Research Report

2022 Cybersecurity Performance Summary

CYBER THEORY

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm.
We constantly collect and analyze the latest customer data segmented by security practitioner, industry and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona. With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompasses all aspects of cybersecurity as well as the related fields of fraud, audit, compliance and risk management.

CONTACT INFORMATION

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018

Table of Contents

2022

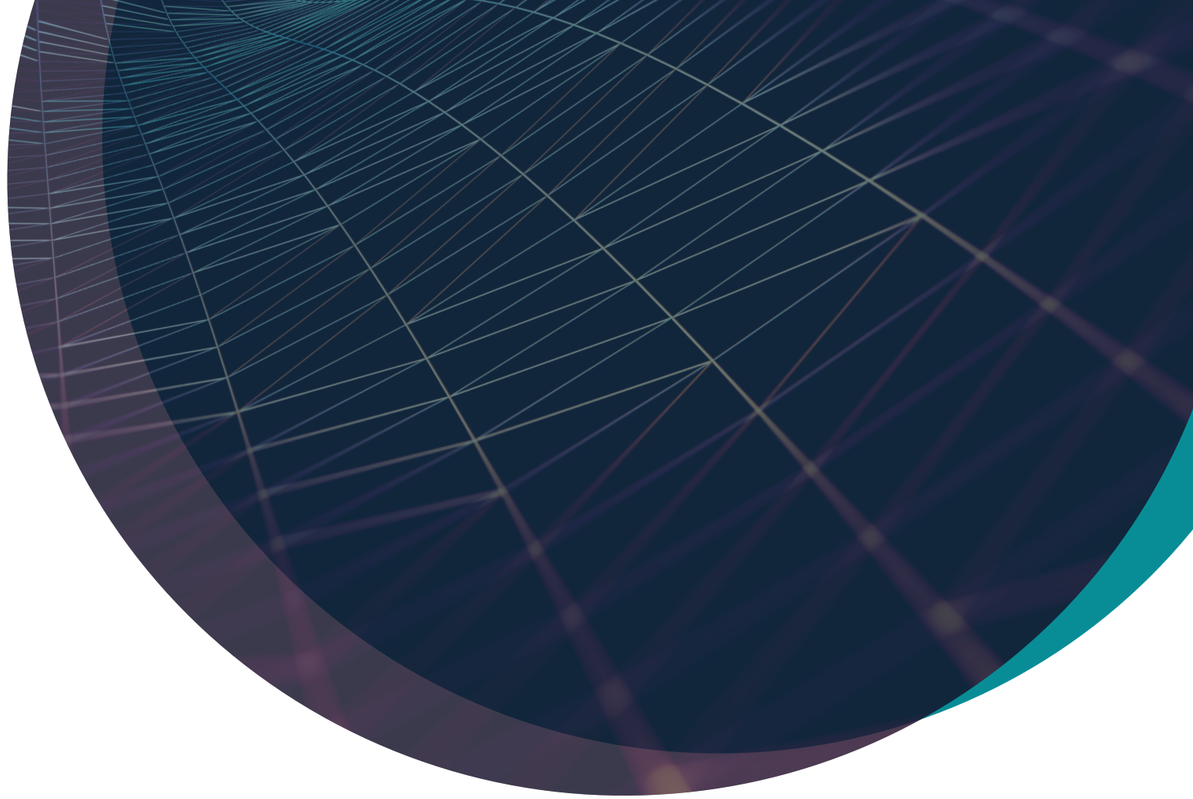
Performance

Summary

In summarizing the global cybersecurity performance for 2022, we decided to do something different. Instead of using data to describe threats, breaches and compromises by category as we usually do, we analyzed cyber incident data from a group of companies representing different industries to tell the story of the main cyber risks that grew in 2022 and are likely to present serious cybersecurity challenges in 2023.

Ransomware, Human Error

and Poor Hygiene



We think that reporting on ransomware is a good service to folks who need to better prepare for that class of attack, but there are so many who do that already, we had nothing new to add and didn't see the need. It was similar for human error and poor hygiene. There is no question but that those three threats will lead the way next year. But, again, they have been reported and advised to death. If folks don't recognize that hygiene is a huge problem and still can't figure out how to attend to the solution, nothing we can say will help them.

But, because we can't help ourselves, here are a few recommendations for improved hygiene that will serve you well in 2023:

- Securing all RDP. During COVID-19, saw workforces shift to work from home and home networks are often rife with poor security. Solid basic hygiene would include something as simple as strong passwords, multi¬factor authentication, software updates, restricted access and network-level authentication.

- Multifactor authentication. MFA for critical assets and high-risk users is strongly recommended. While far from bulletproof, this tactic can be a strong barrier for attacks that leverage credential-based access or privilege escalation such as ransomware.

- Patch management. Legacy systems, be they OT or IT, chug along on old software with security gaps. After RDP and phishing attacks, vulnerable software is the next largest attack vector, which is why securing communication channels and patching Windows operating system exploits remain vital.

- Disabling user-level command-line capabilities and blocking Transmission Control Protocol port 445. Ransomware threat actors run free or low-cost software and scanning tools, searching for such things as like credential harvesting and internal unsecured port discovery from command-line prompts. If command-line capabilities end up disabled, the company becomes a more difficult target. Also, blocking port TCP 445 on external-facing infrastructure and internal firewalls also helps reduce the attack surface.

- Protect Active Directory. Active Directory is a database and set of services that connects users with the network resources they need to get their work done. The database contains critical information about your environment, including what users and computers there are and who's allowed to do what.

- Education and training. Cyber awareness training and education should be mandatory. You don't need to be a highly trained and skilled cybersecurity professional, but basic changes in behavior and awareness of where and how threats can enter your organization can further reduce risks.

The Big Cyber-Risks Emerging From 2022

These risks are categorized as cloud storage vulnerabilities, code leakage, exposed credentials, third-party and open-source vulnerabilities and exposed shadow assets, including zombie APIs, unsecured DNS's, polymorphic malware and code development. Here are a few stats that lead us to our conclusions:

Code Development

This is personal as we saw within our own outsourcing that our code was left unprotected on GitHub repos, and research says that in 2022, outsourcing code development has led to an increase of over 65% in code leaks. Even with "airtight" outsourcing contracts or SLAs, the risk of poor privacy practices, storage and development practices has led to this significant increase in leaked code.

Public repos are not well protected. GitHub frequently leaks API and cryptographic keys. According to a study from North Carolina State University, over 100,000 GitHub repos leaked API or cryptographic keys in 2022. And in addition, they found that thousands of new API or cryptographic keys leak via GitHub projects every day.

So, whether you are outsourcing or developing in-house with your own team, what can you do to assure data security and eliminate cybersecurity threats? Nothing. But you can mitigate them by following the OWASP secure coding practices, of which, these eight are the keys to help you protect against vulnerabilities.

1. Security by Design
2. Password Management
3. Access Control
4. Error Handling and Logging
5. System Configuration
6. Threat Modeling
7. Cryptographic Practices
8. Input Validation and Output Encoding

Security by Design

Security needs to be a priority as you develop code, not an afterthought. Organizations may have competing priorities where software engineering and coding are concerned. Following software security best practices can conflict with optimizing for development speed. But, a "security by design" approach that puts security first tends to pay off in the long run, reducing the future cost of technical debt and risk mitigation. An analysis of your source code should be conducted throughout your software development life cycle, or SDLC, and security automation should be

Password

Management

Passwords are a weak point in many software systems, which is why MFA has become so widespread. Nevertheless, passwords are the most common security credential, and following secure coding practices limits risk. You should require all passwords to be of adequate length and complexity to withstand any typical or common attacks.

OWASP suggests several coding best practices for passwords, including:

- Storing only salted cryptographic hashes of passwords and never storing plain-text passwords;
- Enforcing password length and complexity requirements;
- Disabling password entry after multiple incorrect login attempts.

Access Control

Take a “default deny” approach to sensitive data. Limit privileges and restrict access to secure data to only users who need it. Deny access to any user that cannot demonstrate authorization. Ensure that requests for sensitive information are checked to verify that the user is authorized to access it.

> “default deny”

Error Handling

and Logging

Software errors are often indicative of bugs, many of which cause vulnerabilities. Error handling and logging are two of the most useful techniques for minimizing their impact. Error handling attempts to catch errors in the code before they result in a catastrophic failure. Logging documents errors so that developers can diagnose and mitigate their cause.

Documentation and logging of all failures, and errors should be implemented on a trusted system to comply with secure coding standards.

System Configuration

Clear your system of any unnecessary components and ensure all working software is updated with current versions and patches. If you work in multiple environments, make sure you're managing your development and production environments securely. Outdated software is a major source of vulnerabilities and security breaches. Software updates include patches that fix vulnerabilities, making regular updates one of the most vital, secure coding practices. A patch management system may help your business to keep on top of updates.

Threat Modeling

Document, locate, address and validate are the four steps to threat modeling. To securely code, you need to examine your software for areas susceptible to increased threats of attack. Threat modeling is a multistage process that should be integrated into the software life cycle from development, testing and production.

Cryptographic Practices

Encrypting data with modern cryptographic algorithms and following secure key management best practices increase the security of your code in the event of a breach.

Input Validation and Output Encoding

These secure coding standards are self-explanatory in that you need to identify all data inputs and sources and validate those classified as untrusted. You should use a standard routine for output encoding and input validation.

How to Ensure Your Code is Secure

By patching your systems regularly, you're taking these secure coding guidelines to the next level. Patch and vulnerability management is focused on identifying risk and enabling systems to stay up to date. Through these methods and security testing, you're ensuring that your code is properly checked for errors. There is no debate as to whether fundamental hygiene prevents breaches, but the rise in hygiene-related incidents suggests we are unable to manage a hygiene program with any consistency.

> "API security is a key component of modern web application security."

API Attacks on the Upsurge

We've seen a 300% increase in API traffic and a 600% increase in API attacks. API security is a key component of modern web application security. APIs may have vulnerabilities such as broken authentication and authorization, lack of rate limiting, and code injection. Organizations must regularly test APIs to identify vulnerabilities, and address these vulnerabilities using security best practices. How many do this? Very few. The exposure to insecure APIs has skyrocketed and virtually no one is paying attention to the expanding exposure. How big is the threat? Huge. Exposed credentials to increased 50% increase in notable breach incidents, i.e., those with a direct connection and an ability to damage an operation, business or organization. Credentials with elevated permissions expose organizations to greater risk, allowing for the installation of software or reconfiguration of security controls. If a threat actor is able to use elevated credentials, they can access additional hosts, install malware, steal data, and/or disable or modify security controls.

They did a lot of it in 2022 and will do a lot more in 2023. There are so many ways attackers can get into "protected" systems these days – hunting credentials on third party sites, Wi-Fi attacks, weak passwords, network scans, phishing, VPNs all offer weak channels through which bad guys can penetrate and steal credentials, which generally lead to elevated privileges and broad pathways for mayhem.

Leaking Clouds

Remote work has increased cloud adoption and caused cloud storage leaks to increase by 150%. A cloud leak occurs when sensitive data stored in a private cloud instance is accidentally exposed to the internet. The data leak stands apart from other attack vectors such as breaches, attacks and hacks, as they are the only one that is not initiated by a third party. Cloud leaks occur because cloud storage is not always partitioned from the internet at large. This is not intentional, but as with so many other issues in cybersecurity, often the result of pressured workers making "mistakes in configuring firewalls or hybrid cloud instances or S3 buckets.

Implementing solid cloud security practices can help protect against the various threats and vulnerabilities to ensure your infrastructure and data are secure. From securing user endpoints to implementing encryption and highlighting the importance of good password hygiene, getting cloud security right requires attention to a lot of detail. It's also important to try and back off the external pressure to produce rapid digitization projects and/or code development, which will take some of the weight off when it comes to ensuring your company's and customers' safety in the cloud.

Here are some initiatives to minimize cloud leakage

- Although most cloud providers have their own means of protecting their customers' infrastructure, the customer is still responsible for securing their organization's cloud user accounts and access to sensitive data. To reduce the risk of account compromise and credential theft, consider enhancing password management in your organization.
- Add password policies to your cybersecurity program. Describe your employees' expected cybersecurity habits, including having different and complex passwords for different accounts as well as regular password rotation. For a true shift in account and password security, you can deploy a centralized password management solution.
- To ensure employees can perform their duties efficiently, some organizations provide them with extensive access to systems and data at once. Accounts of such users are a gold mine for cyberattackers, as compromising them can make it easier to access critical cloud infrastructure and escalate privileges. To avoid this, your organization can regularly reassess and revoke user privileges. Follow the principle of least privilege, which states that users should only have access to data necessary to perform their job. In such a case, compromising a user's cloud account will only provide cybercriminals with limited access to sensitive data. In addition, control access permissions by having clear onboarding and offboarding procedures, including adding and removing accounts and their privileges.
- To increase transparency in your cloud infrastructure, you can use dedicated solutions to monitor your personnel's activity. By watching what your employees are doing during work hours, you'll be able to detect early signs of cloud account compromise or an insider threat. Suppose your cybersecurity specialists notice a user logged in to your cloud infrastructure from an unusual IP address or during nonworking hours. In that case, they'll be able to react to such abnormal activity in a timely manner, as it indicates the possibility of a breach.

- Similarly, if an employee is acting suspiciously by using forbidden cloud services or taking undesirable actions with sensitive data, monitoring can help you promptly detect this behavior and give you some time to analyze the situation. You should also consider monitoring the activity of any external third parties such as business partners, suppliers and vendors with access to your systems, as they may become another source of cybersecurity risks in your organization.

- Keeping track of privileged users in your cloud infrastructure is particularly important. Usually, system administrators and top management have more access to sensitive data than regular users. Consequently, privileged users can cause more damage to the cloud environment, whether maliciously or inadvertently.

When deploying your cloud infrastructure, it's crucial to check if there are any default service accounts, as they're typically privileged. Once compromised, these accounts will give attackers access to cloud networks and critical resources. To reduce the risk of cybersecurity incidents and increase accountability, you can establish nonstop activity monitoring for all privileged users in your cloud infrastructure, including system administrators and key managers.

- Monitoring user activity is not the only way to minimize the influence of the human factor inside your organization. To protect your cloud infrastructure even more, you can raise your personnel's cybersecurity awareness, with a particular emphasis on phishing.

Even the most sophisticated anti-phishing systems can't guarantee the required level of protection. A recent study of 1,800 phishing emails sent to employees of a company in the financial sector showed that 50 emails bypassed the email filtering service. Fourteen users opened the malicious email, which launched the malware. Although 13 installation attempts were denied, one person managed to install the malware. In reality, even one incident can be enough to infect and compromise the whole system.

You can also teach your employees about signs of phishing and social engineering to avoid disclosing sensitive information. Regular cybersecurity trainings and seminars are the best protection as phishing attacks evolve in method and number.

The biggest mistake in phishing education programs is training without real-life simulations. A simulation should feel like an actual phishing attack, and employees should be unaware of the impending test. You can then track simulation results and determine which employees need additional understanding.

- Cybersecurity compliance with standards, laws and regulations aims to protect consumers' data and provide general guidance for organizations to better secure sensitive data. Without the right security controls and tools in your cloud infrastructure for IT compliance, your organization may lose millions of dollars in fines in case of a data breach.

Prominent cloud computing providers are aligned with the most known compliance requirements. But, organizations using these cloud services still have to ensure their own data processes and security are compliant. Given the lack of visibility in ever-changing cloud environments, the compliance audit process is not easy.

To comply with IT requirements, you must first define which standards pertain to your industry and which your organization must meet. To make this process easier, consider hiring a data protection officer or DPO who will provide you with expert knowledge in cybersecurity and IT compliance.

- Losses from a data breach can increase if you can't quickly detect, contain and eradicate cybersecurity threats. The longer a threat remains in your cloud environment, the more data an attacker can exfiltrate or delete.

Alternatively, a fast response to a cybersecurity incident can limit the extent of damage. You should develop an incident response plan to ensure your cybersecurity team can act efficiently in an emergency. This plan must outline strict rules and procedures for different scenarios and each different role.

Misconfigurations

The $100 million Capital One breach happened because the attacker took advantage of a misconfiguration in the Amazon Web Services web application firewall, which was deployed along with the open-source Apache web server to provide protections against several classes of vulnerabilities that attackers most commonly use to compromise the security of web-based applications.

The misconfiguration of the WAF allowed the intruder to trick the firewall into relaying requests to a key back-end resource on the AWS platform. This resource, known as the "metadata" service, is responsible for handing out temporary information to a cloud server, including current credentials sent from a security service to access any resource in the cloud to which that server has access.

In AWS, exactly what those credentials can be used for hinges on the permissions assigned to the resource that is requesting them. In Capital One's case, the misconfigured WAF for whatever reason was assigned too many permissions, i.e., it was allowed to list all of the files in any buckets of data and to read the contents of each of those files.

The type of vulnerability exploited by the intruder in the Capital One hack is a well-known method called a Server Side Request Forgery attack, in which a server - in this case, CapOne's WAF - can be tricked into running commands that it should never have been permitted to run, including those that allow it to talk to the metadata service.

Cloud leakage is not an AWS problem exclusively. Microsoft Azure, Oracle, Google and IBM Cloud have all had their share. But in all cases, the default position is significant to note – it's private. In order to leak, permissions have to be altered by a human. Today when these public permissions are allowed, the boundary between "the cloud" and the internet dissolves. This data then becomes accessible to anyone.

Here are some efficient ways to minimize security misconfiguration:

- Establish a hardening process that is repeatable, so that it's fast and simple to deploy correctly configured new environments. The production, development and QA environments should all be configured in the same way, but with distinct passwords used in every environment. Automating this process will easily establish a secure environment.
- Install patches and software updates regularly and in a timely way in every environment. You can also patch a golden image and deploy the image into your environment.
- Develop an application architecture that offers effective and secure separation of elements.
- Run scans and audits often and periodically to identify missing patches or potential security misconfigurations.
- Ensure a well-maintained and structured development cycle. This will facilitate the security testing of the application in the development phase.
- Train and educate your employees on the significance of security configurations and how they can affect the general organization's security.
- Encrypt data at rest to prevent data from exploitation.
- Apply genuine access controls to both files and directories. This will help offset the vulnerabilities of files and directories that are unprotected.
- If using custom code, use a static code security scanner before you integrate the code into the production environment. Security professionals must also perform manual reviews and exercise dynamic testing.
- Review cloud storage permissions, including S3 bucket permissions. Incorporate updates and reviews of all security configurations for all updates, security patches and notes into your patch management process.
- Put in place an automated process. This makes certain that security configurations are applied to all environments continuously.

Shadow Asset Targeting and

Open-Source Vulnerabilities

The 280% growth in vulnerable shadow assets during 2022 leads to a doubling in 2023. According to CQ Prime Threat Research, roughly 5 to “billion, or 31%, of the 16.7 billion malicious requests observed in 2022 targeted unknown, unmanaged and unprotected APIs, commonly referred to as shadow APIs and zombie APIs, spanning a wide range of use cases.

These ranged from sneaker bots attempting to grab the latest Dunks or Air Jordans to stealthy attackers attempting a slow trickle of card testing fraud on stolen credit cards, to pure brute force credential stuffing campaigns. Driven by high-volume content scraping as a precursor to shopping bot and gift card attacks, attacks on shadow APIs surged in April 2022 and have continued to rise in volume throughout the year.

If you create and sell software to the U.S. government, you will shortly need to attest to the security of your software supply chain – or they will stop using your software. Why? Because attacks on software supply chains have increased 735% in the past three years, and patient nation-states and criminal syndicates are looking to disrupt national interests, making federal agencies a major target. Executive Order 14028 requires all federal agencies to validate the software supply chain of their vendors per NIST guidance. With NIST guidance now in place, agencies must comply starting in early 2023.

The questions you should be asking yourself now is how this change affects your process and product and organization and how you can ensure compliance are met across a diverse application portfolio.

The rest of us need to worry about open-source software, APIs, supply chain, Java libraries and a hundred other transitive dependencies and vulnerabilities found throughout the open-source ecosystem. NPM is the world’s largest software registry, and NPX and Yarn are popular registries for software developers. The NPM registry contains over 800,000 code packages. NPM is free and relied on by over 11 million developers worldwide. Resolving a vulnerable NPM transitive dependency, which is a dependency that is not directly used in your project, but brought in by other third-party components, is at best, hard.

Imagine the size of the problem space – almost 1 million code packages, used by 11 million developers, full of transitive dependencies developers will never understand, see or be aware of in any other context – yet we plow ahead, pushing multiple releases out daily. What could possibly go wrong?

The Log4Shell critical vulnerability, for example, that affected millions of enterprise applications remains a common cause for security breaches a year after it received patches and widespread attention and is expected to remain a popular target for some time to come. Its long-lasting impact highlights the major risks posed by flaws

> “280% growth in vulnerable shadow assets during 2022 leads to a doubling in 2023.”

in transitive software dependencies and the need for enterprises to urgently adopt software composition analysis and secure supply chain management practices. Log4Shell, officially tracked as CVE-2021-44228, was discovered in December 2021 in Log4j, a widely popular open-source Java library that’s used for logging. Initially disclosed as a zero-day, the project’s developers quickly created a patch, but getting that patch widely adopted and deployed proved challenging because it relies on developers who used this component in their software to release their own updates.

The issue was further complicated by the transitive nature of the vulnerability because software projects that incorporated Log4j included many other third-party components or development frameworks that themselves were used as dependencies for other applications. Use of the Log4j library itself was not even a requirement, as the vulnerable Java class called JndiManager included in Log4j-core was borrowed by 783 other projects and is now found in over 19,000 software components.

Log4j Exploitation Will

Remain a Challenge

"We assess that the threat of Log4j exploitation attempts will remain a challenge for organizations well into 2023 and beyond," researchers from Cisco's Talos group said in their end-of-year report. "Log4j's pervasiveness in organizations' environments makes patching challenging. Since the library is so widely used, Log4j may be deeply embedded within large systems, making it difficult to inventory where all software vulnerabilities may be in a particular environment."

According to data from vulnerability scanning specialist firm Tenable, 72% of organizations still had assets vulnerable to Log4Shell as of Oct. 1, 2022, a 14-point improvement since May but still a very high percentage. The average number of vulnerable assets per organization decreased from 10% in December 2021 to 2.5% in October, but Tenable observed 1 in 3 assets having a Log4Shell recurrence after initially achieving remediation.

The number of vulnerable Log4j downloads every day is in the hundreds of thousands, which is evidence that this isn't an open-source maintainer problem but an open-source consumer problem. This is proof that companies simply don't know what is in their software supply chain.

The exploitation of vulnerabilities in publicly facing applications, which included Log4Shell, was tied with phishing for the position of top infection vector during the first half of the year, according to data from Cisco Talos's incident response team. In Q3, application exploits were the hird-most-common infection vector and included the targeting of VMware Horizon servers vulnerable to Log4Shell.

In highly regulated industries, simplifying compliance is all about visibility. A single source of truth across complex cloud infrastructure can make life for security teams so much easier.

But, throughout the year, Cisco Talos has seen Log4Shell being leveraged in cyberespionage operations by APT groups as well, including North Korea's Lazarus Group, threat actors associated with Iran's Islamic Revolutionary Guard Corps, and the China-linked Deep Panda and APT41 groups.

"Log4j is still a highly viable infection vector for actors to exploit, and we expect that adversaries will attempt to continue to abuse vulnerable systems as long as possible," the Cisco Talos researchers said. "Although threat actors remain adaptable, there is little reason for them to spend more resources developing new methods if they can still successfully exploit known vulnerabilities." We will see many more successful attacks based on Log4Shell infection vectors throughout 2023.

"Log4j's pervasiveness in organizations' environments makes patching challenging. Since the library is so widely used, Log4j may be deeply embedded within large systems, making it difficult to inventory where all software vulnerabilities may be in a particular environment."

Unsecured DNS

Domains are a critically important element of internet infrastructure; they are also woefully exposed and exploitable. Their functionality and security rely upon many factors. Name server delegations introduce complex and subtle interdependencies between domains and their authoritative name servers.

A compromise of any name server in the delegation hierarchy can lead to a hijacking scenario. Targeted name server compromises in the delegation hierarchy can facilitate a complete hijack of a domain or set of domains. A compromised name server is capable of diverting DNS requests to malicious servers controlled by threat actors and can be weaponized for phishing attacks, MiTM, watering hole vectors or several of many other attack scenarios. It turns out that over 95% of cyberattacks, malware and bots rely on unsecured DNS to be successful.

Many security teams don't inspect DNS traffic for threats because they assume queries sent over DNS protocol and port 53 are benign. Other organizations don't inspect DNS traffic because the sheer volume of that traffic is overwhelming and looking for a sign of something malicious in that traffic is like looking for a needle in a haystack. This takes a great deal of time and resources - often too great an investment for organizations, especially those that assume DNS does not pose a significant threat.

Domain hijacking is the act of changing the registration of a domain name without the permission of the original owner, or by abuse of privileges on domain hosting and domain registrar systems. Domain name hijacking is devastating to the original domain name owner's business and has wide ranging effects, including financial damages, reputational damage and regulatory impact. We frequently see living examples of surprisingly large, savvy companies whose DNS's are unsecured - companies such as Boeing, Capital One, Bank of America and Okta, for example.

DNS is a massive and often overlooked attack surface that requires the same scrutiny and protection given to web and email. It can be used for malware delivery, command and control, or data exfiltration. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack.

According to Palo Alto Networks Unit 42 threat research team, 85% of malware in 2022 used DNS to the initiate C2 procedures. Attackers establish reliable command

channels that are difficult to take down or identify since DNS is such a reliable way to maintain a connection to DNS servers. As adversaries increasingly automate their attacks, it becomes almost impossible to identify and stop those threats. Attacks using DNS are growing and malware using domain generation algorithms has grown 124% year over year since 2021. Understanding how adversaries abuse DNS is the first step to stopping attacks on the network and minimizing cybersecurity risks. To protect against threats over DNS, CISOs need superior detection combined with analytics to empower their security personnel with the context to quickly and effectively craft policies and respond to threats.

In December of 2020, SolarWinds was a victim a supply chain attack on its SolarWinds Orion® software.

In order to carry out this attack, the threat actors registered domains in 2019 and left them dormant for over a year before using them in their attack. By leaving these domains dormant, they were able to bypass reputation-based checking done by security

vendors. During this dormant phase, the SUNBURST Trojan periodically contacted its C2 domain to report status and receive commands. When the C2 domain was finally activated, the majority of burst DNS requests were for new subdomains. The Trojan dynamically constructed these hostnames with DGAs to tunnel sensitive data out of the victim's network. Full details of the SolarStorm supply chain attack are available at Unit 42's blog post.

Visibility into the DNS traffic enables a security team to identify malicious and benign traffic and trends. Context around security events allows everyone to understand why a domain was blocked and the history of that domain.

Security teams can then use this intelligence to optimize their policies and security posture as well as identify the nature and scope of any malicious activity so they can quickly move to remediate any issues.

Acceptance presages preparation. We have seen every breach this year trace back to an unsecured DNS domain. That is fact. What we will end up doing about it in 2023 is anyone's guess.

Polymorphic Malware

It is difficult to both detect and mitigate malware if it is constantly morphing. That is what polymorphic malware can do. Polymorphic malware uses the concept of polymorphism not for efficiency but for the purpose of evading detection. The idea behind polymorphic malware is that if a particular malware strain is known for having certain properties, then new versions of that malware can avoid detection if slight changes are made. This allows endless malware files, which all perform the same function, to appear sufficiently unique that they are not recognized as malware.

Polymorphic code has been found in all types of malware. This means that it will be used for:

- Ransomware and extortio;
- Keyloggers for the purpose of stealing your passwords;
- Rootkits that provide remote access to your computer;
- Browser manipulation that redirects your browser to malicious websites.

Polymorphic malware enabled by machine-learning algorithms and artificial intelligence will be used to bypass two-factor authentication and other authentication security measures in 2023. Detection is hopeless. The key is in prevention and detection through AI and ML operating in real time. Until that capability is developed and comes to market, here is a proven set of safe cybersecurity practices that might help:

- Keep software up to date: While polymorphic malware will change its appearance, the targets are usually the same. Most software companies maintain security updates to protect their tools, so it's essential to keep up with any patches on client and server computers.

- Don't open odd links or attachments: Email continues to be cybercriminals' preferred entry point, so it's a prime opportunity to stop polymorphic infections. In addition to deploying email security tools, train employees not to succumb to phishing attacks and not to open any suspicious links — even from known email addresses.

- Update passwords: Lists of known passwords and other information are regularly bought and sold on the dark web, so requiring employees to regularly change their passwords can thwart attacks. Like the previous caveat against opening suspicious attachments, this requirement should also be part of regular employee security awareness training.

- Back up your data: It cannot be repeated often enough: Back up your data on a regular basis. Data backups can save a company millions of dollars and thwart ransomware attacks.

- Use heuristic and behavior detection: Security software that uses current information about known polymorphic malware techniques can prevent an infection. A heuristic approach, for example, will prevent certain viruslike actions, such as encrypting important files. Behavior-based detection can alert users to previously unreported polymorphic threats based on, for example, unusual access requests.

Polymorphic viruses have a long history, having appeared in earnest in 2015, and cybercriminals have had many years to develop more advanced techniques to hide their appearance and infections. Polymorphic malware is used extensively and successfully in all types of cyberattacks, including ransomware, but by following best cybersecurity practices, defenders have a chance of survival in the interim. What, of course, needs to happen is the development of better forms of protection and defense based on AI and ML. We look forward to that.

The Skills Shortage

It is well known that the cybersecurity industry has an employee and skills shortage. Joseph Blankenship, a senior analyst for security and risk at Forrester Research, suggests organizations look inward for current employees who might be well suited for security careers and then recruit and train them for those new roles. There may be plenty of individuals out there - such as networking admins, developers, systems engineers and even security analysts - with the chops needed for the job. In my former role as CISO, this approach has always worked well for me. You get high potential, known-quantity trainees with great fundamental IT skills and create an entry-level employment funnel at the same time.

The U.S. government is also working to improve the recruitment process. The CIA is working with the industry to recruit more security pros by promoting diversity through the hiring of more women and minorities. Additional security employment indicators include the following:

At the end of 2021, there was a security workforce gap of 377,000 jobs in the U.S and 2.7 million globally, according to the "(ISC)2 Cybersecurity Workforce Study, 2021."

The "ISACA State of Cybersecurity 2021 Part 1" survey tells us that 61% of organizations feel they are understaffed in terms of cybersecurity professionals. Fifty percent of respondents said applicants were not sufficiently qualified for security positions. According to that same survey, a key challenge with filling cybersecurity positions is that only 31% of human resources staff understand their organization's cybersecurity needs. Adding to the problem space, the study also found that only 27% of recent graduates in cybersecurity education programs are properly prepared for the workforce.

According to Symantec, two-thirds of cybersecurity decision-makers feel like quitting. Part of the reason for a skills gap is that security experts leave their jobs at an alarming rate. Symantec also found that 4 in 5 security professionals said they are burned out. Survey respondents said they feel set up for failure in a profession where the everyday role is reaching a state of chronic overload. The Joe Sullivan verdict has not helped.

Cybersecurity is a high-salary field to work in, particularly in North America. The "ISC)2 Cybersecurity Workforce Study, 2021" study stated that the average salary for a cybersecurity professional in North America was $119,898. That figure drops to $78,618 in Europe and falls even lower in Latin America to $32,637.

CyberEd comes online in January and will offer revolutionary courseware organized in learning paths and academies that focus student learning on specific job roles and outcomes consistent with the NIST/NICE framework and guidelines. We hope to make a dent in the problem space.

> "Only 27% of recent graduates in cybersecurity education programs are properly prepared for the workforce."

CYBER THEORY

cybertheory.io
212.518.1579 • info@cybertheory.io
530 7th Avenue, New York, NY 10018