SANS

Analyst Program

Whitepaper

SANS 2021 Top New Attacks and Threat Report

Written by **John Pescatore**

August 2021

ANOMALI BlackBerry cisco corelight

DOMAINTOOLS ExtraHop LogRhythm

RAPID7 SOPHOS Cybersecurity made simple. THREATQUOTIENT

Introduction

The media covers many breaches and outages, and backward-looking statistics related to how many attacks occurred in cyberspace abound. However, you have to search harder to find solid advice about threat detection and prevention. The industry needs expert analysis of how security managers should prioritize to increase effectiveness and efficiency in dealing with known threats while also moving forward to minimize the risk from emerging attacks.

For the past 15 years, the SANS Five Most Dangerous Attacks expert panel at the annual RSA Security Conference has filled that gap. This SANS whitepaper begins with a baseline of statistics from reliable sources of breach and malware data and then summarizes SANS instructors' expert advice from the RSA panel, which details the emerging threats to look out for in 2021 and beyond.

2021 Breach and Threat Baseline Data

Because the pandemic delayed the RSA Security Conference and the annual SANS New Attack and Threat panel, this year's SANS Attack and Threat report focuses less on what occurred in 2020 than it does on world security trends post-lockdown. As in previous reports, we start with a baseline from data collected by the Identity Theft Resource Center (ITRC).[1] The ITRC has followed a consistent methodology for many years, using only verified information from publicly disclosed breaches. This data does not include attacks such as denial of service but does include the most recent ransomware attacks.

Figure 1 shows a comparison of incidents and individual identities affected during the first quarters of 2021, 2020, and 2019. Highlights include:

- The total number of individuals affected in Q1 2021 was down by 87% compared to Q1 2019 and down by 62% compared to Q1 2020.
- The Healthcare sector suffered the most breaches across all three years.
- Government, Healthcare, Non-Profit, Professional Services, and Retail showed the largest growth in individuals affected from Q1 2020 to Q1 2021, while Hospitality, Transportation, and Technology showed the largest declines.

Sector	Year					
	Q1 2021		Q1 2020		Q1 2019	
	Breaches/ Exposures	Individuals Impacted	Breaches/ Exposures	Individuals Impacted	Breaches/ Exposures	Individuals Impacted
Education	24	109,964	9	450,699	24	63,699
Financial Sevices	51	1,757,543	35	1,296,259	42	344,547
Government	11	647,917	14	21,993	17	992,541
Healthcare	77	3,217,102	86	1,418,842	79	2,770,941
Hospitality	6	53,152	5	5,228,414	10	1,168,132
Manufacturing & Utilities	38	375,493	9	1,065,490	24	27,840,515
Non-Profit/NGO	15	502,603	8	13,811	4	9,908
Professional Services	30	3,562,693	16	308,532	23	35,655
Retail	20	505,394	9	14,922	24	82,366,979
Technology	23	4,009,575	14	120,082,886	15	88,841,615
Transportation	15	136,609	6	672,726	2	54,761
Other	53	35,728,923	28	1,089,984	36	179,863,657
TOTALS	**363**	**50,606,968**	**239**	**131,664,558**	**300**	**384,352,950**
Individuals affected per breach		**139,413**		**4,702,305**		**1,281,176**

Figure 1. Comparison of Incidents and Individual Identities Affected During Q1 of 2019, 2020, and 2021 (Source: ITRC)

[1] "Notified," Identity Theft Resource Center, https://notified.idtheftcenter.org/s/

The ITRC noted that the rise in supply chain attacks (which often insert malicious capabilities into targets but don't immediately exploit them) increased the lag between when the initial compromise occurred and when related malicious activity started and the damage was discovered. For example, the SolarWinds breach occurred in March 2020 but was not discovered until more than eight months later, and in many cases no damage has yet to occur. Although as many as 18,000 SolarWinds customers downloaded the compromised Orion software, the actual number and size of exposures across those customers remain largely unknown.

The ITRC data also shows that most successful attacks begin with credentials obtained by attackers via phishing attacks and business email compromises (BECs). This situation remains unchanged from previous years.

The Microsoft semi-annual Security Intelligence Report used to be a reliable source of attack trends against Windows PCs and servers, but Microsoft no longer produces it and instead publishes an annual Microsoft Digital Defense report.[2] The latest version (September 2020) also identified phishing and BECs as the most common initial attack vector and highlighted two additional trends:

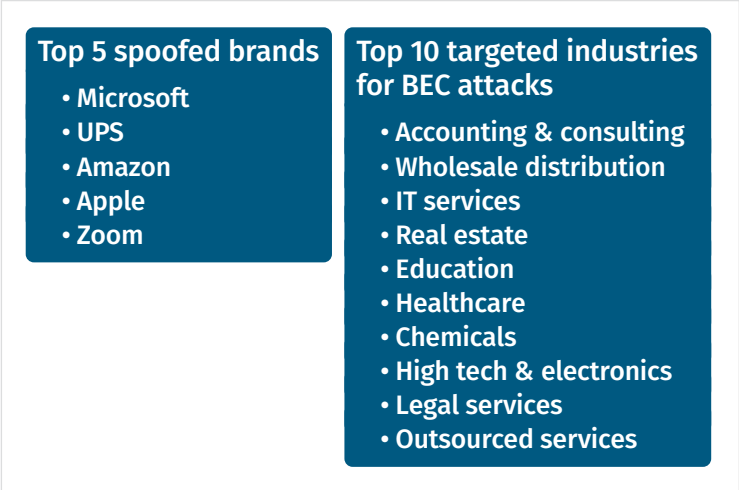

Figure 2. Most Spoofed Brands and Targeted Industries, per Microsoft's Digital Defense Report

- Threat actors increasingly target the C-suite and directors, using deeper research into their targets and customized phishing attacks.
- Phishing attacks increasingly use brand spoofing (see Figure 2) to improve target click-through rates.

The Verizon Data Breach Investigation Report (DBIR) is another valuable source of data.[3] The 2021 DBIR also validated phishing and BECs as the most common initial compromise vector, and it showed significant growth in those techniques, particularly in Covid-19-related attacks. The DBIR also reported that ransom demands as part of malware attacks causing breaches nearly doubled. Increasingly, ransomware attacks expose information—not just encrypt it—and breach events include ransom demands.

Figure 3, pulled directly from the DBIR, shows the change in Covid-19-related action varieties. Figure 4, (on the next page) also from the DBIR, presents the top action varieties in breaches. The good news is that the data shows a decrease in system administrator error-driven causes. The bad news is that phishing and stolen reusable credentials showed growth.

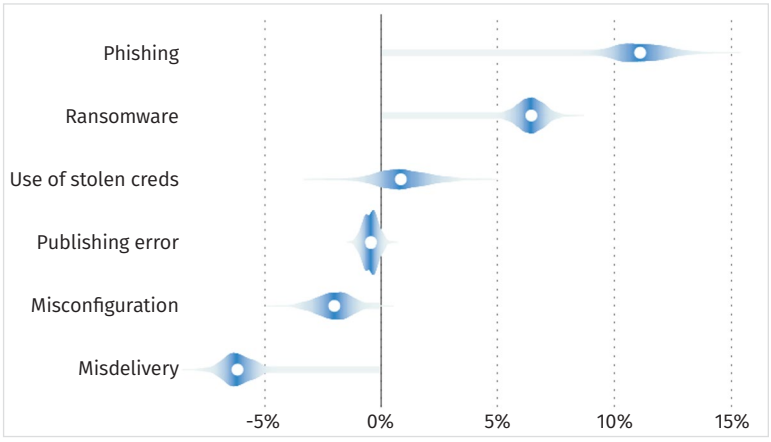

Figure 3. Change in COVID-19-Related Action Varieties[4]

[2] Digital Defense Report, September 2020, www.microsoft.com/en-us/download/details.aspx?id=101738

[3] "DBIR 2021 Data Breach Investigations Report," www.verizon.com/business/resources/reports/dbir/

[4] "DBIR 2021 Data Breach Investigation Report," Figure 22, p. 16.

The first quarter of 2021 showed a decrease in the number and size of breaches as the world began to emerge from full pandemic lockdown. However, we have no reliable statistics on the financial impact of cybersecurity attacks. The growth in supply chain and ransomware attacks during late 2020 and the first half of 2021 did not result in reported increases in records breached, but those types of attacks did result in more complex impacts on businesses. The Colonial Pipeline incident resulted in not only revenue loss for the company itself but also disruption of numerous physical supply chains when gasoline became unavailable. The following section provides SANS instructors' views on some of the key changes in attack techniques in supply chain and ransomware attacks.

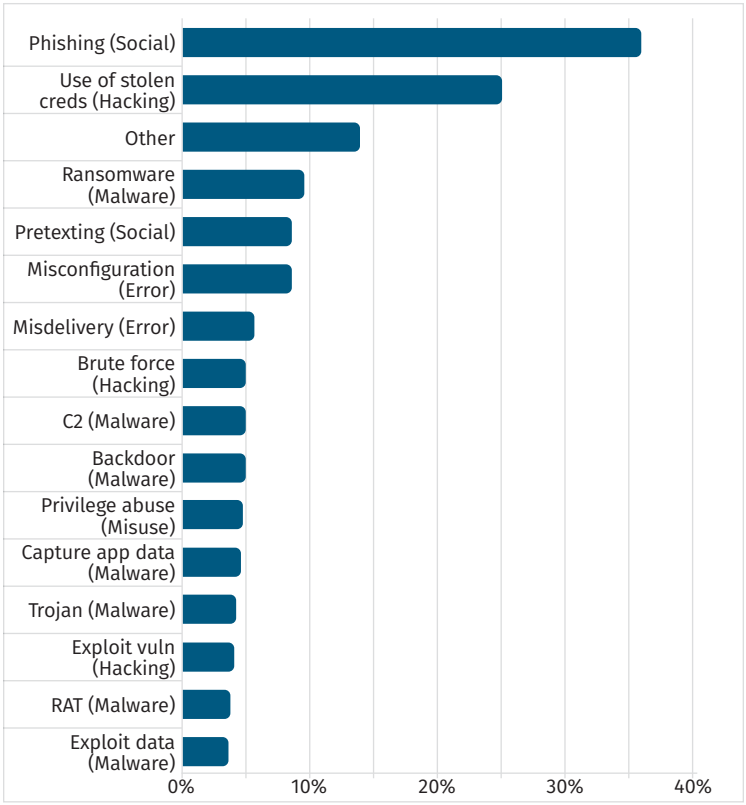

Figure 4. Top Action Varieties in Breaches[5]

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

RSA Conferences started in 1991, and they have grown into one of the largest cybersecurity conferences in the world. For the past 15 years, SANS has presented a panel in which its top experts detail their views of the most dangerous attacks just starting to affect enterprises. Over the years, the predictions made by the SANS instructors at these sessions have proven highly accurate with regard to eventual real-world damage.

Figure 5. RSA Conference 2021 SANS Panel

The 2021 threat expert panel (moderated by SANS founder and research director Alan Paller and shown in Figure 5) included:

- **Ed Skoudis—**SANS faculty fellow and director of SANS Cyber Ranges and Team-Based Training
- **Heather Mahalik—**Senior instructor at SANS Institute and senior director of digital intelligence at Cellebrite
- **Johannes Ullrich—**Dean of research at SANS Technology Institute and founder and director at Internet Storm Center
- **Katie Nickels—**Senior instructor at SANS Institute and principal intelligence analyst at Red Canary

[5] Adapted from "DBIR 2021 Data Breach Investigations Report," www.verizon.com/business/resources/reports/dbir/, Figure 20, p. 15.

Ed Skoudis: Undermining Software Integrity

Ed Skoudis addressed the SolarWinds attack, which severely compromised hundreds of companies and government agencies.[6] A *supply chain* attack such as this seeks to attack all the companies that have the compromised company (in this case, SolarWinds) as part of their software supply chain. The NotPetya ransomware attack used this technique in 2017 and thus compromised updates to Ukrainian accounting software and caused large companies such as FedEx and Merck to report financial impacts of more than $300M each.[7]

Skoudis pointed out that SolarWinds is part of a large attack category he calls "undermining software integrity." He stated that many applications are actually compilations of several software packages or modules, many of which are open source. Skoudis cited a recent paper that documented 174 malicious packages available online that attackers had used to compromise applications in use at many companies.[8] See Figure 6.

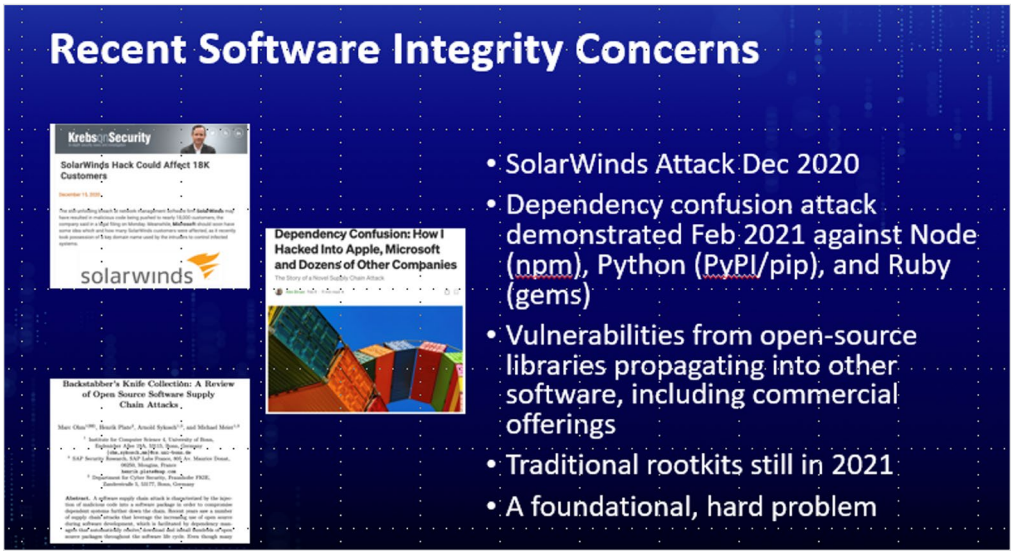

Figure 6. Recent Software Security Concerns

Although executables coming in as email attachments or as part of employee web browsing raise suspicion in most enterprises, often those same enterprises trust most shrink-wrapped software. Whereas they often test updates to operating systems for compatibility issues, they rarely examine updates to applications to determine whether they (and any incorporated modules) have been compromised or have had hidden malicious capabilities inserted.

Mitigation

Skoudis says that we need a number of key security controls to minimize the risks of attacks undermining software integrity.

Accurate software inventory. To protect or monitor software in use, you have to know it is in use. The Center for Internet Security's Critical Security Controls are a widely accepted framework for essential security hygiene. Control 2 is Inventory and Control of Software Assets, which states, "Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution."[9]

> **"There's no single solution to the problem of software integrity and to software supply chain management. But there are a lot of different things that we can apply."**
>
> **—Ed Skoudis**

[6] "The US Is Readying Sanctions Against Russia Over the SolarWinds Cyber Attack," Insider, www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12

[7] "Russia Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," The Washington Post, www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

[8] "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks," https://arxiv.org/pdf/2005.09535.pdf

[9] "CIS Control 2: Inventory and Control of Software Assets," Center for Internet Security, www.cisecurity.org/controls/inventory-and-control-of-software-assets

Software bill of materials. An asset inventory provides visibility into the applications in use in your business but does not tell you which packages, modules, or external services those applications consider integral. Skoudis explained that the concept of a software bill of materials (SBOM) has been developed by a National Telecommunication and Information Administration working group to provide that level of visibility. An SBOM is defined by the US Department of Commerce as "effectively a nested inventory, a list of ingredients that make up software components."[10]

Although the concept of an SBOM is well understood, only standards and wide adoption will make the idea useful. Current standardization effort examples include the following:

- **Software Package Data eXchange (SPDX)** is hosted by the Linux Foundation, with more than 20 software, systems, and tool vendors; foundations; and system integrators participating.[11]
- **CycloneDX** is a lightweight SBOM standard designed for use in application security contexts and supply chain component analysis. It is managed by the CycloneDX working group, with connections to OWASP.[12]
- **SWID** tags record unique information about an installed software application, including its name, edition, version, whether part of a bundle, and more.[13] International standard ISO 19770-2 (referenced in the footnote link) specifies the structure of SWID tags.

Other frameworks for bills of materials have been proposed that would enumerate the expected behavior or other attributes of applications. These efforts are not part of standards-based efforts yet, but if adopted would provide a powerful tool in protecting against supply chain attacks such as SolarWinds Sunburst.

File integrity monitoring (FIM). Organizations should monitor critical files and executables for rapid indication and verification of any changes. FIM tools use digital signatures and other approaches to detect changes, and we can combine them with backup and recovery systems to safely restore to a known good version. FIM tools would have helped SolarWinds detect the changes to Orion production builds but would not have enabled enterprises to detect malicious actions by the updated Orion packages they installed.

Threat hunting. Actively looking for indications of a compromise is a proactive step required to detect advanced attacks that get through standard levels of defenses. Network activity monitoring tools and endpoint detection and response software provide a base level of capability, but advanced attackers are skilled at building capabilities to evade known security tools. Threat hunting generally involves skilled security analysts looking for unusual or suspicious activity and determining whether an incident is already underway. As Skoudis says, "It's a really good idea to do threat hunting on a periodic and regular basis to look for things that our automated tools haven't detected or discovered."

---

[10] "Software Bill of Materials," National Telecommunications and Information Administration, United States Department of Commerce, www.ntia.gov/SBOM

[11] "The Software Package Data Exchange," The Linux Foundation, https://spdx.dev/

[12] "OWASP CycloneDX," OWASP, https://owasp.org/www-project-cyclonedx/

[13] "Software Identification (SWID) Tagging," Computer Security Resource Center, National Institute of Standards and Technology, https://csrc.nist.gov/Projects/Software-Identification-SWID/guidelines

Purple teaming. Organizations increasingly rely on "red teams" to conduct active, hands-on attack simulations so they can measure whether their "blue teams" can detect, block, and eradicate these actions. A purple teaming exercise is a cooperative exercise between red and blue teams, often focused on a particular threat scenario, such as the compromise of a key software package such as SolarWinds. The blue team improves its detection and prevention capabilities, while the red team learns more about how attackers will counter those techniques. In a purple team exercise, each side (red and blue) shares lessons learned in an after-action review to advance their capabilities.

Heather Mahalik: Improper Session Handling

Heather Mahalik discussed two attack types, starting with improper session handling. Modern applications, especially mobile applications, start out like traditional applications and require the user to authenticate. Today's mobile applications, however, often have to communicate with multiple backend services and then respond to new requests from the user, without having to ask the user to enter credentials every time. To enable this process, application protocols include software "tokens" that can be securely exchanged to allow one of two scenarios: the user device to say, "I'm still Sally, and I'm still logged in"; or the mobile app process A to request of server app process B, "Please send Sally's account balance."

When done correctly, all is well. Improper session handling occurs when applications or protocols do not properly secure the tokens or attackers think of new ways to attack approaches that had been considered secure. This technique has been on the OWASP Top 10 software vulnerability list[14] for many years, but the rush to support a fully work-from-home workforce has broadened the range of applications in use, including many applications not originally designed with enterprise-class security. See Figure 7.

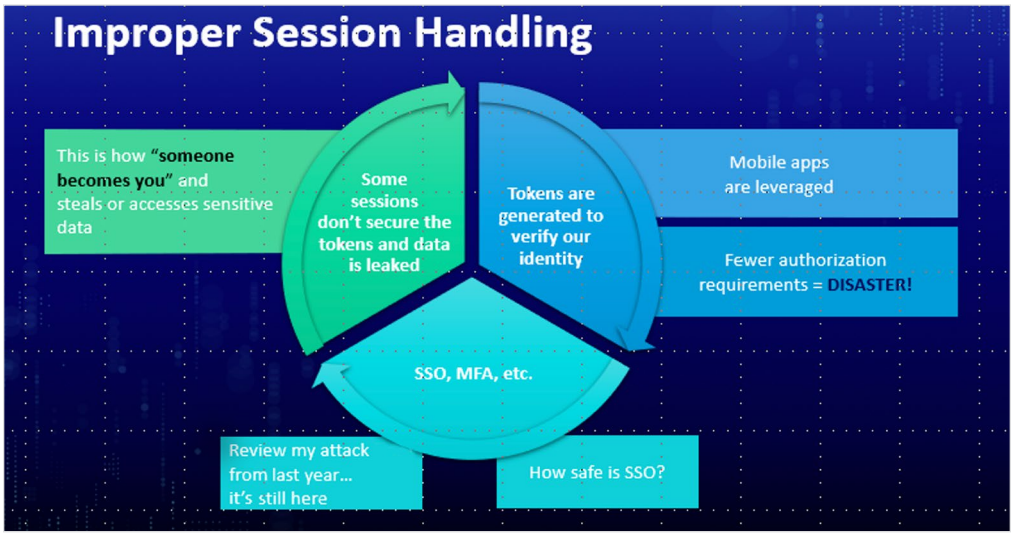

Figure 7. Issues Raised in Improper Session Handling

Mahalik detailed a related attack: exploiting crypto done badly. To secure sessions and tokens, enterprises often use public and private key cryptography for encryption and integrity services. Done right, encryption can enable secure sessions and protect data. However, very few developers are cryptography experts, and so they often implement cryptography badly. Managing cryptography keys must also be done securely, but developers take shortcuts to improve performance or to simplify the user experience, making the attacker's job much easier.

[14] "M9: Improper Session Handling," OWASP, https://owasp.org/www-project-mobile-top-10/2014-risks/m9-improper-session-handling

Mitigation. For users, Mahalik recommends always logging off an application when you finish with a session. This action will at least minimize the time a vulnerable session or token remains active. Don't check the box that will leave a token active for seven days or perhaps forever. Think of it as you would an ATM transaction: Would you leave that session open for the next person to drive through the bank ATM lane, or would you rather have to insert your card and log on again next week when you need some cash.

> **"For applications, trust but verify. Validate. Test it. Try to break it. See whether you can crack it. See if any traces are left behind."**
>
> **—Heather Mahalik**

Enterprises developing or installing apps should minimize permissions and keep token lifetimes short. Enterprises should use application security testing tools or services[15] on applications developed in-house to detect weak session handling and other vulnerabilities and require external application vendors to demonstrate the use of such tools. Where untrusted applications must interface with critical business systems, enterprises should deploy segmentation and enhanced monitoring to reduce risk.

Johannes Ullrich: Corrupting and Reverse Engineering Machine Learning

Johannes Ullrich pointed out that modern detection techniques have gone from totally depending on simple signature-based techniques to incorporating machine learning capabilities.[16] Signature-based detection proves effective and efficient for detecting known malware or attack traffic patterns but is useless against new attacks. Although signature-based detection has a low false positive rate, attackers have many ways to easily avoid signature-based detection approaches, thereby driving up false negatives.

Machine learning uses algorithms to detect patterns in data and classify those events into categories that can be declared safe, dangerous, or unknown. Depending on policy and the level of trust in the ML algorithms, safe traffic/executables could be allowed through, dangerous ones could be blocked, and unknown ones could be subject to additional inspection or quarantining.

The level of trust in the ML detection algorithm and products is critical. "Bad" ML could lead to the worst of both worlds: high false positive *and* high false negative rates simultaneously! Trust in ML has both a pre- and post-deployment aspect:

- **Pre-deployment ML trust—**Vendors are overhyping ML capabilities in many products. Enterprises need to have visibility into what is implemented in the product and evaluate performance to validate claims.
- **Post-deployment ML trust—**Ullrich points out that attackers can target ML algorithms with data attacks to corrupt the algorithms to cause their attack techniques to be classified as safe.

[15] "10 Types of Application Security Testing Tools: When and How to Use Them," Software Engineering Institute, Carnegie Mellon University, https://insights.sei.cmu.edu/blog/10-types-of-application-security-testing-tools-when-and-how-to-use-them/

[16] "AI/Machine Learning: What is Actually Working in Cybersecurity," www.rsaconference.com/Library/presentation/Virtual%20Summit/2021/aimachine-learning-what-is-actually-working-in-cybersecurity

To differentiate between *safe* and *dangerous*, we need to train ML models with samples of typical traffic. Ullrich says an attacker could influence the training data in various ways to evade detection. A typical ML training scenario is to run "known good" traffic or data through the model for some period of time before having it analyze real data. If attackers can mix malicious samples in with that known good data, false negative rates would increase, and malicious traffic would be allowed through.

Another scenario common with ML-based malware detection is to train the algorithm on "known bad" samples using known malware. Ullrich points out that the known bad malware comes from the bad guys, and they can influence those samples. He uses the example of attacker that sends your employees two different email streams of malicious attachments: a high number of attachments with malicious Microsoft Office macros and a smaller number of emails aimed at privileged users with links to a website that has been compromised with an obscure cross-site scripting vulnerability. This could cause the ML algorithm to classify those emails as safe.

> **"One of the most basic threats when it comes to machine learning is if the attacker actually is able to influence the samples that we are using to train our models so that the attacker has access and is able to manipulate our samples, our training data."**
>
> **—Johannes Ullrich**

Ullrich detailed two other ML-related attack scenarios:

- **Reverse engineering ML—**Attackers can acquire the same ML-based security products you use and send you a stream of malware at the same time that they feed it to their own copy of the product. The attacker would then analyze the indicators the ML model has developed and use that to craft an attack that your security products are likely to classify as safe traffic.
- **Brute force—**Security devices are often choke points for business traffic, especially when complex detection algorithms require large amounts of CPU cycles and volatile memory. If the security control becomes overwhelmed, enterprises have to decide whether to fail closed (don't pass any traffic, disrupting businesses but ensuring no gap in detection) or fail open (pass all traffic, enabling business to continue but resulting in a period of exposure where attackers can be certain malicious traffic will get in). Either approach leads to risk.

Mitigation. To prepare for these types of attacks, Ullrich said the most important proactive step is understanding how the ML models work and being aware and in control of the training data that is being used. Because both normal and malicious traffic changes over time, all ML products require tuning. Depending on the volatility of your environment, tuning could represent significant workload. It will require SOC analysts and engineers to have knowledge of ML concepts and techniques in general and what is used in your security controls in particular.

Katie Nickels: Evolving Ransomware Techniques and Motivations

Katie Nickels noted that ransomware is commonly considered as similar to a denial-of-service attack in that it affects the availability of data or applications: Attackers encrypt business-critical data or executables. Ransomware attacks disrupt business, and the attackers demand a ransom to end the DoS attack (upon payment of which they provide their victims with the decryption keys).

> **The costs of dealing with a breach of customer or business information can be just as high as the business disruption impact from loss of data availability."**
>
> **—Katie Nickels**

Security experts once considered backup and recovery capabilities a complete antidote to ransomware. However, since 2019, attackers have routinely been including data exfiltration as part of the ransomware attack and using the threat of disclosure as part of ransom demands. This changes the calculus for victims because attacks no longer affect just data availability; they also impact the data confidentiality. If they were impacted by a ransomware attack in which data was exfiltrated, victims must also consider any regulatory requirements to report a data breach.

More importantly, Nickels points out that since 2019 attackers have routinely been including data exfiltration as part of the ransomware attack and using threat of disclosure as part of ransom demands. Backup and recovery capabilities remain important, but the costs of dealing with a breach of customer or business information can prove just as high as the business disruption impact from loss of data availability.

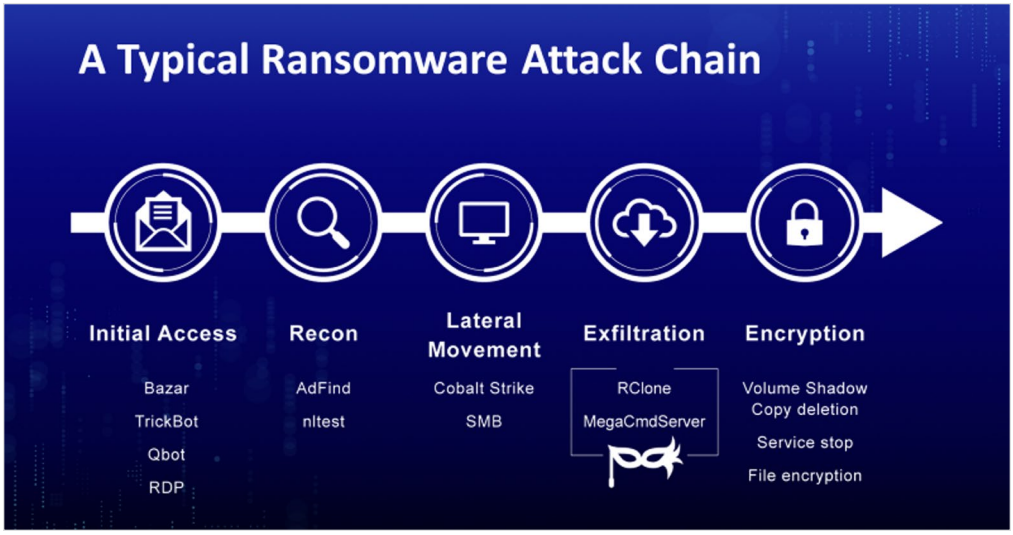

Figure 8. A Typical Ransomware Attack Chain

Mitigation. These ransomware/exfiltration attacks often use available tools such as RClone (file-sharing tool supported by most cloud services) and MEGA CMD (file encryption and file transfer tool for the MEGA Cloud service), but the attackers try to hide their use by renaming the executables. Nickels says that tactic provides an opportunity for detection by looking for executables that have been renamed. Because exfiltration usually occurs before encryption, preventing the use of these file-sharing tools can impede the entire attack. Figure 8 details a typical ransomware attack chain.

Best Practices for Improving Defenses Overall

Each SANS instructor detailed mitigation techniques for the attack methods he or she described. Effective and efficient security controls require selecting security controls and a security architecture that the organization can operate and enhance to support SOC analysts in preventing, detecting, and responding to all threats.

Common security controls that can reduce the likelihood of damage across all the threats described include those from the following list:

- **Avoiding reusable passwords—**A phishing attack that captures privileged user credentials and passwords enables more than 70% of all damaging attacks.[17] Microsoft research has shown that just adding in SMS messaging to a mobile phone as a second authentication factor would stop 99.9% of all phishing attacks.[18] 2FA (two-factor authentication) is not unbreakable, but it raises the bar against attackers and forces them to use techniques that are much easier to detect than when they are in control of internally connected PCs.
- **Essential security hygiene—**Configuration management, timely patching, privilege minimization, network segmentation, and application control can prevent the majority of malicious executables from being effective even if the attack does manage to install them. Implementation Group 1 of the CIS Critical Security Controls[19] is a minimum starting point for lowering the risk of the attack techniques described in this paper. Reaching that level enables movement to higher levels of protection such as advanced endpoint detection and response and automation.
- **Threat hunting/purple teaming—**Protecting information against attackers is never static because the bad guys will continue to find ways around controls and software developers will find new ways to write vulnerable code. Active investigation of anomalies and suspicious behavior to find new compromises quickly will reduce business damage by reducing the attacker's time on target. Having your defensive blue team and your penetration testing red team work cooperatively in purple team exercises can do the same by running scenarios that include all the attack techniques described.
- **Integrated intelligence information—**By integrating detailed, accurate, and timely threat information into your processes, you can increase prevention and reduce time to detect by taking advantage of information from other organizations, professional threat researchers, and the vast variety of information available from sources such as DNS records, ISP, and certificate authorities.

In the United States, President Biden's "Executive Order on Improving the Nation's Cybersecurity" contained all the above as requirements for meeting the challenges of increasing threat levels against business-critical systems.[20] The usual mix of skilled cybersecurity staff developing repeatable and adaptable security processes taking advantage of effective security technology is needed to achieve those goals. From that base, organizations can deploy advanced controls that use machine learning, continuous monitoring, and verification to increase prevention capabilities, reduce time to detect/respond, and minimize business impacts from constantly evolving threats.

---

[17] DBIR 2021 Data Breach Investigations Report," www.verizon.com/business/resources/reports/dbir

[18] "Microsoft: Using multi-factor authentication blocks 99.9% of account hacks," www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks

[19] "CIS Controls V7.1 Implementation Groups," www.cisecurity.org/white-papers/cis-controls-v-7-1-implementation-groups

[20] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 2021, www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

Summary

Cybersecurity is challenging, largely because of the following three large-scale trends, all of which are beyond the control of the security team:

- **Innovators continually and unpredictably think up new technologies, protocols, and applications.** They do so generally with a focus on speed, ease of use, and profitability. Security, not so much.
- **Business leaders adopt new technologies quickly, and fast followers not long after.** Businesses are not willing to lose first-mover advantages to wait for security maturity.
- **Hackers, criminals, and malicious nation states move quickly to exploit the vulnerabilities that result.**

This whitepaper focused on that last trend and presented the expertise of four top SANS instructors. Early insight into the vulnerabilities that result from new technologies and rapid business adoption allow security managers, architects, and analysts to look for gaps in current security processes and controls and take proactive steps to minimize them. According to Chris Crowley,[21] another top SANS instructor, "A SOC is successful when it intervenes in adversary efforts to impact the availability, confidentiality, and integrity of organization's information assets. It does this by proactively making systems more resilient to impact and reactively detecting, containing, and eliminating adversary capability."

The SANS mantra emphasizes action to prevent more attacks, to more quickly detect what gets through, and to minimize business disruption through timely and precise mitigation actions. To do so against the emerging threats documented in this report doesn't necessarily require new approaches to security, but it does mean addressing gaps; increasing speed and accuracy of response; and assuring the skills of your team, the completeness of your processes, and that the capabilities of your security technology are up to the challenge, especially in these key areas:

- Replacing reusable passwords with multifactor authentication
- Essential security hygiene, including configuration management, timely patching, privilege minimization, and network segmentation and application
- Proactive and continual threat hunting/purple teaming
- Integrated accurate, timely, and relevant intelligence information
- Gaining support for big jumps in endpoint and cloud system protection by building security into all user devices and application/server workloads

[21] Christopher Crowley, SANS senior instructor profile, www.sans.org/profiles/christopher-crowley

About the Author

John Pescatore joined SANS as director of emerging security trends 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 US 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.

Sponsors

SANS would like to thank this paper's sponsors:

ANOMALI®

BlackBerry®

cisco™

corelight

DOMAINTOOLS®

ExtraHop

LogRhythm®

RAPID7

SOPHOS
Cybersecurity made simple.

THREATQUOTIENT