SIM2K
Adapting Technology to Your Business Needs

8•21
Information you can use

SIMformation

Eskenazi Ransomware Attack

For months SIMformation has discussed ransomware attacks on companies around the globe. And maybe you were thinking, "We live in Indiana, nobody will target companies here in flyover country..." Well, the pigeons have come home to roost.

Eskenazi Health said an attempted ransomware attack caused the hospital to go on diversion August 4th. A hospital spokesperson said their monitoring systems functioned as they should have and proactively shut down their network.

At the time of the initial incident, a spokesperson said current monitoring indicates that no patient or employee data had been compromised. Hackers are going after U.S. hospitals with a fresh wave of cyberattacks this week just as coronavirus cases surge around the country.

For those not familiar with Eskenazi Health, it is a health-care service provider that operates a 315-bed hospital, inpatient facilities, and community health centers throughout Indianapolis. The network was crippled by a ransomware attack that began between 3:30 and 4 a.m., a spokesperson said. By 8 a.m. Eskenazi Health was turning ambulances away and diverting patients to other hospitals as a result of the ransomware incident.

"A ransomware attack happened," an Eskenazi spokesperson reported, confirming that all of Eskenazi Health's locations – its hospital, its inpatient facilities, and its community health centers – are impacted. The spokesperson added that Eskenazi Health was working to contain the ransomware by shutting down some services and operations in order to try to keep the malware from spreading through its systems.

"[We] took all of our systems down so they wouldn't get breached," the spokesperson said, confirming e-mail systems and electronic medical records were down for several days after the initial attack while mitigation efforts continued.

Three weeks after announcing that the hospital had experienced a cyber attack, Eskenazi Health is warning its employees, providers, current and former patients and vendors to monitor their financial accounts for suspicious action.

Now, nearly a month after the ransomware attack, while hospital officials initially said that they did not believe that any employee or patient information had been compromised in the attack, Eskenazi Health said that officials have subsequently learned that some data was "obtained by bad actors" and released online. Forensic experts have identified the files and are now examining them for any personal information. If the health network learns that anyone had information stolen, they said they will let those affected know and offer them protection and credit monitoring services, the release said. However, so far there is no evidence that the breach led to bank or credit card fraud. Eskenazi Health added that the hospital does not plan to make any payment to the cybercriminals and that its system worked as it should. The Federal Bureau of Investigation has been notified and is investigating the incident, hospital officials said.

While the hospital went on diversion for a days after the attack and some elective procedures were postponed, Eskenazi Health is currently open and operating. The health system's website is up and working but the website of the Marion County Public Health Department has been down in an incident related to the cyberattack. (Marion County's Health & Hospital Corporation oversees both entities.) Staff at the Marion County Public Health Department are prepared to take requests and assist with limited services such as birth certificates and immunization records, administrating vaccines, and responding to food and housing complaints by phone contact, but on-line activities are unavailable due to this attack.

Scott Shackelford, the Chair of Cyber Security Risk Management at IU, said this is a constantly evolving fight. "It's an arms race and both attackers and defenders are learning from each other in real-time," he said. "Unfortunately, it's still a lot easier to be an attacker than a defender. You only need to find one point of vulnerability, one chink in that armor to get in."

Shackelford said everyone, from employees to executives, needs to be prepared for these types of attacks. "Ultimately we also have to empower people, to give them the knowledge to exercise basic cyber hygiene in the way we're all doing our part to exercise personal hygiene these days," Schackelford said.

Both Shackelford and Park agree, every company needs to be prepared for this and make cybersecurity a top priority. Small businesses, hospitals, and even bigger companies or organizations can be victims. "It's not a hopeless situation, there are resources out there for any sized healthcare organization to

Eskenazi Health is not alone. Sanford Health, a Sioux Falls, South Dakota-headquartered health system which includes 46 hospitals and care locations in 26 states and 10 countries, said it had been hit with a cyberattack in recent days.

So here are major health care organizations in Indiana and South Dakota being impacted by ransomware attacks. No network is immune from an attack. There are steps you can take to help prevent cybercriminals from invading your network, and SIM2K can help assess your current profile and recommend steps you can take to protect your company.

A Win Against Cybercriminals

Ukrainian law enforcement officials announced they had arrested several individuals involved in criminal activity committed by the Clop ransomware gang that helped popularize the "double extortion" model of not only threatening to encrypt a victim's files, but also threatening to release confidential data that was stolen in an earlier breach.

According to Ukrainian authorities, law enforcement officials also shut down infrastructure that was used to spread the cybercrime gang's ransomware, which was first spotted in February of 2019 as a new variant of the Cryptomix family. Ukrainian law enforcement reportedly said that the Clop ransomware gang has caused roughly $500 million in financial damages, and that the individuals arrested could face up to eight years in prison.

The international coordination effort represents at least the second time this year that countries have come together to fight cybercrime. In January, a coalition of countries collaborating through Europol helped take down Emotet by also attacking its infrastructure. But whereas the Emotet takedown seems to have caused a significant disruption to that cyberthreat, the arrests made against Clop could present a smaller roadblock. That's because none of the actual members of the Clop ransomware gang were caught. Instead, the arrests involved money launderers. A security firm stated "The law enforcement raids in Ukraine associated with CLOP ransomware were limited to the cash-out/money laundering side of CLOP's business only. We do not believe that any core actors behind CLOP were apprehended and we believe they are probably living in Russia."

The arrests also represent the second time in weeks that authorities have targeted a cybercrime gang by following the money. In early June, the US Department of Justice announced that it had recovered the majority of the ransom payment made by Colonial Pipeline to its attackers, the cybercriminal group called Darkside. By tracking the ransomware payment through the public Bitcoin ledger, the Department of Justice and the FBI managed to retrieve 63.7 bitcoins.

Cryptocurrencies have long been abused to fund cybercrime, and, perhaps with the recent retrieval of Colonial Pipeline's ransom payment, that intersection will continue to be closely scrutinized. If so, it would fall in line with the Ransomware Task Force's recommendations made in April, which suggested that governments lean further into regulating cryptocurrency.

While Clop was not particularly active last year—it did not enter the top 10 malware threats for businesses or consumers in 2020—the operators behind the ransomware still found ways to squeeze their victims. Inspired last year by the ransomware group Maze, Clop infiltrated company networks to steal sensitive data and then demanded that those organizations pay a ransom to keep the data secret. But this year, Clop refined that tactic by targeting corporate executives' machines, hoping that executives would have more access to sensitive files and data. The idea was simple: Better access to sensitive data, better chance that a victim will pay to keep that data from being published.

Clop virus' name originates from a Russian "klop," which means "bed bug." It is one of the worst computer threats that makes entries in the Windows Registry to attain durability and could start or restrain processes in a Windows domain to stay hidden from the usual antivirus program and computer user.

Exchange Hacks Continue

The U.S. Cybersecurity and Infrastructure Security Agency is warning of active exploitation attempts that leverage the latest line of "ProxyShell" Microsoft Exchange vulnerabilities that were patched earlier this May, including deploying LockFile ransomware on compromised systems.

The vulnerabilities enable adversaries to bypass ACL controls, elevate privileges on the Exchange PowerShell backend, effectively permitting the attacker to perform unauthenticated, remote code execution. "An attacker exploiting these vulnerabilities could execute arbitrary code on a vulnerable machine," CISA said.

The development comes a little over a week after cybersecurity researchers sounded the alarm on opportunistic scanning and exploitation of unpatched Exchange servers by taking advantage of the ProxyShell attack chain. Originally demonstrated at a hacking contest in April this year, Proxy Shell is part of a broader trio of exploit chains discovered by a security researcher that includes ProxyLogon and ProxyOracle, the latter of which concerns two remote code execution flaws that could be employed to recover a user's password in plain text format.

Now according to researchers from Huntress Labs, at least five distinct styles of web shells have been observed as deployed to vulnerable Microsoft Exchange servers, with over over 100 incidents reported related to the exploit between August 17 and 18. Web shells grant the attackers remote access to the compromised servers, but it isn't clear exactly what the goals are or the extent to which all the flaws were used.

More than 140 web shells have been detected across no fewer than 1,900 unpatched Exchanger servers to date, Huntress Labs CEO Kyle Hanslovan tweeted, adding "impacted [organizations] thus far include building manufacturing, seafood processors, industrial machinery, auto repair shops, a small residential airport and more." The Huntress team analyzed one system infected with ProxyShell and LockFile ransomware and found a unique tactic. "The configuration file for the Exchange internet service was modified to include a new 'virtual directory,' which practically redirects one URL endpoint to another location on the filesystem," which helps an attacker hide the webshell outside of areas monitored by ASP directories.

"If you don't know to look for this, this is going to slip under the radar and the hackers will persist in the target environment. Additionally, the hidden webshell discovered on this host uses the same XML/XLS transform technique that we have seen previously," Huntress advised.

SIM2K is a Huntress partner and has been kept apprised of this situation from them, and is watching our server logs for any activity that Huntress may detect. We have updated our clients to the most recent patches designed to thwart these attacks, but will continue to watch for any new updates that may be issued as this Exchange issue continues to evolve. Call us for 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 214, Indianapolis, IN 46250. Call us at (317) 251-7920 or e-mail sales@sim2k.com. Visit us at www.sim2k.com.

Android User? Watch Out!

A Netherlands security research firm has uncovered a new Android dropper app, dubbed Vultur, that delivers legitimate functionality, then silently shifts into malicious mode when it detects banking and other financial activities.

Vultur, found by ThreatFabric, is a keylogger that captures financial institution credentials by piggybacking on the current banking session and stealing funds right away – invisibly. And just in case the victim realizes what is happening, it locks down the screen.

(Note: Always have your bank's phone number so that a direct call to a local branch might save your money — and keep the number on paper. If it's on your phone and the phone is locked, you're out of luck.)

"Vultur is able to monitor applications that are launched and start screen recording/keylogging once targeted application is launched," according to ThreatFabric. The security firm also noted that screen recording is launched every time the device is unlocked to capture the PIN-code or graphic password used to unlock device. Analysts tested the Vultur capabilities on a real device and confirmed that Vultur successfully recorded a video of entering PIN-code/graphic password when unlocking device and entering credentials in the targeted banking application.

The report continued, "Vultur uses droppers posing as some additional tools, like MFA authenticators, located in official Google Play Store as a main distribution way, therefore, it is hard for end users to distinguish malicious applications. Once installed, Vultur will hide its icon and request Accessibility Service privileges to perform its malicious activity. Being provided with these privileges, Vultur also activates self-defensing mechanism that makes it hard to uninstall it: if victim tries to uninstall trojan or disable Accessibility Service privileges, Vultur will close the Android Settings menu to prevent it."

It is worth noting that using biometrics to log in to a financial app – common these days on both Android and iOS – is an excellent move. In this situation, though, it won't help here as the app piggybacks on the live session.

ThreatFabric did offer three suggestions for getting out of Vultur's grip:

1. Boot the phone into safe mode, preventing the malware from running and then try and uninstall the app.
2. Use ADB (Android Debug Bridge) to connect to the device via USB and run the command {code}adb uninstall <malware_package_name>{code}
3. Perform a factory reset. Of course, this will wipe all data and installed apps off your phone, so do this as last resort.

Vultur shows that malware is not just for PCs, but any device that can access personal information. Be alert for any suspicious activity, and call SIM2K if you believe you have been compromised.

"Random Tid-Bytes"

Zoom Expanding Services

Zoom announced plans buy cloud call center service provider Five9 in a $14.7 billion all-stock transaction. Subject to shareholder approval, the acquisition is expected to close in the first half of 2022. The acquisition could allow the company to hedge its video bets after 18 months of unprecedented growth as both companies and individual users turned to the videoconferencing platform to stay in touch with co-workers, family, and friends. While the need for videoconferencing is unlikely to go anywhere, even with offices re-opening, Zoom appears to be looking to capitalize on its growing customer base by expanding services. This is an interesting acquisition for Zoom, but analysts say that a part of the market that Zoom targets is an IT leader in a mid-size business or smaller that has responsibility for all communication. In that segment, it is very feasible that there will be a responsibility for buying contact center technology. So while the jury is still out on this purchase, it may offer Zoom new avenues for growth.

Voice assistants are maturing

Ten years since Siri arrived, the voice assistant market is maturing and voice search is beginning to proliferate across multiple devices. Products from Amazon, Google, and Apple all deliver voice assistants and already one in four US adults owns a smart speaker. Juniper Research predicts that voice-based ad revenue will reach $19 billion by 2022, but the best ads are always native search results. A recent study showed the growth in this market. More than 30% of us now use voice assistants daily, and around 23% of us use them several times a day. Nearly everyone is aware that these things exist. 60% of users aged 18-24 and 36% of those who are 25-34 years of age are using Siri more than any other assistant. Alexa is more widely used across older demographics, while Google Assistant is also popular. However, just 27% of US voice assistant users feel comfortable using them in public, which means we rely on them at home, in the car, or on an iPhone when out and about. Among those who don't yet use voice assistants, 42% said concerns about privacy have stopped them doing so, while 32% just don't trust the assistants. The report states that most of us use Siri and the other assistants to control music (73% of users) and check the weather (80% of users), and confirms 91% of users have searched using voice. So where does this industry go from here? Voice assistants are becoming contextually aware, as well as capable of providing answers to questions while being offline. We're also seeing increasing use of voice assistants in business. Enterprise voice assistant architectures let business users build their own voice controls to manage their own internal business systems, while apps such as Shortcuts let users extend what their existing voice assistants can do.

Apple iPhones Monitored

Amnesty International has revealed that NSO Group, an Israeli 'surveillance as a service' company, has created and sold an iMessage attack that can be used to spy on journalists, activists, and political representatives using their iPhones. What makes this latest attack particularly dangerous is its exploitation of zero-click vulnerabilities, meaning targets don't even need to read or open the iMessage carrying the hack. Amnesty says all iPhones and iOS updates are vulnerable to the exploit, which gives attackers "complete access to the device's messages, e-mails, media, microphone, camera, calls and contacts." This raises concerns about privacy in the future as the door is now open for surreptitious hacks.

Windows 365 Muddies Waters

Microsoft has introduced Windows 365, a new service that provides virtual PCs to customers. Rather than provide only the operating system or the OS and bits of other software – notably productivity applications in the form of Office – Microsoft will soon also serve up "hardware," virtual machines running on its vast cloud of Azure servers.

Dubbed "desktop as a service" (DaaS, in keeping with other, similar acronyms) by some, Microsoft's tagged its offering as "Cloud PC" as in "Windows 365 is your PC in the cloud."

While DaaS in general, and Windows 365 specifically, has the potential to dramatically change how computing takes place in commercial settings, there's nothing inevitable about it. Many will object to ceding the privacy of a local box to the servers of, in this case, Microsoft.

And Microsoft, already active in PC manufacturing with its Surface line – originally touted as examples for OEMs, something that's been discarded as a talking point – puts itself into further conflict with hardware partners with Windows 365. When the desktop is streamed, what purpose does a high-powered laptop-on-the-lap serve? Will OEMs be relegated to making cheap Chromebook-like machines that need only run a browser?

So what exactly is Windows 365? At its simplest, it's a virtualization service that provides a Windows desktop and first- and third-party applications to users with both PC and non-PC hardware. Think of it as a streaming service. Rather than stream movies and TV shows, it streams the output of a Windows 10-powered PC. The controller is the keyboard, touchscreen, mouse, even the microphone of whatever device is in front of the user. It's also the latest incarnation of the thin computing model, which harks to the beginnings of digital computing when the computer was massive and endpoints were unintelligent terminals. Like that model, Windows 365 runs the virtual desktop on servers at a distance; the data is transferred over the Internet rather than an organization's network.

Microsoft launched Windows 365 on Aug. 2 for businesses. It's likely that Microsoft will offer the service to consumers and very small shops at some point. But that's not going to happen right out of the gate. Microsoft will charge a flat monthly rate per user, rather than basing the cost on the amount of activity, as in the amount of Azure resources consumed.

What performance can you expect from this "virtual PC" being provided? Microsoft listed a dozen possible virtual machine configurations, from the most basic (2 cores, 4GB of memory and 64GB of storage) to the more advanced (8 cores, 32GB RAM and 512GB of storage space). And the cost? Although Microsoft listed 12 configurations, it collected them into just 5 groups. It's possible, then, that there may be as few as 5 different price points for Windows 365 licenses. One pricing hint came from an insider who spotted a $31 per user per month cost for the 2-core, 4GB memory and 128GB storage option. That would be $372 annually.

But don't confuse Windows 365 and Microsoft 365. The Microsoft 365 license gives you the right to use the included productivity software. The Windows 365 license pays for the virtual PC Microsoft has built and maintains on its servers that run the operating system you paid for. It's no different than if you were on a physical PC. You paid for that with one invoice. You paid for the Microsoft 365 license with another.

There is still a question about maintaining the Windows 365 "machines." Microsoft certainly can, since the "devices" are on their servers. But while there is no clear evidence one way or another, suspicion is that customers will continue to be responsible for updates. Any device able to run a web browser should be able to act as a Windows 365 endpoint; in-browser is one of the two ways to stream a desktop. The other is Microsoft Remote Desktop. And Microsoft claims that if you have enough bandwidth to stream movies, then you will have enough bandwidth to support Windows 365 (although pundits say to be ready for the buffering icon interrupting your work!)

At the same time, Microsoft has announcing its first price increase for its Office 365 and Microsoft 365 services in a decade. The price increases will affect commercial and business users of Microsoft's software as a service (SaaS) offerings next year, with no changes to pricing for education or consumers.

Microsoft's updated pricing will go into effect on March 1st, 2022. These price changes mark "the first substantive pricing update since we launched Office 365 a decade ago," says Microsoft. They also come as Microsoft has reported a record year of revenue growth thanks to cloud services like Office 365. Microsoft has more than 300 million paid seats for Office 365, so the price changes will certainly bump Microsoft's profits and revenue even further next year.

While larger businesses will have benefitted from bulk discounts and deals over the past decade, it's the small businesses that will feel the effects of an increase in pricing as the economy starts to recover from a pandemic. Either way, Microsoft has added more than 20 apps to Office 365 since it originally launched, including Microsoft Teams, OneDrive, SharePoint, and To-Do.

The Windows 365 product is just beginning to roll out so has not been tested in an enterprise setting, so SIM2K will continue to monitor its progress and report future developments. And, we did want all clients utilizing Office 365 to be aware that the Microsoft price increase is coming so that your tech budgets for 2022 can reflect this bump in costs. Call us for more information on any Microsoft product or service.

SIM2K
6330 E 75th St., Suite 214
Indianapolis, IN 46250
317.251.7920 • 800.746.4356
www.sim2k.com • sales@sim2k.com