SIM2K
Adapting Technology to Your Business Needs

10•17
Information you can use

SIMformation– BREAKING NEWS

KRACK Attack Breaks WiFi Security

A devastating flaw in Wi-Fi's WPA security protocol makes it possible for attackers to eavesdrop on your data when you connect to Wi-Fi. Dubbed KRACK, the issue affects the Wi-Fi protocol itself – not specific products or implementations – and "works against all modern protected Wi-Fi networks," according to the researcher that discovered it. That means that if your device uses Wi-Fi, KRACK likely impacts it – including, and especially – smartphones.

KRACK (short for Key Reinstallation AttaCK) targets the third step in a four-way authentication "handshake" performed when your Wi-Fi client device attempts to connect to a protected Wi-Fi network. The encryption key can be re-sent multiple times during step three, and if attackers collect and replay those re-transmissions in particular ways, Wi-Fi security encryption can be broken.

This could enable the attackers to eavesdrop on all traffic you send over the network allowing them to steal sensitive information such as credit card numbers, passwords, chat messages, e-mails and so on.

The United States Computer Emergency Readiness Team also issued this warning as part of its KRACK security advisory. "The impact of exploiting these vulnerabilities includes decryption, packet replay, TCP connection hijacking, HTTP content injection, and others." HTTP content injection means the attacker could sneak code into the websites you're looking at to infect your PC with ransomware or malware. At this time it is not known if this vulnerability has been (or is being) actively exploited in the wild. The vulnerability was discovered by a "white hat" hacker and the IT industry was alerted months ago before this news went public to permit companies to "fix" this issue so hopefully that will derail any attempts to use this exploit.

Microsoft released security updates on October 10th and customers who have Windows Update enabled and applied the security updates are now protected. Also, implementations can be patched in a backwards-compatible manner. That means that your device can download an update that protects against KRACK and still communicate with unpatched hardware while being protected from the security flaw. Given the potential reach of KRACK, expect those patches to come quickly from major hardware and operating system vendors.

Until those updates appear for other devices, companies can still take steps to safeguard against KRACK. The easiest thing would be to simply use a wired ethernet connection, or stick to your cellular connection on a phone. That's not always possible though.

If you need to use a public Wi-Fi hotspot – even one that's password protected – stick to websites that use HTTPS encryption. Secure websites are still secure even with Wi-Fi security broken. The URLs of encrypted websites will start with "HTTPS," while unsecured websites are prefaced by "HTTP." Alternatively, you can use a virtual private network (VPN) to hide all of your network traffic. And again, keep your security software up to date to protect against potential code injected malware.

KRACK is a different sort of attack than previous exploits, in that it doesn't go after devices, it goes after the information you use them to send. So while the data stored on your phone is safe from hacking, whenever you use it to send a credit card number, password, email, or message over Wi-Fi, that data could be stolen.

While any device that sends and receives data over Wi-Fi is at risk, the researchers who uncovered the attack said Android devices were more at risk than other mobile phones. Google has already confirmed that it is aware of the issue and will be distributing a patch, and Apple said that all current iOS, macOS, watchOS, and tvOS betas include a fix for KRACK

Also, don't forget about your Wi-Fi routers, not just your PCs and phones. Check to see if your router has any pending firmware updates. Most people aren't as vigilant in updating their routers so log into your admin page and install any waiting updates. If there aren't any, it's a good habit to check back every day, since companies will be rolling out patches over the coming weeks.

While SIM2K will be checking on your business equipment, this warning extends to your home, so be sure any home Wi-Fi routers are updated, too. Call us for more information on protection from the KRACK exploit.

SIM2K
Adapting Technology to Your Business Needs

10•17
Information you can use

SIMformation

"Simming" – Synthetic Identities

Credit report company Equifax said this month that an additional 2.5 million Americans may have been affected by the massive security breach of its systems, bringing the total to 145.5 million people who had their personal information accessed or stolen.

The information stolen earlier this year included names, Social Security numbers, birth dates and addresses — the kind of information that could put people at significant risk for identity theft.

Why is the Equifax data breach such a "big deal'? It opens the door for "simming," – synthetic identity theft. This scam relies on creating identities rather than stealing existing ones. Identity thieves blend the stolen names, SSNs, birthdates and addresses into new identities to open credit lines.

Barely on the radar a half decade ago, the technique may already account for as much as 20% of credit card loans that go bad. Synthetic identity theft probably cost banks at least $6 billion in 2016, the payments consulting firm estimated last month, based on an analysis of major lenders' data on soured loans.

The crimes are increasing just as banks have won a long-sought victory against fraud. The financial industry spent years arm-twisting retailers to upgrade their credit card terminals so they could accept computer chips. This is supposed to prevent criminals from stealing numbers, printing their own plastic, and going on shopping sprees that leave banks on the hook. Synthetic theft, meanwhile, has been in the wings, making headlines after the arrest of pioneering con artists or crime rings – including one that allegedly made off with $200 million. But perhaps because synthetic identity theft requires a lot of time, the incidents never seemed to add up to a crime wave. That's starting to change.

Synthetic fraudsters buy stolen SSNs or try to guess numbers not in use, then combine them with a sham identity. Using other people's real addresses, they begin applying for cards. Banks usually reject the first requests after seeing that the applicant has no credit profile. Still, the banks' inquiries generate placeholder profiles with a credit bureau. Thieves keep applying for cards until a lender eventually opens an account. Then the long con starts. Fraudsters can spend years faithfully paying the monthly bills for the cards – which they may have forwarded to P.O. boxes or their own homes – while watching credit limits tick higher. After an identity is established, they sign up for more cards. They may add authorized users to the accounts, establishing additional identities that can later seek their own credit. When the scheme is ripe, the fraudsters charge everything to the hilt, a phase commonly known as "busting out." Payoffs can stretch into the tens of thousands of dollars. The identities are then discarded.

When a synthetic account goes bad, lenders often assume a good customer fell on hard times. Their collections departments may waste months trying to reach the borrower before realizing it was all a fiction.

The most prized data for synthetic fraud are the SSNs of people who don't use credit, including infants and children, because they give the thief a blank slate to work from. For decades, banks easily deflected attempts to use a child's SSN because the owner's birth year was baked into their digits. But in 2011, the Social Security Administration began randomizing numbers from start to finish. Despite this risk, synthetic credit card fraud is primarily a problem for banks, which are forced to eat the losses when a fraudster busts out and disappears. The true holder of a stolen SSN may have some difficulty applying for credit but isn't responsible for any unlawful activity.

The SSA does operate a database that lenders can use to confirm an applicant's name, birth date, and SSN. Banks pay a one-time $5,000 enrollment charge plus a fee every time they look up someone, which requires handwritten consent from the customer. Banks, which try to control costs by serving customers online or by phone, have pushed for the agency to allow a more modern form of digital consent. The SSA says that roughly 86 companies have enrolled in its verification service. "Safeguarding the public's information is a top priority," it said. The agency "does not accept electronic signatures on the consent form."

Synthetic fraud is starting to pop up in data across the industry. The unemployment rate and credit card write-offs typically move in lockstep. But as the unemployment rate continued its steady decline this year, the five largest U.S. card issuers saw combined write-offs surge. That disconnect is at least partly attributable to synthetic fraud. Banks started becoming particularly concerned after noticing write-offs were climbing among borrowers with higher credit scores.

Card issuers try to prevent synthetic fraud by noting which computers and tablets customers use to file credit applications. But one "Simmer" who was arrested filed 90% of his 750 applications by phone, using hundreds of mailing addresses, according to an affidavit filed by prosecutors. Capital One eventually detected his activity with fraud analytics software. According to prosecutors, the bank realized that a variety of cardholders happened to be making transactions with the same cluster of merchants and PayPal accounts.

This is why protecting against data breaches is important not only for you as a company, but as a consumer. The Equifax breach has provided a treasure trove of information that will enable fraudsters to easily set up synthetic identities, and your personal data may be co-mingled into a new identity. SIM2K urges you to monitor your credit information carefully, especially now.

Hackers Hit Cloud-based E-mails

Deloitte, one of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential e-mails and plans of some of its blue-chip clients. Deloitte provides auditing, tax consultancy and high-end cybersecurity advice to some of the world's biggest banks, multinational companies, media enterprises, pharmaceutical firms and government agencies. Deloitte clients across all of these sectors had material in the company e-mail system that was breached.

Deloitte discovered the hack in March this year, but it is believed the attackers may have had access to its systems since October or November 2016. The hacker compromised the firm's global e-mail server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas". The account required only a single password and did not have "two-step" verification, sources said.

E-mails to and from Deloitte's 244,000 staff were stored in Microsoft's Azure cloud service. In addition to e-mails, the hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information. Some e-mails had attachments with sensitive security and design details.

The breach is believed to have been US-focused and was regarded as so sensitive that only a handful of Deloitte's most senior partners and lawyers were informed. Responding to questions from industry media, Deloitte confirmed it had been the victim of a hack but insisted only a small number of its clients had been "impacted". It would not discuss how many of its clients had data made potentially vulnerable by the breach.

Though all major companies are targeted by hackers, the breach is a deep embarrassment for Deloitte, which offers potential clients advice on how to manage the risks posed by sophisticated cybersecurity attacks. "Cyber risk is more than a technology or security issue, it is a business risk," Deloitte tells potential customers on its website. While today's fast-paced innovation enables strategic advantage, it also exposes businesses to potential cyber-attack. Embedding best practice cyber behaviors help our clients to minimize the impact on business." Deloitte has a "CyberIntelligence Center" to provide clients with "round-the-clock business focused operational security."

This is not schadenfreude on our part - we don't enjoy seeing a company that makes such a pitch to clients about security being hacked. What it does point out is that everyone is at risk for potential breaches or malware. This is why every SIM2K client should take security very seriously. We have taken on several new partners in the cybersecurity field to give you the best possible defenses against attacks, but everyone needs to be aware of the risks and assess their exposure. Call SIM2K for assistance in hardening your network and putting in advanced tools to protect your data.

Don't Like Edge? Here's Help

Don't like the Windows 10 Microsoft Edge browser? You're not alone. Only 20% of all Windows 10 users ran Edge as their main browser as of August 2017, down from 24% a year earlier, according to Computerworld. Still, that's a lot of people running the browser, and many of them might run it only because Microsoft has made it the Windows 10 default.

There are plenty of reasons to move to a different browser. Start off with extensions – or more precisely, the lack of them. Edge was finally given extension support in August 2016, but even now the number of extensions is extremely low — only about 65. Chrome and Firefox each have thousands, so Edge certainly trails these two browsers in this category. And, if you are a Gmail user, Edge isn't the browser for you, either. Edge won't display Google Inbox, which is a far more efficient way to manage mail than the default Gmail interface.

Edge also has a number of awkward or just plain weird behavioral quirks. Open a new tab, for example, and there's no address bar on it. To visit or URL or do a search, you have to type them into the search box. But when you're visiting a site, you use the address bar. Speaking of the address bar, it doesn't show the protocol being used on a web site, such as http or https. Edge will show the lock icon for https sites, but it's nice to be able to see the entire address including the protocol, rather than having to look for a lock icon.

If you decide you want to switch to another browser as your default, it's easy to do. You'll need to first install the other browser on your system. After that's done, click the Windows 10 Start button and click the Settings icon that appears on the left-hand side of the screen. (It looks like a little gear.) You can also type "settings" into the search box and click the Settings result that appears at the top of the screen.

In the Settings app screen, select Settings > System > Default apps. If you've upgraded to the Windows 10 Creators Update, which was released in April 2017, select Apps > Default apps.

On the Default apps screen, scroll down to the bottom of the display. When you get to the bottom of the screen, you'll see Microsoft Edge under the "Web browser" listing. Click the Microsoft Edge icon and you'll see a pop-up with a list of your installed browsers. Click the browser that you would like to be your default browser. As you'll see when you click it, Microsoft doesn't particularly want you to switch. A screen appears asking you to stay with Edge. Click "Switch anyway," and your new browser will now be the default. No need to restart.

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.

There Will be Office 2019

Microsoft announced that there will be a successor to Office 2016, the non-subscription version of the application suite, and that the upgrade would ship in about a year. The bundle, named Office 2019, will be geared to customers, primarily corporate customers, "who aren't yet ready for the Cloud," according to Microsoft.

But other than that description, Microsoft was vague about Office 2019 as a "perpetual" license, one that lets the customer run the suite as long as desired without further payments, unlike Microsoft's Office 365 which is "rented" to users who pay a monthly (or annualized) fee to use the software.

Microsoft indicated the launch of the suite should occur during the second half of next year. Because the perpetual licensed version of Office 2019 will be built from code already released as Office 365 ProPlus – and because a beta of Office 2019 will debut in mid-2018 – it is likely that Microsoft will use the March 2018 feature upgrade for Office 365 ProPlus subscribers as the basis for Office 2019. The three months between the March 2018 appearance of the ProPlus feature upgrade and the July 2018 launch of the Office 2019 preview will give Microsoft time to digest feedback from customers and fix any bugs that surface.

The feature set may not be revealed until mid-2018, when Microsoft releases a preview of the suite. Microsoft hinted at some of what will make it into Office 2019, such as Ink replay in Word and Morph in PowerPoint, which have been available to Office 365 subscribers for one and two years, respectively. There's little to no chance that Office 2019 will include any groundbreaking new features since the perpetually-licensed version of the suite is built by taking the accumulated changes since the predecessor appeared — the changes issued to Office 365 subscribers over the past several years.

It is believed that Microsoft will offer Office 2019 to commercial customers via volume licensing, but it may be questionable to assume that it will sell single-copy versions at retail. **Microsoft will, at some point, discontinue sales of Office perpetual licenses, analysts have agreed.** (Microsoft has made no secret that it prefers subscriptions – Office 365 in this case – for the recurring revenue they generate.) Dumping single-copy one-time purchases would be the logical place to start reducing the perpetual option.

Earlier this year, Microsoft slashed the rights of users running non-subscription Office when it announced that perpetual-licensed versions of **Office 2016 will be barred from connecting to Microsoft's cloud-based services, including hosted e-mail (Exchange) and online storage (OneDrive for Business)** after Oct. 13, 2020. Under the new rules, owners of a perpetual license for Office 2016 can use those services only during the first half of their 10-year support lifecycle, the portion Microsoft dubs "mainstream", which for Office 2016 ends October 13, 2020. By releasing Office 2019 next year, Microsoft will give enterprises a year or so to migrate from Office 2016 (or an earlier edition) before the cloud service cutoff.

So, for clients not comfortable with the Office 365 Cloud-based Office, there will be a stand-alone version. We will keep you advised as Microsoft's plans become firm.

"Random Tid-Bytes"

CCleaner Holds Malware

Hackers have successfully breached CCleaner's security to inject malware into the app and distribute it to millions of users. Security experts discovered that download servers used by Avast, the owner of CCleaner, were compromised to distribute malware inside this software. CCleaner has been downloaded more than 2 billion times according to Avast, making it a popular target for hackers. Dubbed "crap cleaner," it's designed to wipe out cookies and offer some web privacy protections. This is an unusual attack as software similar to CCleaner is trusted by consumers. By exploiting the trust relationship between software vendors and the users of their software, attackers can benefit from users' inherent trust in the files and web servers used to distribute updates. The malware itself appears to have been designed to use infected PCs as part of a botnet. 2.27 million users have been affected by the attack, and Avast believes it was able to prevent the breach harming customers.

Too Much Charge for Smartphones?

With Apple finally bringing native wireless charging to its iPhone line, the technology will become more widely adopted by consumers and corporations. But, given the ease of just placing the phone on a charging mat, is it possible to "overcharge" a device? According to the Argonne Collaborative Center for Energy Storage Science (ACCESS), you cannot overcharge a battery, but keeping it fully charged may hasten the degradation of the battery. As a lithium-ion battery charges and discharges, ions pass back and forth between a positive and a negative electrode. As a battery charges, the positive electrode gives off lithium ions that move to the negative electrode and are stored as energy. As the battery discharges, those ions move back to the positive electrode to be used as electricity. As those lithium ions move back and forth, the electrolyte that acts as the transport medium degrades over time. The higher the state of charge, the faster the electrolyte degrades. Therefore, it's best not only to keep your smartphone below its top charge, but also to keep the charging and discharging pendulum from swinging wildly.

Microsoft Introduces "Teams" - aka Skype

Microsoft's Skype for Business will be replaced by Teams, which is slated to become the primary communications client within Office 365. The Teams instant messaging platform – which is bundled with the company's Office 365 productivity suite – was launched only six months ago as a rival to Slack. According to Microsoft, there are now 125,000 organizations using the software globally. Teams is already running on Skype's cloud-based infrastructure for video and audio calls, which Microsoft is "evolving rapidly." Skype for Business has been the primary tool for video conferencing and enterprise chat since taking over from chat application Lync. Team will replace Skype for Business "over time," says Microsoft as it will release a new version of Skype for Business in the second half of 2018. Microsoft is positioning Teams as the central tool for "intelligent communications" and says it will include new tools such as recording and transcribing discussions, subsequently adding notes and recordings after a call, as well as basic calling features as the ability to make and receive public network calls from the applications, as well as call hold, call transfer and voicemail.

Life After WannaCry

WannaCry ransomware worm spread rapidly across a number of computer networks in May of 2017. After infecting a Windows computers, it encrypted files on the PC's hard drive, making it impossible for users to access them, then demanded a ransom payment in bitcoin in order to decrypt the files. Now that the immediate panic has subsided, more facts on this infection are coming out.

A number of factors made the initial spread of WannaCry particularly noteworthy: it struck a number of important and high-profile systems, including many in Britain's National Health Service; it exploited a Windows vulnerability that was suspected to have been first discovered by the United States National Security Agency; and it was tentatively linked by Symantec and other security researchers to the Lazarus Group, a cybercrime organization that may be connected to the North Korean government.

The WannaCry ransomware had several components:

- An application that encrypts and decrypts data
- Files containing encryption keys
- A copy of Tor (the dark web browser)

The program code was relatively easy for security pros to analyze. Once launched, WannaCry tried to access a hard-coded URL (the so-called kill switch); if it can't, it proceeds to search for and encrypt files in a slew of important formats, ranging from Microsoft Office files to MP3s, leaving them inaccessible to the user. It then displays a ransom notice, demanding $300 in Bitcoin to decrypt the files.

The attack vector for WannaCry is more interesting than the ransomware itself. The vulnerability WannaCry exploits lies in the Windows implementation of the Server Message Block (SMB) protocol. It is believed that the U.S. National Security Agency discovered this vulnerability and, rather than reporting it to the infosec community, developed code to exploit it, called EternalBlue. This exploit was in turn stolen by a hacking group known as the Shadow Brokers, who released it in April. Microsoft itself had discovered the vulnerability a month prior and had released a patch, but many systems remained vulnerable as the patch had not yet been applied.

Even if a PC had been successfully infected, WannaCry didn't necessarily begin encrypting files. That's because, it first attempted to reach a specific URL. If it could reach this address, WannaCry shut itself down. Researchers are not clear as to why this was built into the malware, but some feel this was an attempt to evade detection by the anti-virus software researchers. This is how WannaCry was defeated – a researcher did discover this URL, registered the domain (for $10.69) and set up a site there, which acted as a "kill switch" for the ransomware.

Ironically, the patch needed to prevent WannaCry infections was actually available before the attack began: Microsoft Security Bulletin MS17-010, released on March 14, 2017. Despite this update being flagged as critical, many systems had not been updated by the May release of WannaCry.

For those unpatched systems that were infected, there is little remedy beyond restoring files from a safe backup — so let that be a lesson that you should always back up your files. Of course, SIM2K offers backup services and defenses with our SIM2K SafetyNet Pinnacle managed service plan, giving you updates, backups and anti-malware protection.

While those monitoring the bitcoin wallets identified in the extortion message say that some people are paying the ransom, there was little evidence that files were truly decrypted, so a full restore was required. As noted, Microsoft released a patch for the SMB vulnerability that WannaCry exploits two months before the attack began. However, it initially was only available for currently supported versions of Windows, which notably excluded Windows XP. There are still millions of internet-connected Windows XP systems out there, as well as machines running Windows 7.

After the initial dust settled, various security researchers began working to try to figure out the origins of WannaCry. Symantec had a provocative take: they believed that the code might have a North Korean origin. They traced Wanna Cry back to an earlier version that used stolen credentials to launch an attack, authored by the Lazarus Group. The Lazarus Group is a hacking group that has been tied to North Korea. Beginning their run in 2009 with crude denial of service attacks on South Korea, they have become increasingly sophisticated, including the Sony hack a year ago.

On the other hand, without an explicit claim of responsibility, it's impossible to know for sure that either the initial wave of WannaCry attacks or the later copycat attacks were directed by North Korea, since malware code is copied liberally by various groups.

Despite the origins, the quick spread of WannaCry drives home the dangers of "zero-day" malware attacks or those that hit prior to critical software patches being applied. That is why SIM2K recommends a "defense in depth" approach, going beyond just anti-virus software and to include predictive protection such as CylancePROTECT® which prevents cyberattacks from being successful by providing a proactive security posture with higher efficacy than traditional antivirus. Using artificial intelligence and machine learning to identify malware before it can execute, CylancePROTECT prevents advanced threats that traditional anti-virus software cannot. CylancePROTECT prevents over 99% of malware before it can execute. including system- and memory-based attacks, scripting, spear phishing, zero-day malware, privilege escalations, and malicious and potentially unwanted programs. This is also part of our Pinnacle service.

Please contact SIM2K for more information on cybersecurity, defense against ransomware and other malware, and how we can put CylancePROTECT to work for you, adding another layer to your defenses against the "bad guys."

CYLANCE

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