SIM2K
Adapting Technology to Your Business Needs

4•21
Information you can use

SIMformation

Advanced Security Tool now Available

SIM2K is now able to offer advanced cybersecurity tools through our partnership with Huntress Labs. Huntress finds and stops hidden threats that can bypass preventive security tools to protect you from today's determined cybercriminals.

Huntress provides an underlying layer of managed detection and response, so you can be defended against malicious footholds, ransomware and more. Their human-powered threat hunting goes beyond automation, providing the hands-on support and expertise needed to stop advanced attacks. It is a Cloud-delivered managed breach detection service designed to accelerate security adoption, provide deeper visibility and enable faster response to constantly evolving security challenges.

Huntress enables finding and stopping hidden threats that sneak past preventive security tools. By focusing on a specific set of attack surfaces, vulnerabilities and exploits, their platform helps SIM2K protect our customers from persistent footholds, ransomware and other attacks.

Huntress offers a unique combination of automated detection and human-powered threat hunting, so that even the most sophisticated attackers won't stand a chance against security defenses.

Unfortunately, hackers are getting smarter. Rather than mounting a direct attack, cybercriminals are abusing legitimate applications and processes to slip into your systems undetected. Once inside, they establish a quiet foothold for their next move – often the deployment of malware to cripple systems, or ransomware to encrypt and steal sensitive data. Huntress detects these footholds to identify – and eliminate – persistent actors that are dwelling in protected environments.

Huntress also protects against Ransomware. There is a reason ransomware is such a popular tool in the modern hacker's tool box: it is highly effective. The sooner ransomware can be detected, the more likely it is it can be stopped from spreading and taking down an entire network. Huntress uses what it calls "Ransomware Canaries" (like the old canaries in a coal mine) to enable faster detection of potential ransomware incidents. These are small lightweight files which are placed on all protected endpoints, and if those files are modified or changed in any way, an investigation is immediately opened with their ThreatOps team to confirm whether those changes are the result of a ransomware attack or malicious encryption.

The Huntress agent is installed on workstations and servers to capture, collect and send metadata about potential threats to the Huntress cloud for analysis. Their automated engine performs initial analysis of the data collected by the agent. Then their ThreatOps team reviews the full context of that data to determine the classification which cannot be completely replicated through automation. Then, with the threat identified and confirmed, SIM2K receives a report with recommended actions to eliminate the threat.

Should there be a security issue detected, the report that Huntress sends SIM2K includes remediation instructions along with a "one-click" approval process to initiate action, giving us fast response to any incident. SIM2K should be taking action before you ever discover that there is a possible problem on your network.

And, as a Cloud-based service, Huntress will automatically update their services to keep up with constantly evolving threats. This will not require any action on your part, nor will SIM2K need to "touch" your network to install patches or updates unless a specific threat is identified that requires remediation at your end. Otherwise, new protection is rolled out through the Cloud to all covered devices as the malware is parsed at Huntress, not on your desktop or server.

SIM2K is offering Huntress as a new service for our clients. It is an add-on over our basic security offerings like Cylance and SIM2K® MAVerick. Once installed on your network, we will be able to monitor potential threat activity from a dashboard, and then work in conjunction with the Huntress ThreatOps team to mitigate any exposure you might face.

This exciting new technology is available to SIM2K clients now at affordable rates. If you are interested in learning more, look for an invitation in the near future for an informational webinar we will be holding with Huntress that will explain the protection in more depth and have specific examples of how it works to protect you. In the meantime, if you have questions or are interested in Huntress protection for your business, feel free to call or e-mail Ben at SIM2K!

Cloud Files Mysteriously Deleted

Microsoft SharePoint and Microsoft Teams users report files are missing or moved to the Recycle Bin after the recent Azure Active Directory outage the last week of March, when Microsoft suffered a massive outage that affected almost all cloud services, including Microsoft 365, Teams, XBox Live, Exchange Online, Outlook.com and Sharepoint. Microsoft later confirmed that the outage was caused by a configuration issue in their Azure Active Directory Service.

Since then, numerous Microsoft SharePoint administrators were reportedly bombarded with client calls about missing files in their SharePoint folders. When looking into the issue, they found the SharePoint folder structure to be intact, but all of the files were missing. Eventually, the deleted files were found in SharePoint's cloud recycle bin, or in some cases, a local PC's Recycle Bin. One administrator discovered that all of the files show the same deleted time, were previously located in a variety of SharePoint folders, and the folder structure remained intact on SharePoint, meaning a user couldn't have accidentally deleted the data. Another user reported that thousands of files were being deleted and the only way to stop this was to change the affected users' password.

Microsoft released the following notice:

> "Some users may have received some form of notification indicating that their files were deleted; such as a message from OneDrive stating 'Remove files from all locations', or a notice that their files were being removed from their synced folders and placed into a recycle bin. Impacted users can manually initiate a resync to resolve the problem by restarting their machine. Subsequent file syncs will restore the files to the appropriate local folders."

While the Microsoft advisory states that the outage had caused local data to become unavailable, that does not explain why the files are being deleted from SharePoint's cloud folders and why users continue to see this happening after the outage resolved. Furthermore, whilw Microsoft stated that "subsequent file syncs restore the files to the appropriate local folders," admins were not finding this to be the case and have had to perform a manual restore.

To make matters worse, numerous Microsoft Teams Free users report that files shared on their channels are no longer accessible in either the desktop or web client. When attempting to access files, users are shown errors, such as the one below, stating that the file may have been deleted or that the user may not have permission to view it. Microsoft escalated a "fix" for this, but never provided an explanation for either the Sharepoint or Teams issues.

This points out the need to have a robust backup solution in place, even for Cloud storage. It is not enough to trust that a Cloud vendor will be careful with your files or be able to find, locate and restore them in a timely fashion. SIM2K offers several backup storage and verification tools, and can work with you to ensure your data is being backed up and that there is a way to recover files should the need arise. Call us for details.

Watch out for Magnetic Jewelry

We had a user with a recurring problem: the laptop's screen would blank out while in the middle of working (e.g. typing an e-mail). It would only happen when the laptop was on power and not docked. When it first happened we logged the fault with Dell and thought it was a "glitch" in the operating system.

However, this continued to occur, so we looked into it deeper. It was then noticed the user wears a magnetic bracelet (for pain relief). Whenever the bracelet went near the bottom right corner of the wrist-rest area, the screen would blank. It appears the magnetic bracelet was triggering the laptop's switch to turn the screen off when the lid is closed, putting the device into "Sleep Mode."

So please be cautious about wearing any magnetic items around laptops and tablets. Whether it is just a magnetic clasp (like shown to the left) or a full magnetic bracelet like our user, the presence of a magnetic field can cause issues with electronics. Years ago people were cautioned about placing anything magnetic around diskettes and external hard drives, as it was felt that this might erase or otherwise corrupt stored data, but shielding has improved over the years and diskettes are no longer used.

The worry here was that magnets would delete the information stored on your hard drive. Because of how hard drives work, magnets won't delete anything from your hard drive. Your hard drive has a very powerful magnet inside that controls the read-write head movement. If the magnet inside the drive itself doesn't delete information, any magnet that isn't insanely powerful won't wipe it either.

While a magnet isn't going to wipe your hard drive, if you leave a powerful magnet directly on top of your hard drive there is a slight chance that it could cause damage to the hard drive itself while it's functioning. The easy solution: don't put a magnet directly on top of your hard drive during use. By doing that, you can be confident that your hard drive, and the information stored on it, is completely safe.

Speaking of external devices and magnets, you might ask, "What about a USB flash drive?" The short answer is that USB drives cannot be harmed or altered by magnetic fields. The drives are not built from magnetic materials. So magnets pose no danger to any flash memory including SSDs, SD cards, and external hard drives.

So while a magnetic bracelet won't damage your data, just be aware it might put your laptop to sleep. Call SIM2K if you have any questions or concerns about odd happenings with your tech.

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.

Apple Now a Target

With 23% of enterprise PCs deployed in 2020 apparently being Macs, Apple's platforms are becoming keen targets for criminal enterprise. The problem for criminals: Apple's inherently solid security, along with the capacity to rush security upgrades out to millions of users because of the company's non-fragmented platforms, makes doing so quite difficult. In response, attackers appear to be returning to the drawing board and now seem to be working to inject attacks early on in the process. The way they see it is that if you can't persuade people to download Apple malware, you need to inject it inside applications users already trust.

The latest illustration of this approach is called "XcodeSpy", a variant of a legitimate open-source project Xcode users might choose to build animated tab bars. XcodeSpy attempts to install malware on Macs used by software developers. This corrupted version of this developer tool has been found in an infected code library in the wild.

Once installed, this software quietly executes a script that downloads backdoor software that monitors what the developer does via the microphone, camera and keyboard. While this sounds pretty rough, it's no reason for over-reaction. But it should serve as a warning to Apple developers in all walks of life, (particularly in enterprise IT) to ensure they are completely certain of what third-party tools and open-source packages they use when building applications.

The logic of using developers unknowingly adding malware into their legitimate software makes complete sense. Even in Apple's curated App Store model, iPhone, iPad, and Mac customers have built a big sense of trust in the way they download and install software. Indeed, given that Apple continues to add friction to the experience of downloading software from outside its stores, malware makers know that the best way to distribute their wares is via the App Store itself.

This must ultimately be the prize they seek – to build an attack mechanism that silently infects enough developers of legitimate Apple apps so that the apps they then sell via Apple's store carry malware into devices belonging to millions of users. Apple's highly secure platforms are tough to break, but there's a big profit motive to try to do so.

Given that the weakest link in any security chain is now and always has been the user, no surprise then that those with a nose for this kind of security subversion are spending time figuring out how to trick developers into unwittingly becoming their own secret attack vectors.

This means developers in the Apple ecosystem will need to security audit their software code repositories a little more often in future, as they have been identified as potentially being the weakest link in the security chain.

"Random Tid-Bytes"

Facebook Hack Releases Half-billion Names

A massive hack on Facebook occured in 2019. Now, the personal data of more than half a billion Facebook Inc. users reemerged online for free on April 3, a reminder of the company's ability to collect mountains of information and its struggles to protect these sensitive assets. The leak includes personal information on 533 million Facebook users, such as phone numbers, Facebook IDs, full names, locations, birth dates, bios and in some cases e-mail addresses. "This is old data that was previously reported on in 2019," a Facebook spokesperson said. "We found and fixed this issue in August 2019." At the time, the company addressed a flaw in its technology that allowed the information to leak out. However, once such data escapes from Facebook's network, the company has limited power to stop it from spreading online. The personal data belonging to more than 533 million people is in the hands of hackers. And that sort of data will never change. Personal details like e-mails and phone numbers can be used to target individuals in various ways, even if Facebook's security protects everyone else from previous breaches. Ironically, Facebook CEO Mark Zuckerberg's own personal information, including his cell phone number, is part of the data release in this hack. To check if your information has been released in this, or any other hack, you can go to this website: https://haveibeenpwned.com/ and enter your e-mail address to see if your personal data is involved in any data breach.

Microsoft Edge To Match Google Chrome Updates

Microsoft has synchronized the release schedule of its Edge browser with Chrome's, which Google had earlier announced would accelerate to an every-four-week pace. "As contributors to the Chromium project, we look forward to the new 4-week major release cycle cadence that Google announced, to help deliver that innovation to our customers even faster," said the Microsoft Edge team's blog post. In March, Google said it would speed up the release tempo of Chrome to match that of Mozilla's Firefox by reducing the current six-to-eight-week schedule to just four weeks. The change won't happen overnight, but instead will take place in the fall, when the span between versions 94 and 95 will fall to four weeks. Microsoft had little choice but to go along with the change to release timing. The only alternative would have been to delay Edge releases, which for users would be unacceptable. Also per Google's plans, Microsoft will offer a less-frequently updated edition of Edge aimed at commercial customers. This "Extended Stable" release will upgrade every eight weeks, skipping every other build, but will be serviced by security updates on a two-week tempo.

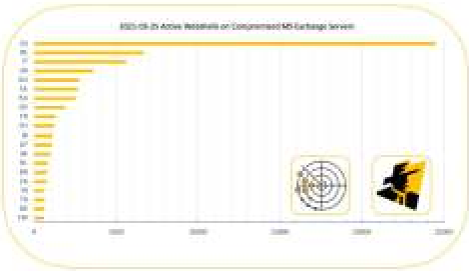
Ring! Ransomware Calling

The"bad guys" are adopting new outreach techniques designed to shame victims into paying up. Malware has relied on shame and the threat of exposure for years. These threats are most closely linked to people at home, with sextortion, where victims are told there is footage of them watching pornographic material, or engaging in sexual activity, being one of the biggest. If they don't pay the Bitcoin ransom, scammers will release the footage to the world. Now the scammers are utilizing voice calls to journalists and victim's business partners to generate payments. The scammers are assuming that warning businesses that their data may have been exposed in an attack on of their partners will create further pressure for the victim to pay.

Exchange Hack Continues to Vex IT Security

New data suggests someone has compromised more than 21,000 Microsoft Exchange Server e-mail systems. In an interesting twist, the malware invokes the name of an IT security expert and blogger – KrebsOnSecurity and him by name. Here is his take on the situation, as he (Brian Krebs) discussed on his website:

> Let's just get this out of the way right now: It wasn't me.
>
> The Shadowserver Foundation says it has found 21,248 different Exchange servers which appear to be compromised by a backdoor and communicating with {brian.krebsonsecurity.top} [Note: this is not a safe domain so do not attempt to follow!]
>
> Shadowserver has been tracking the waves of attacks targeting flaws in Exchange that Microsoft addressed in early March with an emergency patch release. The Shadowserver Foundation Europe has been keeping a close eye on hundreds of unique variants of backdoors (a.k.a. "web shells") that various cybercrime groups worldwide have been using to commandeer any unpatched Exchange servers. These backdoors give an attacker complete, remote control over the Exchange server (including any of the server's e-mails).



> On Mar. 26, Shadowserver saw an attempt to install a new type of backdoor in compromised Exchange Servers, and with each hacked host it installed the backdoor in the same place: "/owa/auth/babydraco.aspx."
>
> "The web shell path that was dropped was new to us," said a Shadowserver director. "We have been testing 367 known web shell paths via scanning of Exchange servers."
>
> OWA refers to Outlook Web Access, the Web-facing portion of on-premises Exchange servers. Shadowserver's honeypots saw multiple hosts with the Babydraco backdoor doing the same thing: Running a Microsoft Powershell script that fetches the file "krebsonsecurity.exe." Oddly, none of several dozen anti-virus tools currently detect this as a malicious file.
>
> The Krebsonsecurity file also installs a root certificate, modifies the system registry, and tells Windows Defender not to scan the file. Shadowserver says the Krebsonsecurity file will attempt to open up an encrypted connection between the Exchange server and an IP address, and send a small amount of traffic to it each minute.
>
> Shadowserver found more than 21,000 Exchange Server systems that had the Babydraco backdoor installed. But they don't know how many of those systems also ran the secondary download from the rogue Krebsonsecurity domain.
>
> "Despite the abuse, this is potentially a good opportunity to highlight how vulnerable/compromised MS Exchange servers are being exploited in the wild right now, and hopefully help get the message out to victims that they need to sign up our free daily network reports," the group says.

There are hundreds of thousands of Exchange Server systems worldwide that were vulnerable to attack (Microsoft suggests the number is about 400,000), and most of those have been patched over the last few weeks. However, there are still tens of thousands of vulnerable Exchange servers exposed online. On Mar. 25, Shadowserver tweeted it was tracking 73,927 unique active webshell paths across 13,803 IP addresses. Exchange Server users that haven't yet patched against the four flaws Microsoft fixed earlier this month can get immediate protection by deploying Microsoft's "One-Click On-Premises Mitigation Tool" available from the Microsoft website.

The motivations of the cybercriminals behind the Krebonsecurity dot top domain are unclear, but the domain itself has a recent association with other cybercrime activity — and with harassing this author. I first heard about the domain in December 2020, when a reader told me how his entire network had been hijacked by a cryptocurrency mining botnet that called home to it.

"This morning, I noticed a fan making excessive noise on a server in my homelab," the reader said. "I didn't think much of it at the time, but after a thorough cleaning and test, it still was noisy. After I was done with some work-related things, I checked up on it – and found that a cryptominer had been dropped on my box, pointing to XXX-XX-XXX.krebsonsecurity.top'. In all, this has infected all three linux boxes on my network." What was the subdomain I X'd out of his message? Just my Social Security number. I'd been doxed via DNS."

Microsoft has pushed out a new update for their Microsoft Safety Scanner (MSERT) tool to detect web shells deployed in the recent Exchange Server attacks. Microsoft disclosed that four Exchange Server zero-day vulnerabilities were being used in these attacks against OWA servers. Known as 'ProxyLogon,' these vulnerabilities are being used by Chinese state-sponsored threat actors to steal mailboxes, harvest credentials, and deploy web shells to access the internal network.

When Microsoft disclosed these attacks, they released updated signatures for Microsoft Defender that will detect the web shells installed using the zero-day vulnerabilities.

This Exchange hack continues to be a concern for security pros and administrators and should not be discounted. SIM2K has applied all necessary patches and continues to monitor systems for any subsequent attacks. And apparently, the "bad guys" are making this a personal thing against security pros, too.

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