SIM2K
Adapting Technology to Your Business Needs

8•20
Information you can use

SIMformation

Deepfake Ransomware

Forward-looking security experts see some futures they dread and, frankly, would rather un-see. This is because, in the underground market and forums, there is sustained interest in ransomware and the surprisingly cheap offerings of deepfake services to match every cyber miscreant's campaign of choice. Mash them together and what do you have? Deepfake ransomware.

News about ransomware continues to be relevant, especially for businesses, its consistent targets. It seems that organizations of all sizes cannot cope, especially now that perimeters have been essentially decimated by remote work. And cybercrime gangs don't keep using the same malicious tools for long. Most of the time, these tools evolve in time and with the crime.

So what is "Deepfake Ransomware?" Deepfakes are the manipulation of media such as still images and/or videos accompanied by voice, using artificial intelligence (AI), resulting in a believable composite that is challenging to the naked eye and/or software. Ransomware is malware that holds the victim's files hostage, either by encrypting important files or locking victims out of certain computer features to prevent them from performing remediation steps, until a ransom is paid.

Combining these two leads to deepfake tech can be used in ransomware campaigns or vice versa. This is feasible, albeit a bit of a mindbender. One security expert, who dubbed this as "RansomFake" a "type of malicious software that automatically generates fake video, which shows the victim performing an incriminatory or intimate action and threatens to distribute it unless a ransom is paid." The cybercriminal behind such a campaign would offer their targets the option to permanently delete the video file after payment is received. In more risque applications, a recent report from Trend Micro reveals that there is great interest in how deepfakes could be used for sextortion or for bypassing authentication protocols that rely on image verification when using certain sites, such as dating sites. This report also considers deepfake ransomware an emerging threat because it takes extortion-based ransomware to the next level.

Deepfake ransomware could also happen this way: A threat actor creates deepfake video of their target. Takes screenshots of this video and, pretending to be a legitimate contact of their target, sends them the screenshots and a link to the supposed video that they can watch themselves if they are in doubt.

Curious and perhaps half-convinced, half-scared, the target then clicks the link, gets redirected to the short clip of themselves in a compromising state and all the while, ransomware is being downloaded onto their system. Or, the link may not lead to a purported video after all but to the auto-downloading and execution of a ransomware file. Remember that deepfakes cannot just manipulate videos and voices but still images as well.

Thankfully, this level of extortion hasn't been seen in the wild (yet). Nonetheless, the potential for this campaign to destroy a target's reputation is exceedingly high. It doesn't really matter whether a video of someone is real or doctored to look real. As humans, we tend to believe what we see, because if you can't trust your own eyes, what can you trust?

Is there a way to protect against deepfake ransomware?

For this particular campaign, patching software for vulnerability holes is not needed – although you should be doing this religiously anyway.

A way to counter deepfake ransomware is at the beginning: Do not give cybercriminals the material they need to create something destructive and hold you responsible for. By this we mean watch what you post on social media in general: selfies, group pictures, TikTok videos, and other images are all up for grabs. You should think long and hard about who you're sharing your content with and where.

Do an audit of your current photos and videos online and who has access to them. Weed out public-facing photos as much as you can or set them to be viewed by certain groups in your pool of contacts. If they're not photos you posted yourself, simply un-tag yourself, or ask your contact to take them down.

When it comes to dealing with messages from people within your network, whether you personally know them or not, if you have other means to reach out to them other than social media platform, do so to verify two things: [a] Are they the person you're really talking to?, and [b] If they are, did they actually send you those private messages about a purported video of you floating around the web that they found somewhere?

Furthermore, always be suspect of links, especially those purportedly sent by someone you know. Here's the thing: people are less likely to believe a stranger who is just "being nice" than someone they may know personally and is concerned about them. Cybercriminals know this, too. And they will do whatever they can to make you believe the scam they're attempting to pull on you.

The "bad guys" are always attempting to stay one step ahead of the security experts in technology, and sometimes the best security practice is to stay vigilant as to your digital practices. Anything that looks out of the ordinary, or mysterious shipping notices for goods you have not ordered, should always raise your alarm level to the "do not click" status. SIM2K offers training for your employees on looking out for suspect messages and ways to up your security. Call us for details.

Laptop Shortage Hits Schools

Schools across the United States are facing shortages and long delays, of up to several months, in getting this year's most crucial back-to-school supplies: the laptops and other equipment needed for online learning.

The world's three biggest computer companies, Lenovo, HP and Dell, have told school districts they have a shortage of nearly 5 million laptops according to interviews with over two dozen U.S. schools, districts in 15 states, suppliers, computer companies and industry analysts.

As the school year begins virtually in many places because of the coronavirus, educators nationwide worry that computer shortfalls will compound the inequities — and the headaches for students, families and teachers. "You can't have a kid do distance learning without a computer," said the superintendent of a California school district, which was set to order 5,000 Lenovo Chromebooks in July when the vendor called them off, saying Lenovos were getting held up from a missing component from China, so the district switched to HPs and was told they would arrive in time for the first day of school Aug. 26. The delivery date then changed to September, then October.

Chromebooks and other low-cost PCs are the computers of choice for most budget-strapped schools. The delays started in the spring and intensified because of high demand and disruptions of supply chains. Then came the Administration's July 20 announcement targeting Chinese companies it says were implicated in human rights abuses. The Commerce Department imposed sanctions on 11 Chinese companies, including some Lenovo suppliers, which the company says will add several weeks to existing delays. School districts are asking the Trump administration to resolve the issue, saying that distance learning without laptops will amount to no learning for some of the country's most vulnerable students.

A Lenovo official told California's Department of Education the company has a backlog of more than 3 million Chromebooks. There are no nationwide tallies on the numbers of laptops and other devices that schools are waiting for. The Associated Press found that some of America's biggest school districts are among those with outstanding orders of Chromebooks. Smaller districts in Montana, New York, Indiana, Maryland, Ohio, New Hampshire and elsewhere are also waiting on laptop orders, with delivery dates that have become moving targets.

The shortage stems from exceptionally high demand at a time when the personal computer industry is still recovering from pandemic-driven precautions that shut down the factories of major PC suppliers in China during February and March. Just as the supply chain started ramping back up, new orders poured in from huge companies and government agencies with large numbers of employees working from home – in addition to school districts scrambling to secure machines, according to Gartner Research. To make matters worse, many school districts underestimated their needs during spring ordering, assuming that traditional in-person classes would resume in the fall. With so many customers ordering laptops at the same time, PC manufacturers may be put in the uncomfortable position of deciding who gets them first. Those kind of pecking orders threaten to push small school districts to the back of the laptop line.

Google Fi Wireless Service

Google Fi may sound like some weird sort of ritual – "he's been Googlefied!"— but it is actually a Google-owned wireless service can both save you money and step up your smartphone security situation. It is different that traditional wireless plans, and might not be for everyone, but has some interesting twists.

Google Fi is technically an MVNO, or mobile virtual network operator, an entity that provides wireless service without actually owning the network infrastructure behind it. In other words, it doesn't have its own network like AT&T or Verizon; instead, it has an arrangement with those same sorts of carriers that allows it to tap into their networks and repackage access to their service under its own brand and arrangement.

In the U.S., Fi uses a combination of T-Mobile and U.S. Cellular. That's one of its distinguishing features, in fact: When you use Google Fi with a phone that's designed for the service, it's able to seamlessly switch you between those networks based on which one has the strongest service at any given moment. You won't be aware that it's happening. Your phone just shows that you're connected to Google Fi, but behind the scenes, the device continuously seeks out the best possible network for your location and bops you around as needed.

Google Fi also incorporates public Wi-Fi networks into its coverage, provided you're using a phone designed for Fi use. And like mobile networks, this switch occurs automatically. Anytime you're in range of a publicly available Wi-Fi network that Google has determined to be "high-quality and reliable" your Fi phone will switch over to that instead of using your regular mobile network. You'll see it happen in retail establishments with open Wi-Fi networks or anywhere else that has Wi-Fi available without the need for any sort of sign-in.

What is nice is that Fi automatically encrypts your data anytime it's connected to a network in that manner, using a special Google-provided virtual private network (VPN) — which means no one else on the network could monitor your connection and see what you're doing as is often the risk when using public wi-fi.

Compatible phones include Google's own Pixel devices. You can, however, also use Fi with most other reasonably recent Android phones or even iPhones. As long as a device is unlocked and compatible with T-Mobile's network, it should work on Fi — at least, from a technical perspective. This service is currently only available in the US. For an individual user, Fi charges you $20 a month for basic service, which gives you unlimited calling and texting. On top of that, you pay $10 for every gigabyte of mobile data you use each month — or whatever percentage of that number ends up being relevant, all the way down to the third decimal. So if, for instance, you used 2.202GB of mobile data in a month, you'd pay $22.02. And, you pay only for the amount of mobile data you actually use. You can find details at www.fi.google.com.

SIMformation is the monthly newsletter from SIM2K. Information presented here is designed to inform you of trends in the business world affecting information technology. For questions or comments, write SIM2K, 6330 E. 75th St., Suite 336, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Be Aware of these Scams

We live in an app-based world. From laptops to smart TVs, applications are used nearly everywhere. Learning which apps are safe can be tricky as cybercriminals continue to find new ways to exploit your trust.

The latest scam involves third-party apps that request unusual permissions. Users are easily fooled into downloading these third-party apps because they are registered on legitimate app stores and are designed to work in conjunction with popular products such as Microsoft OneNote or GSuite. The app is pretty harmless on its own, but shortly after downloading it you'll receive an e-mail related to this app, and the email includes a phishing link. If you click this link, it will cause the third-party application to request special permissions such as the ability to read and write to files on your behalf. If you grant the app these permissions, you'll give the bad guys unlimited access to your sensitive information.

Don't fall victim to this scam! Remember the following:

- Never click on a link within an email that you weren't expecting.
- Only download apps from trusted publishers. Remember, anyone can make an application and scammers can use any image, text, or logo to make the app seem legitimate.
- When using a work device, reach out to your IT department before downloading new apps or granting app permissions. They can decide if the application is legitimate and safe to use.

Sneaky "Service Desk" Scam

A new phishing attack is using a number of tactics to trick unsuspecting users into handing over their login credentials. The e-mail claims you have unread e-mails due to your cloud storage being full. It then gives you options to resolve the issue. Clicking on either link sends you to a phony login page for your service provider. And any information on this page will be sent directly to the scammers.

What makes this scam so sneaky? First, the phony log-in page not only looks official, but also functions like a real login page. Only passwords that meet real requirements are accepted. If an acceptable password is entered, you are redirected to the actual website of the service provider you just provided credentials for. Second, the e-mail is sent from a no-reply address using the domain "servicedesk.com". Most of us are used to seeing e-mails from support desks, which makes this sender feel legitimate. Third, the e-mail itself bypasses security filters that you may have in place by using a combination of factors that makes your e-mail security filters think the link is secure.

Don't be fooled! Remember these tips:

- Phishing e-mails are often designed to create a sense of urgency, in this case, the idea that you're missing important e-mails. Think before you click, the bad guys rely on impulsive clicks.
- E-mail security filters can only do so much to protect your sensitive information. Stay alert and help create a human firewall for your organization.
- When an e-mail asks you to log in to an account or online service, log in to your account through your browser and not by clicking the link in the e-mail. That way, you can ensure you're logging into the real website and not a phony look-a-like.

"Random Tid-Bytes"

Covid-19 May Delay 5g iPhone

While announcing flat revenues, Qualcomm has managed to maintain its business during the pandemic. But the company has warned fourth-quarter guidance might be impacted by a delayed product launch. "Our guidance for the fourth quarter of fiscal 2020 includes an impact attributable to a planning assumption of an approximate 15% year-over-year reduction in handset shipments due to COVID-19, including a partial impact from the delay of a global 5G flagship phone launch," a spokesman said. It is not certain that it is Apple being referenced, but it remains a major Qualcomm customer and is expected to install Qualcomm's 5G radios inside the iPhone 12. So if a customer has a delayed product launch and that deal is enough to reduce earnings by 15% then it has to be a major hardware manufacturer. And there just aren't that many around manufacturing product at that kind of scale.

Microsoft Torpedoes Outlook

If you run Outlook on Windows, you probably couldn't get it to work for about four hours on July 15. There has been a lot of internal finger-pointing inside Microsoft, but it looks like the problem stemmed from a bad fix made to Microsoft's servers. Hard to believe a crippling bug like that could roll into production without raising an alarm somewhere, but it happened. Microsoft built some fancy new checking mechanism into the more recent versions of Windows-based Outlook. It was working just fine until… somebody changed something on Microsoft's servers. Oops – no more Outlook. Many folks discovered that they could use a browser and just log into their account at outlook.com – the problem was with the Windows-based version of Outlook. Microsoft fixed the bug four hours later by updating its servers.

Smishing Attacks

E-mails are a quick and easy way for cybercriminals to phish for your information—but it's not their only tool. Smishing, or SMS Phishing, is another way the bad guys try to trick you. Many of us are used to receiving legitimate promotions, reminders, and security notifications via text message. These messages—both real and fake—are brief and often include links, so it can be difficult to spot a smishing attempt. One recent example involves scammers posing as your local postal service while sending malicious text messages as part of their smishing attack. The message claims that you have a package waiting for pick up, but to see more information you must click the link in the text. If you click the link, you're taken to a phony verification page. Here, you're asked to enter your banking information in order to verify your identity. If you provide any information on this page, your data is sent directly to the cybercriminals – giving them full access to your bank account. Keep the safety guidelines in mind – are you expecting a package? Don't click on a link in an e-mail or text – enter the shipper's website by typing in the address yourself in your browser. Or, call your local post office and just ask. E-mail scams are bad enough, let alone now branching out into text messaging as well.

Do Chromebooks Need Extra Security?

Yes! Google recently removed 106 malicious apps from the Play store that would seek out personal information on your device. So don't believe the hype that Chromebooks are secure "as-is" and add extra anti-virus and spyware protection. Call SIM2K for help.

The FBI Weighs in on Windows 7

The Federal Bureau of Investigation has sent a private industry notification (PIN) to partners in the US private sector about the dangers of continuing to use Windows 7 after the operating system reached its official end-of-life (EOL) earlier this year.

"The FBI has observed cyber criminals targeting computer network infrastructure after an operating system achieves end of life status," the agency said. "Continuing to use Windows 7 within an enterprise may provide cybercriminals access in to computer systems. As time passes, Windows 7 becomes more vulnerable to exploitation due to lack of security updates and new vulnerabilities discovered. With fewer customers able to maintain a patched Windows 7 system after its end of life, cybercriminals will continue to view Windows 7 as a soft target," the FBI warned.

The Bureau is now asking companies to look into upgrading their workstations to newer versions of the Windows operating system. However, in some cases, the PC's underlying hardware may not support the upgrade to a much more powerful system like Windows 10, a challenge that the FBI acknowledged in its alert, citing costs that companies might need to support to buy new hardware and software. "However, these challenges do not outweigh the loss of intellectual property and threats to an organization," the FBI said – suggesting that companies should keep an eye on the bigger picture down the road and how future losses from possible hacks might easily outweigh today's upgrade costs.

The agency specifically cited the previous Windows XP migration debacle as the perfect example of why companies should migrate systems as soon as possible, rather than delay. "Increased compromises have been observed in the healthcare industry when an operating system has achieved end of life status. After the Windows XP end of life on 28 April 2014, the healthcare industry saw a large increase of exposed records the following year," the FBI said.

Furthermore, the FBI also cited several powerful Windows 7 vulnerabilities that have been frequently weaponized over the past few years. This includes the EternalBlue exploit (used in the original WannaCry and by multiple subsequent crypto-mining operations, financial crime gangs, and ransomware gangs) and the BlueKeep exploit (which allows attackers to break into Windows 7 devices that have their RDP endpoint enabled).

The agency said that despite the presence of patches for these issues, companies have failed to patch impacted systems. In this case, replacing older and abandoned systems may be the best solution overall.

While companies are looking into upgrading systems, the FBI recommends that they also look into:

- Ensuring anti-virus, spam filters, and firewalls are up to date, properly configured, and secure.
- Auditing network configurations and isolate computer systems that cannot be updated.
- Auditing your network for systems using RDP, closing unused RDP ports, applying two-factor authentication wherever possible, and logging RDP login attempts.

Even for organizations that have pushed towards upgrading their PC environment from Windows 7 to Windows 10, there is still the potential that there could be some Windows 7 devices left lurking on the network – and it could be a good idea for companies who have upgraded their architecture to double-check something hasn't been missed.

Devices ranging from laptops users have brought from home to things like marketing kiosks and virtual billboards could all potentially be running on Windows 7 and could all have potentially been missed in initial examinations of the network.

Businesses should ensure they really do know what's on their networks – because with Windows 7 out-of-support, hackers will be looking for any unsupported and unpatched device they can take advantage of as an entry point into the network.

In addition to Windows 7, Windows Server 2008 and 2008 R2 also reached their end of support lifecycle at the beginning of 2020. Microsoft is no longer providing free security updates on premises, non-security updates, free support options and online technical content updates. While users can continue to use these products, they will also be vulnerable to data breaches and other cybersecurity threats.

If you are unsure as to the status of the PCs on your company network, please call SIM2K and we can conduct an audit of all devices that connect to your network and make recommendations as to security and necessary upgrades to protect your business information.

SIM2K
6330 E 75th St., Suite 336
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com