2022

ATTACK VECTORS REPORT

WAR ROOM

RSM

TABLE OF CONTENTS

Prepared by: Erica Cummings, Jonathan Slusar, Blaire Grassel, Kristen Gecewich, Trevor Strunk, Ryan Shockling, Nicholas Hamm, Ayush Nangia

ABOUT THIS REPORT

Each year, RSM publishes an Attack Vector report, which leverages our internal database of penetration tests performed for our clients to provide insight into trending attacks performed by threat actors to obtain credentials, establish persistence within a targeted network and compromise sensitive data.

While we often observe the same attacks being performed year after year, threat landscapes are consistently evolving, and threat actors are finding new ways to bypass security patches and other mitigating factors deployed by organizations' cybersecurity and information security teams.

Methodology

To develop the report, we pulled data for organizations that engaged with RSM for both a penetration test and a NIST Cybersecurity Framework (CSF) maturity or risk assessment. Reports for each organization were reviewed to determine their overall risk ratings, level of compromise, attack vectors leveraged and maturity in each NIST CSF function. We then reviewed the data for any trends or notable observations.

For this year's report, we have incorporated additional data from previous years to provide an enhanced view of the present threat climate. Additionally, given the prevalence of internal compromises over external, we chose to focus the bulk of our analysis on internal attack vectors, and then compared this data to maturity scores.

We thank you for your interest in this year's report and hope you find it beneficial for your own personal knowledge and to better mitigate attacks and reduce risk.

OVERVIEW

During our penetration tests, we found success with both new and older techniques. Our most successful attack vectors exploited weak passwords, technical misconfigurations and missing patches, suggesting that gaps in user awareness are still just as much of a concern as technical exposures.

As we compared compromise rates against maturity scores, we found that the organizations that had the highest overall maturity scores had lower rates of compromise, when compared to organizations with lower maturity scores. Based on this data, stronger security controls and processes do make a difference; however, they do not inoculate organizations against compromise. Many of the organizations with higher maturity scores were still able to be compromised via attack vectors exploiting both technical control deficiencies and weaknesses in user awareness.

As security professionals, we know that tools may fail. Vendor updates may not perfectly fix a problem. Users who typically have a high level of security awareness may make a mistake. Security controls are not perfect. Based on our observations for how to effectively guard against a compromise, organizations should take a holistic approach to security that requires them to:

Identify what they should be protecting and formalize a strategy for doing so

Protect their environment by implementing and managing effective security controls

Detect anomalies and threats through both proactive and reactive measures

Respond to cyber events in a way that contains impact and mitigates damage

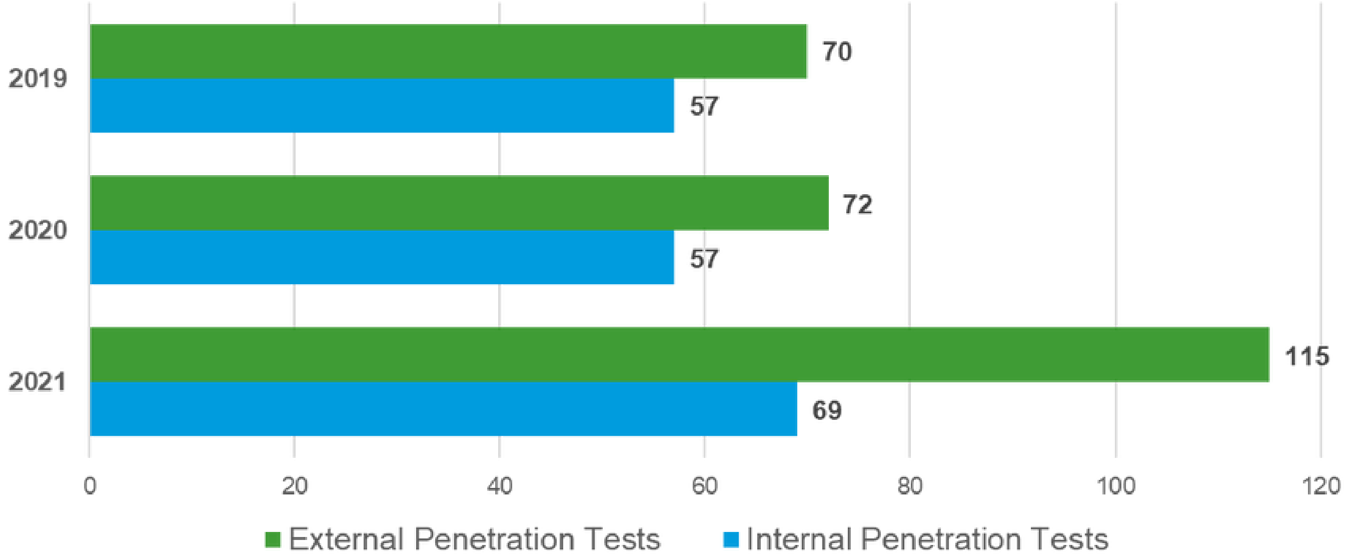
Recover lost data and damaged systems so that they can return to normal operations as quickly and safely as possible.

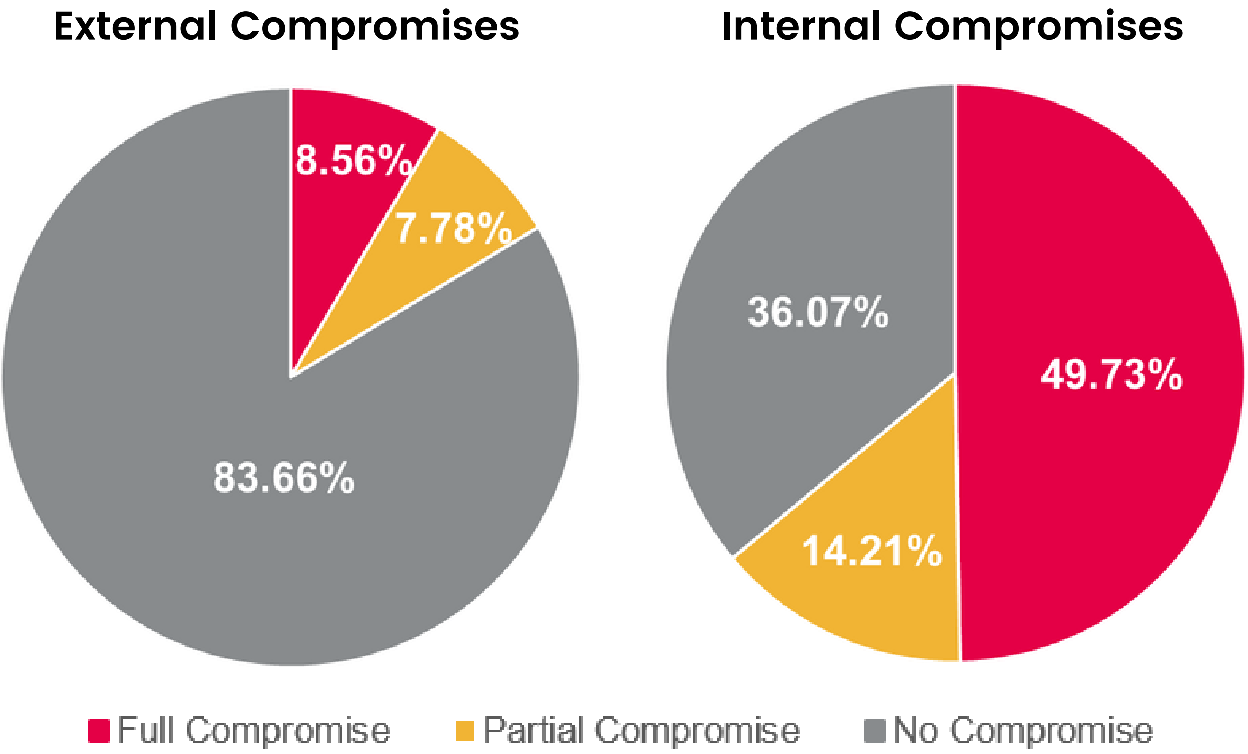
Stronger security controls and processes make a difference

PENETRATION TESTING AT A GLANCE

257
External Penetration Tests

183
Internal Penetration Tests



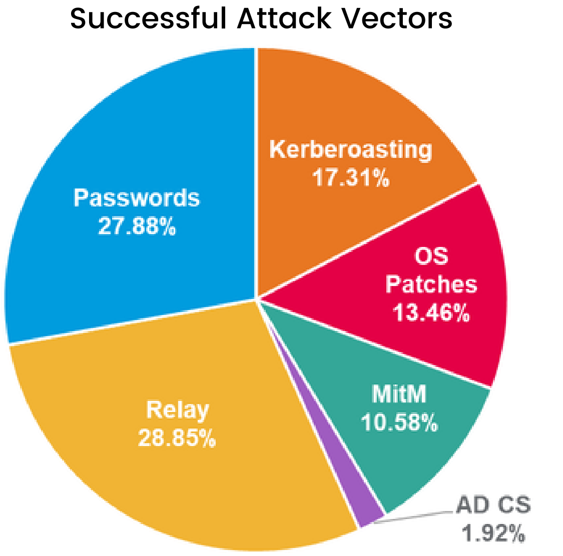


- Full compromise: We achieved a level of access that would have allowed us to retrieve sensitive data, modify configurations, create/modify accounts, and/or move freely throughout the network. Typically, this was accomplished by compromising a domain administrator (DA) account.
- Partial compromise: We were able to establish a significant foothold in the environment, though we may not have compromised a DA account.

INTERNAL ATTACKS

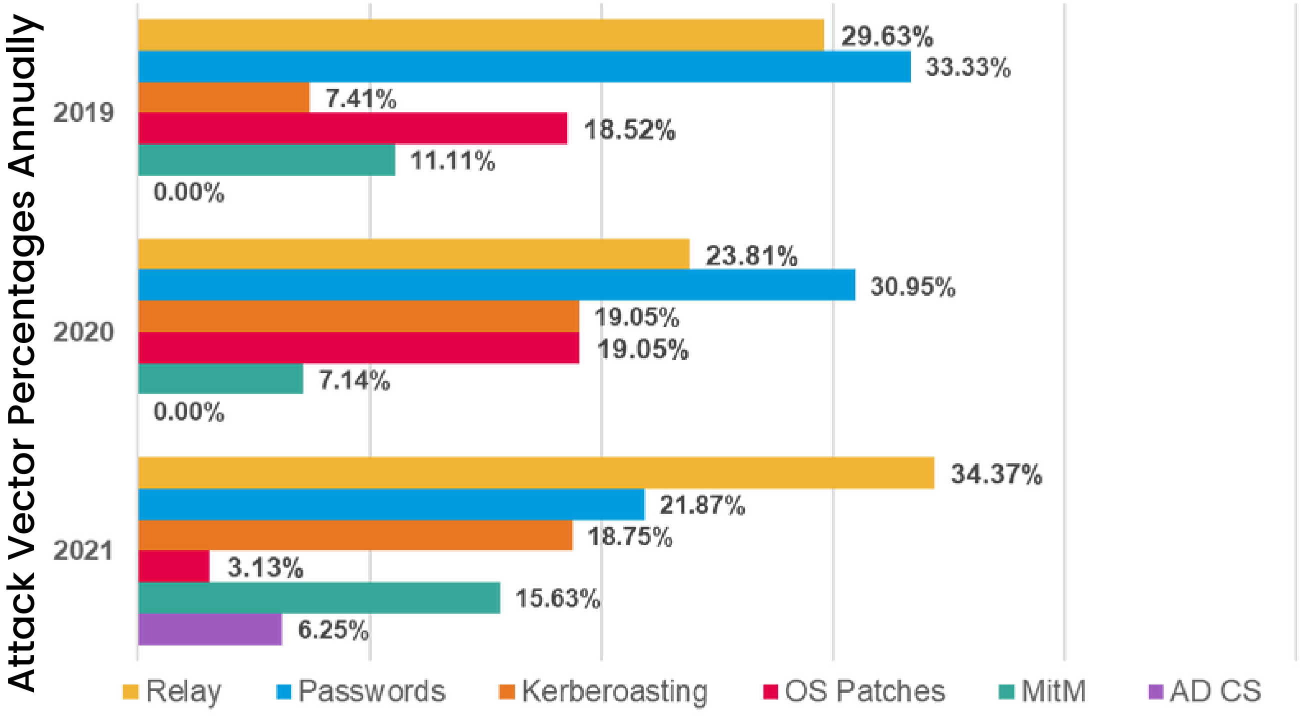
When analyzing our internal penetration test data from 2019-2021, we found that password spraying and relay attacks were the most common successful attack vectors, comprising more than half of all total vectors used in compromises.

Attacks such as relaying and Kerberoasting can be common because they require very little access to perform, typically preying upon protocols and settings that are present on most networks. In addition, these techniques are relatively simple to perform, meaning that even novice attackers can often do them successfully.



The above pie graph represents individual instances of attack vectors identified in full compromises. Subsequent percentages within the "Attack Vectors" portion of the report represent the percentage of full compromises that involved the identified attack vector, taking into account that some instances of compromise involved more than one attack vector.

However, the ease of the above attacks should not discount user awareness as a concern. Employee decisions and actions continue to have a high likelihood of being exploited. Password spraying is one of the first techniques many attackers rely upon, because they know that given the option, employees will often choose passwords that are easy to guess. As the data shows, weak passwords are a major source of compromise.



ATTACK VECTORS

Relay Attacks

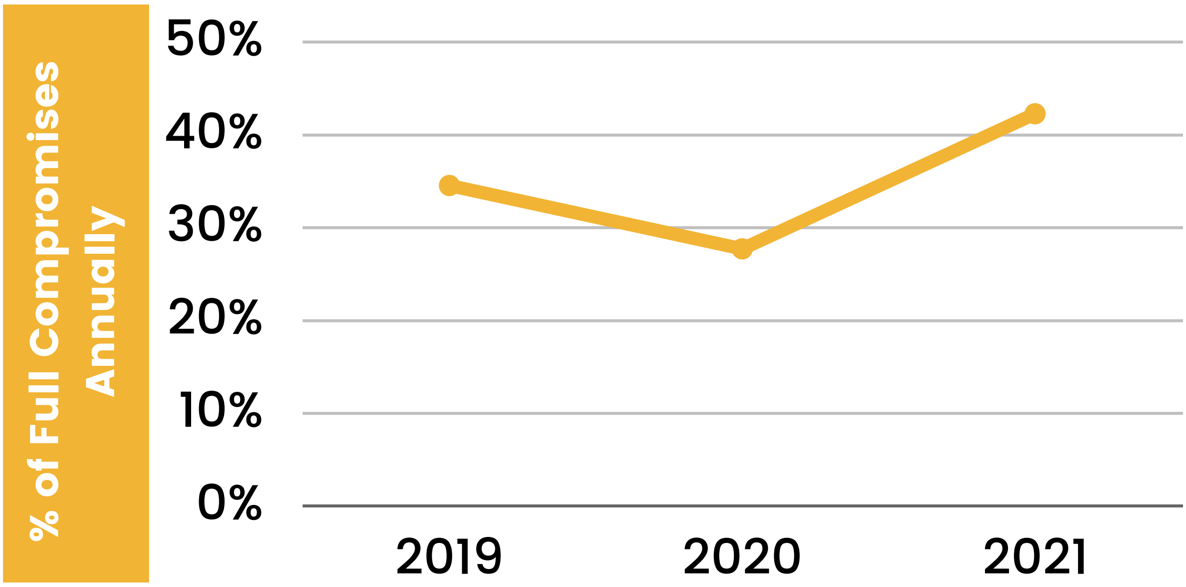
One of the most common avenues used by threat actors attempting to gain unauthorized access to a target network is the relay attack. One third of all internal compromises achieved by RSM from 2019-2021 used a form of relay attack. These attacks are so common primarily because they rely on the identification of traffic present on a network, a scenario that is almost certain to be the case for any network containing sensitive data.

33%

Of Full Compromises Used a Relay Attack

To perform a relay, attackers use the traffic they have identified and attempt to gain unauthorized access by exploiting this traffic and intercepting communications to trick machines on the network into allowing them to authenticate.

In particular, the highly popular Server Message Block (SMB) relay attack relies on one of the most common authentication protocols available, New Technology Lan Manager (NTLM). This makes it very apparent why the SMB relay attack is so common. NTLM is present on most Windows systems, and attackers who know how to exploit it may go to this attack as a first choice when attempting to gain unauthorized access to a network.



Once NTLM traffic has been identified, the attacker can listen in on network traffic with the goal of intercepting some form of authentication challenge being exchanged between the client and server. Authentication challenges are comprised of three parts:

1. First, the client requests to authenticate to a particular location on the network.

2. Second, the server replies with a challenge that involves the client encrypting a message with a hash.

3. Finally, the client encrypts the message with its hash and sends the message to the server, which, upon receiving it, decrypts it using the client hash. As long as the decryption is successful, this will lead to a successful authentication.

SMB relay attacks seek to exploit this process by capturing the traffic from the client prior to it being returned to the server. The tester or attacker then sends the encrypted message to the server, essentially posing as the client. The server conducts operations as normal and decrypts the message, but instead of authenticating the client to the server like normal, the authentication is granted to the individual conducting the attack.

Associated Risk

The amount of risk associated with a successful relay attack depends on the user the attacker impersonates. If the user is low-level and has minimal privileges, then the attacker may be able to cause some harm, but the amount of damage will be less than if the user had elevated privileges. If the attacker is able to impersonate an administrator, the level of risk relating to this attack can be very high.

Business Impact

The impact can differ depending on the user who is being impersonated. If it is a low-level user, the attacker will have limited access and may only be able to cause minimal damage. If the user is a privileged account such as an administrator, the attacker will again have access to whatever that administrator has access to, possibly sensitive data and other privileged information. Impersonating a domain administrator could even result in a full domain compromise.

REMEDIATION

One of the best mitigations for those using NTLM is to ensure that SMB signing is enabled and required. This means that messages from the client to the server will be validated to ensure that they were not tampered with. However, the best way to protect yourself from SMB relay attacks is to use Kerberos as your authentication protocol rather than NTLM.

Password Spraying

32%

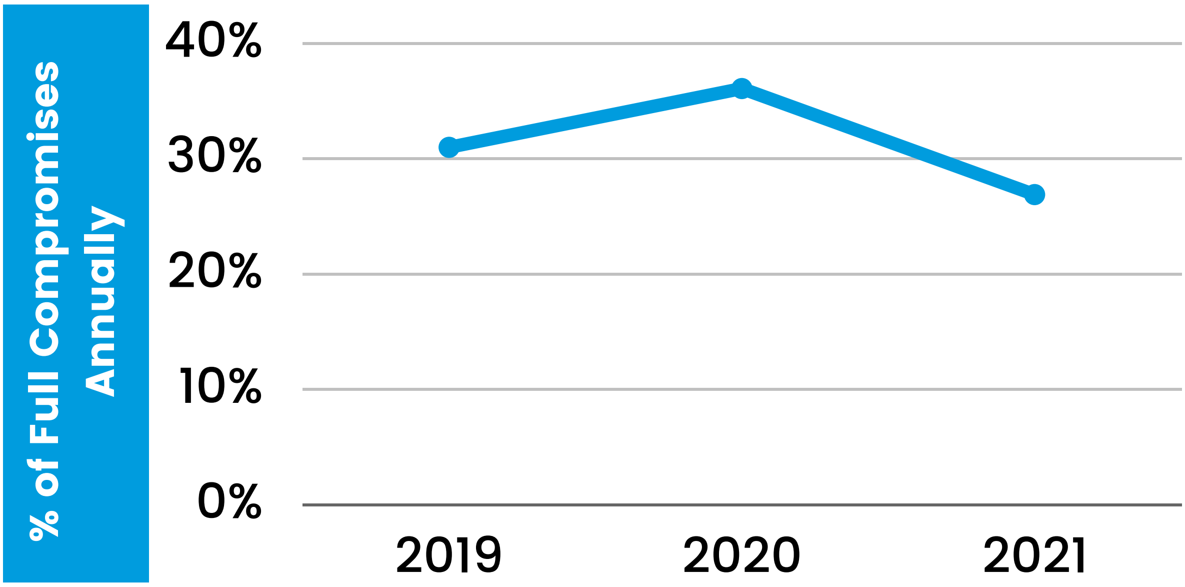
Of Full Compromises Took Advantage of this Attack

Password spraying, also known as a reverse brute-force attack, is a common technique used by threat actors when attempting to gain unauthorized access to a network.

To perform this attack, an attacker only needs two relatively accessible items, which is one of the reasons this attack is so prevalent: employee names and knowledge of the naming convention for employee emails or usernames.

Obtaining this information is not particularly difficult. By scraping the internet using common sites such as LinkedIn, attackers can compile a list of company employees. If any of these employees have listed their contact information, then the attacker has likely already found the naming convention for company emails as well.

Company sites are another common source of employee emails—most organizations will list employee contact information right on the front page. With this information, an attacker can apply the email naming convention to the enumerated list of employees to create a list of employee emails and begin the attack.



Common Passwords

Weak passwords often include some of the following:

- **"Password"**
- **Season**
- **Local sports team**
- **Company name**
- **"Admin"**
- **Username**
- **123**

When performing a password spraying attack, an attacker will attempt several weak passwords against a large number of users. Research shows that people often choose easy-to-guess passwords that contain dictionary words and phrases. That is why this attack is so prevalent: it preys on the tendencies of people. Furthermore, it does not need to exploit a large mistake that was missed by a multitude of employees. In order to gain access to a network via password spraying, an attacker only needs to find one employee with a weak password.

Associated Risk

The risk associated with password spraying often relates to the compromised account. A successful attack will grant access to everything the compromised employee can access. If the employee is a low-level user and does not have many privileges on the network, the result may not be catastrophic. However, if the account belongs to a privileged user with an elevated level of access, the attacker will likely be able to cause a far more significant amount of harm.

Business Impact

The impact this type of attack has on a business can vary. If a low-level account is compromised, an attacker may be able to obtain some damage, but a majority of the harm may be reputational. However, if the attacker gains access to a privileged account, sensitive data and all other information could be at risk, potentially resulting in a full compromise.

REMEDIATION

The best way to ensure that your organization is not compromised by this attack is to require users to set strong passwords. If users are given the option, they will often choose short, weak passwords. In addition to setting strong password requirements via policy, organizations should educate all employees, especially those with high-level access, on how to create strong passwords.

Kerberoasting

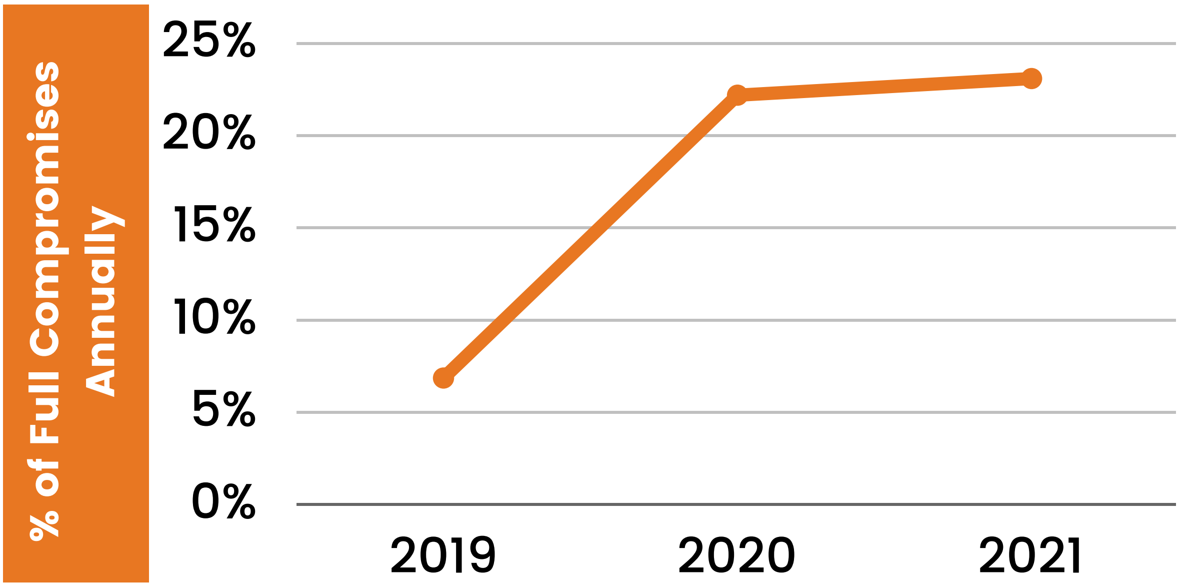
18%

Of Full Compromises Leveraged Kerberoasting

Many people who are familiar with the risks inherent in cybersecurity may assume that these risks are mostly reliant on hackers who can exploit software or hardware vulnerabilities to break through standard defenses. However, there are serious risks inherent even to properly working network systems if they are not fully configured for the highest security.

Kerberoasting attacks are perfect examples of how much access an attacker can gain when a network protocol works just as designed, and why organizations should configure their networks even against "functional" network protocols.

Kerberoasting is a common attack vector that leverages the Kerberos network authentication protocol in order to harvest hashed passwords. These hashes are associated with Active Directory (AD) user accounts which are configured with service principal names (SPNs).



Essentially, if an attacker is connected to the target environment, they can exploit the Kerberos protocol by requesting Kerberos tickets that are associated with target accounts. These tickets contain data encrypted with the NTLM hash of the target account. Once they have these hashes, they can attempt to crack them in an offline brute-force attack. If successful, this attack would give the attacker the target user’s password in plaintext, allowing them to easily compromise the environment.

By analyzing RSM's penetration testing engagements, we determined that 18% of compromises were facilitated by a Kerberoasting attack. These compromises were often also facilitated by weak passwords; if the targeted AD user account is employing a weak password, then a threat actor will likely crack the captured hash. In addition, as Kerberos requests are common, an attacker can often capture these hashed passwords without detection, making this attack all the more dangerous.

Associated Risk

Significant risks come with a Kerberoasting attack, most critically that a successful attack can result in a compromise of the targeted account. If an attacker uses Kerberoasting to gain access to a privileged account within the target environment, they can then perform further attacks to move laterally within a network. Attackers can even leverage a successful Kerberoasting attack to fully compromise the target environment.

Business Impact

Business environments can be impacted very seriously by a successful Kerberoasting attack. If the attacker is able to achieve a domain compromise, they could proceed to perform administrative actions and obtain sensitive or confidential information. Attackers could also gain access to file shares, create or modify users or modify system settings. It is even possible for the attacker to capture password hashes for all domain users and potentially crack them in an offline brute-force attack. As this would represent even broader access to the network and its users, such a technique could result in further account compromises.

REMEDIATION

To prevent a successful Kerberoasting attack, remove SPNs from all domain administrator accounts; instead, create a dedicated nonhuman account with a long and complex password with the minimum necessary privileges to run the service.

Missing OS Patches

15%

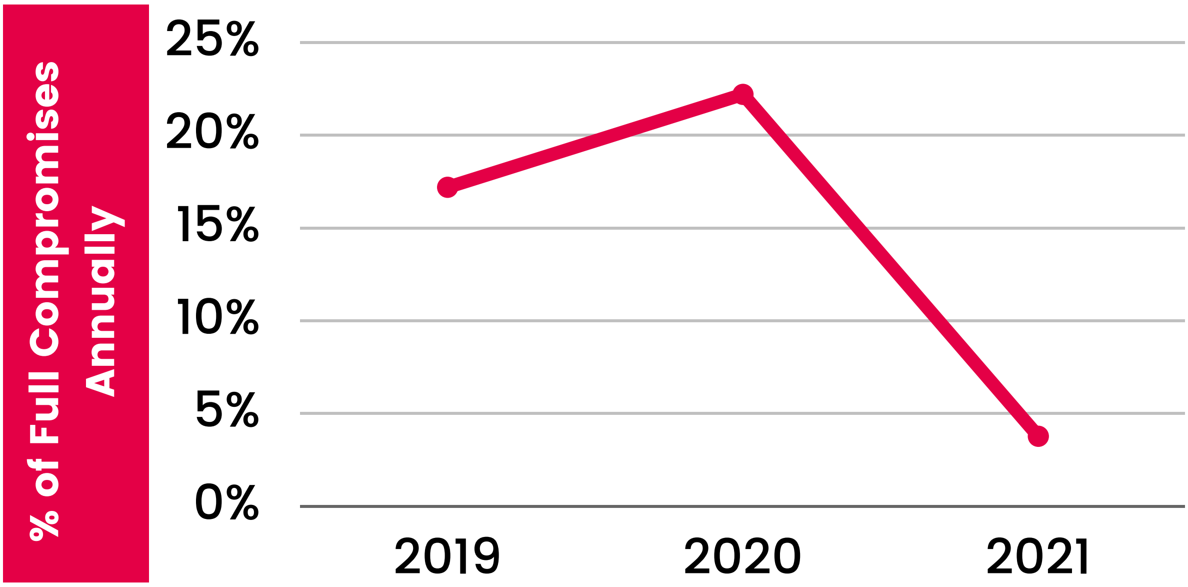
Of Full Compromises Took Advantage of Missing OS Patches

Often, software vendors such as Microsoft release security patches for their products. Instead of a full-scale upgrade, patches are smaller, targeted updates that address vulnerabilities discovered in the current version of the product. The vulnerabilities fixed by these patches are often critical issues that can be exploited by cyber attackers to gain access to sensitive information or even infect systems with ransomware.

The results of our analysis indicate that patching continues to be a common issue for many organizations. Some of the most common missing patches identified in our engagements include MS17-010, BlueKeep, and Zerologon, all of which affect the Microsoft Windows operating system and can be used by attackers to compromise an organization's systems.

Associated Risk

The risk associated with missing patches varies depending on the patch. Most critical patches have published exploits accessible to anyone with an internet connection.



MS17-010

MS17-010, which exploits a vulnerability in the Server Message Block (SMB) protocol when systems are unpatched, can grant an attacker SYSTEM access to the affected machine without providing any credentials.

BlueKeep

BlueKeep is tied to the Remote Desktop Protocol (RDP) service and can also result in SYSTEM access; in addition, this vulnerability has the ability to self-replicate and spread to an entire network without any additional effort on behalf of the attacker.

Zerologon

Zerologon is an elevation of privilege vulnerability affecting the Netlogon Remote Protocol (NRPC) interface which allows for an uncredentialed user to bypass authentication and connect to remote systems and, from there, execute a variety of calls such as password changes in order to gain control over target systems or a whole network.

Business Impact

The impact resulting from successful exploitation of missing OS patches can be substantial, ranging from compromise of individual machines to complete control over an entire network environment. An attacker with this kind of access could use it to execute malicious code, make changes to the environment, exfiltrate confidential data and more.

In May 2017, the notorious WannaCry attack, which targeted the vulnerability addressed by the MS17-010 patch, was deployed worldwide, affecting as many as 200,000 computers globally and causing at least hundreds of millions of dollars in damages.

It is notable that 93% of the environments compromised using missing patches were missing the MS17-010 patch on one or more systems, despite the patch being released half a decade ago. This is why developing a patch management program and applying critical patches as soon as possible is crucial to protecting an organization's systems and information.

REMEDIATION

Preventing missing patches requires an organization to maintain a robust patch management program. Patch management is considered one of the most basic forms of protecting systems. This is because without a formalized patch management process and by not patching systems with critical security patches, even the most rudimentary hackers can gain full access to devices within a network.

MitM Attacks

Another method often used to target organizations' networks is known as the Man-in-the-Middle (MitM) attack. MitM is a term for when an attacker positions themselves in a conversation between a user and an application. This allows the attacker to eavesdrop, relay communication and modify what each party is saying.

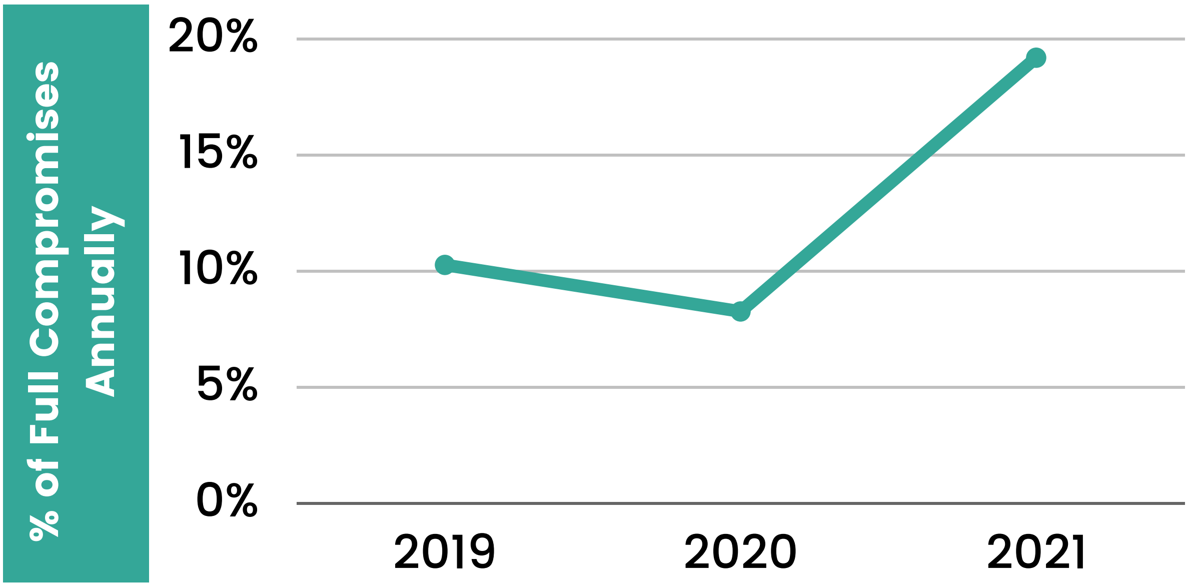
12%

Of Full Compromises Used a MitM Attack

There are many types of MitM attacks, but two we often see are related to outdated (Link-Local Multicast Name Resolution [LLMNR]/NetBIOS Name Service [NBT-NS]) and misconfigured (Internet Protocol version 6 [IPv6]) traffic types.

LLMNR/NBT-NS

LLMNR and NBT-NS are enabled on Windows-based operating systems by default and are used to perform name resolution for the names of remote systems on networks without a Domain Name Service (DNS) server or DNS client configuration. If a system cannot resolve a host name using the local host file or through a DNS request, a system with LLMNR or NBT-NS enabled will make a broadcast request on the local subnetwork requesting the IP address of a specific host. Attackers can intercept these broadcasts and respond, claiming to be the resource in question.



IPv6

Typically, any machine on a network must first be assigned an IP address by a DHCP server. Most DHCP servers still use IPv4 rather than the more up-to-date IPv6. By default, hosts on the network are constantly looking to be assigned an IPv6 address. What is known as an IPv6 DNS MitM (or spoofing) attack can be executed by posing as a DHCP server using IPv6, causing PCs on the network to connect to a spoofed DHCP server.

Other MiTM Attacks

Other common MitM attacks include:

- **WIFI EAVESDROPPING**
- **EMAIL HIJACKING**
- **IP SPOOFING**
- **DOMAIN NAME SYSTEM (DNS) SPOOFING**
- **SSL STRIPPING AND HIJACKING**
- **SESSION HIJACKING AND COOKIE THEFT**

Associated Risk

A MitM attack gives malicious actors a chance to intercept a wealth of sensitive information such as usernames, passwords, protected health information (PHI) and Payment Card Industry (PCI) data. Captured LLMNR/NBT-NS and IPv6 traffic can be relayed to potentially gain access to user accounts and other sensitive information.

Business Impact

If a malicious actor is successful in gaining valid usernames and passwords, they may be able to further their attack and obtain access to and even steal sensitive company data. Capturing PHI or PCI data can cause even further financial and reputational damage.

REMEDIATION

To prevent common MitM attacks, the best step is often to disable unnecessary network communication protocols where possible. This is best accomplished via Group Policy Object (GPO).

Misconfigured AD CS

Active Directory Certificate Services (AD CS) is a Microsoft product that performs public key infrastructure (PKI) functionality that provides file system encryption and user authentication. AD CS integrates with AD and enables the issuing of certificates, which can be used for authentication purposes.

2%

Of Full Compromises Used an AD CS Attack

The information that is included in a certificate correlates an identity, or subject, to a public/private key pair. An application can then use the keys to validate the identity of a user. Certificate Authorities (CAs) are responsible for issuing certificates.

At a high level, clients generate a public-private key pair, and the public key is placed in a certificate signing request (CSR) message along with other details such as the subject of the certificate and the certificate template name. Clients then send the CSR to the Enterprise CA server. The CA server checks whether the client can request certificates. If so, it determines whether it will issue a certificate by looking up the certificate template AD object specified in the CSR.

Next, the CA will check whether the certificate template AD object's permissions allow the authenticating account to obtain a certificate. If so, the CA generates a certificate using the "blueprint" settings defined by the certificate template and using the other information supplied in the CSR, if allowed by the certificate's template settings.

The CA signs the certificate using its private key and then returns it to the client. The CAs issue certificates with settings defined by AD objects known as certificate templates. These templates are collections of enrollment policies and predefined certificate settings which address questions including:

- How long is this certificate valid for?
- What is the certificate used for?
- How is the subject specified?
- Who is allowed to request a certificate?

Associated Risk

There are several escalation, or ESC, attacks that are known today. The most common ESC attacks are ESC1 and ESC8. The former can be used to impersonate virtually any user on a domain, while the latter can be used to relay authentication to gain access to target machines, such as Domain Controllers. Refer to the sidebar for more details on these attacks.

Though 2021 saw few compromises with this attack, we anticipate that this attack vector will be a significant issue for organizations in coming years.

Business Impact

With the misconfigurations mentioned above, an attacker only needs to have a valid account on the environment to impersonate essentially any other domain account, such as a Domain Administrator, and to compromise the environment. Because most Domain Administrator accounts have unlimited access within a network, the attacker can then search for sensitive information, such as Social Security Numbers (SSNs), Personally Identifiable Information (PII), PHI or PCI data, and can also cause disruption to systems within the environment.

ESC1: Misconfigured Certificate Templates

An attacker can specify a different Subject Alternative Name (SAN). By default, during certificate-based authentication, certificates are mapped to AD accounts based on a user principal name (UPN) specified in the SAN. If an attacker can specify an arbitrary SAN when requesting a certificate that enables domain authentication, and the CA creates and signs a certificate using the SAN, the attacker can become any user in the domain. This could be used to target a Domain Administrator account.

ESC8: NTLM Relay to AD CS HTTP Endpoints

An attacker identifies a CA that supports HTTP-based web enrollment to request a certificate. An attacker needs to relay authentication from one system to the CA. For instance, an attacker can coerce a Domain Controller's (DC) authentication and relay it to the exposed HTTP endpoint on the CA to request a client authentication certificate. The attacker can then use the certificate to request the TGT for the DC's computer account and subsequently, request the NT hash to successfully authenticate against itself.

REMEDIATION

Organizations should remove AD CS HTTP endpoints if they are not required. This includes Certificate Authority Web Enrollment and Certificate Enrollment Web Service. If the AD CS HTTP endpoints are needed, disable NTLM authentication at the host and IIS level or enforce HTTPS and Extended Protection for Authentication.

MATURITY ANALYSIS

NIST CSF

Maturity Analysis

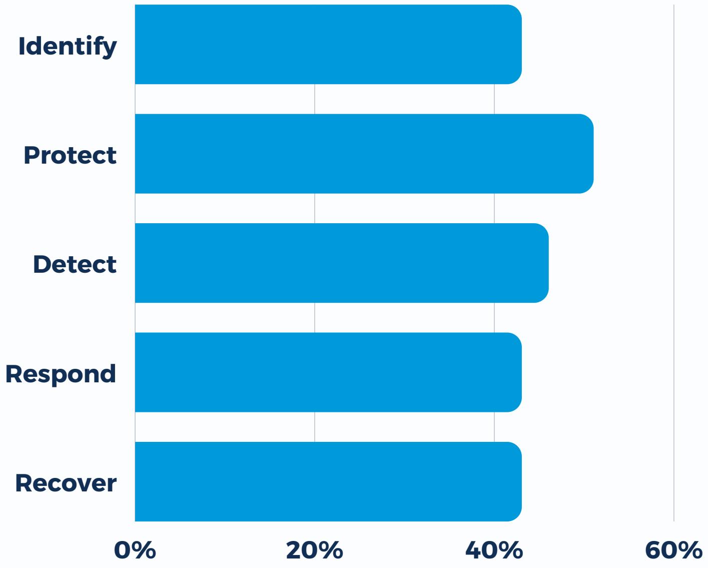
As we have already discussed, analyzing attack vectors helps us understand trends and identify the low-hanging fruit that attackers seek to exploit. This is important because each compromise and attack vector we have discussed represents potentially devastating impacts to a business: Data breaches. Loss of availability of critical applications. Halt to business operations. Disrupted revenue streams. Regulatory fines and penalties. Tarnished reputation. Loss of public trust. Our analysis, therefore, helps us understand the specific mitigations organizations can take to directly reduce their risk of compromise through these common attack vectors.

However, it is important to note that addressing these specific attack vectors is not enough. In fact, perhaps the most prominent takeaway from our Attack Vectors Reports over the years is that a dedicated attacker will infiltrate a target network eventually. Tactical fixes are important, but protecting your environment requires much more than applying a patch, disabling a protocol or adjusting an account's access privileges. Tactical fixes act only as temporary band-aids if they are not embedded in strategic initiatives that provide a means of continuous improvement, oversight and support.

That's why this year, we wanted to take a deeper dive into an organization's potential for compromise in relation to the overall strength of its security program. To this end, we looked at organizations where we performed both penetration testing and cybersecurity maturity assessments to see if we could identify strategic ways that organizations can reduce their potential for compromise—or to reduce the impact, should an attack occur.

Maturity Scores

Our cybersecurity maturity assessments leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to determine the overall maturity of a security program. During these assessments, we assess the governance and implementation of the NIST CSF controls within an organization's environment. This approach provides insight into the organization's ability to identify, protect, detect, respond to and recover from a cyber event, which are the five functions of the NIST CSF.



Overall Average Maturity Scores

As we examined the distribution of NIST CSF maturity scores, we classified organizations into the following three tiers, according to their overall average maturity scores:

23% of the organizations we reviewed fell into the top tier of overall average maturity scores (between 66% and 100%).

43% of the organizations we reviewed fell into the middle tier of overall average maturity scores (between 33% and 65.9%).

34% of the organizations we reviewed fell into the bottom tier of overall average maturity scores (between 0% and 32.9%).

Maturity Trends

Not surprisingly, the vast majority of organizations have implemented security controls in their environment to some degree. Very few organizations have done nothing from a security perspective, even if security was more of an afterthought, or if only rudimentary controls were in place. Most organizations (including those in the bottom tier) have baseline tools and processes in place to cover fundamental areas of network security. But whether these tools and processes were married to a comprehensive risk management strategy—one that takes into consideration business objectives, data management, digital transformation and the user experience—is another story.

It should be noted that it is not appropriate or feasible for all organizations to aim for top maturity scores in all areas. Rather, security efforts should be focused on areas of greatest risk and aligned to the organization's risk tolerance. Still, important lessons can be gleaned by examining trends between tiers, especially when we compare the potential for compromise within each tier.

	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
TOP TIER	70%	77%	76%	79%	77%
MIDDLE TIER	46%	53%	49%	45%	45%
BOTTOM TIER	21%	31%	22%	17%	16%

Average Maturity Scores by Tier

Top Tier Trends

Organizations in the top tier were typically marked as having repeatable and adaptive security processes that were aligned to a formal risk management process. Additionally, they typically had formal documentation that outlines their security goals and standards.

Moreover, their security objectives and expectations were well known throughout the organization and reinforced through robust security awareness training. Furthermore, top tier organizations tended to have some mechanisms to regularly measure, report on and improve their security controls so that they could remain proactive in their security stance.

THE MOST MATURE ORGANIZATIONS TAKE A "DEFENSE IN DEPTH" APPROACH AND HAVE A MORE COMPREHENSIVE SECURITY STRATEGY.

Notably, top tier organizations had relatively even scores across all functions in the NIST CSF (all functions averaged between 70% and 79%). In contrast, there were much bigger disparities between each function in the bottom tier (compare the 31% average Protect score to the 16% Recover score in the bottom tier).

This suggests that the most mature organizations take a “defense in depth” approach and have a more comprehensive security strategy. They also adequately prepare for the very real possibility that a cyber attack or business interruption will occur. As we discuss later, these efforts made top tier organizations less likely to experience a compromise during a penetration test.

Middle Tier Trends

These organizations were aware of their cybersecurity exposures and had several controls in place to protect their systems and their data. They generally recognized that a security strategy should involve people, process and technology, though they may have still been working towards optimizing this strategy and integrating these efforts.

MIDDLE-TIER ORGANIZATIONS STRUGGLE TO PRIORITIZE RESPONSE AND RECOVERY PROCEDURES, AND THEY COULD PAY A BIG PRICE FOR BEING ILL-PREPARED WHEN AN INCIDENT OCCURS.

In middle tier organizations, cybersecurity efforts were not always united under a cohesive security governance and risk management strategy, and/or there was no formal process to ensure that all aspects of security were continually improving.

The Protect function scored the strongest among middle tier organizations in terms of maturity, while Respond and Recover scored the lowest, though the disparity between the maturity of each NIST CSF function was not nearly as wide as it was for bottom tier organizations.

Still, the fact that Respond and Recover scored the lowest suggests that many organizations struggle to prioritize their incident response, disaster recovery and business continuity procedures, and they could pay a big price for being ill-prepared when an incident occurs.

Bottom Tier Trends

Bottom tier organizations typically had some protective measures in place (endpoint protection, firewalls, detection tools, device encryption), but almost all of them lacked a formal risk management and security governance strategy to guide security efforts. Moreover, security processes were generally more reactive—rather than proactive—in nature. In these organizations, security tended to be one-dimensional, centered around having a few technologies that are tacked on top of existing processes, rather than security being integrated into business operations from the outset.

ORGANIZATIONS IN THE BOTTOM TIER OFTEN LACK A PROCESS TO ERADICATE THREATS OR RESTORE DATA AND SYSTEMS IF/WHEN THEIR PROTECTIVE TECHNOLOGIES FAIL.

Furthermore, many of these organizations suffered from resource restraints. Often, they simply did not have the personnel to perform security tasks and manage security projects, hence an over-reliance on tools and technologies that were not actually very effective.

This is reflected in higher Protect scores for the bottom tier, with notably low Respond and Recover scores. As we will discuss next, the bottom tier was also the group that was most likely to be compromised during a penetration test. Therefore, the lack of formal response and recovery procedures could exacerbate the impact of a compromise, as these organizations may not have a process to eradicate the threat or restore data and systems if (when) their protective technologies fail.

Maturity and Potential for Compromise

We compared levels of compromise (during a penetration test) based on relative maturity scores (as determined during the NIST CSF maturity assessment). Based on this analysis, we noted an inverse correlation between the maturity of an organization's security program and their vulnerability to compromise. In other words, more mature organizations were indeed less likely to experience a full network compromise.

29% of **top tier** organizations experienced a full (17%) or partial (12%) compromise during a penetration test.

40% of **middle tier** organizations experienced a full (28%) or partial (12%) compromise during a penetration test.

41% of **bottom tier** organizations experienced a full (33.9%) or partial (7.1%) compromise during a penetration test.

Takeaways and Recommendations

Based on these results, we see that the maturity of your security program does matter. Having a strategy for identifying your most valuable assets, implementing the correct protections, detecting security events, responding to threats and recovering from an incident can in fact reduce the likelihood and impact of a compromise.

Mature organizations were less likely to experience a compromise... but they were still vulnerable.

It is equally important to note, however, that higher maturity scores were not a warranty against compromise. Though organizations with higher maturity scores were less likely to be compromised, they were still vulnerable. There is no panacea for all security issues, threats and attacks, and we need to remember that given enough time and resources, an attacker will find a way.

So what should organizations do? How can they reduce the likelihood and impact of a compromise, both from the attack vectors listed in this report as well as other attack vectors that might be more applicable to their environment?

In the short term, we recommend addressing any low-hanging fruit related to the attack vectors described earlier. As discussed above, there are often tactical ways that can reduce your potential for compromise from these attack vectors.

From a more strategic perspective, we recommend ensuring that you have a well-rounded approach to security. Using the NIST CSF functions can provide an outline of the basic elements that should be part of your security strategy.

Identify

- Know your environment. In a shocking number of our penetration tests, we compromise systems or applications or software that the organization's IT team did not even realize were in their environment (due to shadow IT, lack of centralized asset management, etc.). If you have a better understanding of the assets in your environment, you will be better able to protect them.
- Limit the amount of data processed and stored in your environment. When there is less sensitive data, there is less to protect, and less for an attacker to steal.
- Formalize security governance and risk management. Identify security stakeholders, roles and responsibilities to ensure important security tasks are not overlooked. Additionally, document security policies and procedures, as well a formal risk management strategy. This can help create accountability, clarify security goals, establish risk tolerance levels, communicate security objectives and foster a culture of security.
- Understand your third party risk. Third parties can create pathways into your environment. Ensure you vet your third parties, use only trusted third party tools and monitor third party access in your environment.

Protect

- Implement targeted control improvements. Based on a risk assessment, seek to enhance protective safeguards where they will have the biggest risk mitigation. Use research such as this Attack Vectors Report and other cyber threat intelligence to ensure your network and system protections can mitigate attacker techniques.
- Don't mistake tools for security. There is a plethora of security tools and technologies out there, but too often, organizations install new technologies without building the processes around them to ensure they can be managed effectively. Seek to optimize the tools you already have, and make targeted investments in technologies that will have a measurable impact to your security posture.
- Train your users. Year after year, we see that many of our most common attack vectors continue to exploit weaknesses in user behavior. This year is no exception, as password attacks were the second most common attack vector, and weak passwords can play a role in the success of other attack vectors as well. Despite all the advances that have been made in authentication mechanisms and email protections, users continue to choose easily guessable passwords, click on phishing links and store sensitive data in insecure locations. Effective training can not only reduce this risk but also empower your users to proactively identify and report suspicious activities.

Detect

- Support your tools with formal processes. Often, organizations implement tools to log events and detect anomalous activity but do not have a process to review logs or respond to alerts and continuously tune/improve them. Your detection capabilities are only as strong as what you do once events are detected.
- Investigate use of a managed security services provider (MSSP). Many organizations who do not have the bandwidth to handle monitoring in-house have found a great return on investment by offloading these tasks to a third party. If this is the case, ensure that roles and responsibilities between you and your provider are clearly articulated.

Respond

- Formalize and test incident response procedures. Attacks will happen, and inadequate response efforts can greatly expand the scope and impact of an attack. Therefore, it is imperative to have a procedure that outlines guidance for triage, containment, mitigation, prioritization, escalation, notification and communications regarding the incident.

Recover

- Formalize and test business continuity and disaster recovery procedures. Whether it's a widespread cyber event that impacts business operations (such as ransomware), a natural disaster, or a global pandemic, effective BC and DR procedures will help ensure you can restore critical applications, retrieve backup data and continue to conduct business.

About RSM

Consulting services to successfully align your security program with your enterprise risk management and compliance obligations

In today's rapidly evolving business landscape, organizations are facing more complex regulations and standards. Balancing business risk with business needs becomes challenging as a result. CISOs and security leaders must now manage risk across a variety of distributed technologies such as cloud, IoT and traditional architecture. While a strong risk and compliance approach is essential for any successful security program, many security teams struggle to design and execute a security strategy that is built to effectively manage risk across the enterprise while also considering both current and future regulatory/standards compliance needs.

Security leaders can no longer be reactive when it comes to risk assessments. Instead, the role of cybersecurity needs to be elevated within the organization so security teams can make recommendations that proactively address regulatory, contractual and legal requirements that align with the overall business strategy. When seeking an external provider to help with cybersecurity risk and compliance, risk leaders need a partner who understands their business needs and challenges and can simplify risk and compliance to reduce cost and complexity.

RSM's security and risk professionals are more than technology specialists—we're also experienced business analysts. We have in-depth knowledge of current security and risk issues and trends as well as insight into your specific industry and business processes. Our professionals will take the time to understand your business and create strategies to ease the burden of compliance while engaging the business to identify and manage risk. This will help move your security program to the next level, enabling effective identification and strategic decision-making for cybersecurity risk, alignment with enterprise risk efforts, efficient management of controls for risk reduction and proactive management of regulatory, contractual and legal requirements as part of day-to-day business.

Whether you're trying to enhance or build your risk and compliance program, facing pressure from clients about security practices or reacting to a new compliance requirement, we'll help meet your security and risk needs through a cost-effective approach and standardized processes.

Acknowledgements

This report would not have been possible without the contributions noted below:

- Ken Smith, who sponsored this report and has championed the work of the Technical Writing team
- Mitch Johnson, who assisted with the collection and aggregation of our testing data
- The following individuals, who provided the first phase of data analysis:
    - Nic Draves
    - Shahram Farhadi
    - Sabah Mawj
    - Nino McGowan

We thank you for reading!

RSM US, LLP

RSM US, LLP
30 S Wacker Dr
Suite 3300
Chicago, IL 60606
312-634-3400

www.rsmus.com
www.warroom.rsmus.com

For questions, please contact:
Ken Smith
National Cyber Testing Leader
ken.smith@rsmus.com
216 622 1012

Disclaimer

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is
responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.