrough
https://www.kaspersky.com/blog/roaming-mantis-malware/22427
https://securelist.com/roaming-mantis-part-v/96250

This SWITCH security report was written by Dieter Brecheis and Michael Fuchs.

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.