SIM2K
Adapting Technology to Your Business Needs

2•18
Information you can use

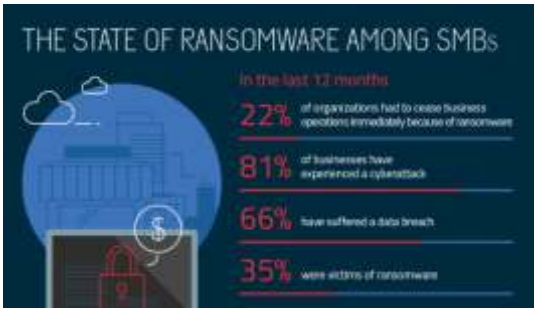
SIMformation

Ransomware Still an Issue

We may be going to excess in our discussions about Ransomware, but in 2017 this was a major problem for companies and we have already seen a hospital in Indiana be forced to pay the ransom to decrypt files in 2018. So obviously this is not going away, nor has everyone learned the lessons on preventing a malware infection. So, let us review the basics once more.

Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

There are several different ways that ransomware can infect your computer. One of the most common methods today is through malicious spam, or malspam, which is unsolicited e-mail that is used to deliver malware. The e-mail might include booby-trapped attachments, such as PDFs or Word documents. It might also contain links to malicious websites.



graphic by Malwarebytes

Malspam uses social engineering in order to trick people into opening attachments or clicking on links by appearing as legitimate – whether that's by seeming to be from a trusted institution or a friend. Cybercriminals use social engineering in other types of ransomware attacks, such as posing as the FBI in order to scare users into paying them a sum of money to unlock their files.

Another popular infection method, which reached its peak in 2016, is malvertising. Malvertising, or malicious advertising, is the use of online advertising to distribute malware with little to no user interaction required. While browsing the web, even legitimate sites, users can be directed to criminal servers without ever clicking on an ad. Malvertising often uses an infected invisible webpage element to do its work. This page redirects the user to an exploit landing page, and malicious code attacks the system from the landing page via exploit kit. All this happens without the user's knowledge, which is why it's often referred to as a drive-by-download.

There are three main types of ransomware:

Scareware, which as it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A legitimate cybersecurity software program would not solicit customers in this way. If you do have security software, you wouldn't need to pay to have the infection removed—you've already paid for the software to do that very job.

Screen lockers When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

Encrypting ransomware which is the truly nasty stuff. This is the exploit that grabs all your files and encrypts them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get hold of your files, no security software or system restore can return them to you. Unless you pay the ransom – for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

Mac Attack. If you are an Apple user, you are not safe, either. Mac malware authors dropped the first ransomware for Mac OSs in 2016. Called KeRanger, the ransomware infected an app called Transmission that, when launched, copied malicious files that remained running quietly in the background for three days until they detonated and encrypted files. So, Mac ransomware is not theoretical.

Mobile ransomware. Mobile ransomware typically displays a message that the device has been locked due to some type of illegal activity. The message states that the phone will be unlocked after a fee is paid. Mobile ransomware is often delivered via malicious apps, and requires that you boot the phone up in safe mode and delete the infected app in order to retrieve access to your mobile device. So even your smartphone can be ... dumb ... about infected files.

SIM2K can help you train your employees on what to look out for and then can check your backups to be sure you are getting everything you need covered to restore your business should you be infected with ransomware. We install CylancePROTECT® for our clients to ward off infections, but they still can occur and we should be the first call you make if targeted. Stay Vigilant!

YouTube Ads Corrupted

YouTube was recently caught displaying ads that covertly leach off visitors' CPUs and electricity to generate digital currency on behalf of anonymous attackers, it was widely reported. Word of the abusive ads started in late January, as people took to social media sites to complain that their anti-virus programs were detecting cryptocurrency mining code when they visited YouTube. The warnings came even when people changed the browser they were using, but always occurred when the person was visiting YouTube.

Researchers with anti-virus provider Trend Micro said the ads helped drive a more than three-fold spike in Web miner detections. They said the attackers behind the ads were abusing Google's DoubleClick ad platform to display them to YouTube visitors in select countries, including Japan, France, Taiwan, Italy, and Spain.

The ads contain JavaScript that mines the digital coin known as Monero. In nine out of 10 cases, the ads will use publicly available JavaScript provided by Coinhive, a cryptocurrency-mining service that's controversial because it allows subscribers to profit by surreptitiously using other people's computers. The remaining 10 % of the time, the YouTube ads use a private mining JavaScript that saves the attackers the 30% cut Coinhive takes. Both scripts are programmed to consume 80% of a visitor's CPU, leaving just barely enough resources for it to function.

YouTube was targeted because users are typically on the site for an extended period of time. The longer the users are watching videos means more time for the mining program to generate the cryptocurrency – thus more money. To add insult to injury, the malicious JavaScript in at least some cases was accompanied by graphics that displayed ads for fake AV programs, which scam people out of money and often install malware when they are run.

A Google representative said these ads were blocked in less than two hours, but evidence supplied by Trend Micro and on social media showed various ads containing substantially the same JavaScript ran for as long as a week. The representative didn't respond to follow-up questions seeking a timeline of when the abusive ads started and ended.

As the problem of Web-based cryptomining has surged, a variety of AV programs have started warning of cryptocurrency-mining scripts and giving users the option of blocking this activity. While drive-by mining is an abuse that drains visitor's computing resources and electricity, there is no indication that it installs ransomware or other malware, as long as people don't click on a malicious download.

Between SIM2K® MAVerick and CylancePROTECT®, we believe our clients are protected from any mining scripts running, but you should be aware of this exploit for your home PC use. Contact us for more details.

Continued Fallout from Intel Flaw

If you own a PC from Dell, HP or Lenovo, chances are very good that the BIOS or UEFI firmware update you installed earlier this month is bad – all part of the Meltdown/Spectre mess.

Intel announced a "Oops! Never Mind" order over its Meltdown/Spectre-related firmware updates. In turn, the major PC makers issued their own call-backs for the updates they released. The bottom line: If you updated your BIOS or UEFI this month, you'll almost undoubtedly have to do it again just to get rid of the buggy code. Then you'll have to upgrade the firmware once again, at a later time. But nobody knows yet just when or how.

Intel has posted a list of buggy microcode families, including most of the current processors including Haswell, Broadwell, Skylake, Kaby Lake, and Coffee Lake chips. That covers a very large percentage of Intel-based Windows PC shipped in the past five years. (If you have an older PC, be aware – they never "fixed" it anyway.) Most people don't download firmware updates from Intel. Instead, the system manufacturer – most likely Lenovo, Dell, or HP – integrates the microcode into their own BIOS/UEFI upgrades, then pushes those out to retail machines. That's where this problem has exploded.

For example, Dell did release a BIOS update, then a few days later released this statement:

> *Dell is advising that all customers should not deploy the BIOS update for the Spectre (Variant 2) vulnerability at this time. We are removing the impacted BIOS updates from the web and suspending further BIOS updates for affected platforms.*
> *If you have already applied the BIOS update, please wait for further information and an updated BIOS release, no other action is recommended at this point. Please continue to check back for updates.*

HP and Lenovo issued similar statement reflecting their update processes. The only major company not addressing this call-back is Microsoft, so if you are a Surface owner, keep your eyes open.

Our advice is the same as it's always been: Sit tight. There are no known Meltdown/Spectre exploits in the wild as yet, and when they do appear, they probably won't be directed at your PC. Give this issue more time to be sorted out, for as we said in last month's SIMformation, a hacker has to be on your actual network to trigger any such exploit, so the risk is low and we can wait for a "real" fix from Intel.

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.

Windows 10 Data Collection Revealed

Microsoft has given Windows 10 testers a peek at an app that shows exactly what diagnostic data the company collects from customers and transmits to its own servers. The issue of Windows 10's telemetry has dogged the operating system since its debut, with critics taking Microsoft to task for over-zealously harvesting information, for refusing to describe what data it collects, and for preventing customers from opting out.

With the release of Windows Insider build 17083 on Jan. 24, Microsoft addressed the criticism about transparency by putting an app, named "Diagnostic Data Viewer," into the hands of beta participants. Although currently available only to Insiders. the viewer is scheduled to be released in the next Windows 10 upgrade,. probably in March or April.

According to Microsoft, the viewer shows "the exact data uploaded to Microsoft" and lets users search for specific diagnostic events as well as filter the events for one or more broad categories, such as "Product and Service Usage" or "Software Setup and Inventory.

But it's felt to be highly unlikely that the new app signals Microsoft will yield to its customer critics, said an one analyst. Instead, it was probably prompted by the company's continued discussions with European Union members about the impending General Data Protection Regulation (GDPR), which goes into force in May. Under GDPR, companies must obtain explicit consent from their customers for any use of personalized information,

Microsoft is expected to defend its telemetry practices, even as the company makes incremental concessions on secondary fronts, because the data is crucial to how Microsoft now services Windows. This is, in part, because so many people are relying on Windows Defender as their antivirus. Microsoft needs a certain amount of telemetry to keep that and security updates working. Microsoft needs to know that the latest antivirus signature has been applied, and how many people have applied a security patch.

Microsoft uses diagnostic data to identify problems; it then makes fixes and expands the pool of potential recipients. For example, the Intel chip issue with Meltdown and Spectre is one area where Microsoft needs to collect data. Microsoft needed to get a handle on how many users had installed the patch that was issued and immediately called back *(see story on page 2)*. This would give the company an idea of how exposed their products were to this firmware upgrade that caused more harm than it fixed.

Privacy has long been a concern with Windows 10, and the release of this app is a first step towards more transparency over the data Windows 10 does gather. When released,. the IT world believed that this new OS snooped into all browsing habits and stored data, and Microsoft has spent the intervening years debunking those rumors. The Diagnostic Data Viewer may help put these concerns to bed.

"Random Tid-Bytes"

Firefox Browser Improvements add Speed

Mozilla has released Firefox 58 for Windows, macOS and Linux, building on the break-from-the-past Quantum edition of November by boosting page load speeds with changes to how the browser handles JavaScript. Firefox updates in the background, so most users only need to re-start their browser to get the latest version. Mozilla usually updates Firefox every six to eight weeks, although the interval tends to lengthen around the end of each year; the last time it upgraded the browser, to version 57, aka "Quantum," was Nov. 14, about 10+ weeks ago. One of the new features will improve the speed of the browser by separating processor steps used to compose a web page, characterizing the change as one that "more efficiently paints your screen, using a dedicated CPU thread." Previously, the bulk of the page composition was done on a single processor thread, but this improvement shifts some of the work – executing the graphics draw commands and thus generating the pixels to be put on the display –- to a thread all its own. By reducing the main thread's workload, it is more likely that Firefox will be able to compose pages in time to keep high frame rate chores from skipping frames. This release also improves Mozilla's Tracking Protection. When enabled, it blocks a wide range of content, not just advertisements but also in-page trackers that sites or ad networks implant to follow users from one site to another.

Changes coming to Safari, as well

Apple is about to introduce Service Workers in its' Safari browser. Service Workers allow background scripts to power offline web applications and should make it possible (for example) for developers to build Web apps that can work even when offline. This may mean web services you can save to your Home screen like any other app, use of the camera from within a web page, background sync and other ways to make web apps that will work online or offline. They are part of an industrywide initiative to enable developers to build Progressive Web Applications, browser-based apps that can also work offline thanks to Service Workers' ability to cache data for offline use. Apple is also working on a Web App Manifests specification, a second technology that is required to make Progressive Web Applications a reality on Safari. This carries important information, such as names, descriptions, icons and so on, required to create an app interface. When you combine Service Workers with Web App Manifests, it can create JavaScript-based apps that can be run from the Home screen and act like apps (ie. with a user interface).

PCI To Allow PIN Entry on Devices

The PCI Council, the group that oversees payments from Visa, Mastercard,and all, has approved allowing PINs to be entered into smartphones and tablets. In the U.S., this change is limited to debit card transactions, which use a PIN. Most other places in the world have chip and PIN rather than our chip and signature. The big change is that merchants will no longer need a typical hardware-based POS system and card dip mechanism. That can now all be handled by a mobile device with a chip-reading dongle. For some merchants that have held off accepting payment cards because of the hardware costs, this could make a huge difference.

Are You Prepared For the Zombie Apocalypse?

Disasters come in all shapes and sizes. It's not just catastrophic events such as hurricanes, earthquakes and tornadoes, but also incidents such as cyber-attacks, equipment failures (and perhaps Zombies) that can be classified as disasters.

Companies and organizations prepare by creating disaster recovery plans that detail actions to take and processes to follow to resume mission-critical functions quickly and without major losses in revenues or business.

In the IT space, disaster recovery focuses on the IT systems that help support critical business functions. The term "business continuity" is often associated with disaster recovery, but the two terms aren't completely interchangeable. Disaster recovery is a part of business continuity, which focuses more on keeping all aspects of a business running despite the disaster. Because IT systems these days are so critical to the success of the business, disaster recovery is a main pillar in the business continuity process.

Economic and operational losses can overwhelm unprepared businesses. One hour of downtime can cost small companies as much as $8,000, midsize companies up to $74,000, and large enterprises up to $700,000, according to a report from the IT Disaster Recovery Preparedness Council. Another survey showed that 54% of those companies participating had experienced a downtime event that lasted more than eight hours over the past five years, and two-thirds said their businesses lost more than $20,000 for every day of downtime.

> *"The natural tendency is to try to name or define what the worst case scenario is. This becomes a fatal flaw because it shapes the entire planning effort thereafter, even if it is at a subconscious level. So when we insert a named scenario - pandemic, earthquake, cyber-attack, etc., – we automatically start thinking and planning in terms of response/recovery for that specifically and subconsciously defined incident. When this occurs we not only tend toward a tunneled view in our planning efforts, but we are also in danger of increasing our risk and exposure. This is because there will be a hyper-focus on only one or two specific areas in what we think is the worst-case scenario, and not the actual event."*
>
> *From the Disaster Preparedness Council*

Even if your company already has a disaster recovery plan of some sort, it may be time for an update. If your company doesn't have one, don't jump in feet first without doing risk assessment. Identify vulnerabilities to your IT infrastructure and where things could go wrong. A prerequisite is knowing what your IT infrastructure looks like. This is where SIM2K can help you with the examination of your infrastructure and potential weak spots to be addressed.

Knowing where things could go wrong doesn't mean that you start creating worst-case scenario plans. A recent blog post in the Disaster Recovery Journal suggests that naming the worst-case scenario in business continuity planning can be dangerous by drawing attention away from other significant threats. The key is to focus on "managing the crisis, restoring business critical functions and recovery."

- A disaster recovery plan should include the following:
- Statement, overview and main goals of the plan.
- Contact information for key personnel and disaster recovery team members.
- Description of emergency response actions immediately following a disaster.
- Diagram of the entire IT network and the recovery site.
- Identifying the most critical IT assets and determining the maximum outage time. Get to know the terms Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO indicates the maximum 'age' of files that an organization must recover from backup storage for normal operations to resume after a disaster. If you choose an RPO of five hours, then the system must back up at least every five hours. The RTO is the maximum amount of time, following a disaster, for the business to recover its files from backup storage and resume normal operations. If your RTO is three hours, it can't be down longer.
- List of software, license keys and systems that will be used in the recovery effort.
- Technical documentation from vendors on recovery technology system software.
- Summary of insurance coverage.
- Proposals for dealing with financial and legal issues.

The plan should be coordinated by IT team members responsible for critical IT infrastructure within the company. Others who need to be made aware of the plan include the CEO or a delegated senior manager, directors, department leaders, human resources and public relations officials, depending on the size of the organization. Outside the company, vendors associated with disaster recovery efforts (software and data backup, for example) and their contact information should be known.

Once the plan is written and approved by management, test the plan and update if necessary. Be sure to schedule a time for a review period and/or audit of the disaster recovery functions. Update, update, update as events transpire (large or small). Don't just put the plan in a desk drawer and hope that a disaster doesn't occur.

If a disaster has occurred, it's time to start your incident response. Make sure that the incident response team (if it's different from the disaster recovery planning team) has a copy of the disaster recovery plan. Incident response involves assessing the situation (knowing what hardware, software, systems were affected by the disaster), recovery of the systems, and follow-up (what worked, what didn't work, what can be improved).

So maybe it is not Zombies to be concerned with, but ask yourself if your business can survive with a prolonged outage of your IT infrastructure. Be prepared. Contact SIM2K for more information on how we can work with you to create a Disaster Preparedness Plan for your company.

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