I. Back and forth in the pipeline: hacking and rehacking the US fuel firm Colonial Pipeline with Ransomware as a Service

In the January/February 2021 security report, we highlighted the growing threat that cyberattacks posed to critical infrastructure. And it wasn’t long until an emergency situation confirmed this state of affairs. On 7 May, cyber extortionists brought one of the US’s largest fuel supply networks to a complete standstill: news of the Colonial Pipeline hack spread like wildfire through the global media landscape, establishing the feat as one of the most spectacular cyberattacks in recent history. Since nearly half of all fuel (gasoline, diesel, kerosene) consumed on the US east coast passes through the system, US President Joe Biden declared a state of emergency in the region two days after the hack. Images of people filling plastic bags and other inappropriate containers with gasoline forced the US Consumer Product Safety Commission into action, and it warned consumers about safe gasoline storage. Speculation of a state-motivated attack by Russian hackers was rife. Finally, the payment of 75 bitcoin (about USD 4.4 million at the cryptocurrency’s value at the time) put an end to the nightmare after eight days. Although cybersecurity firms and cyberdefence authorities strongly advise against paying ransoms, Joseph
Blount (Colonial Pipeline’s CEO) had ordered the payment because he believed it was not clear how much damage would have been done to the system as a whole. Unfortunately, both for Blount and Colonial Pipeline, what happened next only confirmed the official advice not to pay up. The multi-million dollar payment did not bring about the desired liberation. The decryption codes supplied were so ineffective that external security firms and US authorities had to be called in to reboot the systems.

‘DarkSide’, the extortion software used, is offered by the Russian hacker group of the same name as Ransomware as a Service on the dark web. The hackers took advantage of a weakened security situation caused by the coronavirus crisis and staff working from home, not to mention a serious defensive flaw in the pipeline operator’s security system. They apparently hacked into Colonial Pipeline’s systems using a leaked password obtained from the dark web using a VPN account that did not require two-factor authentication. Although the account itself was no longer in use, it was also not completely inoperable. Since it could still be used to establish a VPN connection, the blackmailers sneaked through this forgotten backdoor and encrypted the data in the accounting systems. Since about 2.5 million barrels (approx. 400 million litres) rush through the pipelines daily and are billed automatically, the operators were forced to stop deliveries and shut down the technical systems.

The DarkSide criminals also came under pressure too. Referred to in the media as state-commissioned terrorists, a statement by the group made it clear that it was not affiliated with any government agency and that it was not pursuing any sociopolitical or ideological goals. The only goal was to make money. It even closed the statement by promising to introduce a moderation process that would in future allow the group to check which companies its partners wanted to blackmail using the DarkSide ransomware in order to avoid social consequences.

Unimpressed by this ‘penitent and responsible business policy’, the FBI set about tracking both the extortionists and the ransom. On 7 June, the US Department of Justice announced that most of the ransom – 63.7 bitcoin at the current value of about USD 2.3 million – had been recovered. The sum is 85% of the ransom due to DarkSide customers; the Russian ransomware lenders, meanwhile, keep 15% for their services, according to the calculation made by Tom Robins of blockchain analytics firm Elliptic for the New York Times.

With a federal judge’s permission, the FBI had gained access to a bitcoin wallet through undisclosed means and seized the ransom money received there. The fact that the FBI managed to penetrate the blockchain, which was previously believed to be anonymous, decentralised and tamper-proof, and hack at least some accounts caused the price of bitcoin to plummet 12.5% after the Department of Justice’s press conference. For their part, the FBI and the Department of Justice both called on companies to seek cooperation as soon as possible if they fall victim to a cyberattack.
II. Meat and greed – the world’s largest meat processing company pays a hefty USD 11 million ransom after a ransomware attack

JBS, the global Brazil-based meat processing company, is likely to comply with the above call for cooperation with the FBI. The world’s largest provider is responsible for a quarter of beef production and a fifth of pork production in the US. Following a ransomware attack in early June, all of the group’s US, Canadian and Australian plants were initially shut down. JBS employs more than 250,000 people in 190 countries. As was the case with the Colonial Pipeline hack, the FBI has accused Russian cybercriminals of being the perpetrators. Without actually naming the group, the FBI warned that it was one of the ‘one of the most specialised and sophisticated in the world’. From this statement, Bloomberg concluded that REvil/Sodinokibi, a Russian hacker group, was behind the attack. REvil had boasted on a dark web blog that it had obtained blueprints of Apple’s latest products after a break-in at a Taiwanese Apple supplier’s systems.

Shortly after the attack, JBS stressed that plants in other countries – and the company’s backup servers – were unaffected. Andre Nogueira, CEO of JBS USA, was confident that the systems could be restored from backups. After all, JBS employs more than 850 IT specialists and spends USD 200 million annually on its IT equipment.

But on 9 June, Nogueira was forced to admit that the group had paid a ransom of USD 11 million in bitcoin. The extortionists had apparently done more than just encrypt data that JBS could recover. JBS not only had to deal with the fact that data had been encrypted on its servers, but also with the fact that the blackmailers had stolen it and threatened to publish it.

The growing number of attacks by Russian hackers on important US facilities and companies that provide basic services have security and foreign policy officials in both countries on edge. On 16 June, they will also be the subject of talks between Russian President Vladimir Putin and US President Joe Biden in Geneva.
III. When Android devices catch the flu: FluBot, the banking trojan, spreads to Android devices

It started out in Spain, Hungary and Poland, and has an active presence in a growing number of countries. It is finding its way onto more and more Android devices and goes by three different names. But its mode of attack is always smishing (phishing with text messages) – and it’s spreading at an alarming rate: FluBot (also known as Cabassous and FakeChat) is a highly dangerous banking trojan that is wreaking criminal havoc mainly in Germany, but also popping up in Switzerland, Italy and other countries around the world.

FluBot’s ingenious infection mechanism is the reason why it is spreading so swiftly. Users of Android devices receive a text message about a pending package delivery and are prompted to track or manage it by clicking on the link to a package delivery company’s fake app. This does not come from Google’s Play Store, but is activated by means of sideloading (which is why FluBot doesn’t work on Apple’s iOS devices, since the app would have to be downloaded from the App Store). The sender and the link can both vary. Although the FluBot criminals started out by using familiar brands such as FedEx, UPS or DHL Express, they are increasingly using fakes that spoof the national postal service.

Once loaded, the app asks users to activate the accessibility service. At this point, the app poses a triple threat, because the FluBot backers can control the device as a normal user would.

1) The accessibility service automatically allows reloading of other programs (even malware).
2) It stops the fake app from simply being deleted.
3) It allows FluBot to observe and even override all user actions on the compromised device.

And what makes this malware particularly nasty is the fact that the user can no longer access the app installed by FluBot. Instead, they receive a message telling them that installation has failed. Nevertheless, the malware extracts names and phone numbers of the user’s contacts, as well as their text messages, bank details and other private information. It can also execute other commands, such as making calls, listening to messages, accessing the internet or sending smishing texts. Even ones that spread FluBot further.

Read more:
https://www.tagesanzeiger.ch/arnee-meldet-sicherheitsluecken-bei-lernplattform-792963574253
https://www.spiegel.de/netzwelt/netzpolitik/fleischkonzerne-jbs-zahlte-cyberkriminalen-elf-milionen-dollar-loesegeld-a-c7c6357c-6b2e-42cf-ba24-1af135f571b
https://www.nzz.ch/technologie/ransomware-angriffe-fleischproduzent-jbs-bezahlte-11-milionen-dollar-an-erpresser-l1h.1628409
SWITCH-CERT customers can download a PDF file that shows the steps required to stop the spread of Android malware and limit the damage if devices are already infected.

Read more:
https://blog.f-secure.com/flubot-android-malware
https://www.ncsc.gov.uk/guidance/flubot-guidance-for-text-message-scam
Android Flubot Factsheet v20-20210601_165309.pdf, please request from SWITCH

IV. Russian cyber spies attack government and NGO networks

Russian president Vladimir Putin likes to come across as a masculine, outdoorsy type doing manly outdoor activities such as hunting and fishing. When Russian cyber spies phish in the networks of western authorities or global NGOs, they usually do so undercover rather than outdoors. Although Russia’s official stance is to vehemently deny any responsibility for such attacks, Tom Burt (Microsoft’s Corporate Vice President, Customer Security & Trust) warned in a blog post in late May that Russian cyber spies had launched a large-scale phishing raid on more than 3,000 email addresses of more than 150 NGOs, think-tanks and government agencies. Most of these are based in the US, but targets have also been identified in another 24 countries. The attack was also confirmed by cybersecurity firm Volexity, based in Reston, near Washington, DC.

Russian cyber spies from the Nobellium group – which had attacked the US software company SolarWinds a year earlier in ‘the largest and most sophisticated attack the world has ever seen’ (quote from Microsoft President Brad Smith) – were responsible for the attacks. In December 2020, cybersecurity experts reported that the systems of Texas IT firm SolarWinds had been hacked. Its Orion software is used by more than 33,000 customers to manage IT systems, including government agencies, such as the US Department of Homeland Security and the US Department of the Treasury, not to mention flagship companies with huge customer bases, such as Microsoft. Flying under the radar for months, Nobellium had infected Orion updates with spyware that installed a backdoor for Nobellium’s espionage activities when the updates were delivered to customers’ servers. According to a former Department of Homeland Security chief, it could take years before all the infected networks are secure again.

Nobellium apparently didn’t want to wait that long, because it launched a new wave of attacks that targeted, among others, NGOs critical of the Russian government. The hackers gained access to the mailing list of aid organisation USAID and used it to send authentic-looking phishing emails containing a link. If the link is clicked, the malware installs a backdoor on the corresponding device, enabling a wide range of cybercriminal activities (see the second Microsoft link below for the technical details).

Microsoft’s Tom Burt believes that Nobellium’s new attack is disturbing for three reasons.
First, according to Burt, both attacks taken together show that Nobelium is attacking trusted technology companies or institutions in order to use their products (software updates) or their contacts (mass emails) to undermine that trust and maximise the effectiveness of their cyberespionage operations.

Second, Nobelium’s activities and those of similar players demonstrate that they tend to launch attacks against organisations abroad, but which are directly related to issues in the countries in which the attackers are based. Burt concludes that these groups are very close to state agencies and is calling for…

…third, clear rules governing nation-state conduct in cyberspace. Burt suggests that the Paris Call for Trust and Security in Cyberspace and the recommendations of the Cybersecurity Tech Accord and the CyberPeace Institute should be followed.

To quote the last line in Chris Rea’s song ‘Gone Fishing’: May as well go fishing… Here’s hoping that the husky-voiced singer is wrong for once.

Read more:
https://blogs.microsoft.com/on-the-issues/2021/05/27/nobelium-cyberattack-nativezone-solarwinds

---

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.