SIM2K
Adapting Technology to Your Business Needs

1•21
Information you can use

SIMformation

Microsoft Steps in to Halt SolarWinds Hack

Microsoft took a series of dramatic steps against the recent SolarWinds supply chain attack. Through four steps over four days, Microsoft flexed the muscle of its legal team and its control of the Windows operating system to nearly obliterate the actions of some of the most sophisticated offensive hackers out there. In this case, the adversary is believed to be APT29, aka Cozy Bear, the group many believe to be associated with Russian intelligence, and best known for carrying out the 2016 hack against the Democratic National Committee (DNC).

While details are continuing to emerge, the SolarWinds supply chain attack is already the most significant attack in recent memory. According to SolarWinds, Microsoft, FireEye, and the Cybersecurity and Infrastructure Security Agency (CISA) the attackers compromised a server used to build updates for the SolarWinds Orion Platform, a product used for IT infrastructure management. The attackers used this compromised build server to insert backdoor malware into the product (called Solorigate by Microsoft or SUNBURST by FireEye).

According to SolarWinds, this malware was present as a Trojan horse in updates from March through June 2020. This means any customers who downloaded the Trojaned updates also got the malware. While not all customers who got the malware have seen it used for attacks, it has been leveraged for broader attacks against the networks of some strategically critical and sensitive organizations.

Those attacked include FireEye, the US Treasury Department, the US Department of Commerce’s National Telecommunications and Information Administration (NTIA), the Department of Health’s National Institutes of Health (NIH), the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Homeland Security (DHS), and the US Department of State.

Microsoft did four things over the course of four days that effectively undid the work of the attackers.

1) On Dec. 13, the day this became public, Microsoft announced that it removed the digital certificates that the Trojaned files used. These digital certificates allowed Microsoft Windows systems to believe that those compromised files were trustworthy. In this single act, Microsoft literally overnight told all Windows systems to stop trusting those compromised files which could stop them from being used.

2) That same day, Microsoft announced that it was updating Windows Defender, the anti-malware capability built into Windows, to detect and alert if it found the Trojaned file on the system.

3) Next, on Tuesday, Dec. 15, Microsoft and others moved to “sinkhole” one of the domains that the malware uses for command and control. “Sinkholing” is a legal and technical tactic to deprive attackers of control over malware. In Sinkholing, an organization like Microsoft goes to court to wrest control of a domain being used for malicious purposes away from its current holder, the attacker. When successful, the organization can then use its ownership of that domain to sever the attacker’s control over the malware and the systems the malware controls. Sinkholed domains can also be used to help identify compromised systems: when the malware reaches out to the sinkholed domain for instructions, the new owners can identify those systems and attempt to locate and warn the owners.

4) Finally, on Wednesday, Dec. 16, Microsoft changed Windows Defender’s default action for Solorigate from “Alert” to “Quarantine,” a drastic action that could cause systems to crash but will effectively kill the malware when it finds it.

Taken together, these steps amount to Microsoft first neutralizing and then killing the malware while wresting control over the malware’s infrastructure from the attackers. By the end of these measures, the attackers were left with barely a fraction of the systems under their control.

Also, SolarWinds has been able to reverse engineer the malicious code injection source, allowing it to learn more about the tool. Their analysis suggests that the malware used multiple servers and mimicked legitimate network traffic to circumvent threat detection used by SolarWinds and other security companies. The Sunburst code appears to have been designed to proved the perpetrators a way to enter an IT environment and avoid firewalls an other scurity controls within the customer’s environment. While not able to specifically identify the source, it is understood to be a foreign nation-state. This analysis of the malware will enable SolarWinds to put in additional safeguards against its future use against their security products.

This hack is also changing how security companies approach malware – now moving more to an assumption that malware is already present within a system and attempting to ferret it out to stop it, rather than the traditional tools that are designed to stop it from entering a system. The sophistication of this attack shows that what was considered the “best defense” against malware can be circumvented and work undetected within the IT environment, prompting the shift in approach.

SIM2K sent out an advisory last month noting that while we do use some SolarWinds offerings, these compromised products are not part of our business model, and thus nothing we have employed should present a danger for any of our clients. But this event does show the dark side of the IT industry and the need to be vigilant against malware. SIM2K is dedicated to best practices to help your company harden your network and protect your data. Call us for any concern you have about your security profile.

Ransomware Attack – Again

Managed IT services provider NetGain Technologies was forced to take some of its data centers offline following a ransomware attack launched in late November. The company claims that it took down "a number" of its data centers as a protective measure in an effort to "contain this threat and restore services".

Although NetGain fell victim on November 24th, it was not until December 4th that the company started to e-mail clients, warning them that they may experience "system outages or slowdowns" due to the ransomware attack. Over the following weekend, the company started to shut down data centers in a bid to isolate the ransomware attack and rebuild affected systems.

In a missive to clients, the company added that it was "running tools and scans to detect, isolate, and clean-up any affected environments" alongside security specialists and experts in post-incident recovery that it had drafted in. However, it remains unable to give clients a firm estimate when it will be able to restore services. According to one of its customers, before bringing data centers back online NetGain needs to rebuild its domain controllers, and scan its networks. Then it will need to scan each individual server for malware or other anomalies.

The client added that the attack had targeted the data center operator's domain controllers, which manage networks of thousands of servers, but it also needs to make sure that the attackers have not got any further than that. Services began to be restored later the next week following scans, and after other security checks and security updates have been completed. More than 60 staff have been working around the clock to resolve the issue.

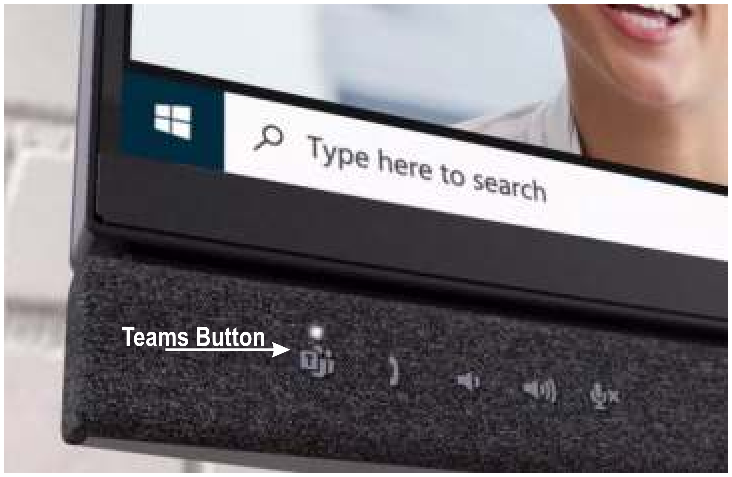
The NetGain compromise comes as ransomware attackers are starting to up their game with partnership platforms, and streamlining their attack tools to better evade detection. In addition, some have started to exfiltrate data from compromised systems before launching their attacks in order to give themselves extra leverage over their victims.
The attackers then threaten to release sensitive data if their ransom demands are not met. In some instances, companies have been taken down for a month or more.

At the end of December in 2019, global foreign exchange company Travelex was forced to take its systems down throughout January following a ransomware attack launched on New Year's Eve. Customers across the world with foreign exchange tied up in Travelex foreign currency cards were unable to access their cash as a result. Banks that relied upon Travelex to provide foreign exchange were forced to suspend the services. The company reportedly paid a ransom of $2.3 million to the attackers in a bid to restore their systems, but the one-two punch of the ransomware outbreak followed by the drastic reduction in global travel wrought by the global COVID-19 outbreak saw the company collapse into bankruptcy in August 2020.

Dell Monitors for Teams

Dell is launching three new monitors next month, and all of them come with a dedicated Microsoft Teams button. Dell claims it has created the "world's first video conferencing monitors certified for Microsoft Teams," after Microsoft started certifying displays, webcams, and headsets last year. Three monitors will be available next month, all offering quick access to Microsoft Teams.

The button will let Microsoft Teams users quickly launch the app to make and receive video calls. Hands-free commands will also be supported through Cortana and the built-in microphone.
This is the first time to place a Microsoft Teams button on a monitor, but headset manufacturers have been quick to add buttons that support Microsoft's communications app. New and existing headphones got deeper integration with Teams last year, just as usage of the app was soaring at the start of the pandemic.



The Teams button is the main surprise with these displays, but Dell's trio of videoconferencing monitors also have some useful specs designed for an era where remote work and video calling is key. Each includes a 5-megapixel pop-up infrared camera, which supports facial recognition with Windows Hello. Dell also bundles a noise-canceling microphone and dual 5-watt integrated speakers. There is even a built-in mode to reduce blue light emissions.

Dell is launching (R to L below) a 24-inch (FHD) version for $519.99, a 27-inch (QHD) model for $719.99, and a curved 34-inch (WQHD) variant for $1,149.99. All three will launch on February 16th.

SIM2K is a Dell Partner and we will be able to source these monitors (and any other Dell hardware) for those interested. Please call SIM2K for details or for ordering information.

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.

California Passes Tougher Privacy Act

In November, Californians approved a ballot measure, Proposition 24, a.k.a. the California Privacy Rights Act (CPRA), to create a new consumer data privacy agency. It puts California yet another step ahead of other states in terms of privacy productions for consumers – and data security requirements for enterprises. The CPRA toughens some requirements, brings California more in line with the GDPR (the European privacy law), and creates a new state agency – the California Privacy Protection Agency. Previously, the state's attorney general dealt with consumer privacy issues on top of all their other responsibilities. Data privacy now gets a dedicated agency with a $10 million basic budget, plus it will also get part of the fines and settlements it collects from companies that break the law. The law goes into effect on January 1, 2023 and enforcement will begin six months later giving companies two years to prepare.

A couple of aspects of CPRA will reduce companies' potential risks and liabilities. First, the current California privacy law applies to companies serving at least 50,000 California residents, households, or devices. The CPRA raises this to 100,000 and removes "devices" from that list. Businesses won't be held responsible for CPRA violations committed by third parties if certain agreements are in place and the business partner themselves is in compliance with CPRA. The new rules also prohibit businesses from retaining personal information "longer than absolutely necessary," which could be a problem, since when it comes to deleting data, companies believe that "some data is good, more data is better, all data is best." Data can be analyzed by machine learning and AI systems and can help companies develop new products, services, and applications, so a vague directive here is open to interpretation.

Another big change has to do with how consumers allow their information to be shared. Under the earlier law, companies had to offer California customers the opportunity to opt out of having their data sold to third parties. Now, that includes all kinds of sharing, not just sales. Another difference is that companies will have additional worries about data breaches. For example, breach liability now covers e-mail addresses when used in combination with a security question. If a data breach involves information about minors, the fines can be tripled. Another change is that consumers no longer must show that they were harmed by a breach.

Companies have already started seeing privacy-related lawsuits. Last month, children's clothing retailer Hanna Andersson agreed to a $400,000 settlement in response to a class-action lawsuit stemming from a 2019 data breach. Other companies that have already been sued under the old law include Salesforce, Walmart, online stationery retailer Minted, the Sunshine Behavioral Health Group, TikTok, Zoom, and Houseparty.

Experts believe this expanded law will hit small- and medium-sized companies harder, as they are not likely to have the resources to fight a legal battle as major companies can do. And, as California does, often the country follows, so we may see this act become the model for other states' to implement. If you collect customer data, be prepared to audit your practices to be sure you are in compliance.

"Random Tid-Bytes"

Time to Trash Flash

Although Adobe stopped serving updates for its Flash Player last month – and disabled the plug-in on Jan. 12 – Microsoft will be in charge of uninstalling the software from Windows PCs. Adobe recommends that users remove Flash from their personal computers to "help secure your system since Adobe does not intend to issue Flash Player updates or security patches after the End of Life date." But Microsoft has a plan to scrub Flash from all Windows 10 and Windows 8.1 PCs this year, a plan that doesn't rely on users taking action. Microsoft added the "Update for Removal of Adobe Flash Player" to the Microsoft Update Catalog on Oct 26. The update, also identified as KB4577586, permanently removes Adobe Flash Player as a component of the Windows OS devices. Users can select the appropriate-to-their-OS version of KB4577586, then download and apply it to their PC. Microsoft noted that the update removes only the Flash Player installed by Windows. "If you installed Adobe Flash Player manually from another source, it will not be removed," says the bulletin. This tool will be included in the monthly "Cumulative Updates" and "Monthly Rollups" from this point forward. In other words, KB4577586 will be automatically installed and activated, permanently removing Flash Player from the system. You may wish to check all your devices – work and home – to be sure Flash is trashed.

Android Users – Helpful Tip

Android's permission system has come a long way over the years, and with Android 10 and 11 in particular, Google has given a lot more control over how exactly apps are able to access sensitive areas of data. With Android 10, users gained the ability to give apps access to the users' physical location only when the app is actively being used instead of being "on" all the time, as previously had been the case. And, with Android 11, this has been expanded with a new option to allow an app access to your location, camera or microphone only on a limited, one-time basis (a single session) with that permission expiring as soon as you close the app. But in both of those cases, itis up to you to make sure you have your permissions set up the way you want – and that is pertinent particularly if you're using a phone that was upgraded to Android 10 or 11. In any upgrade-involving instance, any apps you might have installed before the upgrade would have been given regular, unrestricted permissions within the older Android environment – and thus would only be affected by the new options if you were to manually go in and revisit their settings. So, to check:

- Open the Privacy section of your system settings and tap the line labeled "Permission manager."
- Look through the various permissions listed there, paying particular attention to "Camera," "Location," and "Microphone" (especially if you have Android 10 or 11).
- As you tap each permission, see what apps have access to it. If you come across anything that doesn't seem like it needs access to a certain area – or maybe doesn't need full, ongoing access to it – tap its name and then adjust its permission setting as needed.

Plus, this is the time to undertake an app cleanse. First, it clears up clutter – both in terms of the space an app takes up on local storage and the visual space it requires on your home screens, where it makes harder for you to find the things you genuinely use and seek out regularly. Plus, having unused apps on your phone can slow your system or wear your battery down, as lots of apps run in the background at least some of the time and needlessly use up your phone's resources.

The Future of the Office

Ten months after the World Health Organization declared COVID-19 a global pandemic, triggering a worldwide shift to a work-from-home model, employers are trying to plan when and how to safely bring employees back into physical office spaces. With employee anxiety, social distancing regulations, and technology investments to consider, reopening offices could prove to be even more complex than shutting them down.

The COVID-19 vaccines now rolling out offer hope for reopening this year, but it could well be six months or more before they're available to most office workers. Even then, employers will have to continue using workplace health and safety measures developed during the pandemic to ensure that their employees feel safe and comfortable once they're back. Whether employers wait until all their workers are vaccinated or begin a staggered return-to-office strategy sooner, the time to make plans is now. And companies need to recognize that how employees think about the office has forever changed.

As one company executive said, "[Employers] can't think that the employees coming back to the office are the same workers that left them back in March. This is a different breed of employee; they have a different knowledge set and they have a different set of expectations."

The workplace of the future will likely be unrecognizable to the one people left back in March 2020, as businesses grapple with a number of key challenges: social distancing measures, protecting employee health, and minimizing the anxiety that returning to work might cause. Some of these challenges can be dealt with in a practical way. For example, small meeting rooms that don't allow employees to be socially distant will be closed off. Other challenges are much more complex, and this is where organizations will turn to technology for help.

When it comes to technology that will enable offices to reopen safely, organizations should take a cue from digitally forward factories and manufacturing plants where smart technology and internet of things (IoT) devices are already prevalent. Factories use IoT technologies on production lines to react to machine failures but also to pre-empt them. Smart cameras can act as both IoT sensors and processing platforms, with many now able to perform machine learning processes on the device itself. In an office setting or other public space, smart cameras can be used to monitor social distancing. Comanies can train the camera to understand what the distance should be and how far two people are standing from each other. If they then get too close, the camera issue an alert. The camera doesn't necessarily have to identify the people, but can simply trigger a warning to let management know there's been a breach of social distancing guidelines. Likewise, a camera could be used at a building entry to detect whether employees and visitors are wearing face masks. If it detects a person without a mask, it won't open the door.

Many companies are now looking for IoT-type solutions to assist with managing their workforce. To accommodate this growing need, some of the startups that produce industrial machine learning and predictive maintenance tools have now added technology aimed at non-manufacturing workplaces such as schools, hotels, offices, and other public spaces.

Without the right technology solutions in place, offices will struggle to reopen; however, that's not the only area of consideration for companies looking to fling open their doors. 'Returner anxiety' is a very real employee wellbeing issue that organizations need to be sensitive to. A May 2020 survey of UK workers found that 44% of respondents felt anxious about returning to an office, and 31% were concerned about having to commute to work.

As things currently stand, reopening offices does not mean every employee will suddenly be sitting at a desk the first week. A combination of social distancing guidelines and limited office floorspace means that we're likely to see the creation of the "hybrid office" where some employees choose to come in and are able to work seamlessly with those who remain remote. This will mean a continued emphasis on tools such as Zoom and Microsoft Teams that boost remote collaboration. A year ago, using these would have required explaining these collaborative working platforms to employees. Now it seems that everybody is an expert in Teams and Zoom.

In the short term, the hybrid office will mimic the way most people worked for the majority of 2020, except some colleagues on video calls might be sitting at their desk, six feet away from anyone else and wearing a face mask. In the longer term, a new "work from anywhere" culture will become the new normal, but companies will still need collaborative workspaces located close to major metropolitan areas. Although employees may spend most of their time working remotely, if they do need to be with the team or need access to enterprise-grade recording video and audio technology, they can quickly get to one of those local collaboration hubs.

One of the biggest challenges is going to be changing employers' preconceived notions around working. CEOs who have historically wanted to see people in the office to ensure productivity are going to have to adjust their mindset and understand that hard work is not directly linked to being physically present in an office. The experience of the "work at home" model has resulted in many organizations looking seriously at downsizing the amount of real estate they occupy.

But even if you only have two people in an office, a full health and safety assessment will need to be done. For companies that are considering reopening offices, decision makers might be feeling some anxiety about allocating resources to ensure a safe transition. Many companies report that employees are excited about what these changes might mean for the future of work – being empowered to work from anywhere. New York, for instance, has long had a cultural problem when it comes to remote working – there's a perception that if you're not in the office, you're slacking off. Now that is changing. People are excited about the fact that they can work from anywhere.

So if your office has been closed due to Covid-19, and you are considering bringing back employees, just don't throw open the doors and expect things to be like they were. IT can help to smooth the transition and provide new safeguards to make a more safe and secure environment for your employees in these stressful times.

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