SANS

Analyst Program

Whitepaper

SANS 2022 Top New Attacks and Threat Report

Written by **John Pescatore** and **Terry Hicks**

September 2022

LogRhythm™

Introduction

In the past, security managers had to work hard to convince CxOs and boards of directors of the potential risks associated with using the internet. These days, breaches and successful ransomware attacks are in the news constantly, and most business leaders now recognize that the internet can be a dangerous place. However, that doesn't mean security managers have provided CxOs and directors a clear strategy and vision regarding how the business can increase its effectiveness and efficiency in dealing with known threats while minimizing the risk from emerging attacks moving forward.

For more than 15 years, the SANS Institute's expert panel at the annual RSA Conference has filled that gap. This SANS whitepaper, which begins with a baseline of statistics from reliable sources of breach and malware data, summarizes the SANS instructors' expert advice from the most recent RSA panel, which details the emerging threats to watch for in 2022 and beyond.

2021/2022 Breach and Threat Baseline Data

Because the pandemic delayed the 2022 RSA Conference and the annual keynote panel discussion, "The Five Most Dangerous New Attack Techniques,"[1] this year's report focuses less on what occurred in 2021 and more on the first quarter of 2022 (1Q22) along with projections for 2023.

As in previous reports, we'll start with a baseline from data collected by the Identity Theft Resource Center (ITRC).[2] The ITRC has followed a consistent methodology for many years, using only verified information from publicly disclosed breaches in the United States. These data do not include events such as DDoS attacks, but they do include more recent ransomware attacks.

Table 1 shows a comparison of incidents and individual identities affected during 1Q22 and the full years of 2021 and 2020.

Table 1. Comparison of Incidents and Individual Identities Affected During FY20, FY21, and 1Q22 (Source: ITRC)[3]

Sector	Year					
	Q1 YTD 2022		FY 2021		FY 2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	21	106,099	125	1,681,483	42	974,054
Financial Sevices	68	3,384,769	279	19,973,772	138	2,687,084
Government	13	294,027	66	3,244,455	47	1,100,526
Healthcare	73	2,560,465	330	28,216,273	306	9,700,238
Hospitality	6	56,451	33	238,445	17	22,365,384
Manufacturing & Utilities	52	247,852	222	49,777,158	70	2,896,627
Non-Profit/NGO	18	558,362	86	2,339,646	31	37,528
Professional Services	46	1,719,850	184	22,725,185	144	73,012,145
Retail	18	272,950	102	7,212,912	53	10,710,681
Technology	16	10,832,588	79	44,679,488	67	142,134,883
Transportation	8	20,930	44	569,574	21	1,208,292
Other	65	719,620	308	79,538,669	172	43,391,302
Unknown	-	-	4	35,232,664	-	-
TOTALS	**404**	**20,773,963**	**1,862**	**295,429,724**	**1,108**	**310,218,744**
Individuals affected per breach		**51,421**		**158,662**		**279,980**

[1] RSA Conference presentation overview, www.rsaconference.com/usa/agenda/session/The%20Five%20Most%20Dangerous%20New%20Attack%20Techniques

[2] Identity Theft Resource Center, "Notified," www.idtheftcenter.org/notified

[3] Q1 Data Breach Analysis, ITRC, www.idtheftcenter.org/publication/q1-2022-data-breach-analysis/

Highlights from this comparison include the following:

- The average size of a breach is declining. The 1Q22 average breach size was less than one-third the size of the average 2021 breach, and the 2021 breach size was down 5% from 2020's figure. This is largely due to attackers going after smaller businesses (especially in the healthcare vertical) and state and local government agencies.
- Extrapolating 1Q22 across the full year (using an adjustment factor, because 1Q is historically a slower breach period) suggests that growth is likely to be seen in manufacturing, healthcare and nonprofit/nongovernmental organizations in 2022, while education, government and retail attacks will probably decline. Most other verticals are likely to see similar attack quantities as in 2021 across FY22.

The rise in breaches at smaller organizations means larger companies must pay more attention to the security levels of their smaller suppliers. Two frameworks will help them ensure supplier compliance: the American Institute of Certified Public Accountants' Supply Chain Risk Management Reporting Framework[4] and the National Institute of Standards and Technology's updated SP 800-161 Supply Chain Risk Framework.[5]

The ITRC data also show that business email compromises/phishing represented the single largest attack vector—the root cause of more than 51% of all compromises. Many larger organizations have begun moving to some form of multifactor authentication (MFA) for email logins, which has been shown to thwart more than 99.9% of all phishing attacks.[6] In June 2022, the U.S. Department of Homeland Security (DHS) directed all U.S. federal agencies to move to MFA for all Microsoft Exchange use. This will help drive larger government suppliers to also adopt MFA, but smaller businesses and government agencies will likely be slow to do so.

Because it's based on detailed investigations of real-world breaches, Verizon's 2022 Data Breach Investigations Report (DBIR) is another useful source of data, though changes each year in methodology and reporting limit year-to-year comparisons.[7] This year's DBIR validates the need to move to MFA and away from reusable passwords, reporting that 60% of breaches were enabled by stolen credentials or phishing attacks (see Figure 1).

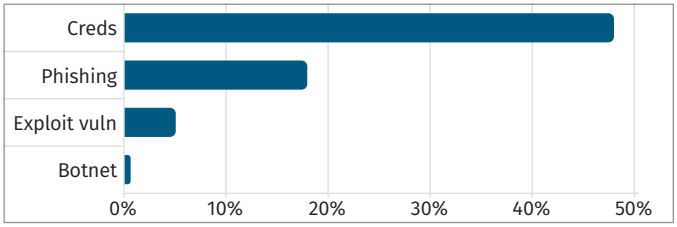

Figure 1. Primary Enablers of Non-Error, Non-Misuse Breaches[8]

[4] American Institute of Certified Public Accountants, "SOC for Supply Chain," https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/soc-for-supply-chain

[5] National Institute of Standards and Technology, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

[6] "One simple action you can take to prevent 99.9 percent of attacks on your accounts," www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

[7] Verizon, "2022 Data Breach Investigations Report," www.verizon.com/business/resources/reports/dbir

[8] Verizon, 2022 DBIR

The 2022 DBIR also shows the importance of supply chain security, finding that 60% of system intrusions were due to partner compromises, most involving reusable passwords at a partner or supplier. Of equal magnitude were compromised software updates (such as the SolarWinds incident) across commercial software and open source software (see Figure 2). Both of these issues once again highlight the need for improvements in supply chain security.

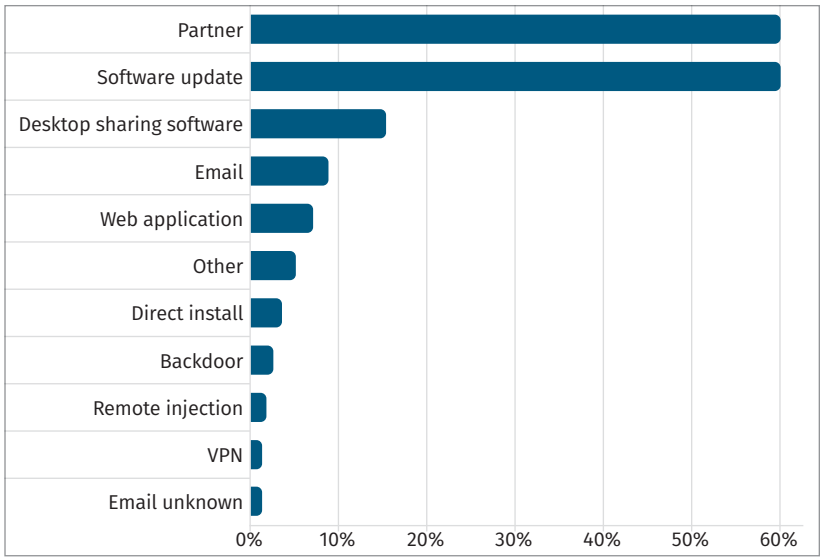

Figure 2. Top Action Vectors in System Intrusion Incidents[9]

New threats are often enabled when the business uses new technology. The rapid growth of software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and mobile applications is the biggest recent technology trend, and attackers have followed the trend.

The Cloud Security Alliance (CSA) bases its "Top Threats to Cloud Computing" report on survey data and working group inputs.[10] This year, the working groups found 19 threat vectors representing the most common attack paths for cloud-related security incidents, and the CSA surveyed 700 security professionals to rank those 19 vectors in order of importance. The top 11, shown in Table 2, cover the vast majority of attacks.

Once again, poor identity protection (essentially the ability to thwart phishing attacks and other attempts to steal reusable passwords) ranked as the most critical area. Lack of basic security hygiene in cloud administration and application development by the IT organization (insecure interfaces and APIs, misconfiguration and inadequate change control, lack of cloud security architecture and strategy, and insecure software development) filled out the top five, and supply chain/third-party compromises (which did not make the top 11 in 2019) ranked sixth.

Table 2. Most Common Attack Paths, 2022
(With Changes from 2019 Rankings)

	2022 Ranking	2019 Ranking
Insufficient management of identity, credentials, access, and keys	1	4
Insecure interfaces and APIs	2	7
Misconfiguration and inadequate change control	3	2
Lack of cloud security architecture and strategy	4	3
Insecure software development	5	—
Unsecured third-party resources	6	—
System vulnerabilities	7	8
Accidental cloud data disclosure	8	—
Misconfiguration and exploitation of serverless and container workloads	9	—
Organized crime/hackers/advanced persistent threats	10	11
Cloud storage data exfiltration	11	—

[9] Verizon, 2022 DBIR

[10] Cloud Security Alliance, "Top Threats to Cloud Computing," https://cloudsecurityalliance.org/research/working-groups/top-threats

Conclusions

Three major issues emerge from an analysis of these reports:

1. **Reusable passwords continue to be an "Attack me" sign attached to critical business applications.** Moving to MFA does not make compromises impossible, but it does raise the bar, blocking 99.9% of phishing attacks.
2. **Attackers will find and go after the weak link in company supply chains.** The Target breach of 2013 caused many companies to increase the level of scrutiny and monitoring of their remote contractors, but attackers are still finding too many opportunities to compromise smaller suppliers and attack those suppliers' large customers.[11]
3. **Basic security hygiene is still Job No. 1.** Studies looking at real-world causes of damaging incidents invariably report that 70% or more could have been averted by deploying Implementation Group 1 of the CIS Critical Security Controls.[12]

Hear from the Experts: SANS Threat Panel at RSA Conference 2022

The RSA Security Conference, which began in 1991, has grown to be one of the largest cybersecurity conferences in the world. For the past 16 years, SANS has presented a panel discussion at the conference in which its top experts detail their views of the most dangerous attacks that are just beginning to impact enterprises. Over the years, the predictions made by the SANS instructors at these sessions have proved highly accurate forecasts of future real-world damage.

The 2022 threat expert panel (seen in Figure 3) consisted of:

- Moderator **Ed Skoudis**, President, SANS Technology Institute College and SANS Faculty Fellow
- **Katie Nickels**, certified instructor at SANS and director of intelligence at Red Canary
- **Johannes Ullrich**, dean of research at the SANS Technology Institute and founder and director of the Internet Storm Center
- **Heather Mahalik**, senior instructor at SANS and senior director of digital intelligence at Cellebrite
- **Rob Lee**, chief curriculum director and faculty lead at SANS

Figure 3. RSA Conference 2022 SANS Panel

[11] USA Today, "Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers," May 23, 2017, www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[12] Center for Internet Security, "V7.1 Introduces Implementation Groups to the CIS Critical Security Controls," www.cisecurity.org/insights/blog/v7-1-introduces-implementation-groups-cis-controls

Katie Nickels: Living Off the Cloud; Bypassing MFA

In previous years, SANS has warned that living-off-the-land attacks, where adversaries use the operating system's own features to attack it, are a major growth area in threats. Nickels indicated that she is now seeing living-off-the-cloud attacks, where attackers use inexpensive and easy-to-set-up cloud services to launch their attacks, and they also take advantage of insecure configurations as entry points to compromise the target's cloud services.

Living Off the Cloud

Nickels illustrated the living-off-the-cloud attack with recent exploits where attackers used ngrok, a common cloud-based tool used by developers (see Figure 4).

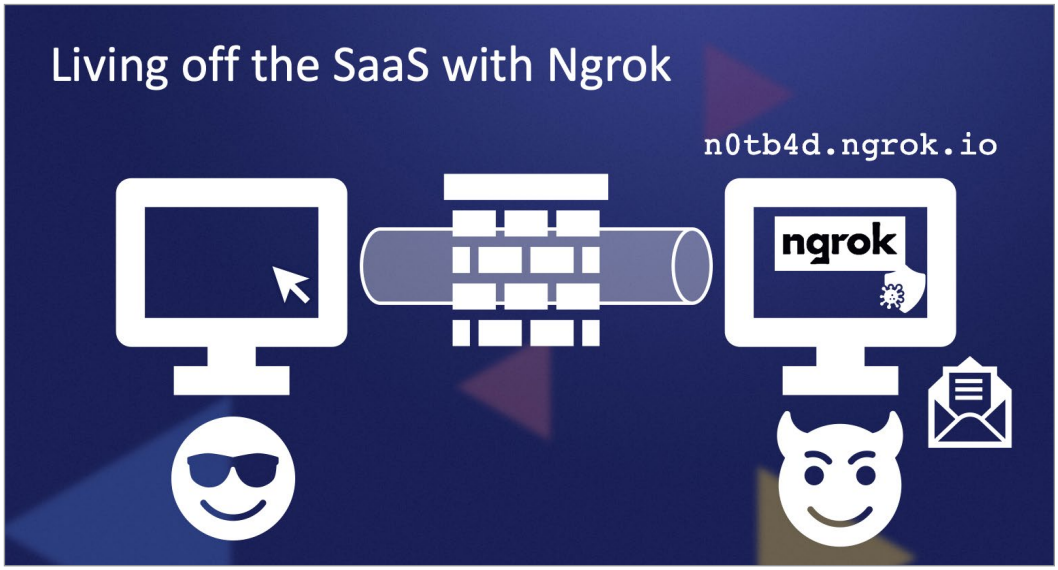

Figure 4. A Living-Off-the-SaaS Attack

The vendor of the tool, also called ngrok, boasts that it allows developers to " . . . [s]pend more time programming—one command for an instant, secure URL to your localhost server through any NAT or firewall."[13] Unfortunately, both developers and attackers can gain that advantage if ngrok can be used without sufficient security controls. An attacker who uses the same cloud tool that developers are using also has an easier time evading detection.

Nickels also outlined recent attacks that used Microsoft OneDrive to get users to click on URLs that delivered Qbot or Qakbot malware. OneDrive storage-as-a-service is included in Microsoft 365 and Office 365 plans, as well as in SharePoint plans, and is often enabled without the IT organization even planning on using it.

"It's not just enough to pay attention to the operating systems, the endpoints. Adversaries and a lot of their intrusions are using cloud services of different types for a lot of really good reasons."

—Katie Nickels

Mitigation

What's the answer? Training is a big part of it. Nickels mentioned a classic SANS poster that reads, "Know Normal . . . Find Evil,"[14] and pointed out that its message—the importance of focus—is more relevant than ever. This type of behavior detection has always raised the risk of false positives, however. Security professionals and end users alike must learn how to identify dangerous activity and then rapidly and accurately differentiate it from normal business activity.

[13] GitHub, https://github.com/praveen-jangir/Local-Online-Server-using-ngrok

[14] SANS DFIR Twitter account, https://twitter.com/sansforensics/status/910905241406787587

Although there has been massive overhype about the use of artificial intelligence (AI) and machine learning (ML) in cybersecurity tools and products, there have been advances in specific uses of ML to prioritize events so that an analyst can first investigate the events most likely to be malicious. *SANS SEC595: Applied Data Science and Machine Learning for Cybersecurity Professionals* is an example of a course that enables security analysts to make effective use of ML's capabilities.[15]

Sharing lessons learned is also important. When the ngrok team learned of the malicious use cases that Nickels discussed, it responded immediately. Cloud service providers need to be informed of vulnerabilities so that they can harden their defenses and improve future releases, as well.

"Multifactor [authentication] remains an incredibly powerful force for security, but attackers have already launched attacks to bypass MFA. Keep using it, but be thoughtful in how you implement it."

—Katie Nickels

To do all these things efficiently and effectively, a solid base of basic security hygiene is needed or security resources will be consumed putting out easily avoidable fires. Maintaining visibility into network traffic, having timely and accurate vulnerability and threat data and performing log monitoring and analysis are critical capabilities that need to be in place.

MFA Bypass

As we have already noted, moving from reusable passwords to MFA is the single biggest security improvement for deterring real-world attacks. However, MFA is not trivial to implement, and there always must be some backup authentication path, in case the user can't log in using the preferred MFA approach. Adversaries have already been probing MFA configurations and services and finding ways to bypass the added level of security.

Nickels illustrated this threat with an example from a 2021 report from the U.S. Cybersecurity and Infrastructure Security Agency wherein Russian state-sponsored attackers brute-forced their way into an account by guessing a password and gaining control.[16] (See Figure 5.)

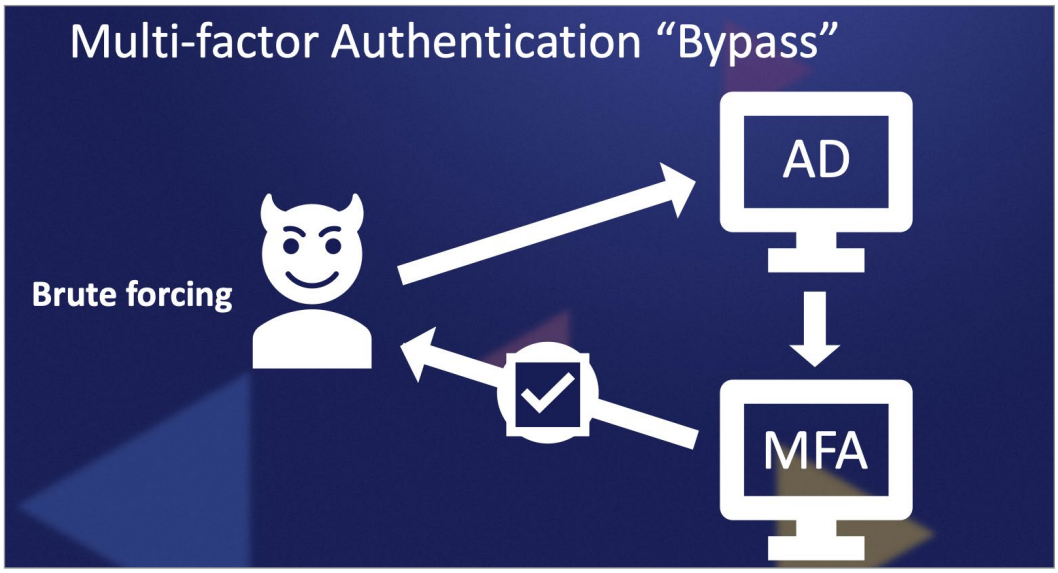

Figure 5. Bypassing MFA

The account was old and had been disabled in the MFA service that would have allowed deeper access, but IT administration had not disabled it in Active Directory. From AD, the attackers re-enabled the MFA service, essentially bypassing MFA (by re-enabling it) and then enrolling a new device that the attackers controlled. Game over.

---

[15] SANS Institute, "Manage Your Team," www.sans.org/cyber-security-courses/applied-data-science-machine-learning

[16] Cybersecurity & Infrastructure Security Agency, "Alert (AA22–074A), Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and 'PrintNightmare' Vulnerability," www.cisa.gov/uscert/ncas/alerts/aa22-074a

Mitigation

Moving from passwords to MFA requires a well-planned effort to avoid business disruption. Part of that effort includes keeping MFA secure and deciding which backup approach will be used when the MFA solution is not available. For the specific attack Nickels discussed, she said enterprises must make sure that when an account is disabled in MFA, it should be disabled in AD as well. But the "Know Normal . . . Find Evil" approach is still critical. Security professionals must be able to identify what's normal for user accounts—and what isn't.

Johannes Ullrich: Attacks Against Backups

Enterprises tend to have a diverse set of backup technologies, Ullrich noted. Often, backup methods have been added on top of older methods through the years—like the rings of a tree—as IT has evolved from mainframes to departmental computing to client/server to PC-centric and, most recently, to cloud. Almost all these types of backup methods require some form of software agent be installed on a user's PC. And they all have vulnerabilities (see Figure 6).

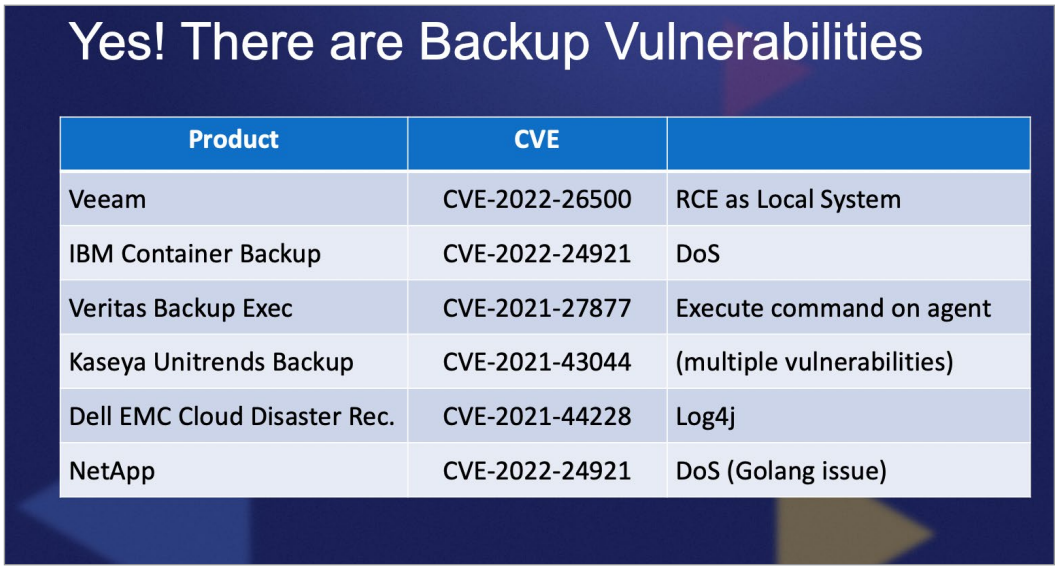

Figure 6. Backup Vulnerabilities

Backing Up: Prepare for Unique Attacks

Ullrich predicted that unique attacks that can be launched against these backup solutions will emerge. The complexity that inevitably comes with this array of devices and agents makes backup management a serious concern. Ullrich said that IT Ops (or sometimes security) professionals tend to set up a management solution for a type of backup; configure it per the vendor's defaults of what to back up, where to back it up, etc.; and then let everything run from there.

> **"Do you know where your backups are? . . . Backups are often forgotten."**
>
> **—Johannes Ullrich**

This enables living-off-the-land attacks. Your most sensitive data have essentially been instrumented for the attacker, who will use one or more of the approved backup systems to attack the data. An attacker can simply go into the backup solution and configure a second destination, and you are sending the attacker your most sensitive files as part of backup processes that have already been designated as normal operations. And the more enterprises rely on cloud backup, the greater the threat of living-off-the-cloud attacks, as Nickels explained. If the same cloud service provider is being used for cloud backups as for cloud services, it becomes even trickier to tell when something unusual is happening.

Legitimate backups—and network monitoring systems, as well—present security monitoring and detection problems, because they send enormous amounts of data across the network, sometimes with proxies, and often with encrypting agents. Huge amounts of data tend to result in false positives being reported by data leak prevention (DLP) systems and network intrusion detection systems (IDSs). To reduce those false positives, DLP and IDS controls are often tuned to ignore backups, either by declaring the software to be trusted or by not inspecting payloads during defined backup times. Attackers will take advantage of these practices.

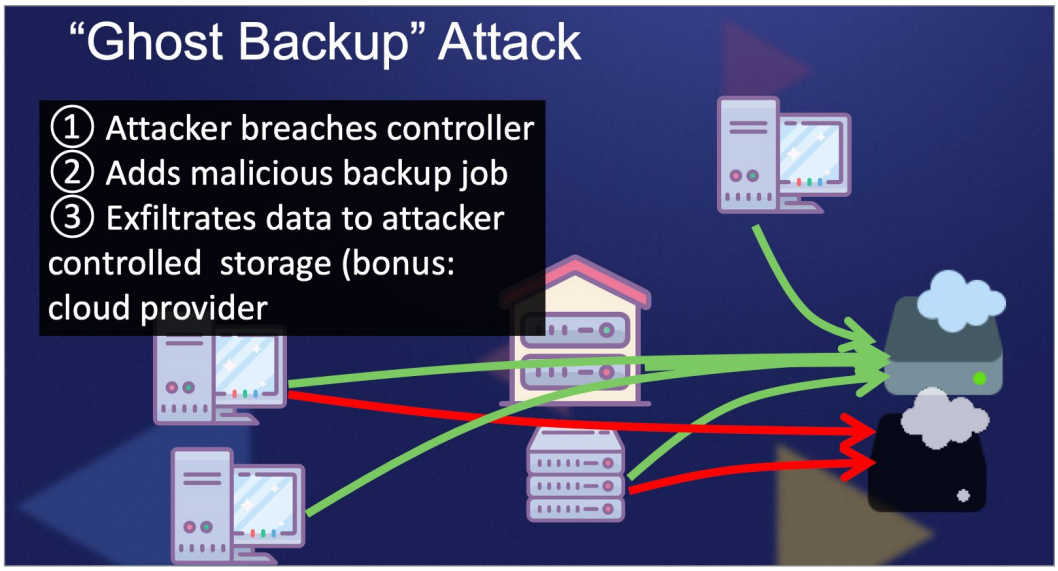

Figure 7. "Ghost Backup" Attacks

Mitigation

Backups are obviously critical to protecting against crashes, as well as ransomware and other attacks aimed at making critical data or executables unavailable, Ullrich said. It's important to make sure that only the things that must be backed up are backed up, he advised—minimizing the attack surface of your backup architecture. Make sure that multiple layers of backing up do not cause unintended consequences, but preferably have multiple tiers of backup that go to disparate locations—ideally at least one of which is protected by an air gap and uses read-only media types. Ensure you have an accurate inventory of all backup locations that you plan to have stored.

> **"For each backup solution, we have some unique attacks that could be launched against it."**
>
> **—Johannes Ullrich**

Heather Mahalik: New Takes on Old Techniques

In a recurring theme for this year's panel, Mahalik discussed old and familiar attack techniques with new and unfamiliar uses. As we've seen, attackers continue to use tried-and-tested techniques even as they try out new approaches. And why wouldn't they? Those techniques are cheap, they're readily available, they work and they can be repurposed in new and dangerous ways.

> **"Don't think you're not important enough to be stalked."**
>
> **—Heather Mahalik**

Stalkerware

The first of the techniques Mahalik discussed was stalkerware—inexpensive, readily available software that's typically used to track someone's activities. Stalkerware has historically required access to a device, and it is often installed by parents on their children's phones. But with malicious stalkerware, gaining access to a device can be as simple as getting someone to click on a link in an email. Security professionals have spent years training end users to avoid doing that, but it still happens, and it likely always will.

Next, Mahalik talked about the Pegasus stalkerware, sold to governments as a "cyber intelligence" tool by the Israeli company NSO Group. Pegasus enables a zero-click install on vulnerable versions of Android and iOS. It was first discovered on the phones of human rights activists in 2016, and a broad investigation in 2021 known as the Pegasus Project found more than 50,000 phone numbers that had been compromised by it (see Figure 8).[17]

In the August 2, 2022, issue of NewsBites, SANS published news reports of the European Union's investigation of a commercial company that also sells spyware targeting a (now patched) Windows vulnerability to law firms, banks, and consultancies.[18]

Figure 8. Zero-Click Exploit for iOS and Android

Mitigation

Barring drastic measures such as enabling the lockdown mode that Apple is introducing (see sidebar), mitigating the risk of stalkerware at enterprise scale usually means using mobile device management (MDM). MDM processes and products can be used to maintain the safest possible phone OS configuration, reducing both the risk of known malicious executables being installed and the time it takes to detect when potentially risky applications are loaded on a phone. User awareness and education programs should address stalkerware, emphasizing the employee's personal risk, as well as the risk to the enterprise.

Apple Announces Lockdown Mode

On July 6, 2022, Apple announced it would soon release a lockdown mode capability for iPhones.[19] Apple's lockdown mode is specifically designed to ". . . protect users who may be personally targeted by some of the most sophisticated digital threats, such as those from private companies developing state-sponsored mercenary spyware." The option is directly targeted at Pegasus, but it should also prove effective against other forms of stalkerware. Lockdown mode will not be widely used, because it disables many risky but useful functions, such as clickable links, and blocks all executable attachments. However, many CEOs need that level of protection and may be willing to live with the restrictions. Lockdown mode will be available in 3Q22.

[17] The Guardian, "The Pegasus Project," www.theguardian.com/news/series/pegasus-project

[18] SANS NewsBites, "Don't Let Your Twitter Apps Expose API Keys; Assume All Atlassian Servers Are Compromised; Check Phones for DSIRF/Subzero Spyware," www.sans.org/newsletters/newsbites/xxiv-59

[19] Apple Newsroom, "Apple Expands Industry-Leading Commitment to Protect Users from Highly Targeted Mercenary Spyware," July 6, 2022, www.apple.com/newsroom/2022/07/apple-expands-commitment-to-protect-users-from-mercenary-spyware

Worms

Mahalik then discussed a form of malware that was making headlines as far back as 1988: the network worm attack. A worm is malware that can replicate itself and spread to other computers. By their very nature, worms tend to be "noisy," causing a high volume of network traffic by scanning for other machines and then copying themselves over the network. Over the years, however, attackers have gotten more sophisticated in reducing the noise and building in evasion techniques.

> **"Worms are still out there, and they're still doing damage."**
>
> **—Heather Mahalik**

Worms are still out there, and they're still doing damage. The WannaCry ransomware attack included a worm component, and it did tremendous damage in 2017—and is still impacting endpoints in 2022.

Mitigation

Most worms are avoidable using basic security hygiene techniques: appropriate backups for all devices and applications, rapid patching and updating of critical software, continuous vulnerability management and the elimination of reusable passwords by moving to passcodes and MFA. Threat hunting can detect network worms in the early stages, reducing overall impact by lowering time to detect. Because attackers are always improving their methods, maintaining effective defenses against worms and other malware also means constantly updating security skills, completing training, reading documentation and learning about a constantly evolving threat environment.

Rob Lee: Dual-Use Technology Attacks

Lee began his presentation with a disturbing example of a highly advanced threat from the Russian invasion of Ukraine in February of this year. Along with the use of satellite triangulation to target Ukrainian positions, Russian cyber assets used malware called Acid Rain to disable the OSes of Ukraine's ViaSat satellite modems. Acid Rain also destroyed modems in other parts of Europe and even some other critical infrastructure, such as wind turbines. The risk here is that when technology used by the military comes under attack in wartime, similar technology used by private industry is also at risk—even when it's outside the war zone.

> **"[The] high ground is control of information, and the highest ground that we're looking at out there currently is satellites."**
>
> **—Rob Lee**

A solution came, at least temporarily, when SpaceX and the U.S. government partnered to send thousands of Starlink commercial satellite terminals to Ukraine. That enabled the Ukrainian military to use point-to-point communications encryption. Although it immediately came under attack from Russia, Starlink has not been compromised or brought down so far—but commercial users of Starlink are now at much higher risk of disruption, because the technology is an obvious target for Russian attack. Lee noted that there are reports that hostile state actors are already targeting Starlink, and they have probably already released malware aimed at it.

Lee pointed out how many other, nonmilitary functions rely completely on satellite communications. There are other technologies, such as GPS, that also fit the dual-use pattern. When a commercial technology begins to be used by the military, commercial users must understand the increased risks and plan for disruption.

Mitigation

The implications of security threats to satellite networks and other dual-use technologies are extremely serious, and they will inevitably impact governments, the private sector, enterprises and individuals. Private industry cannot defend space-based systems, of course. Therefore, backup communication techniques should be defined for all critical satellite links as mitigation for potential outages, and backups ought to be regularly tested. It is also recommended that threat intelligence sources be monitored for early indications of potential military actions that could impact your use of such technologies.

Best Practices for Improving Defenses Overall

Some cybersecurity best practices will always be required as a foundation to reduce the risk of all threats, including the ones discussed by the panel:

- **Essential security hygiene—**As detailed in the Center for Internet Security's Critical Security Controls[20] and recommended by global cybersecurity agencies,[20] asset visibility and inventory, configuration management, timely patching, continuous vulnerability management, log event monitoring, backup and recovery, privilege minimization, network segmentation and application control can prevent the majority of malicious executables from being effective—even if an attack does manage to install any.

  Implementation Group 1 of the CIS Critical Security Controls[22] is a minimum starting point for advanced concepts such as zero trust. Reaching that level enables movement to higher levels of protection such as application security, advanced endpoint detection and response, and automation that can be effective against the advanced threats described.

- **Accelerated adoption of MFA—**The latest data show that most damaging attacks are still enabled by a phishing attack that captures privileged user credentials and passwords. Two-factor authentication (2FA) is not unbreakable, but it raises the bar against attackers and forces them to use techniques that are much easier to detect than those they can employ when they are in control of internally connected PCs.

[20] Center for Internet Security, "CIS Critical Security Controls," www.cisecurity.org/controls

[21] National Security Agency/Central Security Service, "NSA, Allies Issue Cybersecurity Advisory on Weaknesses that Allow Initial Access," May 17, 2022, www.nsa.gov/Press-Room/News-Highlights/Article/Article/3033563/nsa-allies-issue-cybersecurity-advisory-on-weaknesses-that-allow-initial-access

[22] Center for Internet Security, "CIS Critical Security Controls V7.1 Implementation Groups," www.cisecurity.org/white-papers/cis-controls-v-7-1-implementation-groups

The requirements for essential security hygiene and strong authentication are well known. The hard part is figuring out how to overcome organizational obstacles for successful deployment. Security teams must be able to work effectively with IT operations to deliver the greatest benefit from most security advances, and they also must gain business-unit and upper-management buy-in to ensure that they receive the funding and support necessary for operational changes.

Although improvements in these two security areas will help fend off attacks, advanced adversaries will unquestionably learn how to adapt rapidly and develop more advanced threats. Security processes and controls must continue to evolve. Many organizations must enhance the skill levels of their security teams to be more effective in several specific areas:

- **Threat hunting/purple teaming—**Cybersecurity defenses have never been perfect, and they never will be. Threat hunting tools and techniques allow skilled security staff to detect active threats and compromises more rapidly, thus reducing and often avoiding business damage or disruption. Purple teaming is a cooperative effort between red teams/penetration testers and blue teams/SecOps defenders to learn from each other and drive higher levels of preparedness and lower reaction times.
- **Increasing software supply chain security—**Software security should be an integrated part of any large supply chain security, quality or resiliency program. If such programs don't exist in your organization, at a minimum work with IT and procurement to make sure software and SaaS vendors are required to demonstrate secure development lifecycles. For example, an easy check: Does the software or SaaS provider sponsor a managed bug bounty program? Many do, and it should really stand out if a vendor doesn't.
- **Extending security processes to mobile and cloud-based applications—**Security skills are often very Windows-centric, because vulnerable Windows PCs and servers have long been the most common entry point for successful attacks. However, mobile threats target Android and iOS, and although cloud workloads often run on Windows server images, Linux and VMware knowledge is needed.
- **Securing operational technology and IoT devices—**Threats against critical infrastructure systems are real today, and threats against the IoT are going to increase. Knowledge of those specialized environments requires specialized security skills in many vertical industries.
- **Better data and better integration, not just more data—**Accurate and timely threat information can be integrated with continuous and accurate configuration/vulnerability information to provide high-fidelity prioritization of actions needed to reduce risk. Most enterprises aren't lacking in quantity of intelligence and vulnerability data, but improvements in quality, freshness and integration are needed.

From this base, advanced controls can be deployed to minimize the business impacts of constantly evolving threats: the use of ML and continuous monitoring and verification, better prevention capabilities and technologies that reduce the time to detect and respond.

Summary

This year's SANS Threat Panel had two major themes:

- The urgent need to prepare for and develop defenses against sophisticated, highly advanced emerging threats
- Pointed reminders that some old and familiar attack techniques and attack surfaces remain very dangerous and that essential security hygiene processes and controls are as important and necessary as ever

Sophisticated attacks get the headlines, and sometimes the headlines can help security professionals get management buy-in to enable organizational changes required for improving security. However, many CEOs and boards of directors already understand the dangers; what they need is to hear a coherent strategy from the security group that details how to reduce the risk of those dangers impacting the financial health of the company.

The success stories SANS has seen have rarely started with some scary briefing to management that finally made them understand security. The CISOs and security teams that have avoided being in the headlines are the ones that were able to:

- **Articulate the business benefits that an increase in security/reduction in risk will enable—**The benefits do not have to be return on investment. Other examples include faster time to market through improved vetting processes for software and supply chain security, increases in direct-mail marketing click-through rates that are due to better browser and email security, and fewer business disruptions because threat information is more accurate and integrated.
- **Educate CXOs and directors about solutions, not just problems, and get backing for the changes necessary to solve security problems—**Run tabletop exercises showing how MFA would be no more intrusive than what we all must use on our personal financial accounts.
- **Quickly communicate changes in risks and threats to management and be able to tie them to existing or planned strategies—**A common complaint from board members is that security folk are often great at describing possible "blood in the streets" scenarios but, compared with business managers, are weak on communicating strategies that connect the dots to corporate goals and shareholder concerns.

The answer is a mix of the new and the familiar. Security practitioners must apply the fundamental principles of security hygiene, periodically update their own skills and continually work to change end users' behaviors when they're confronted with threats such as phishing. They must work with the business to understand how to balance security requirements against operational needs. They must also communicate effectively, conveying the importance of their threat control and mitigation efforts and sharing the lessons they have learned.

Sponsor

SANS would like to thank this paper's sponsor: