SANS

A SANS Whitepaper

SANS Top New Attacks and Threat Report

Written by **John Pescatore**

April 2019

Sponsored by:

DomainTools

Introduction

There is no shortage of media coverage of breaches and outages, and there are many places to find backward-looking statistics about how many attacks were launched in cyberspace. What is harder to find is expert analysis of the areas security managers should prioritize in order to increase effectiveness and efficiency in dealing with known threats while also minimizing the risk from emerging attacks. For the past 13 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 two of the most reliable sources of breach and malware data, then summarizes the expert advice from the SANS instructors on the RSA panel, detailing the emerging threats to look out for in 2019 and beyond.

2018 Breach and Threat Baseline Data

To analyze the importance of the new threat vectors, we must establish a baseline of what the current threat environment looks like. There are dozens of reports that enumerate threat counts each year, but most are sponsored by vendors and tend to focus on threat areas that align with the vendors' solutions. They often change methodologies frequently in the name of highlighting something new vs. focusing on long-term issues.

[1] www.rsaconference.com/

The Identity Theft Resource Center (ITRC) End-of-Year Data Breach Report[2] and the Microsoft Security Intelligence Report[3] have been consistently useful in providing unbiased threat data 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 it still gives a good view of trends.

As seen in Table 1, the total number of breaches in 2018 declined 23% when compared with 2017, a promising sign.

Table 1. ITRC Comparison of Breaches in 2017 and 2018[4]

Industry	2018		2017	
	Number of Breaches	Number of Records Exposed	Number of Breaches	Number of Records Exposed
Banking/Credit/Financial	135	1,709,013	134	3,230,308
Business	571	415,233,143	907	181,630,520
Education	76	1,408,670	128	1,418,455
Government/Military	99	18,236,710	79	6,030,619
Medical/Healthcare	363	9,927,798	384	5,302,846
Annual Totals	1,244	446,515,334	1,632	197,612,748

However, the total number of sensitive records exposed more than doubled, largely driven by the enormous scale of the 383 million-record Marriott Corporation reservation system breach. Just removing that one breach from the records tally would change the data to show that the number of sensitive records exposed in 2018 actually *decreased* by more than 60%.

The ITRC report supports the calculation of an important 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.

Excluding the Marriott breach, in 2018 the average number of records per breach declined 58%, from 121,000 in 2017 to 51,000 in 2018. For breaches in the 50,000- to 500,000-record range, a rough estimate of $100 per record in hard costs (not including soft costs such as stock price fluctuation or reputation damage) is accurate.[5]

Using that figure, the average cost of a breach in 2018 was about $5.1 million vs. $12.1 million in 2017. The detailed ITRC data shows that the average was driven down because many smaller targets were breached, a trend that has been continuing for several years. This most likely represents the fact that many larger enterprises have made advances in securing sensitive data (especially the larger "crown jewel" databases), and attackers simply move on to the smaller, more vulnerable targets.

[2] www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

[3] www.microsoft.com/en-us/security/operations/security-intelligence-report

[4] www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf

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

One major blind spot in the ITRC data is that it only tracks breaches. DoS and "denial of access" attacks, such as ransomware and other compromises such as cryptocurrency mining, are not represented. In 2017, both FedEx and Maersk publicly reported that the NotPetya ransomware attack cost them roughly $300 million each,[6] the equivalent of two 3 million-record breaches. The total cost of just the NotPetya malware, looking at only publicly released data, has been estimated at $1.2 billion, or the equivalent of smaller breaches adding up to 12 million records.

As you would expect, the Microsoft Security Intelligence Report (SIR) is nearly 100% focused on attacks against Windows PCs and servers—but the majority of user-focused attacks are aimed at Windows users, and Windows still has a large share of the server OS market. The Microsoft SIR gathers 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 so forth.

The Microsoft SIR also shows declines in many forms of attack during 2018:

- Malware that got past standard AV tools decreased 34%.
- Ransomware attacks were very active in January but declined 75% by December.
- Cryptocurrency mining attacks were very active in March but showed a 73% year-over-year decline.
- User encounters with compromised websites (drive-by downloads) decreased 22% in 2018.

However, one key area showed continued increases: phishing email rates increased 250%, as illustrated in Figure 1, representing slightly more than one out of every 200 emails received by users.

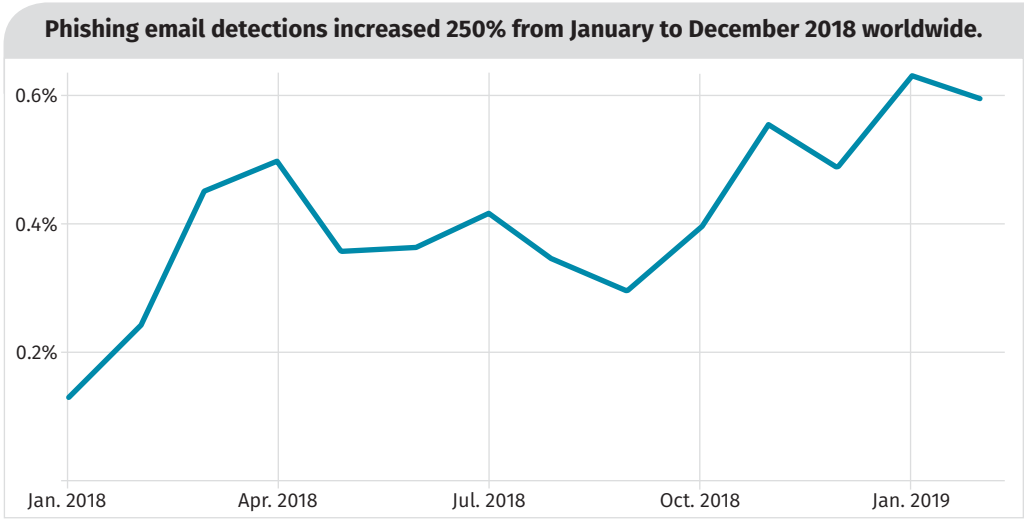

Figure 1. Phishing Attacks Increased[7]

While the Microsoft SIR doesn't provide details, SANS has seen that the most damaging phishing attacks have been targeted against IT admin personnel. Phishing attacks aimed at administrators enable the attackers to obtain passwords with admin privileges to database and application servers. As we'll discuss later, job hunting and professional sites (such as LinkedIn) provide a wealth of information for attackers to craft highly targeted spearphishing campaigns. Social media and other sites provide further levels of personal information that make those inbound spearphishing emails very difficult for even experienced IT personnel to resist.

[6] "NotPetya cyber attack on TNT Express cost FedEx $300m," www.zdnet.com/article/notpetya-cyber-attack-on-tnt-express-cost-fedex-300m and "Shipping company Maersk says June cyberattack could cost it up to $300 million," www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

[7] Adapted from www.microsoft.com/en-us/security/operations/security-intelligence-report, Vol. 24.

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. Minimizing damage from advanced targeted attacks requires quicker detection of suspicious events, leading to faster and more surgical mitigation actions. Consuming and analyzing accurate and timely threat intelligence should be a key input for optimizing security processes, updating playbooks and making security resource decisions.

The key takeaways from the ITRC and Microsoft SIR 2018 data are as follows:

- The absolute volume of inbound malware decreased in 2018.
- The number of enterprises publicly disclosing breaches decreased in 2018.
- Large and business-damaging "mega breaches" caused by targeted attacks continued in 2018, raising the total number of records exposed.
- Phishing emails, the most common attack vector used in targeted attacks, increased in 2018.

Bottom line: Increasing basic security hygiene practices 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, and minimizing vulnerabilities is key to avoiding making the breach list. All software should be tested for vulnerabilities before being deployed in production environments, and all server, PC and network device configurations should be regularly scanned against secure standards.

With this data as background, in the next section expert instructors at SANS provide detailed "threat intelligence" focused on the most dangerous and targeted threats that are emerging today and what you need to do to avoid or minimize damage.

Hear from the Experts: SANS Threat Panel at RSA Data Security Conference

The RSA Conference started in 1991 and has grown to be the largest cybersecurity conference in the world. For the past 13 years, SANS has presented a panel featuring top SANS experts who discuss their views of the most dangerous attacks starting to impact enterprises. 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 2019 threat expert panel,[8] 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 Director of Forensics, ManTech CARD
- **Johannes Ullrich**, Dean of Research, SANS Technology Institute, and Founder and Director, Internet Storm Center

Each SANS expert focused on areas they believed would have the highest impact in the coming year. The key areas include DNS-related attacks, targeted cloud-based personal attacks, and management infrastructure/embedded hardware attacks. The following section summarizes the experts' views of each issue and their advice on how to avoid or minimize damage.

[8] "The Five Most Dangerous New Attack Techniques and How to Counter Them," www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2019, March 7, 2019

DNS-related Attacks

Ed Skoudis detailed two dangerous attacks against corporate DNS services, starting with direct manipulation attacks. Attackers have been obtaining username/password credentials through targeted phishing attacks or via direct attacks on servers or files where passwords or hashes have been stored insecurely.[9]

The attackers use these credentials to log in to DNS providers and domain name registrars, which enables them to manipulate DNS records to redirect traffic to and/or from your organization. A typical approach is to manipulate MX records so that email destined for your organization gets redirected to the attacker's mail servers, allowing the attacker to simply delete your inbound email or to act as a man-in-the-middle and view and modify email.

> *"Bad guys have compromised huge numbers of DNS administrator credentials. Moving to multifactor authentication for DNS administrative access is absolutely critical."*

Attackers also go further by applying for Transport Layer Security (TLS) certificates as the target company, using certificate authorities (CAs) that rely on "verification emails" sent to the target company's domain and that trust responses when the CA receives a return email demonstrating someone clicked on a link in that email. Because the attacker has modified your company's mail records, the attacker's response fools the CA into believing the certificate request came from the legitimate domain owner. The attacker can then send out an HTTPS URL that appears to use a legitimate TLS certificate registered to your company.

These attacks have been given the name *DNSpionage* and there are several detailed reports published about them.[10] In January 2019 the National Cybersecurity and Communications Integration Center (NCCIC), part of the Cybersecurity and Infrastructure Security Agency (CISA), put out a warning about variants focusing on government agencies.[11]

Mitigation—For DNS defenses, the first and most important step is to make sure that multifactor authentication is required as a minimum for whenever DNS administrators are making changes to your DNS infrastructure. This is critical whether internal personnel or a third party manages the DNS infrastructure.

If you have not been using strong authentication on DNS admin accounts, you need to make sure your DNS services have not already been compromised. Skoudis pointed out there are free services you can leverage, such as SecurityTrails, to obtain a list of DNS changes to your domains, and CRT.SH to list changes made to publicly available certificates registered to your domains. Many commercial vendors also offer free trials of their tools that you can use to check key parameters.

You should also ensure that you have migrated to Domain Name System Security Extensions (DNSSEC)[12] across your use of DNS. DNSSEC uses public/private key pairs to create digital signatures that assure data origination authentication and data integrity protection for DNS information. To be effective, your implementation of DNSSEC needs to include both moving to signed DNS records as well as enabling DNSSEC validation.

---

[9] www.sans.org/newsletters/newsbites/xxi/7

[10] "New Hacker Group Behind 'DNSpionage' Attacks in Middle East," www.darkreading.com/attacks-breaches/new-hacker-group-behind-dnspionage-attacks-in-middle-east-/d/d-id/1333350

[11] www.us-cert.gov/ncas/alerts/AA19-024A

[12] www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

Domain Fronting

Skoudis also described "domain fronting" attacks that take advantage of routing methods used by proxies, content delivery networks (CDNs) and other services that need to hide the use of multiple domains to simplify tunneling traffic over HTTPS. Domain fronting allows attackers to obfuscate the external IP addresses they use in order to host malware, provide command and control communications to infected machines, and obscure the destinations to which they exfiltrate data from compromised systems. Figure 2 shows how domain fronting works.

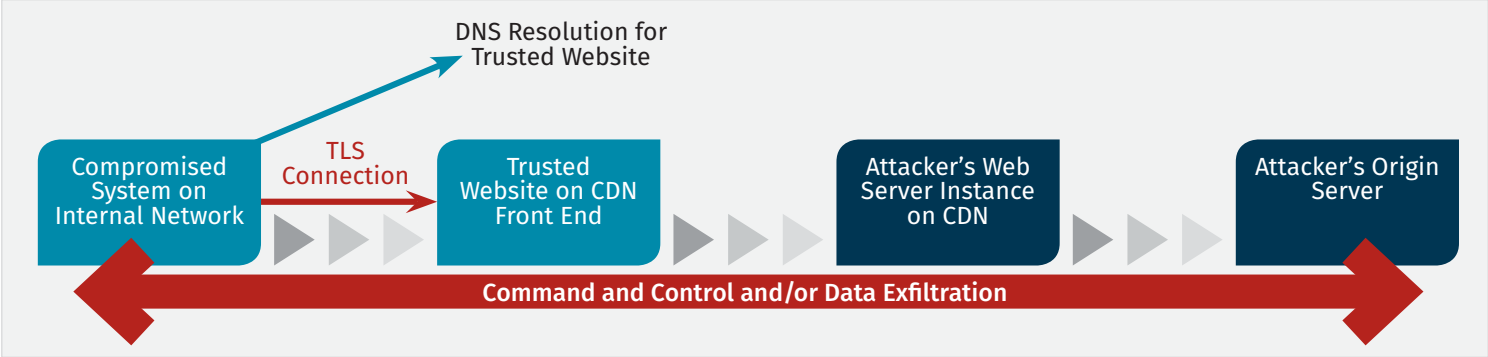

Figure 2. How Domain Fronting Works[14]

On the left side of the illustration is a system that has been compromised with the initial malware payload. On the right is the internet-based server used by the attacker. To carry out the full attack, the attacker needs to have the compromised system and the origin server communicate without security controls recognizing the external IP addresses and domains as suspect or malicious.

> *"Domain fronting is an active and dangerous attack technique. Having the ability to intercept and inspect in-bound and outbound TLS sessions is key to detection and prevention of this attack vector."*

The attacker establishes an account on the same CDN being used by the target enterprise or some other innocuous site that the enterprise trusts. Once the initial payload has compromised the target's internal machine, it sends a DNS request to resolve the URL of some legitimate site also being hosted on that same CDN. The malware establishes an encrypted TLS session to that legitimate site. Next, the malware issues an HTTP 1.1 request with host headers that point to the attacker's site, not the legitimate site. This sleight of hand goes undetected because it is carried over the encrypted TLS connection, enabling a covert two-way communication path to operate between the initial compromised machine and the attacker's server.

In the RSA talk, Skoudis also discussed how attackers can use similar techniques to "launder" their connections through multiple cloud service providers and "disappear into the clouds."

Johannes Ullrich discussed a related issue: To increase the privacy of DNS requests, browser developers and public DNS service providers are supporting DNS over HTTPs or DNS over TLS services. This practice can keep DNS transactions safe from monitoring by government agencies and others, but it can also prevent the security organization from

[14] "The Five Most Dangerous New Attack Techniques and How to Counter Them," www.sans.org/the-five-most-dangerous-new-attack-techniques, RSA Conference 2019, March 7, 2019

getting the visibility needed to detect domain fronting and many other attacks. DNS over TLS has some advantages over DNS over HTTPS, but organizations have to balance privacy and security needs when considering encrypting DNS traffic at all. Where possible, use enterprise-class VPNs that can support both privacy from unauthorized users and full visibility by network management and operations.

Mitigation—Google and Amazon have implemented changes in their CDN services[15] that inspect Server Name Indication (SNI) fields to detect domain fronting, but there are many, many CDN services in use that have yet to do so.

To detect domain fronting, enterprises need the capability to inspect TLS traffic going between internal networks and external hosts. The National Cyber Security Center in the Netherlands provides a well-written guide for implementing TLS interception.[16] Black Hills Information Security provides a free tool called Real Intelligence Threat Analytics (RITA) for detecting domain fronting and other forms of beaconing.[17]

Targeted Cloud-based Personal Attacks

While most of the press attention focuses on mega breaches, Heather Mahalik pointed out the rising threat of attacks aimed more at the "retail" level—attacks targeting individuals to capture their credentials one at a time, much the way robocalls attempt to launch scams one call at a time. Targeted cloud-based personal attacks take advantage of all the information people expose on social media and other internet sites to launch highly targeted phishing attacks or to attempt direct password resets on high-value accounts.

Mahalik used the example of a Google Gmail user who also has an Android or Apple phone and uses common services such as Facebook, LinkedIn, Twitter, Waze and so forth. Many users take advantage of offers these applications make to simplify finding the right restaurant, or the faster route to the airport or to auto-complete a text message. These forms of "help" almost always involve turning on services, such as location or access to email, pictures and others. That provides one level of exposure; but allowing Google access to such information to get a wide range of free services seems like a bargain to many, and the large services such as Google, Amazon and Apple have pretty good records protecting their users' information from direct attacks.

> *"The 'free' online services that people use, especially email and social media accounts, can expose tons of sensitive information. Check sites like* `myactivity.google.com` *to see how [much] of your personal information is exposed by those services and add-on applications."*

However, social media sites and other third-party applications that get installed on phones and tablets can also request access to those same services, using confusing terms of service declarations, or they can take advantage of vulnerabilities (or ambiguous policies) to access that information without user consent or knowledge.

---

[15] "As Google and AWS kill domain fronting, users must find a new way to fight censorship," www.techrepublic.com/article/as-google-and-aws-kill-domain-fronting-users-must-find-a-new-way-to-fight-censorship/

[16] www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-tls-interception/1/NCSC_factsheet_TLS_interception.pdf

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

A glaring example was the widely covered exposure of Facebook user data by Cambridge Analytica in 2017.[18] By tricking people into taking online surveys, Cambridge Analytica could also collect information on the participants' Facebook friends. This expanded the pool of targets from the initial 300,000 individuals to a total of more than 80 million people!

Mahalik also used an example of common posts on social media asking questions such as, "What is your 'hacker name'?" The app then asks for your middle name and your first pet's name and responds, "Your hacker name is Nicole Gizmo," which seems innocuous. However, first pet's name is often used as one of the security questions in password-reset software, making it much easier for an attacker to steal credentials.

Mitigation—Everyone has to make a personal decision on how much personal information they want to expose in order to take advantage of the wide array of free services offered on the internet. However, it is important for each user to start with an informed position and to monitor whether the level of exposure changes over time. Mahalik advised all Gmail users to look at **`myactivity.google.com`** and see how much information Google is giving away directly and to third-party programs, as seen in Figure 3.

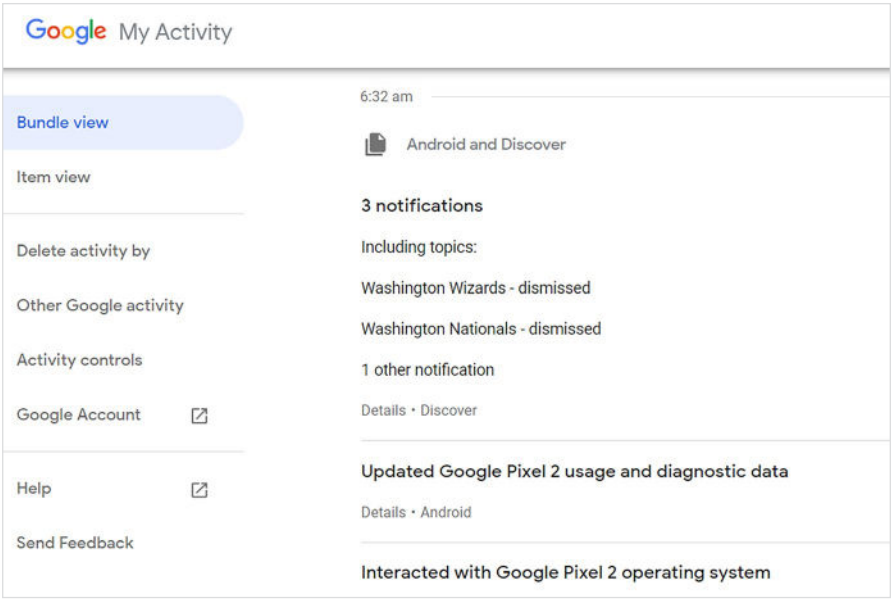

Figure 3. Screen Shot of myactivity.google.com

This site provides a number of tools to reduce the services exposed, as well as providing alerts if something is changed. Most cloud providers have similar services. She also stressed moving to two-factor authentication on all services that support it.

While Mahalik's talk was aimed at individual users, real-world experience shows that personal email and social media is often used where the work/home balance blurs. Corporate security awareness programs should include these guidelines in all user training.

Management Infrastructure/Embedded Hardware Attacks

At the panel, Ullrich detailed attacks exploiting what became known as the Spectre and Meltdown vulnerabilities in AMD, Arm and Intel CPU hardware.[19] These are forms of "transient execution" attacks, which take advantage of badly designed performance enhancement techniques used by the latest versions of those CPUs (such as speculative execution, out-of-order execution and pipelining) and enable attackers to essentially capture all memory contents.

[18] "Cambridge Analytica kept Facebook data models through US election," www.theguardian.com/uk-news/2018/may/06/cambridge-analytica-kept-facebook-data-models-through-us-election

[19] www.rsaconference.com/events/us18/agenda/sessions/11413-The-Five-Most-Dangerous-New-Attack-Techniques,-and-What's-Coming-Next

This year, Ullrich focused on a related area: techniques being used to exploit vulnerabilities in baseboard management controllers (BMCs), most recently in an attack dubbed Cloudborne.[20] BMCs are specialized processors on the motherboards of many servers and appliances that support remote monitoring and maintenance. BMCs work across all types of hardware, under a multivendor standard called the Intelligent Platform Management Interface (IPMI), and enable remote rebooting, reflashing and other forms of remote execution—a bonanza for attackers! To make matters worse, IPMI and BMCs are widely used across all cloud service providers. See Figure 4.

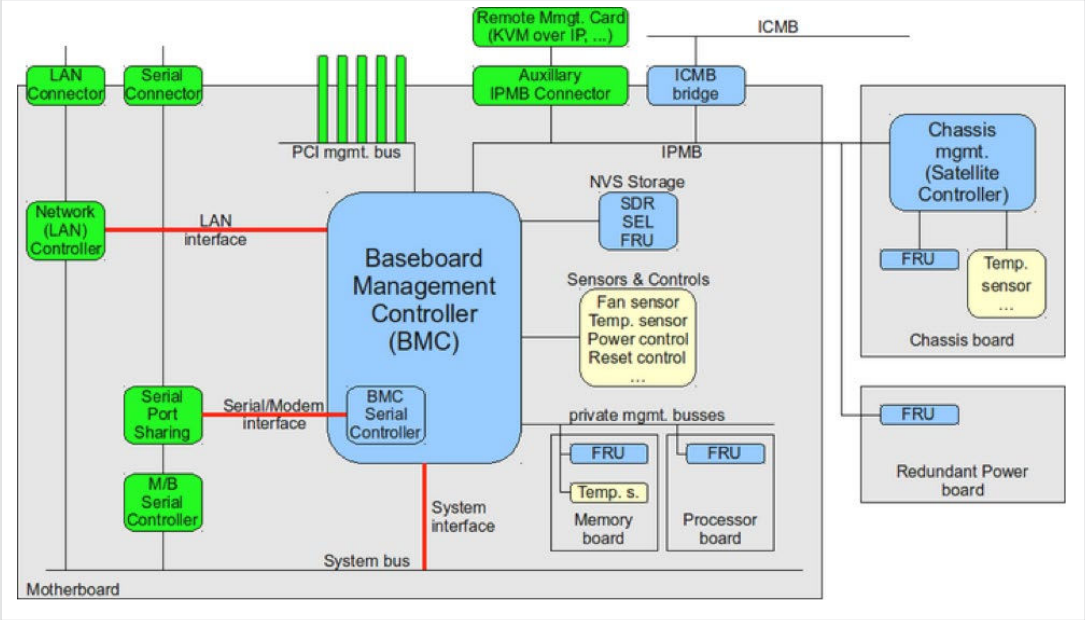

Figure 4. Schematic of IPMI Components[21]

Vulnerabilities in BMCs were discovered as early as 2013, but insecure implementations combined with poor administrative processes have continued to enable exploits. A successful compromise of a BMC allows attackers to essentially remain undetected while having full control of servers at the bare metal level.

The BMC vulnerabilities are part of a broader class of hardware and firmware vulnerabilities that have existed for years and have only recently started being exploited. Ullrich noted the Marvell Avastar wireless system on chip (SoC) Wi-Fi processors have multiple vulnerabilities, including a block pool overflow that enables an attacker to execute arbitrary code of a target by sending it specially crafted packets in response to a Wi-Fi scan.[22] The attacker can then use the compromised machine to monitor wired and Wi-Fi network traffic or to execute malware on the compromised host. See Figure 4.

> *"Vulnerabilities in Baseboard Management Controllers (BMC) found on most server motherboards are being exploited by attackers and giving them bare metal access. Make sure you segregate BMC access onto dedicated management networks and you monitor all traffic on that network and apply the same intrusion detection attention you do to internet connections."*

Mitigation—Ullrich pointed out that the BMC traffic should be segregated to a management network that allows only trusted connections and can be monitored using the same IDS and network monitoring processes and controls used to monitor untrusted external network connections. Do not rely solely on the logging supported by BMCs, because it is reactive at best, and attackers can compromise that function. For your own servers, make sure you change all BMC passwords from the default and that you follow and audit all BMC vendor security recommendations. Change windows should include firmware updates in servers (and laptops/PCs) for your own hardware, and you should query cloud service vendors about their practices related to securely configuring and maintaining BMC and other firmware-related security on servers.

---

[20] "Cloudborne vulnerability affecting baseboard management controllers exposes cloud servers to potential hacking," www.computing.co.uk/ctg/news/3071811/cloudborne-vulnerability-affecting-the-baseboard-management-controllers-exposes-cloud-servers-to-potential-hacking

[21] www.thomas-krenn.com/en/wiki/IPMI_Basics

[22] https://kb.cert.org/vuls/id/730261/

Best Practices for Improving Defenses

Just as most medical professionals know that established practices, such as frequent handwashing, are the foundation for overall health, basic security hygiene has been proven to be the foundation for every successful cybersecurity program. The Center for Internet Security Critical Security Controls[23] 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 the attacks detailed in this paper.

Having an accurate asset inventory—knowing what hardware, operating systems and applications you are protecting—is part of the basic level of the Critical Security Controls, along with continuous vulnerability assessment and mitigation. Collection and analysis of logging data from all levels of networks and hosts are key for rapid and accurate incident response (IR), as well as for satisfying the demands of auditors. Improvements at this basic level raise the bar significantly against broadly launched, mass attacks.

However, the advanced targeted attacks discussed in this whitepaper require organizations to use skills, processes and controls that also effectively implement the higher levels (foundational and organizational) of the Critical Security Controls. Table 2 maps the major mitigation techniques listed against the pertinent sections of the CIS Critical Security Controls:

The Critical Security Controls provide a strong baseline level of effective controls, but every organization needs to perform risk assessment specific to its own business environment, corporate culture and threat analysis. Very targeted attacks against infrastructure services (such as DNS and IPMI) and attacks that target employees outside of the corporate environment will continue to evolve and will continue to require advances in staff skills, security processes and mixes of security controls.

Table 2. Mitigation Techniques and the CIS Controls

Mitigation Technique	Relevant Critical Security Control
Domain Name System Security	CSC 7, 8, 9
Network Segmentation	CSC 12, 14
Network Monitoring	CSC 6, 12
Threat Intelligence	CSC 3, 19
Strong Authentication	CSC 12, 14, 15, 16
Virtual Private Networks	CSC 6
Email Account, Web Data Exposure	CSC 7, 17

[23] www.cisecurity.org/controls/

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: