A SANS Whitepaper

SANS Top New Attacks and Threat Report

Written by **John Pescatore**

April 2020

Sponsored by:

Anomali

Introduction

The impact of the COVID-19 outbreak has reinforced the fact that physical-world incidents can be far more damaging than cyber world attacks. However, the coronavirus has also highlighted two other key points:

- A secure and resilient digital infrastructure is necessary to survive medical and environmental catastrophes.
- The time to address the top threats and risks is before they begin having an impact.

There are many places to find backward-looking statistics of how many attacks were launched in cyberspace. Forward-looking guidance areas that security managers should focus on are harder to find. In times of economic uncertainty, it is even more critical for security teams to prioritize resources to increase effectiveness and efficiency in dealing with known threats while also minimizing the risk from emerging attacks. For the past 14 years, the SANS "Five Most Dangerous Attacks" expert panel at the annual RSA Conference[1] has filled that gap. This SANS whitepaper begins with a baseline of statistics from three of the most reliable sources of breach and malware data; then it summarizes the expert advice from the SANS instructors on the RSA panel, detailing the emerging threats security teams should look out for in 2020 and beyond—and what to do about them.

[1] www.rsaconference.com/

2020 Breach and Threat Baseline Data

Vulnerabilities and attacks don't really pay attention to the calendar: New Year's Day doesn't bring a drastic change in threats. So, it is important to look back to understand what has become commonplace in order to predict what will be the likely types and areas of new threats. Many threat reports are published each year, but there are only a few sources that aren't tied to specific vendor solutions and that use consistent methodologies year over year.

SANS has found the Identity Theft Resource Center (ITRC) Annual Breach Report,[2] the Microsoft Security Intelligence Report (SIR)[3] and the Center for Internet Security's Multi-State Information Sharing and Analysis Capability (MS-ISAC)[4] have been consistently useful through the years.

The ITRC has been tracking publicly disclosed breach information in the US since 2005 and uses a consistent methodology that provides enough visibility and repeatability to make meaningful year-to-year comparisons. About half of the breaches counted do not disclose the number of records exposed, so the absolute value of the numbers underestimates the totals, but still gives a good view of trends.

As noted in Table 1, the total number of breaches in 2019 increased 17% over 2018 after declining 23% the previous year.[5]

Table 1. ITRC Comparison of Breaches in 2018 and 2019[6]

Data Breaches and Records Exposed per Industry per Year						
	2019			2018		
Industry	Number of Breaches	Sensitive Records Exposed	Non-Sensitive Records Exposed	Number of Breaches	Sensitive Records Exposed	Non-Sensitive Records Exposed
Business	644	18,824,975	705,106,352	575	438,952,056	1,570,602,391
Medical/Healthcare	525	39,378,157	1,852	369	10,632,600	2,800
Government/Military	83	3,606,114	22,747	100	18,447,924	60,085,000
Banking/Credit/Financial	108	100,621,770	20,000	135	1,778,658	Unknown
Education	113	2,252,439	23,103	78	1,414,624	39,690
Totals	**1,473**	**164,683,455**	**705,174,054**	**1,257**	**471,225,862**	**1,630,729,881**

At first glance, the data shows that the total number of sensitive records exposed dropped by 65%. However, a small number of very large breaches skews the data. In 2018, the 383 million record breach of the Marriott Corporation reservation system alone is responsible for more than double the total number of records exposed in 2019. Similarly, there was one mega breach in 2019, the Capital One breach of 100 million records, which represented 99% of all financial records exposed last year. If we remove those two mega breaches from the calculation, the total number of records exposed in 2019 dropped 26% compared with 2018. This is a continuance of last year's

[2] "2019 End-of-Year Data Breach Report," www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

[3] www.microsoft.com/securityinsights

[4] www.cisecurity.org/ms-isac/

[5] "SANS Top New Attacks and Threat Report," April 2019, www.sans.org/reading-room/whitepapers/analyst/top-attacks-threat-report-38908, p. 2, Table 1. [Registration required.]

[6] "2019 End-of-Year Data Breach Report," www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

trend of smaller organizations being targeted. Overall, many large enterprises have improved their defenses against attacks based on malware installation, making the standard data exfiltration attack more difficult.

The ITRC data shows that healthcare organizations experienced a big jump in both the number of breaches and the size of the breaches. This is a glaring statistic, given the importance of medical services to deal with the COVID-19 pandemic. Early 2020 reports show an increase in attacks against medical services and related sites.

The ITRC Breach Report supports the calculation of a very useful metric each year: the average number of records exposed per breach. Because the variable costs to the business scale with the number of records exposed, this metric provides a good estimation of the average cost per incident.

The average number of records per breach seems to have declined a whopping 70%, from 374,881 in 2018 to 111,801 in 2019. However, removing the two mega breaches from the data lowers this to only a 37% decrease in the average breach size.

For breaches in the 50,000–500,000 record range, a rule of thumb estimate of $100 per record in hard costs (not including soft costs such as stock price fluctuation or reputation damage) has proven to be accurate.[7] This indicates that the average cost of a breach in 2019 was about $4.4 million versus $7 million in 2018.

Because the ITRC reports focuses on breaches, DoS and "denial of access" attacks—such as ransomware and other compromises that don't involve data exfiltration—are not represented. The Microsoft SIR continually collects information from hundreds of millions of Windows devices that are running AutoUpdate and popular built-in tools such as Microsoft's Malicious Software Removal Tool, Safety Scanner, Windows Defender and other sources. The Microsoft SIR is nearly 100%-focused on attacks against Windows PCs and servers—and the majority of successful user-focused attacks are aimed at Windows users. In addition, Windows comprises a large share of the server OS market.

The SIR generally comes out twice per year, but as of this writing, Microsoft is providing only an online data analysis site rather than formal reports. Mirroring the trend across 2018, the latest data from the SIR showed declines in simple malware attacks. However, two key areas showed continued increases: phishing encounters and ransomware attacks.

Highly Targeted Phishing Campaigns

As noted earlier, many enterprises have improved their capability to prevent or more quickly detect and respond to standard malware insertion attacks. That has driven attackers to focus on the vulnerable human beings in the equation—the users of the PCs or the administrators of servers and cloud-based services. Enterprise phishing awareness and education programs and adoption of stronger email and DNS authentication standards have made it more difficult for phishing attacks to succeed. However, phishing attacks have continued to become more sophisticated and more targeted—and use more "channels," such as text messaging and voice.

---

[7] www.gartner.com/document/485803 [Subscription required.]

The SIR data only shows a minimal year over year growth in phishing encounters (see Figure 1), but you see spikes that represent "campaigns"—targeted waves of phishing against related targets like healthcare or on headline-grabbing events like the COVID-19 virus. As social media and consumer web meeting systems are increasingly used as a result of social distancing, those attacks will increase. Those sites often expose a lot of information that attackers use to create micro-targeted attacks.

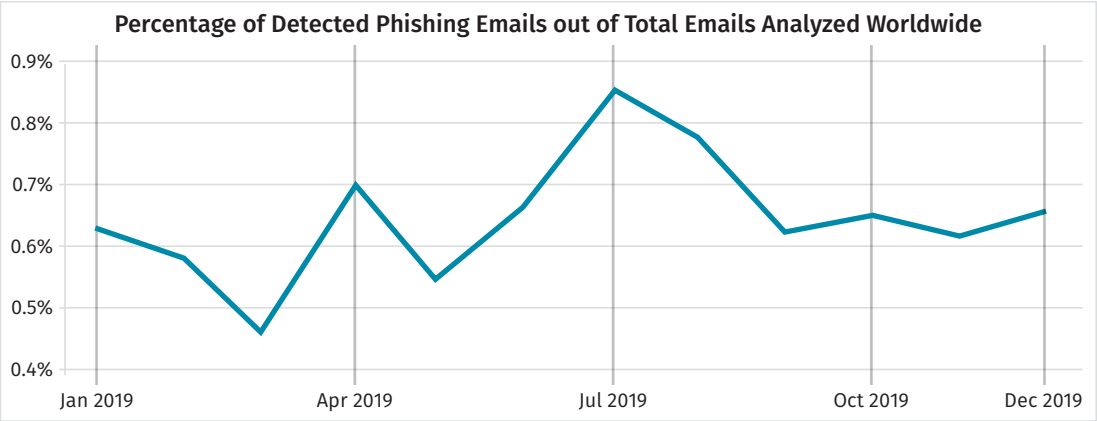

Figure 1. Percentage of Phishing Emails in 2019[8]

Ransomware: The Bane of State and Local Agencies

By now, almost everyone understands what ransomware is[9]—attacks that encrypt files and/or executables to disrupt business and later demand payment (the ransom) for the decryption key. Many of those attacks used simple phishing and malware techniques, and the improvement in anti-phishing and endpoint detection and response have thwarted these attacks. However, many smaller businesses, and in particular state and local government agencies, have been unable to make the same progress. Attackers quickly shifted to target those vulnerable organizations.

Bottom line: Increasing basic security hygiene is key to avoiding or mitigating the majority of commodity attacks. Advances made at this level have caused the overall number of breaches reported in the US to decrease, as illustrated in Figure 2. Minimizing vulnerabilities is also key to avoiding making the breach list. Organizations should test all software for vulnerabilities before deploying it in production environments. Further, they should regularly scan all server, PC and network device configurations for discrepancies against secure standards.

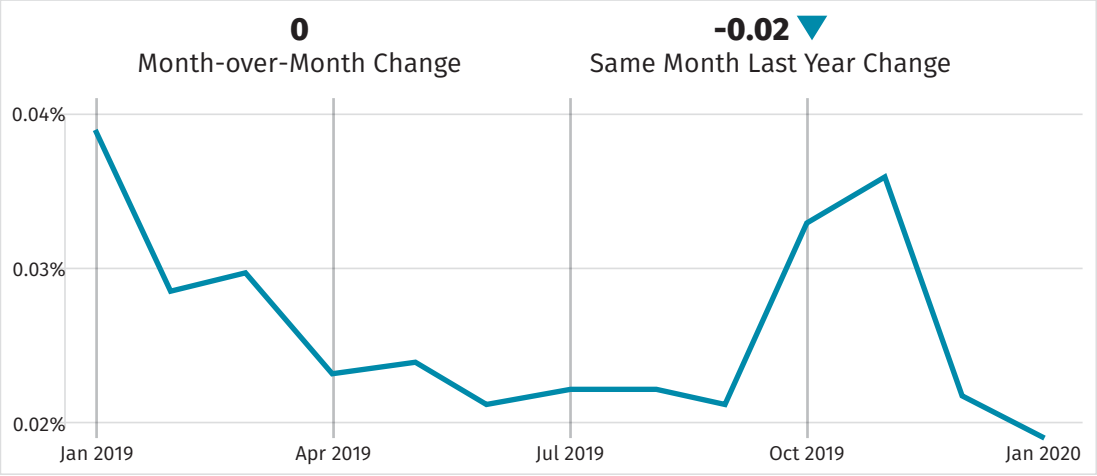

Figure 2. Ransomware Attacks in 2019[10]

[8] "Microsoft Security Intelligence Report: Phishing email detection," www.microsoft.com/securityinsights/Phishing

[9] "OUCH Newsletter: Ransomware," August 2016, www.sans.org/security-awareness-training/ouch-newsletter/2016/ransomware

[10] "Microsoft Security Intelligence Report: Ransomware encounter rates," www.microsoft.com/securityinsights/Ransomware

The attacks that cause the most damage to each corporate victim are the highly targeted attacks—and those continue to increase and are often impossible to completely prevent. The key to minimizing damage from advanced targeted attacks is quicker detection of suspicious events, leading to faster and more surgical mitigation actions. The use of endpoint detection and response tools and advanced capabilities such as browser isolation technology can augment basic security hygiene with damage minimization or prevention capabilities. Consuming and analyzing accurate and timely threat intelligence should be a key input to optimizing security processes, updating playbooks and making security resource decisions.

Ransomware Drill Down: State and Local Governments

The Center for Internet Security runs the MS-ISAC, which provides a central resource for gathering information on cyber threats and sharing of information across state, local and tribal agencies. In 2019, the MS-ISAC observed a 153% increase in state, local, tribal and territorial (SLTT) reporting of ransomware incidents. These incidents were either reported by the victim, disclosed by a trusted third party or found in open source reporting. Figure 3 shows the monthly percentage breakdown of reported ransomware incidents in 2018 and 2019.

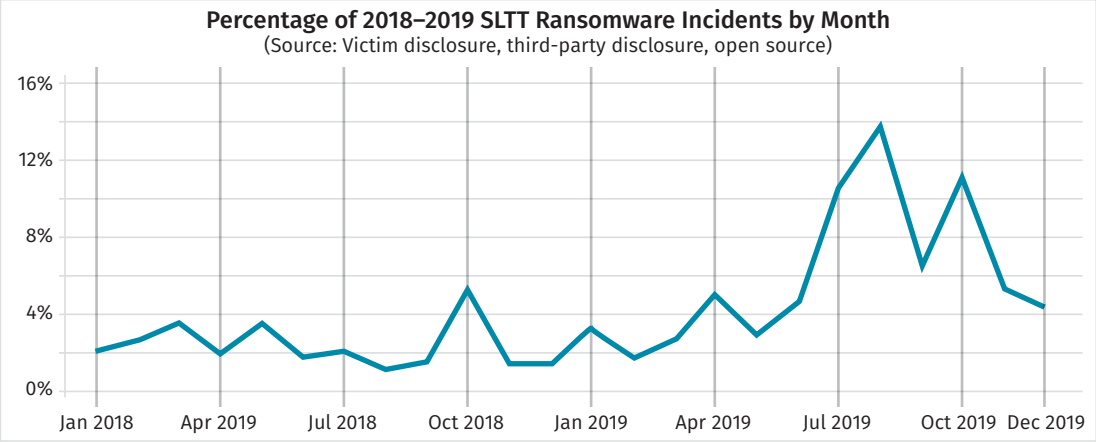

Figure 3. Ransomware Incidents in 2018 and 2019[11]

The MS-ISAC mainly attributes the growth to two types of attacks: a surge in Ryuk ransomware cases and an increase in incidents associated with attackers compromising managed service providers (MSPs) to push ransomware out to their clients. Ryuk, Sodinokibi and Phobos were the three most reported ransomware variants in 2019.

Ryuk establishes network access through the TrickBot banking Trojan. This works because TrickBot infections are widespread, often go undetected for an extended period of time, and can quickly spread throughout a network. The Sodinokibi ransomware variant is most responsible for the increase in MSP-related infections, which leverages the trusted relationship between third-party vendors and their clients. The Phobos ransomware variant typically targets poorly secured Remote Desktop Protocol (RDP) ports as an initial infection vector, despite this being a well-known technique by ransomware attackers for several years. Table 2 shows the 2019 breakdown for these variants.

Table 2. Top 3 Ransomware Variants in 2019[12]

Ransomware Variant	Percentage of Reported Incidents
Ryuk	22.7%
Sodinokibi	10.9%
Phobos	2.8%

[11] www.cisecurity.org/ms-isac/

[12] www.cisecurity.org/ms-isac/

Hear from the Experts: SANS Threat Panel at RSA Conference 2020

The RSA Conference started in 1991 and has grown to be the largest cybersecurity conference in the world. For the past 14 years, SANS has presented a panel featuring top SANS experts who detail their views of the most dangerous attacks starting to impact enterprises.[13] Through the years, the predictions made by the SANS instructors at these sessions have proven to be highly accurate predictors of real-world damage.

The 2020 threat expert panel, moderated by SANS Founder and Research Director Alan Paller, consisted of:

- **Ed Skoudis**, SANS Faculty Fellow and Director of SANS Cyber Ranges and Team-Based Training
- **Heather Mahalik**, Senior Instructor, SANS Institute, and Senior Director of Digital Forensics, Cellebrite
- **Dr. Johannes Ullrich**, Dean of Research, SANS Technology Institute, and Founder and Director, Internet Storm Center

The 2020 Threat Expert Panel (l–r): Ed Skoudis, Heather Mahalik and Dr. Johannes Ullrich

Each SANS expert focused on areas they believed would have the highest impact in the coming year. The key areas include the proliferation of command and control toolkits and frameworks, "living off the land" attacks, very deep persistence, rising risks when users lose even temporary physical control of their mobile devices, and vulnerabilities in perimeter security controls and web agents that span the perimeter. The following summarizes the experts' views of each issue and their advice on how to avoid or minimize damage.

Command and Controls Tools and Frameworks

Ed Skoudis first highlighted the proliferation of command and control (C2) tools and frameworks used by attackers. Most advanced threats proceed along distinct phases delineated in the popular Cyber Kill Chain® model first described by Lockheed Martin.[14] Often, the attacker uses simple techniques to get the first foothold on a target with the installation of a limited malware executable. This executable then calls out to C2 sites controlled by the

> *"We've seen an explosion in the amount and sophistication of tools available to attackers over the last year. There are dozens and dozens of different tools that attackers can use to control systems that they've compromised in target environments. The good news is these tools are also available to penetration testers and red/blue/purple teams to analyze."*
>
> —Ed Skoudis

[13] "The Five Most Dangerous New Attack Techniques and How to Counter Them," www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, February 27, 2020.

[14] "Applying Security Awareness to the Cyber Kill Chain," May 31, 2019, www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

attacker over connections that use techniques to evade detection. The C2 sites will then download more advanced and targeted executables to launch ransomware, data exfiltration or long-term surveillance attacks.

Designing and building a C2 capability is a sophisticated undertaking, often out of the reach of lesser-skilled attackers. C2 toolkits and frameworks provide building blocks so that targeted and evasive attacks become within the reach of all cyberattackers.

There are dozens of different tools that attackers can use to control systems that they've compromised in target environments. Knowledge of the tools is important for penetration testers to emulate adversaries and for red teams to understand the tactics and techniques in use. However, there are so many of these tools, it can be hard to sort them out.

That's why SANS instructor Jorge Orchilles and many other volunteers put together something called the C2 Matrix.[15] The website allows you to analyze all the different C2 channels that are publicly and freely, or even commercially, available for attackers to control their malware in a target environment. It lists all of the different tools and has an interactive display that you can work your way through to see the different feature sets, including different ways to communicate across the network, and other tasks. It is a tremendous learning tool.

Mitigation: To defend against attacks using these tools, Skoudis said security teams need to vigorously monitor and control outbound traffic from their environments. Last year, Skoudis pointed to Rita, a free tool from Black Hills Information Security that looks at network traffic to see if there's beaconing activity.[16] This year he highlighted DeepBlueCLI by SANS instructor Eric Conrad.[17] This is another free tool that you feed Windows event logs into and it applies various analytics. Written in PowerShell, it will tell you which events look suspicious, such as indications of a password spraying or password guessing attack, or indication of lateral movement throughout the target environment.

Application whitelisting and application control go a long way to protect against the C2 frameworks, because they limit what the attacker can run on the target system. But, enterprises have traditionally had difficulties in deploying effective application whitelisting, and attackers have learned how to mimic legitimate applications and evade the less effective controls.

---

[15] www.thec2matrix.com/about

[16] www.blackhillsinfosec.com/projects/rita/

[17] https://drive.google.com/file/d/0ByeHgv6rpa3gNU4wLVZKNjd4cTA/edit

Living off the Land

Skoudis also described "living off the land" attacks, a phrase first put out by Christopher Campbell and Matt Graeber. The idea here is to use the resources and features of an operating system to attack itself and then use that system as a launching point to attack other targets. Skoudis describes this as "using the OS as a rootkit against itself." In effect, what attackers are doing is using pieces of the OS to attack the OS, guided by thinking about what a SOC analyst will interpret when looking at those events. In effect, the attacker is social engineering the analyst by creating malicious effects that look like normal activity on the system.

Skoudis pointed to the Living Off The Land Binaries And Scripts (LOLBAS) project as an excellent project that tries to document every binary, script and library that can be used for living off the land techniques.[18] It includes more than 100 different executables in Linux, macOS and Windows that can be used to attack those systems right from within. The list includes all known binaries, scripts and libraries that could be used by both advanced attackers and pen testers/red teams, including a focus on ways to bypass application controls as mentioned earlier.

Mitigation: In addition to whitelisting, purple teaming is the key area Skoudis pointed to for effective detection and mitigation of living off the land attacks. Blue teams are the security operations teams that architect, deploy and operate security controls. Red teams are the penetration testers and other "friendly adversaries" who test the blue teams' defenses and provide feedback on the weaknesses discovered. Purple teaming is a coordinated effort involving the two groups to examine new attacker techniques such as LOLBAS, develop improved defenses and then see how well they stand up to red team attacks. This can greatly shorten the time to market for effective new defensive strategies. See Figure 4.

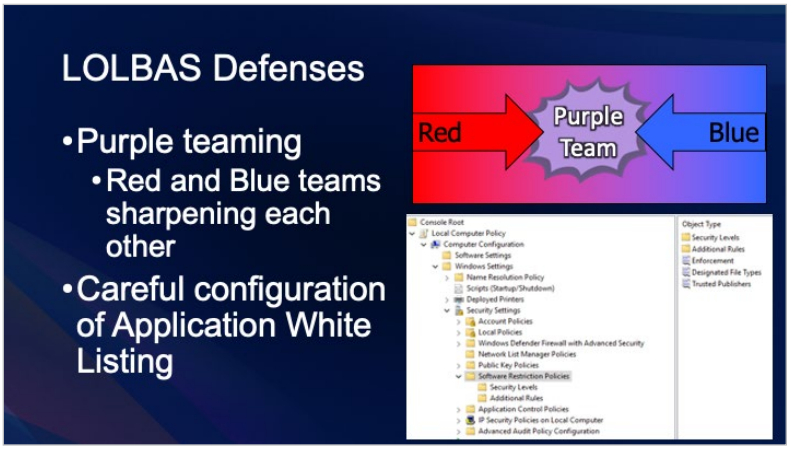

Figure 4. Living Off The Land Binaries and Scripts (LOLBAS) Defenses[19]

Very Deep Persistence

The final area Skoudis detailed was what he called *very deep persistence*, essentially malicious capabilities that are buried within hardware, accessories or components. An older example is Rubber Ducky which is a preprogrammed USB drive that, when plugged into a target, emulates a keyboard and injects keystrokes into the system to launch a terminal window, type in malware, save the malware and then execute the malware.

The FBI recently sent out a flash alert warning of compromised USB drives being received by US citizens with promises of prizes if the ads shown on the device were viewed.

[18] "Living Off The Land Binaries and Scripts (and now also Libraries)," https://github.com/LOLBAS-Project/LOLBAS/blob/master/README.md

[19] "The Five Most Dangerous New Attack Techniques and How to Counter Them," www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, February 27, 2020.

It was fairly revolutionary at the time, but now that same capability has been seen embedded into what appears to be a straightforward USB cable. A version called USB Ninja has been available for as little as $99.[20] It looks and performs just like a smartphone charging cable but has capabilities similar to Rubber Ducky and includes the capability to wirelessly bridge onto a target network.

Rubber Ducky and USB Ninja are just two existing examples. The possibilities for embedding such malicious capabilities into just about anything that can connect (through insertion or wirelessly) to a target or be built into a product are endless.

Mitigation: Skoudis pointed out several levels of mitigation:

- Step up user awareness education. Users should know to use only USB devices and cables that come from IT or in sealed blister packs from reputable vendors.
- Subject vendors with which your organization has no history that are promoting low-cost or free offers to thorough vetting and test their products in a safe environment. Increased vendor risk management is important for enterprises buying any devices (even as innocuous as cables) that connect to or are installed on sensitive business systems.
- You and your supply chain partners need to be vigilant in ensuring security of the supply chain for what is built into your company's products and services.

I Received a Poisoned USB Drive in Snail Mail!

Back in February when I brought in the mail one day at our house, I received a small brown envelope. There was no return address on the pre-printed label, and there was only a bar code—no stamps or postage meter indication. Still, it looked very similar to what you receive when you order some small item online and it comes from China via the US Postal Service.

Inside was a 16GB USB drive of some brand I didn't recognize along with a folded piece of paper with directions and a 2D bar code. The instructions told me to insert the drive in my computer, click on one of the prizes displayed and then go to eBay and buy them—and they would be free! If I wanted to use my phone, I could use the 2D bar code instead.

Being a trained security professional, I've always told everyone to treat USB drives from unknown sources as what as kids we used to call ABC gum—already been chewed gum. You wouldn't pick that up from the ground and put it in your mouth, so don't put an ABC USB drive in your computer's mouth.

I took pictures of everything and went to the FBI and US Postal Service websites to report the incident. I never got any follow-up (other than acknowledging receipt of my input). A week later I smashed the USB to pieces and threw it away just to be safe. It wasn't until I started working on this report that I realized there were widespread campaigns taking this approach.

—John Pescatore

Mobile Devices: The Good News/Bad News

Heather Mahalik focused on attacks taking advantage of the complex—nearly addictive—relationship that users have with their smartphones. The typical user has any number of channels open simultaneously: voice, text messaging, email, social media, websites, and so on. Most smartphones also support multiple network connections, including USB, Wi-Fi, cellular data, Bluetooth and others. Attackers can combine any or all those methods to create very convincing phishing attacks by taking advantage of users' tendencies to treat smartphone replies as urgently time-sensitive—not to mention that users are often driving or eating or crossing streets while using those devices. Acting in haste with a lack of attention is the phisher's goldmine.

[20] "From Spyware to Ninja Cable," Sept. 9, 2019, www.darkreading.com/risk/from-spyware-to-ninja-cable/a/d-id/1335710, February 27, 2020.

Mahalik focused on often-overlooked attack vectors that are very specific to cell phones: planned and unplanned losses of physical control of the device. The *planned* cases are when the user buys a new phone or receives a new phone at work. What happens to the data on those phones and the pre-authenticated access to web apps, cloud services and corporate VPNs? Examples abound of smartphones being sold on eBay or Craigslist—and the buyer finding a treasure trove of information. The old phone might also be returned to the carrier as part of a trade-in on a new model and end up in another country for recycling—possibly before sensitive information is removed from the device.

> *"We are all addicted to our phones, but all too often we temporarily lose track of them. Exploits like* ***Checkm8*** *and* ***Checkra1n*** *have made it increasingly critical to up our games in protecting our mobile devices."*
>
> —Heather Mahalik

Mahalik then explained how *unplanned device losses* are subject to the Checkm8 jailbreak attack that came out in September 2019.[21] Anytime a user has lost temporary physical control of the device, it could be compromised. One high-risk scenario is cell phones left in hotel rooms or temporarily confiscated by airport officials in countries with active, offensive cybersecurity programs. All Apple iOS devices running the Apple A5 to A11 chipsets (essentially all Apple devices through 2017, including iPhone 4 through X) are vulnerable to **Checkm8**. This is a bootrom vulnerability, described by the researcher who discovered it as "permanently unpatchable."

Checkra1n, the exploit for the **Checkm8** vulnerability, came out shortly thereafter, allowing users to jailbreak their own phones and bypass the Apple App Store mechanisms—opening the floodgates for malware onto the iPhone.[22] **Checkra1n** also enables attackers to essentially rootkit the iPhone if they have physical access to the device.

Mahalik then described another scenario that undermines a potential security improvement—using text messaging to a cell phone as two-factor authentication (2FA). The issue occurs when a user moves or changes carriers and, for a variety of reasons, gets a new phone number rather than transferring the old number. All the 2FA services in use are tied to the old phone number, enabling whoever gets the old phone number to subvert 2FA and take over the legitimate user's accounts. Once the number is changed, the race is on.

Mitigation: Mahalik pointed out a number of simple steps to reduce the risk of these attacks against mobile phones:

1. **Lock your phone.** Turn on fingerprint or facial recognition for logon, if your device supports it, and enable the time-out timer to as short a value as you can stand.
2. **Disable old phones.** If you are getting a new phone, either have the IT organization or the carrier sanitize the old phone—or just smash it to bits with a hammer, which can be quite stress-reducing.

---

[21] "New Checkm8 jailbreak released for all iOS devices running A5 to A11 chips," Sept. 27, 2019, www.zdnet.com/article/new-checkm8-jailbreak-released-for-all-ios-devices-running-a5-to-a11-chips/

[22] "Just-Released Checkra1n iPhone Jailbreak Stirs Security Concerns," https://threatpost.com/checkra1n-jailbreak-stirs-concerns/150182/

3. **Use clean phones internationally.** Give all executives traveling to countries that are considered risky for cyberespionage clean phones for the duration of their trip. At the end of the trip, collect those phones and sanitize them.
4. **Reboot vulnerable devices.** At the very least, reboot vulnerable iOS devices after any loss of physical control.
5. **Don't change mobile phone numbers if you don't have to.** If you are going to change numbers (including if you give your kids your old phone), go to every application for which you use 2FA. Temporarily disable it until you get the new number; then reenable 2FA with the new number.

"A strong perimeter is still important for minimizing your attack aperture; but two trends this year have exposed weaknesses in existing security controls as well as driven the need for more aggressive approaches around web agents being installed on user devices."
—Dr. Johannes Ullrich

Attackers Finding Insecurities in Security Products

Dr. Johannes Ullrich focused on two areas where attackers were finding vulnerabilities in security products and how badly written persistent web agents enabled penetration of security perimeters. The traditional perimeter has evolved significantly over the years, as employees have become more mobile and business applications have become increasingly based externally in the cloud as opposed to residing internally in the on-premises data center. The modern perimeter still depends on firewalls and VPNs on the edge, but it increasingly includes a security footprint either on the user's endpoint or in a proxy cloud security service between the user and sensitive applications.

The first attack trend Ullrich pointed out was increased exploitation of vulnerabilities found in critical security products used on the perimeter, such as firewalls and VPNs.[23]

In April 2019, Pulse Secure released patches to its Pulse Connect Secure VPN remote access product.[24] The vulnerabilities included well-known coding weaknesses, such as cross-site scripting, buffer overflows and code injection that enabled attackers to gain authorized access. In December 2019, Citrix released CVE-2019-19781, which detailed a directory traversal vulnerability in the Citrix (NetScaler) Application Delivery Controller that enabled remote file execution.[25] Exploits were seen against both of these vulnerabilities starting in mid-January 2020, as shown in Figure 5.

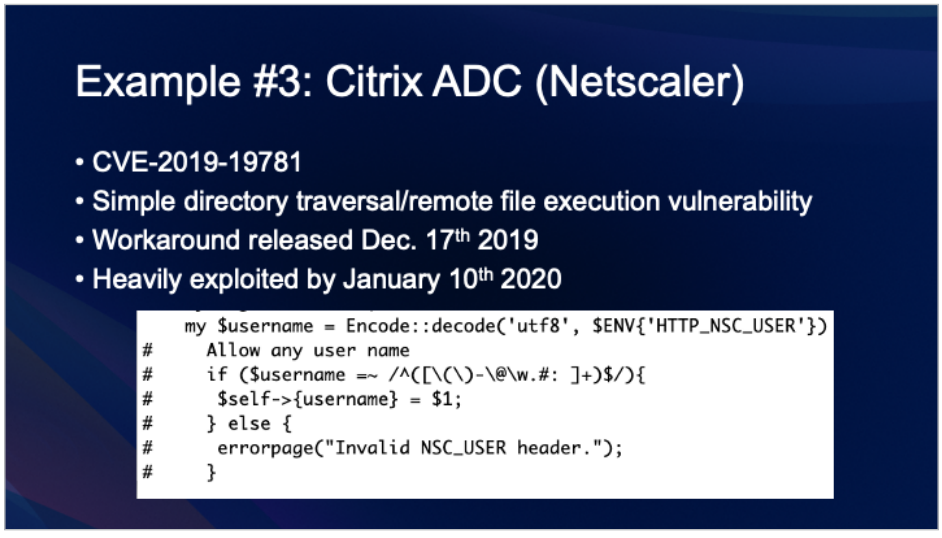

Figure 5. Citrix ADC (NetScaler) Exploit Summary[26]

[23] www.cvedetails.com/vulnerability-list/vendor_id-15824/product_id-33650/Pulsesecure-Pulse-Connect-Secure.html

[24] www.us-cert.gov/ncas/alerts/aa20-010a

[25] https://support.citrix.com/article/CTX267027

[26] "The Five Most Dangerous New Attack Techniques and How to Counter Them," www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2020, February 27, 2020.

Similarly, in July 2019, Palo Alto Networks released a number of patches[27] to the PAN OS operating system that runs under all Palo Alto Networks' next-generation firewall products. The patches address critical code injection and cross-site scripting flaws. Additional critical code injection and privilege escalation vulnerabilities in the PAN OS were announced in November and December 2019, including CVE-2019-17440,[28] an improper restriction of communications vulnerability that enabled attackers to gain root-level access to a device running the PAN OS. Palo Alto Networks gave this vulnerability the highest possible severity of 10, indicating immediate patching was critical.

Critical vulnerabilities in any piece of mission-critical software or appliance are obviously very dangerous and need to be patched as quickly as possible. Unfortunately, many enterprise patching processes and systems do not fully include network and security (or other) appliances that don't allow agents to be installed or otherwise easily accessed.

Mitigation: Ullrich pointed out that the standard advice to limit and monitor access to administrative interfaces is still critical, but is not sufficient when vulnerabilities are exploitable outside the admin interface or in another critical security server such as the VPN used to grant access to the interface.

Additional recommended steps to take:

- Weigh demonstration of security testing by the vendor heavily and evaluate ease of applying patches in requests for proposal (RFPs)/invitations for bids (IFBs) for security appliances.
- As part of any pre- or post-procurement proof-of-concept testing, try some testing yourself if you have skilled penetration testers available.
- Limit your attack surface by turning off all unnecessary features and services.
- Have rapid patching processes and playbooks defined and tested for security-critical products. This may require monitoring multiple vendor websites or mailing lists.

Persistent and Promiscuous Web Agents

The second attack area Ullrich pointed out is the proliferation of persistent web agents. The traditional fat client PC application has largely been replaced with the browser as the universal client. To some extent, that was a move forward in security—fewer insecurely written applications on the user's device is a good thing. If the browser had remained a simple thin client for viewing HTML on websites, it would have been a good thing.

[27] https://security.paloaltonetworks.com/?sort=-date

[28] https://security.paloaltonetworks.com/CVE-2019-17440

However, browsers turned into heavyweight, mini-operating systems with extensions, applets and browser "helper" objects, and all kinds of downloadable executables to "improve" the user experience—at least to improve server's ability to enable more complex interaction with the user. Those tools, of course, greatly increase the attack surface for attackers to probe and penetrate.

Examples Ullrich pointed out included popular online conferencing systems, such as Cisco WebEx, Zoom, and others, as well as the many vendor- and business-support websites. Those services ask the user to allow an agent to be installed, or sometimes the agents are pre-installed by the PC vendor. The agent listens to HTTP requests, and the browser can send a JavaScript-triggered request to that agent and request information from any application running on the system. When the user is at the legitimate website, and if the agent is written securely, it works great. However, if the user is tricked into going to the wrong website by one of those ubiquitous phishing attacks, that website can now load the same JavaScript that the tech-support website loaded, and send requests that end up in a total compromise of the user's PC. This has happened. It is not just a theoretical attack.

Mitigation: Ullrich said the first step is to know what active HTTP listeners are running on your PC.[29] However, many listeners may be in use by IT operations and tech support—you can't just randomly kill them all. Host-based firewalls, endpoint detection and response (EDR) software and secure web gateways can also provide a layer of control.

Additionally, if your business applications include the use of web agents in your products or services, make sure your code avoids common web application software vulnerabilities such as the OWASP Top 10.[30] At a minimum, ensure that the agent software checks and limits the origin of any requests.

Best Practices for Improving Defenses

Very rapidly in 2020, we have been smacked in the face with reminders that standard hygienic precautions are critical to even have a starting point for surviving to fight higher-level threats. The same is true in cybersecurity: Basic security hygiene—having an accurate hardware and software inventory, patching rapidly, educating users about the risk of new technologies such as smartphones and cloud services—is still key. The Center for Internet Security Critical Security Controls[31] is a widely accepted community-driven framework that maintains a prioritized list of the security processes and controls that provide efficient and effective starting points for dealing with many of the attacks detailed in this paper.

[29] "Netcat Cheat Sheet: Pocket Reference Guide," www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

[30] "OWASP Top Ten," https://owasp.org/www-project-top-ten/

[31] www.cisecurity.org/controls/ [Registration required.]

Many of the attacks detailed this year by the SANS experts are in areas where new technology is creating major cracks in how IT has traditionally governed and managed hardware and software. Living off the land attacks use the standardization of operating systems against themselves. Persistent web apps are not software that the IT organization issues or, in many cases, even knows about. Smartphones have long existed in the gray area between personal use and business use. The mitigations for these attacks detailed by the instructors largely represent focusing on plugging these gaps—using new information sources to augment or upgrade well-known security controls with advanced techniques to mitigate new risk areas. On the endpoints, increased privilege management, improved prevention, stronger application isolation and increased fidelity detection and response capabilities should be evaluated. On networks, stricter application-specific traffic controls and more aggressive ingress and egress filtering based on risk inputs are needed. On mobile devices, user awareness and education around the risks of loss of control of the device and plugging into any untrusted physical device or connection should be stressed.

A common thread across the three experts' attack areas is where new approaches and real changes will be needed: supply-chain security. As the impact of the COVID-19 epidemic reverberates over the next few years, already complex supply chains will change in many ways. While fears of international travel may shorten some supply chains, increased demand for remote work will complicate others. Security teams need to prioritize having a place at the table as supply-chain resiliency and survivability plans are being updated or put in place.

Resources

SANS Security Awareness Work-from-Home Deployment Kit,
www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

"SANS Five Most Dangerous Attack Techniques" 2019 Update and Follow-Up,
www.sans.org/the-five-most-dangerous-new-attack-techniques

"How to Evict Attackers Living Off Your Land,"
www.darkreading.com/edge/theedge/how-to-evict-attackers-living-off-your-land/b/d-id/1337420

"'Checkm8' used to jailbreak iPhone X running iOS 13.1.1,"
https://appleinsider.com/articles/19/09/29/checkm8-used-to-jailbreak-iphone-x-running-ios-1311

"Remote Code Execution on most Dell computers,"
https://d4stiny.github.io/Remote-Code-Execution-on-most-Dell-computers/

"What you Need To Know About The Critical Citrix Gateway (Netscaler) Vulnerability CVE-2019-19781," December 31, 2019,
https://www.sans.org/webcasts/about-critical-citrix-gateway-netscaler-vulnerability-cve-2019-19781-112990
[Registration required.]

Sponsor Links

Anomali

"Rise of Legitimate Services for Backdoor Command and Control,"
www.anomali.com/resources/anomali-labs-reports/rise-of-legitimate-services-for-backdoor-command-and-control

"COVID-19 Themes Are Being Utilized by Threat Actors of Varying Sophistication,"
www.anomali.com/blog/covid-19-themes-are-being-utilized-by-threat-actors-of-varying-sophistication

"COVID-19: With Everyone Working from Home, VPN Security Has Now Become Paramount,"
https://forum.anomali.com/t/covid-19-with-everyone-wokring-from-home-vpn-security-has-now-become-paramount/4672

Cyberinc

"Isla – Use Cases: Ransomware,"
https://cyberinc.com/browser-isolation/ransomware

"Isla – Use Cases: Phishing,"
https://cyberinc.com/browser-isolation/phishing

InfoBlox

"Securing Remote Workers in the Age of Teleworking,"
https://info.infoblox.com/resources-whitepapers-securing-remote-workers-in-the-age-of-teleworking
[Registration required.]

"Cyber Threat Reports,"
https://www.infoblox.com/cyber-intelligence-unit/cyber-threat-reports/
[Subscription required.]

"Protect Your Network, Brand and Customers with Custom Lookalike Domain Monitoring,"
www.infoblox.com/resources/solution-notes/protect-your-network-and-customers-with-lookalike-monitoring

"What's Lurking in the Shadows 2020: Exposing how IoT devices open a portal for chaos across the network,"
www.infoblox.com/resources/whitepaper/whats-lurking-in-the-shadows-2020
[Registration required.]

"Remote Office Networks Pose Business and Reliability Risk: A Survey of IT Professionals,"
www.infoblox.com/resources/whitepaper/remote-office-networks-pose-business-and-reliability-risk-survey
[Registration required.]

"An Introduction to MITRE ATT&CK,"
www.infoblox.com/resources/whitepaper/introduction-to-mitre-attck
[Registration required.]

"An Introduction to Zero Trust: A Compelling Cybersecurity Strategy for Defending the Enterprise,"
www.infoblox.com/resources/whitepaper/an-introduction-to-zero-trust
[Registration required.]

"Adopting NIST Cyber Security Framework using Foundational Network Infrastructure,"
www.infoblox.com/resources/whitepaper/adopting-nist-cyber-security-framework
[Registration required.]

Unisys

"Four Reasons to Kill The VPN: Security, Speed, Simplicity and Savings,"
https://assets.unisys.com/documents/global/povpapers/pov_200184_fourreasontokillthevpn.pdf

Verodin

"Verodin 2020 Security Effectiveness Report: Executive Summary,"
https://www2.verodin.com/2020SecurityReport_ExecutiveSummary
[Registration required.]

Verodin Security Instrumentation Platform,
https://www.fireeye.com/solutions/verodin-security-instrumentation.html

About the Author

John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, running consulting groups at Trusted Information Systems and Entrust, 11 years with GTE, and service with both the National Security Agency, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and surveillance systems and "the occasional ballistic armor installation." John has testified before Congress about cybersecurity, was named one of the 15 most-influential people in security in 2008 and is an NSA-certified cryptologic engineer.

Sponsor

SANS would like to thank this whitepaper's sponsor:

ANOMALI®