REPORT

FortiGuard Incident Response Report H1 – 2023

Insights from the Cyber Trenches

FORTINET

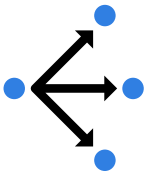
Table of Contents

Executive Summary

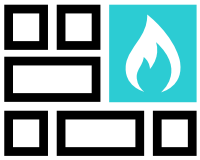
The FortiGuard Incident Response (IR) team provides both proactive and reactive incident response services, which are platform-agnostic and available to all organizations across the globe. Incident response teams like ours get unique exposure compared to many teams working in the cybersecurity field as we are often involved in investigating incidents where the victim's defenses have failed. The experience taken from working alongside these victims in investigating, containing, and evicting adversaries provides actionable insights into what weaknesses resulted in a breach and what is effective at removing them. This report contains many of these insights and takes into account contributing factors from both a human and procedural perspective, as well as observations and trends in adversary tradecraft across a range of intrusions.

We found the following key trends in 1H 2023:

"Human-driven" intrusions that rely on valid credentials, RDP connections, and manual post-exploitation techniques are still growing.



Internal authenticated network connections (endpoint-to-endpoint) were a missed opportunity for detection of lateral movement.



Many investigated incidents had antivirus or firewall detections that partially stopped or at least detected portions of incidents. Opportunities to shut down these attacks were missed, often due to a lack of adequate response, resulting in adversaries achieving their outcomes.

There are significant commonalities across ransomware tactics, techniques, and procedures (TTPs) that victims could have detected using solutions that are most likely already in place but were not being utilized.

Introduction

The threat-intelligence experts at FortiGuard Labs monitor millions of sensors around the globe, 24×7×365. This gives the FortiGuard Labs team a front-row seat to the latest activities and trends occurring in today's dynamic threat landscape. You may be familiar with the FortiGuard Labs Global Threat Landscape Report, where insights into the latest threat trends are published.

Alternatively, this report is based on a dataset collected by the FortiGuard IR team from real-world incidents investigated between January 1 and July 1, 2023. This report offers a snapshot into post-exploitation TTPs employed by a wide range of adversaries across a variety of environments. Report demographics, data sources, and other information are included in the appendix.

The key findings in this report focus on the insights taken from analyzing intrusions that were attributed to adversary activity. In addition to presenting data on TTPs employed as part of these attacks, we can also offer practical recommendations on how to protect against them and insight and guidance on how to avoid the various pitfalls that contributed to investigated incidents.

Using MITRE Frameworks

MITRE ATT&CK Tactics

MITRE ATT&CK is an increasingly popular framework for studying and describing adversary TTPs. MITRE defines 12 tactics, which are groupings of techniques based on the intended outcome of a particular technique.

Using MITRE ATT&CK to describe previous intrusions gives defenders the opportunity to identify commonalities between attacks, which helps prioritize the development of defenses. Given the nature of the changing threat landscape, attack trends will change to some extent over time. However, the cost involved for large-scale adversary operations to change entirely is very high, making trend analysis a key practice for staying ahead of threats.

More information on the MITRE ATT&CK framework is available here.

MITRE D3FEND

MITRE ATT&CK provides a fantastic framework for describing attacker techniques but should not be used as a checklist to validate defenses. This is because the number of implementations for a particular technique is not finite and all implementations are not known. While less adopted than MITRE ATT&CK, the MITRE D3FEND framework is better suited to articulating countermeasures and how they can support organizations in preparing to respond to adversary techniques.

Throughout this report, countermeasure recommendations are provided against corresponding MITRE ATT&CK techniques. Where possible, the corresponding MITRE D3FEND countermeasure ID has been provided with a link to the definition. Where a D3FEND countermeasure is not available, an ATT&CK data source has been provided where possible.

More information on the MITRE D3FEND framework is available here.

Report Findings

Adversary Motivation

The IR team makes an assessment about the likely motivation of the adversary (or adversaries) involved in each investigation.

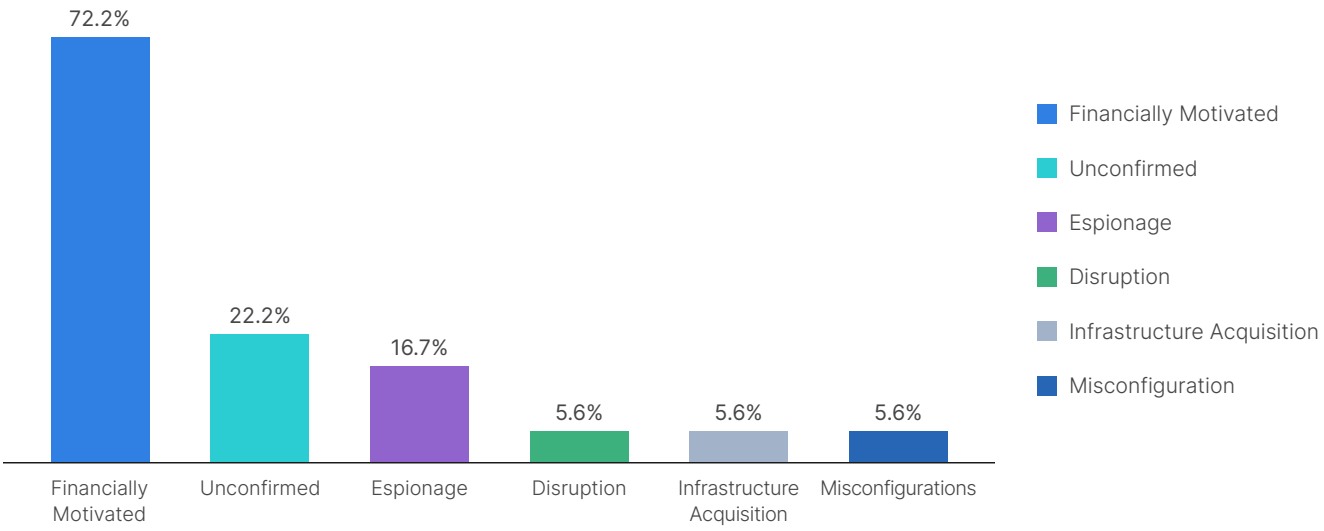


Figure 1: Probable motivations for investigated intrusions

Most investigated incidents were linked to a financially motivated adversary and were predominantly ransomware or extortion-based. In these cases, the victims were contacted regarding ransom payments for encrypted and stolen data.

In several cases where motivation was assessed as espionage, the FortiGuard IR team identified that the adversary had consistent access to a victim's environment and was performing data exfiltration for an extended period prior to deploying ransomware or a disruption effect.

In the limited investigations where the motivation was assessed as infrastructure acquisition, the adversary had prolonged access to an environment but remained in the periphery of victim networks, appearing to stage malware that was never employed in victim networks. We assessed this behavior as the adversary using the victim's environment as a pivot into other victims and a way of obfuscating command and control activities.

Reconnaissance and Resource Development

These tactics most often occur as a precursor to an incident and the artifacts associated with them may be located outside the control of a victim organization. Linking reconnaissance activity to an intrusion can be difficult, thus many events investigated by the FortiGuard IR team lack data related to techniques associated with these tactics. The data below highlights observed Reconnaissance techniques that were attributed to adversary intrusions but given the above should not be considered as representative of all Reconnaissance techniques employed by threat actors over this reporting period.

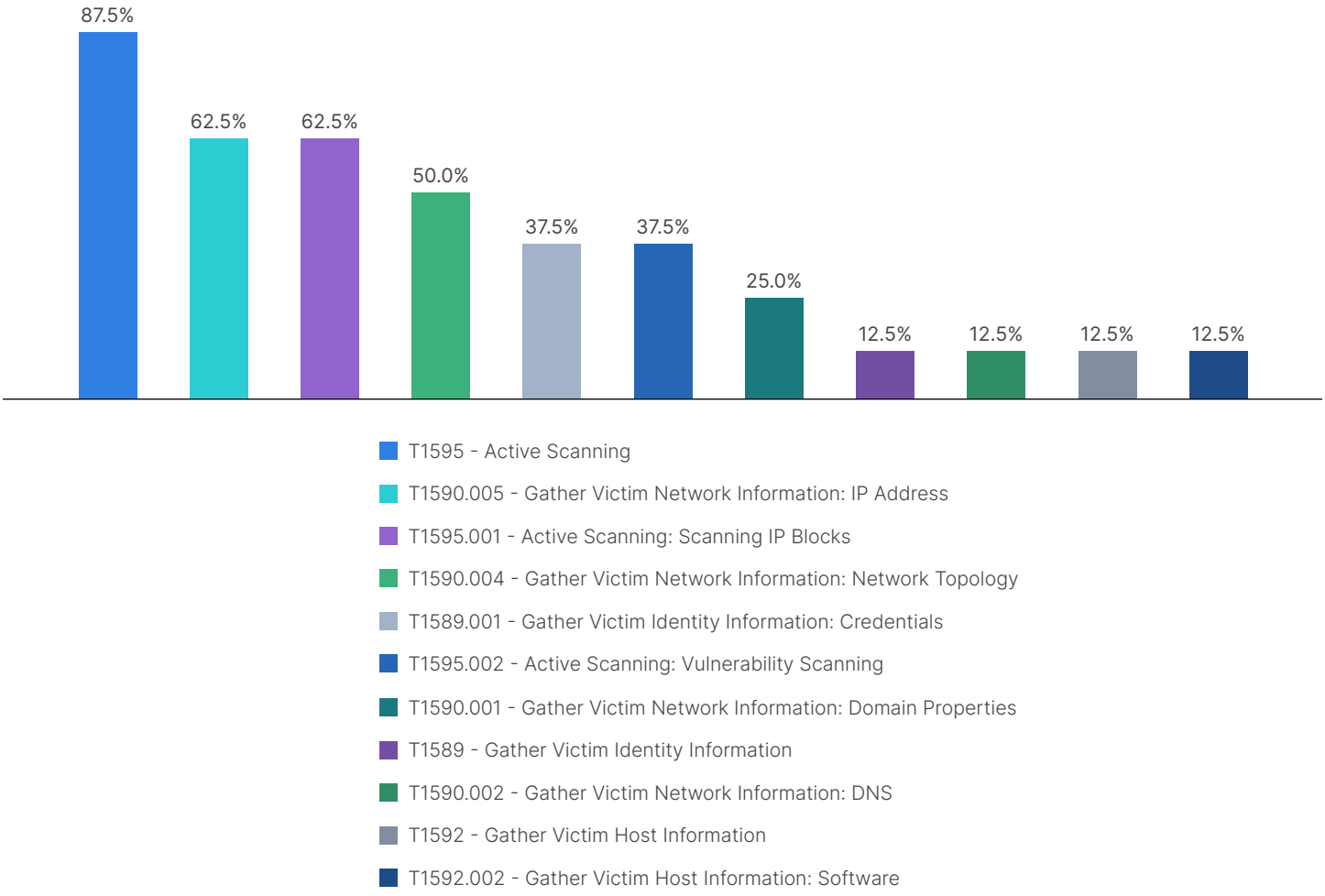


Figure 2: Most prevalent observed Reconnaissance techniques

Typically, techniques from Resource Development do not leave forensic artifacts that can be retrieved from a victim's environment as they are conducted prior to an intrusion. To understand a victim's threat exposure prior to an intrusion, the FortiGuard IR team takes advantage of the FortiRecon service. This service provides the IR team with any information on the dark web related to a victim and allows the IR team to identify adversary capabilities that could have contributed to heightened risk to a victim. For example, the FortiRecon team may identify credentials from a victim user account for sale within the last three months preceding an intrusion. The IR team can then investigate that user login activity to determine whether it could have been the initial access vector. In addition to this support to the IR team, the FortiRecon service monitors the capabilities of various threat actors. This includes identifying working POCs for new vulnerabilities and developments in adversary infrastructure (botnets) and maturity of adversary post-exploitation frameworks.

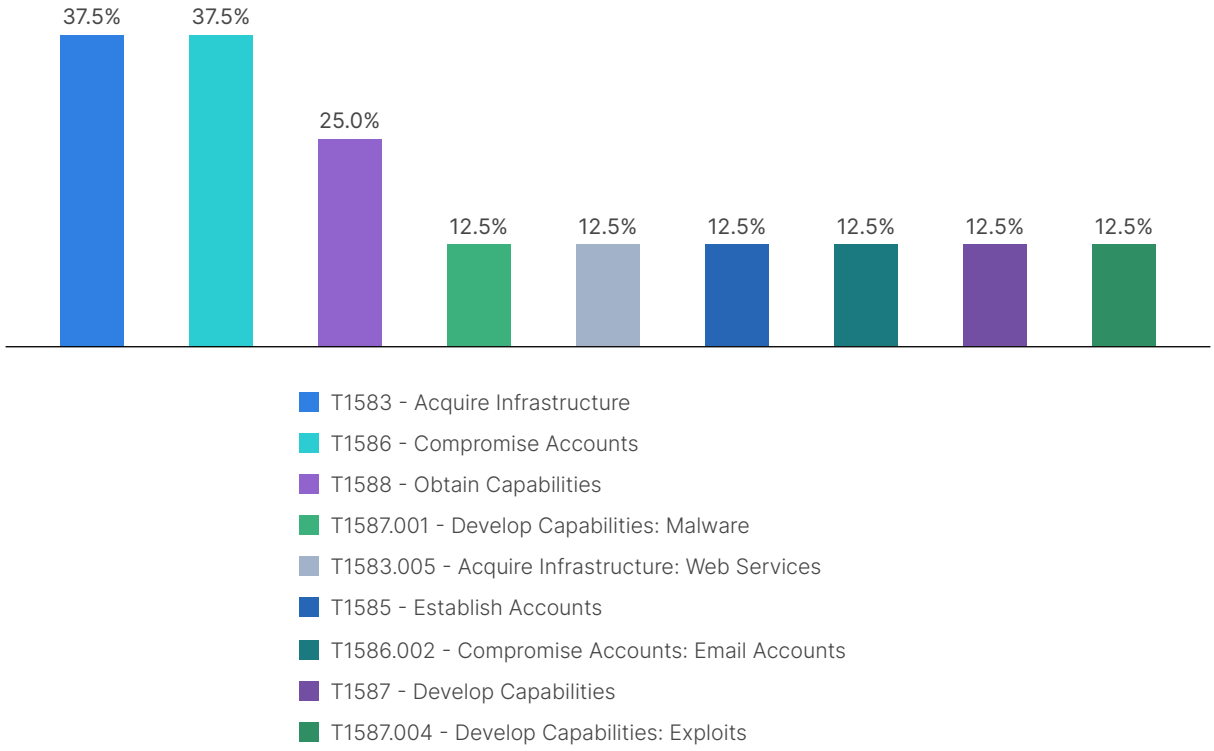


Figure 3: Most prevalent observed Resource Development techniques

Initial Access

The Initial Access tactic groups techniques employed by threat actors to gain first access into a victim environment. In most cases, these techniques represent adversaries breaching network perimeters, which is often the first detection opportunity.

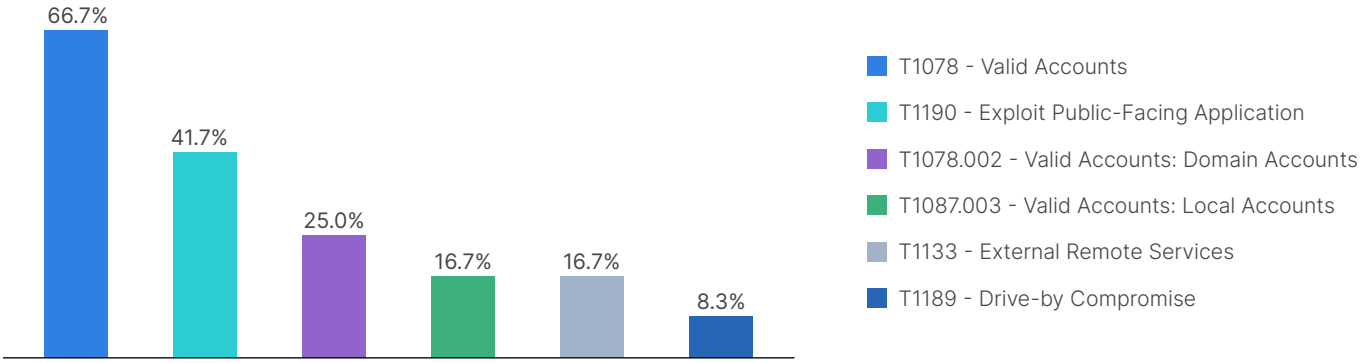


Figure 4: Most prevalent observed Initial Access techniques

The most commonly observed technique for initial access was the use of Valid Accounts (T1078). In these cases, the earliest indicators of an intrusion were related to the use of valid credentials. This highlights growth compared to our data from 2022. The use of valid accounts for intial access occurs for several reasons:

- There was a previous, undetected compromise of the victim network that was not identified or cannot be forensically linked to an investigated incident based on artifacts retrieved at the time of investigation.
- Credentials were compromised through an out-of-band attack such as social engineering or a password-sharing style attack.

In most cases investigated by the FortiGuard IR team, the former is suspected. In many cases, these suspicions were validated as victim organizations had credentials available through initial access brokers or there was evidence of previous compromises within victim environments that indicated credentials had previously been compromised.

Initial access brokers are individuals or groups that specialize in acquiring and selling unauthorized access to computer systems and networks. Initial access brokers have cemented themselves as a core part of the cybercriminal ecosystem likely because of several factors:

- Lowers barrier of entry for intrusions as perimeters are often a bottleneck for accessibility
- Connects targets with adversaries, allowing adversaries to be selective
- Disrupts attribution and threat modeling by separating intrusions into pre-access and post-access

As initial access brokers continue to become ingrained in cybercriminal ecosystems, we can expect to continue to see adversaries with a broad range of motives take advantage of these services. The benefit for defenders in these ecosystems is the inherent delay between when the initial access broker gains access and when the access is available to a buyer. During this time, accesses need to be advertised to attract a buyer, which provides a detection opportunity and a window for a victim to detect anomalous accesses and invalidate associated accounts or tokens. To take advantage of this delay, organizations can look to invest in attack-surface monitoring services to detect potential access sales, such as FortiRecon, to detect compromised credentials before they make it into an adversary's hands.

The more traditional Initial Access method, Exploitation of Public-Facing Applications (T1190), remains the second most prevalent Initial Access technique observed. Vulnerabilities in applications that run as web servers have been identified and actively exploited with vulnerabilities in SolarView,[1] Zoho ManageEngine,[2] MOVEit,[3] WebLogic,[4] PaperCut,[5] and Apache RocketMQ,[6] providing opportunities for initial access through remote code execution (RCE) vulnerabilities.

The fifth most prevalent Initial Access technique was Exploitation of Remote Services (T1133). Implementations of this technique we have observed have predominantly targeted known high-impact vulnerabilities in VPN services hosted on network devices where patches were available at the time of an intrusion. Exploitation of network devices like firewalls and email security devices presents opportunities for more elusive espionage operations as they are typically less monitored than endpoints and their behavior is less understood. This provides opportunities for more advanced actors to extend their dwell time without being detected.

Both of these techniques, T1190 and T1133, rely on vulnerabilities being both present and accessible (via public access). This presents us with two mitigation options:

- Patch known vulnerabilities quickly to remove them before they can be exploited by the masses.
- Reduce publicly accessible services to shrink the opportunity for unpatched and zero-day vulnerabilities to be exploited.

Recommendations

To combat threats that use Initial Access:

- Implement multi-factor authentication (MFA) and monitor MFA logs. Guidance when considering MFA is available from CISA here and Fortinet here.
- Patch vulnerabilities as soon as possible.
- Build the processes to implement hardening actions in response to disclosed vulnerabilities.
- Build formalized, repeatable processes outlining how to perform threat-hunting activities based on known indicators that could be linked to a vulnerability.

- Centralize web server logs associated with external-facing web applications by forwarding generated logs to a SIEM or SOAR solution.

Looking at many of the high-profile vulnerabilities for the first half of 2023, many of the indicators of compromise could be detected through the analysis of web server logs corresponding to a vulnerable service, Process Creation (DS0009) events, and File Creation (DS0022) events on the affected server.

For example, if we look at the PaperCut MF/NG RCE vulnerability (CVE-2023-27350) from earlier this year, the majority of reported exploitation[7] results in the spawning of PowerShell and cmd child processes from the PaperCut process (pc-app.exe). Similarly, the RCE vulnerabilities associated with Zoho ManageEngine[8] also result in anomalous process chains that could be detected through process spawn analysis (D3-PSA) if the process creation data source is collected and centralized.

Execution

Techniques associated with the Execution tactic are those employed to execute code in support of an intrusion.

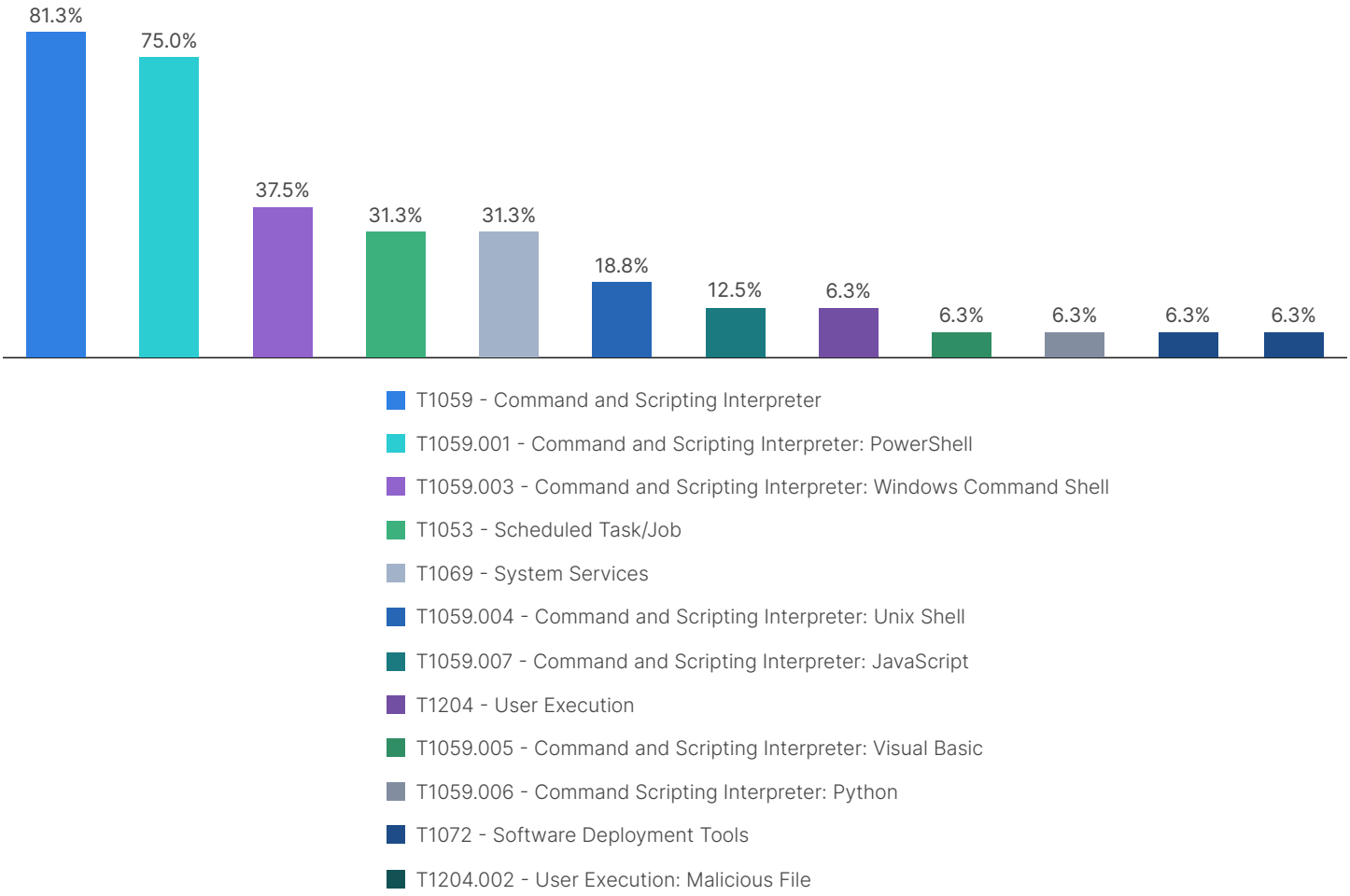


Figure 5: Most prevalent observed Execution techniques

Execution techniques the first half of 2023 were very similar to those from 2022, with the use of PowerShell continuing to reign as the most prevalent form of execution within observed intrusions. The use of Scheduled Tasks (T1053) and System Services (T1569) also remained high, with the ease of usability and the utility of these techniques also supporting Privilege Escalation and Persistence tactics being a key contributing factor.

Compared to previous years' data, the use of Windows Command Shell (T1059.003) dropped off in observed intrusions, especially compared to the continued prevalence of PowerShell. We assess that this is likely because much of the use of the Windows Command Shell performed by adversaries was for implementing techniques associated with the Discovery tactic. Within this half of the year's data set, there is a disproportional representation of ransomware intrusions where there appears to be a growing trend in the use of standalone executables (for example, Advanced IP Scanner and AngryIPScanner) being used to implement techniques associated with the Discovery tactic.

Recommendations

To defend against the use of PowerShell (T1059.001), organizations can enable PowerShell script block logging[9] and centralize and analyze generated logs to monitor PowerShell commands.

Script block logging is a free feature in Windows and can be centralized along with any other Windows event logs into an existing SIEM solution. Detection logic for anomalous PowerShell script block logs is readily available in consumable formats[10] and implementation of this type of logging delivers high ROI. Additional advice on monitoring and securing PowerShell usage is available here and here.

For organizations looking to take further advantage of enhanced logging for detection of anomalous execution events indicative of some of these popular execution techniques, the installation of Sysmon is highly recommended[11] where an EDR agent like FortiEDR cannot be employed. Sysmon allows for the collection of additional logs that can be centralized into a SIEM and analyzed to more easily support functions such as process spawn analysis (D3-PSA) and script execution analysis (D3-SEA) that can be used to detect these execution techniques.

The use of scheduled tasks for adversary execution can be detected and mitigated easily by a modern EDR solution. Where this is not feasible, organizations should look to monitor the Task Scheduler logs to identify anomalous activity. The Task Scheduler logs are enabled by default in the Windows environment and contain information on scheduled task creation, modification, and execution. These logs should be centralized, and new events monitored across an entire organization. By looking at all scheduled task logs across an environment, SOC operators within an organization will be able to tune out false positives and noise from a network's default configuration and more quickly identify anomalies. Look for the following characteristics:

1. **Scheduled tasks being created by anomalous accounts:** The use of scheduled tasks for day-to-day operations or administrative work is likely very rare. Monitor logs for the creation of new scheduled tasks by any user account.
2. **Scheduled tasks being created that reference command line interpreters as their action:** It is anomalous for powershell.exe., cmd.exe, or wscript.exe to be called directly as a scheduled task action. Investigate all scheduled tasks that reference these executables as a priority.
3. **Scheduled tasks that reference files in anomalous locations:** Often malicious scheduled tasks will reference executables stored in a temporary directory or use proxy execution to run scripts in script files stored in anomalous directories. Prioritize investigating scheduled tasks referencing files in temporary user directories or user downloads directories.

Like scheduled tasks, anomalous service usage for execution is easily detected and mitigated by a modern EDR solution but can be easily detected by centralizing and monitoring default Windows event logs. In the case of anomalous service usage, organization should look to monitor the System and Application logs. The System logs contain important system-level events, including service start and stop events, hardware and driver-related events, and other system-level activities and will be the primary source of service information. The Application logs primarily contain logging from applications but may also capture events related to services that are part of applications, such as web servers or database servers, so should also be monitored for useful information for specific services. Once these logs have been centralized, look for the following anomalous characteristics:

- **Unusual service starts and stops:** Monitor logs for unexpected patterns of service start and stop events, especially during non-business hours or outside regular administration windows.

- **Abnormal account usage:** Use logs to identify services running under privileged or unfamiliar or uncommon user accounts, as well as instances where service accounts are frequently changed or modified. The use of services may be associated with the installation of new software, but this will not typically be from individual user accounts when in a corporate environment.

Unrecognized service executables: Monitor for services launched from unusual or non-standard executable paths. As with scheduled tasks, services running from temporary directories or user directories should be investigated as a priority.

Persistence

Techniques employed for Persistence are those that allow an adversary to get back into an environment without the need for an Initial Access technique.

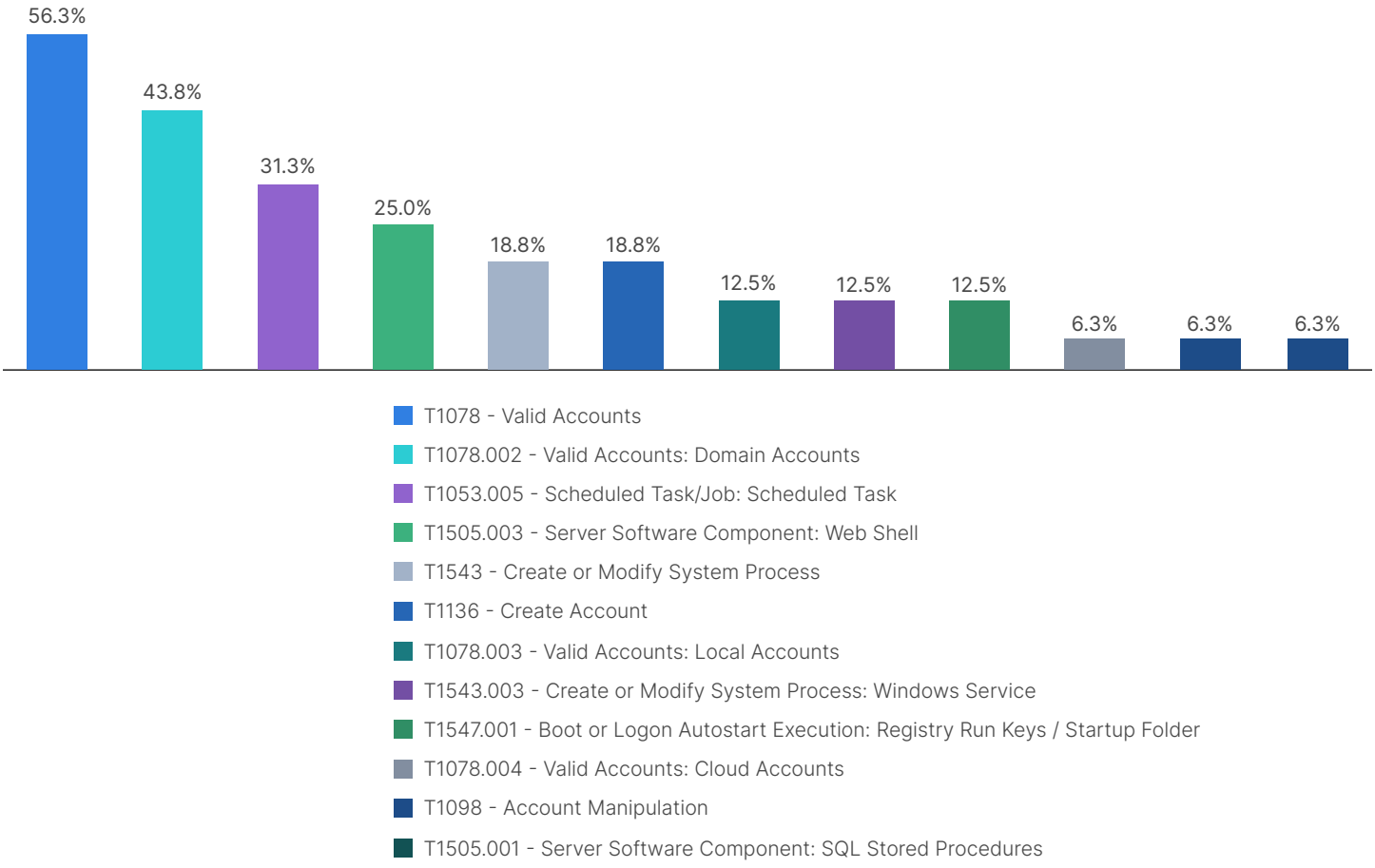


Figure 6: Most prevalent observed Persistence techniques

The increasing trend of adversaries using valid credentials to progress through their kill chains also applies to observed Persistence techniques. The use of Valid Accounts (T1078) was found in over 56% of investigations where a Persistence technique was observed. In many of these scenarios, the adversary delayed employing other persistence mechanisms until after they had performed discovery within a compromised environment and moved to key endpoints, for example, file servers or administrator terminals. This represents a backward step in sophistication for threat actors and forces them to employ more manual methods of operation but allows them to more easily avoid detection and increase the likelihood of success.

The usual Persistence techniques of Scheduled Tasks (T1053.005), Service Creation (T1543.003), and Registry Run Keys (T1547.001) continue to be regularly employed but more sparingly than in previous years.

Recommendations

Persistence has always presented excellent detection opportunities for defenders. Detections for many of the most common Persistence techniques, including the use of Scheduled Tasks (T1053.005) and Service Creation (T1543.003), are readily available through log monitoring. Organizations should:

- Centralize and analyze default Windows event logs with a SIEM solution
- Implement user entity and behavior analytics (UEBA) technology

Privilege Escalation

Privilege Escalation aims to elevate or transfer privileges to an adversary to help implement techniques required for the later stages of an attack. This may be required to subvert existing controls within a victim environment. There was limited evidence of Privilege Escalation techniques in investigated incidents over this reporting period resulting in a limited sample size of techniques. This data has been omitted as it offers little insight to drive usable recommendations.

Defense Evasion

The Defense Evasion tactic groups techniques employed to evade security controls within a victim environment. Typically, indicators associated with these techniques should be treated with a higher level of suspicion as there is limited scope for false positives.

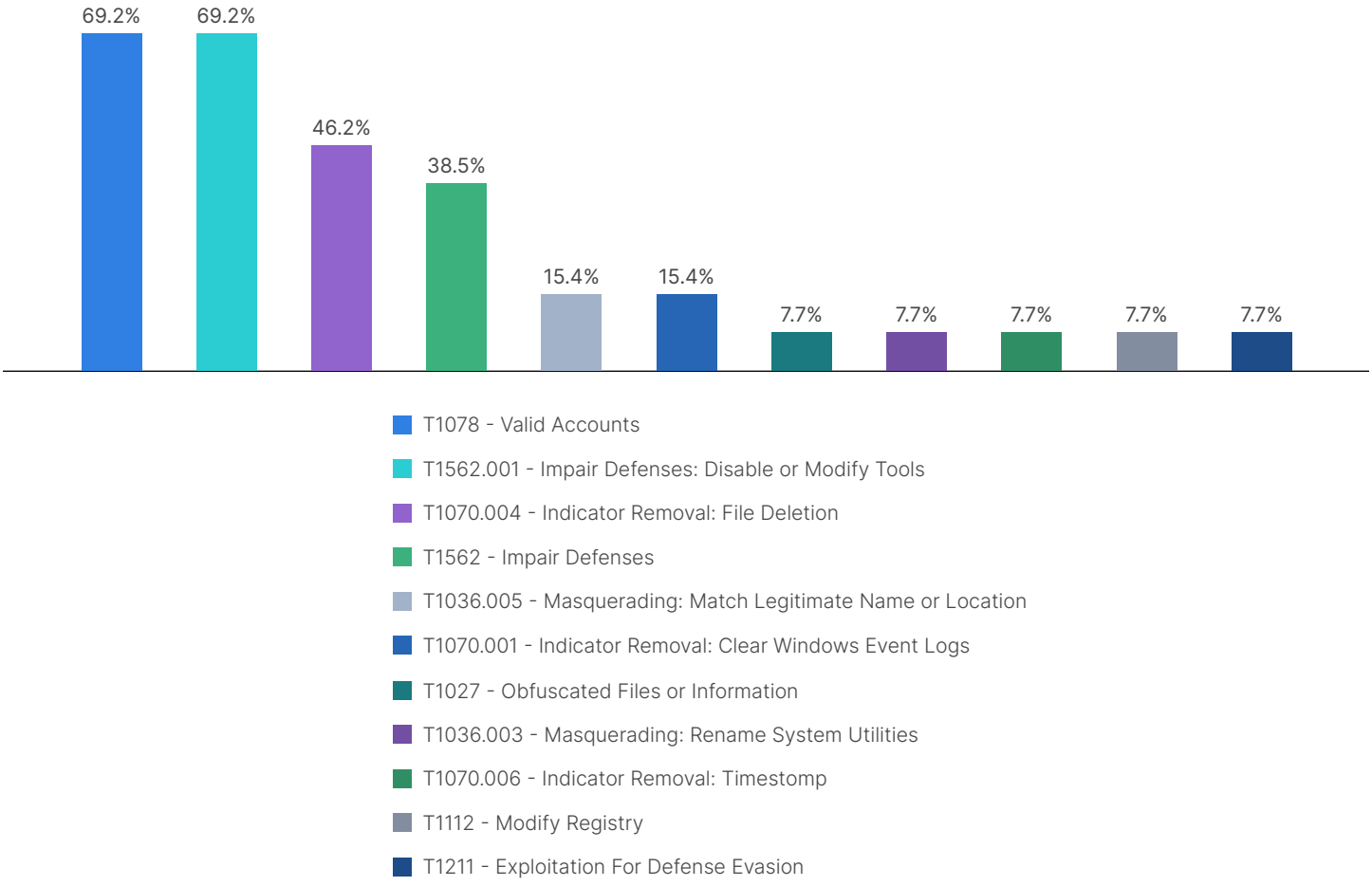


Figure 8: Most prevalent observed Defense Evasion techniques

The use of Valid Accounts (T1078) again dominated this tactic following the same trend as in 2022. By using Valid Accounts, adversaries can avoid arousing suspicion and gain unauthorized access, evading traditional security measures. The use of valid credentials can allow adversaries to bypass security controls until much later in their intrusion, which reduces the time an organization may have to respond. Additionally, the use of a Valid Account makes it more difficult for victim organizations to quickly employ countermeasures without impacting the end-users.

Impair Defenses: Disable Tools (T1562.001) was another common component of intrusions. As with Discovery techniques to be covered later, the barrier for entry here is lowered by easy access to tools like Defender Control,[12] which allows adversaries to easily disable AV solutions like Microsoft Defender. While this technique can be easy for defenders to detect and creates a high-confidence indicator or compromise, the FortiGuard IR team observed this technique being used later in intrusions. This makes it a great detection opportunity, but organizations should be prepared to take swift action if this technique is suspected, as it is typically employed immediately prior to ransomware deployment. The adoption of AuKill in lieu of the popular BackStab tool for more direct targeting of EDR products appears to have taken place in the first half of 2023, with no observed cases involving BackStab being observed in the first six months of the year. Both solutions employ the bring your own vulnerable driver (BYOVD) technique to bypass and disable EDR solutions. The targeting of EDR agents with tools like AuKill, BackStab, and EDRSandBlast over the last few years highlights the impact these tools have on the effectiveness of ransomware and extortion operations.

The third most observed Defense Evasion technique was Indicator Removal: File Deletion (T1070.004). In many investigations, our efforts to understand an intrusion were made more complex as adversaries removed any executables or script files used as part of their intrusion. This made retrieving executable files for malware analysis more time-consuming and slowed down investigations. In some cases, AV and EDR solutions employed by the victim contributed to this issue by deleting suspicious executables and files without first retaining a quarantined copy for later analysis.

Recommendations

Recommendations for detecting and mitigating the use of Valid Accounts (T1078) are highlighted in the Initial Access section above. Despite the same technique being used for multiple tactics, the recommendations on detection and mitigation are the same.

The targeting of defensive tools within a victim environment provides a great opportunity for detection. Track these tools, often executed as services, through default system and application logs. Additionally, these tools often have their own logging that should be centralized to better manage the health of endpoint technology.

And finally, maintain as close to 100% uptime on endpoint solutions as possible and investigate all unplanned outages. Even if an outage is not caused by adversary activity, an outage can leave an endpoint vulnerable, which could allow an adversary to establish a foothold in a network. Monitor the status of the services hosting endpoint solutions like AV and EDR to gain a health check on them. This will help determine the uptime of services and provide an opportunity to detect potential adversary interference. Look for services stopping outside of standard update or reboot cycles, especially where there is evidence of issues with the service (such as service crashes).

In many of the investigations conducted by the FortiGuard IR team, victim organizations had AV alerts related to an intrusion months before the full scale of the intrusion was fully realized. Unfortunately, in many of these cases, the AV solution had not saved a copy of the offending files before deleting them, and the files were unique to the victim's environment. This lack of information prevented the FortiGuard IR team from validating some components of intrusions, slowing down the investigative process. To prevent an "own goal" by deleting malicious artifacts detected by endpoint solutions such as AV and EDR, configure these solutions to safely quarantine a copy of any suspected artifacts before deleting them from an affected host. To enhance the detection of file deletion, leverage free solutions like Sysmon to generate additional logs when executable files such as .exe and .dll files are both created and deleted. Centralize these logs to monitor for file deletion events for executables linked to the use of user or administrator accounts. The creation or deletion of executables by users should be rare outside of normal ephemeral executables created when using some applications, which can be tuned out, and even administrator accounts should be able to narrow this type of event to when administrative actions were being taken.

Credential Access

The Credential Access tactic refers to techniques that adversaries can use to obtain or steal valid user credentials, which they can then use to access additional systems and resources. This tactic often involves methods like password cracking, phishing, or exploiting vulnerabilities to compromise credentials.

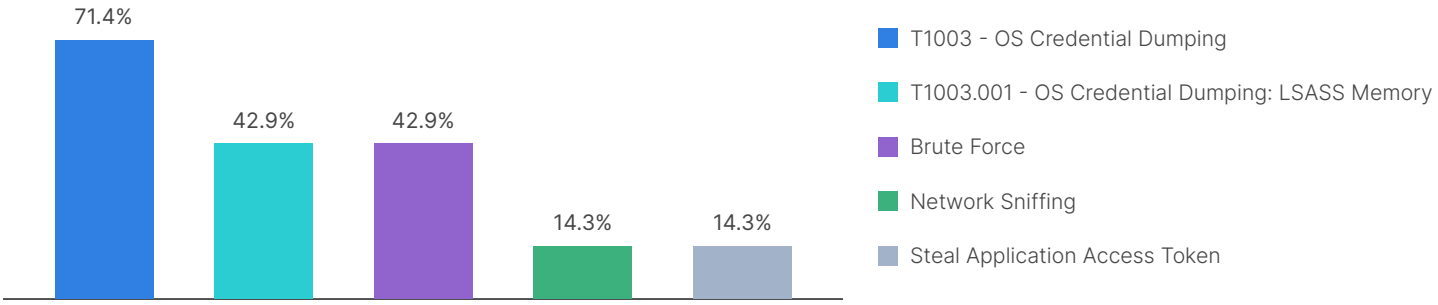


Figure 9: Most prevalent observed Credential Access techniques

Techniques observed over this period showed no significant changes in trends. Among the OS credential dumping sub-techniques, dumping memory from LSASS (T1003.001) continued to remain popular among ransomware operators. The use of Mimikatz continued to be the preferred tool for implementing this sub-technique, closely followed by Process Hacker.[13]

As previously highlighted, the Initial Access method for many of the intrusions was through the use of Valid Accounts (T1078). In many of these cases, credentials had already been compromised as part of a prior intrusion that was not detected by the victim organization nor could adequate evidence be found to determine the credential access technique used as part of a prior compromise.

Recommendations

Use a modern EDR solution to detect most basic implementations of OS credential dumping, especially when performed through the basic use of open-source tools such as Mimikatz or Process Hacker. While modifying the hash of a Mimikatz executable through binary padding or recompiling a fresh binary per-use is rudimentary, from the FortiGuard IR teams experience, this basic tradecraft is often skipped by many ransomware operators. This allows even basic AV solutions to detect known executables that have been associated with previous compromises from being detected and blocked between intrusions. To take advantage of this, at the very least, ensure AV signatures are kept up to date.

Discovery

The Discovery tactic encompasses techniques employed to gather information about the target environment, such as remote systems, network topology, and active accounts. This information aids adversaries in understanding a victim's infrastructure and potential vulnerabilities to enable subsequent stages of their attack.

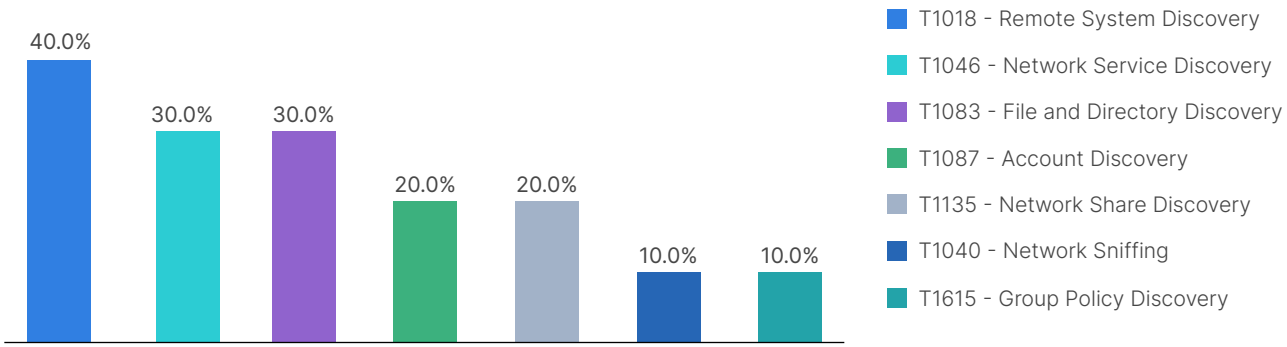


Figure 10: Most prevalent observed Discovery techniques

Historically, many of the techniques used for discovery were implemented through a native shell (Windows Command Shell or Bash) and relied on the use of default native binaries such as net.exe in Windows and ifconfig in Unix. In the first half of 2023, however, almost all intrusions that involved the deployment of ransomware, including those from Blackcat/ALPHV, Lockbit, Black Basta, Royal, and Rhysida, used Advanced Port Scanner or Advanced IP Scanner as a precursor to ransomware deployment. Advanced Port Scanner is a free tool[14] that can be deployed as a standalone executable and allows a user to map network connected devices and their open ports and provide an assessment of the likely service behind an open port. This functionality supports several Discovery techniques that allow an adversary to quickly identify vulnerable services, key file servers, domain controllers, and management interfaces for hypervisors. This can provide an adversary with all the information they need to quickly target key information and services to provide the biggest impact to a victim organization.

Advanced IP Scanner is another free tool,[15] also developed by Famatech. Advanced IP Scanner can be deployed as a standalone executable and is effective for mapping connected network drives and identifying remote hosts within a victim's environment. These two tools appear to be used interchangeably so may be employed based on operator preference.

Recommendations

While the use of legitimate third-party tools like this does not pose direct risk to organizations, they provide a great opportunity to detect potential malicious activity and locking them down can force an adversary away from their preferred Discovery techniques.

Lock down anomalous applications like Advanced IP Scanner and Advanced Port Scanner with application allow listing (D3-EAL) if possible.[16] Otherwise, use application deny listing (D3-EDL). Restrict their use to administrator accounts where these tools are a legitimate part of an administrator's toolkit.

In addition to detecting these discovery tools by monitoring endpoint behavior, leverage network-based detections by looking for scanning behavior. These scanning tools are typically designed to complete administrative functions quickly, which also makes them noisy and easy to detect if organizations have an appropriate level of internal traffic monitoring. Network traffic related to uncommon ports or unused IP addresses can be an indicator of generic, early scanning. Organizations should look to determine what visibility they have of internal network traffic and test some of these scanning tools to see if they could detect with existing telemetry.[17]

Lateral Movement

Techniques associated with the Lateral Movement tactic describe methods that adversaries can use to move laterally within a compromised network once initial access has been acquired. Lateral Movement to key endpoints or to access key information is essential for adversaries to achieve their objectives. It also provides an excellent focal point for organizations when improving detection capabilities. Lateral Movement has historically been overlooked as organizations focus on protecting their environments from outside threats moving in rather than looking at what's already inside their networks.

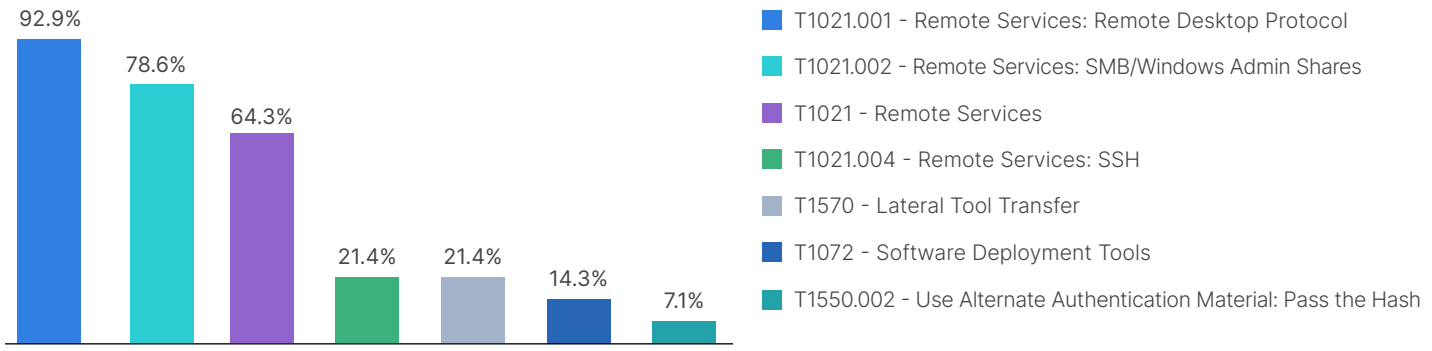


Figure 11: Most prevalent observed Lateral Movement techniques

The widespread use of Remote Desktop Protocol (RDP) (T1021.001) as the most prevalent lateral movement technique further cements the use of valid accounts to progress intrusions. RDP traffic is common for system administrators to use within networks and may not trigger alerts on endpoint security solutions due to the need to use valid accounts. This means it provides a relatively safe method for adversaries to move through a network. In addition, RDP allows access to GUI. Access to a GUI doesn't support operations at scale but provides a feature-rich way of interacting with a compromised host. Access to an endpoint through RDP gives threat actors the ability to copy and paste files to and from the victim endpoint and their own host with minimal forensic artifacts. In many ransomware or extortion cases, we saw adversaries open samples of data such as Microsoft Word documents and PDFs for validation directly through the RDP GUI prior to performing exfil. This rise in "hands-on" intrusions through RDP lowers the technical barrier for ransomware and extortion affiliates, as once they have credentials, they can extract data without having to employ more technical tools.

The use of existing mapped Server Message Block (SMB) drives (T1021.002) for lateral movement and lateral tool transfer was again a main feature of observed techniques. This also requires access to valid credentials. In addition, the use of SMB for lateral movement was especially common to and from file servers. The use of SMB for accessing data was also the most prevalent Collection technique.

Recommendations

- Lock down direct access to the RDP service to only support essential access.
- Avoid having RDP accessible directly from external networks (the internet) to prevent exposure to brute force attacks and direct access through compromised credentials.
- Employ a VPN solution with MFA to centralize connections, secure against compromised credentials (D3-MFA), and limit exposure of the RDP service (if RDP is required for business function).
- Restrict standard users from logging in to remote endpoints with RDP to lockdown use of RDP for lateral movement (T1021.001). This can be done by modifying security policies to only include user groups that need to use RDP in the "Allow logon through Remote Desktop Services" security policy[18] (D3-UAP).
- Consider the use of deception technologies, such as honeypots (D3-CHN), within networks to deceive threat actors with access inside a network. Numerous open-source honeypot implementations are available but are not as robust as commercial solutions such as FortiDeceptor.

In addition to the above hardening guidance, one of the best tools for detecting anomalous RDP access within a network is already in place in a Windows environment and is already freely available, Windows Event Logs. Windows login events, specifically Windows Security logs, are the bread and butter of piecing together activity on an endpoint. The security event log contains, among other things, information related to all logon and logoff events for a particular endpoint. The logon and logoff events have Event ID 4624 and 4625 respectively. By default, Windows endpoints will log local logins and logins with cached credentials on the local endpoint and domain login events on the domain controller.

These events can be used to identify RDP logon events and link these events to a user account, a remote IP, a remote workstation name, and provide windows of time when a connection was active. This information can be centralized and easily used to identify anomalous patterns of behavior.

- Look for non-typical use by particular user groups (D3-ANAA). For example, it is usually not standard behavior for regular users to use RDP to log in to workstations within an environment.
- Look for client-to-client RDP connections (D3-CAA). For example, outside of administrator workstations used for tech support, it is likely not standard behavior for any user to use RDP to log in from one workstation to another workstation.
- Look for RDP connections from remote hosts (D3-UGLPA). Organizations should look to the hardening best practice provided above and deny direct RDP access to endpoints within their environment from external networks. Regardless, if an RDP logon event is observed directly from a remote IP, it should be investigated as suspicious.

SMB/Windows Admin Shares (T1021.002) was the second most observed remote services sub-technique for Lateral Movement. One of the reasons this sub-technique was so high was due to the continued popularity of PsExec for Lateral Movement and Privilege Escalation. PsExec is part of the Microsoft SysInternals suite and is a useful tool often employed by system administrators and threat actors alike to perform administrative functions. Fundamentally, PsExec works by transferring a temporary executable to the Admin$ share of a target endpoint over SMB and then executing that executable as a service through RPC calls, which will then execute a user provided command. To reduce the usability of PsExec and standard SMB usage by adversaries for lateral movement, block all client-to-client SMB traffic (D3-NTF). There is no standard reason for organizations to support client-to-client communications over SMB. File shares should be centralized rather than hosted on individual workstations. SMB should not be blocked for client-to-server or server-to-client without robust testing, as it will have a significant impact on network usability. Note that this will not entirely remove the threat posed by PsExec, as the tool can be altered around the above controls,[19] but it will mitigate against the most prevalent form of usage as well as restricting adversaries' lateral movement options.

Collection

The Collection tactic pertains to techniques adversaries use to gather and consolidate data from compromised systems, often involving techniques like keylogging, screen capture, and data extraction. Once collected, this information can be exfiltrated and used for extortion, sold for profit, or analyzed to meet espionage objectives.

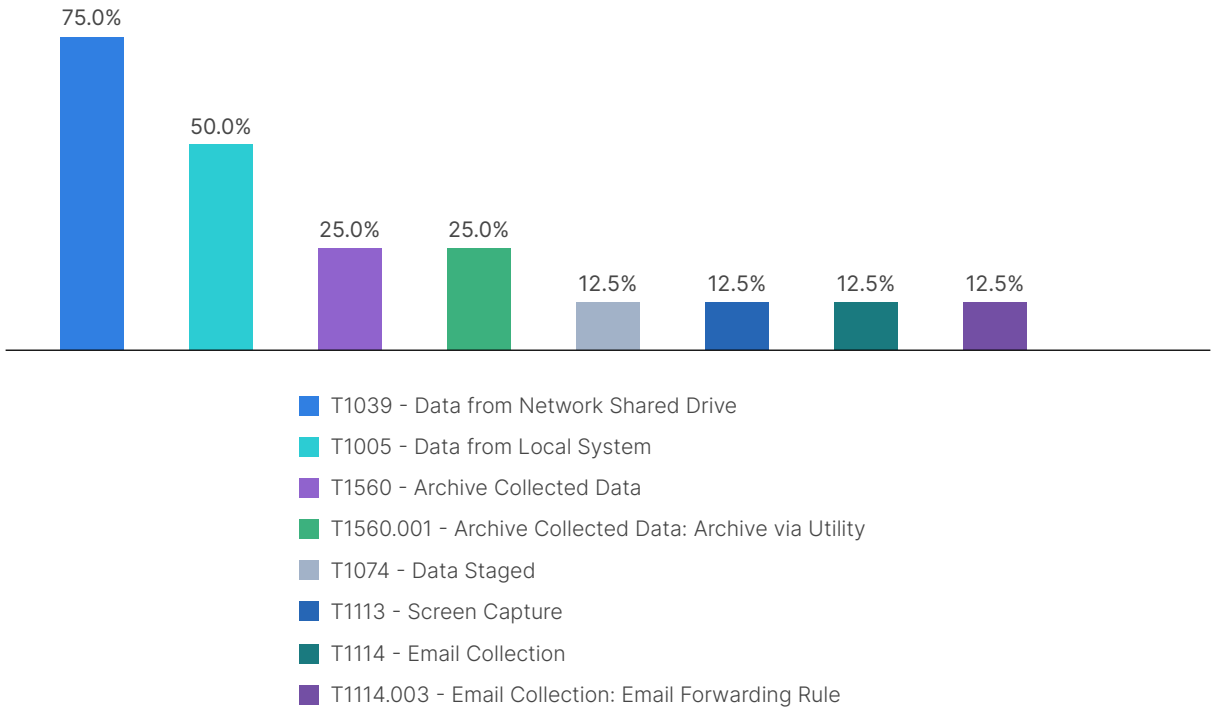


Figure 12: Most prevalent observed Collection techniques

As highlighted previously, the majority of the incidents investigated by the FortiGuard IR team over the last six months have been related to ransomware or extortion attempts. A critical component of these types of intrusions is the collection (and subsequent exfiltration) of sensitive data. Collection from network shared drives (T1039) was the most prevalent technique, followed by collection from the local system (T1005). These statistics don't offer a particularly useful insight as their prevalence is largely related to a typical organizational architecture where the majority of documents are typically centralized in file servers so they can be accessed equally by all workers.

Archive via Utility (T1560.001) remains another popular technique as it can obfuscate the files that were taken by an adversary and can be used to circumvent some watermarking DLP solutions. Fortunately, monitoring endpoint behavior for anomalous archive utility usage or creation can provide great detection opportunities.

Recommendations

Implement the following mitigations to help reduce the effectiveness of adversary data collection and provide detection opportunities:

- **Segment file access and administrative functions into separate user accounts.** Administrators should operate with two sets of accounts: one set they use when performing standard user functions and a separate set of privileged accounts used when performing administrative functions.
- **Monitor for admin access to working files.** Administrator accounts should not be used to access working files. When the administrator account is used to access working data, this could indicate a compromised account. Additional auditing can be enabled to track access to files on a file share by particular users as highlighted in this guidance.
- **Monitor for large volumes of file share accesses over a short period of time.** Automated tools used for large-scale collection and encryption will result in large volumes of file access over a short time period. Implementation guidance for this is provided in point 2 above.
- **Restrict access to archive utilities outside of approved utilities and monitor for usage.** The creation of larger archives or many smaller archives in a short period of time can be indicative of data staging through archiving. Monitor the following data sources to detect this type of activity:
  - Process Creation events (DS0009): Look for executables with names and signatures matching those associated with archiving software in anomalous directories. Tune and baseline for the environment.
  - File Creation events (DS0022): Look for files with known extensions associated with archives and large files being created by unknown executables or by archiving software. Tune and baseline for the environment to prevent detecting normal user usage.

Many modern EDR solutions, such as FortiEDR, support the collection of these data sources related to the behavior of an endpoint. Where an EDR solution is not available, these data sources can be collected through implementing Sysmon or by enhancing the default Windows auditing policy as highlighted here.

Command and Control

The Command and Control (C2) tactic refers to techniques adversaries employ to establish and maintain communication channels between their compromised systems and their remote infrastructure, allowing them to manage and control their malicious operations. Outside of self-propagating worms (typically rare), Command and Control is an essential part of an adversary's operations and thus provides a great focus point for detections.

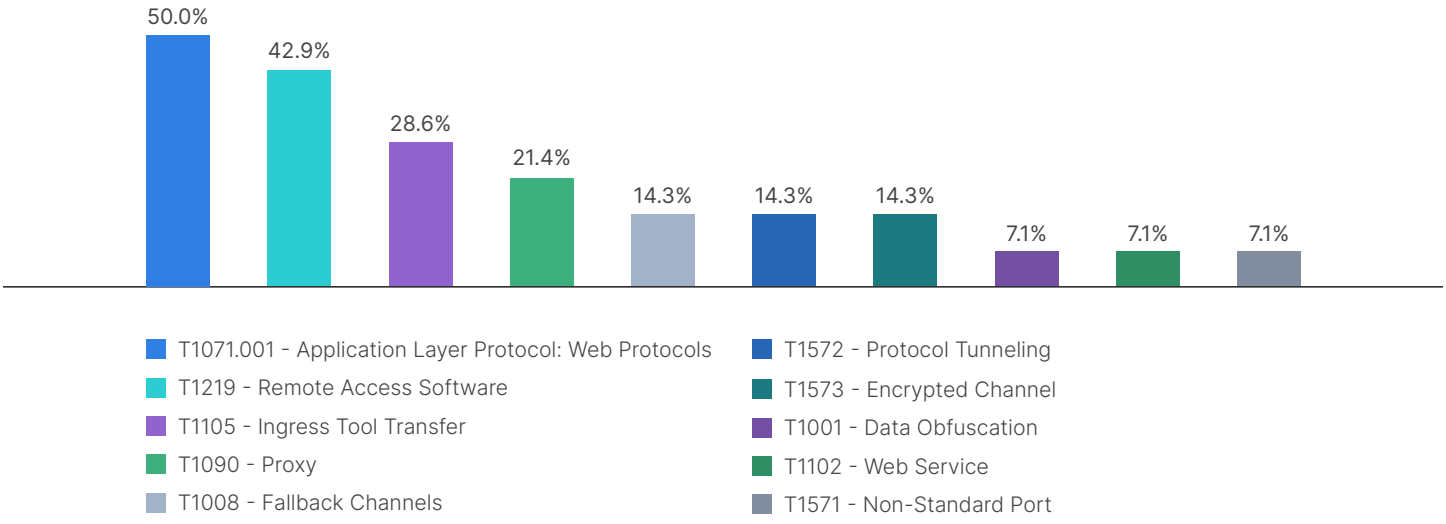


Figure 13: Most prevalent observed Command and Control techniques

Web Protocols continues to be the most prevalent technique, likely due to the large volume and variance in web traffic originating from an endpoint within any given environment. This provides adversaries with the opportunity to blend in with existing traffic. The FortiGuard IR team often finds that much of the observed C2 identified as part of an investigation is linked to known malicious indicators readily available through open-source threat-intelligence sources. This indicates a lack of integration of threat intelligence within many organizations that if it had been leveraged correctly, would have at least impacted the adversary's ability to conduct their operations and meet their outcomes for a particular intrusion successfully.

The use of legitimate remote access software (T1219) continues to be a core component of many ransomware intrusions. This technique was originally outlined in the Conti playbooks, which leaked in August 2021. Ransomware affiliates are still using these same tools to implement these techniques two years later with great success. In the Conti affiliate playbook, the remote access software solutions AnyDesk and Atera were mentioned explicitly with instructions on how affiliates could deploy the solutions in support of Conti's ransomware operations. This represents just one example of how the majority of the intrusions FortiGuard Labs helps investigate are not caused by an increase in the sophistication in adversary techniques and tradecraft but by a failure by organizations globally to stop known technique implementations. While this does not mean that organizations should stop caring about more sophisticated threats, detecting and mitigating these known TTPs represents incredibly low hanging fruit.

Recommendations

- Integrate threat intelligence feeds with existing network monitoring and protection solutions to automate detection and blocking of web traffic to known suspicious or malicious domains, URLs, and IPS services. The method for integrating threat intelligence feeds is heavily dependent on the solutions available in an organization's environment. Threat intelligence feeds organizations consider for integration should be tailored for their operating environment and threat profile as in this situation, a larger volume of feeds and indicators is very rarely better than a higher quality of feeds and indicators. Many countries provide targeted threat intelligence feeds that are often free for organizations that reside in their jurisdiction, such as CISA in the U.S. and ACSC in Australia. Organizations can also consider paid threat intelligence feed services like FortiGuard threat intelligence feeds[20] or FortiRecon Adversary Centric intelligence[21] to further enhance their capabilities.
- When considering approachable countermeasures to mitigate Command and Control techniques, it's hard to do better than simple preparation. Be ready to take action when indicators of adversary Command and Control are observed. Ask:
  - Are the processes in place to detect known C2 connections?
  - Are the processes in place so our teams know what they are expected to respond to?
  - Do teams know what to do when known C2 indicators are detected?
  - Are the tools ready and available to take action when C2 is detected?

  For example, if a connection is observed from an endpoint to a known malicious C2, is the organization able to take action to sever that connection and block future connections? We recommend that organizations build procedures to perform at least the following countermeasures consistently using the solutions available within their environment:
  - Sever an existing connection between an internal host and an external host.
  - Block future inbound and outbound connections to and from a selected IP or domain.
  - Flush DNS cache and sinkhole a selected domain.

  Building the processes to perform these functions will allow organizations to take effective action against adversary C2 in the event of an intrusion.
- Rehearse and exercise these procedures regularly.
- Implement application deny listing (D3-EDL) for all third-party remote access tools that are not used legitimately within the environment to mitigate the threat of adversaries using legitimate remote access tools like AnyDesk and Atera.

While there are many commercially available remote administrative tools on the market, a shorter non-exhaustive list of third-party remote access tools linked to known and observed intrusions is provided below:

AnyDesk
Atera
Syncro
Remcos
ScreenConnect (ConnectWise Control)
Splashtop

Additional guidance on locking down the use of remote access tools was provided by the Cybersecurity and Infrastructure Security Agency (CISA) earlier this year to assist organizations in managing the threat posed by these tools. You can find this guidance here.

Exfiltration

The Exfiltration tactic encompasses techniques adversaries use to transfer or steal data from compromised environments, often employing methods like data compression, encryption, and covert channels to hide the exfiltration of information.

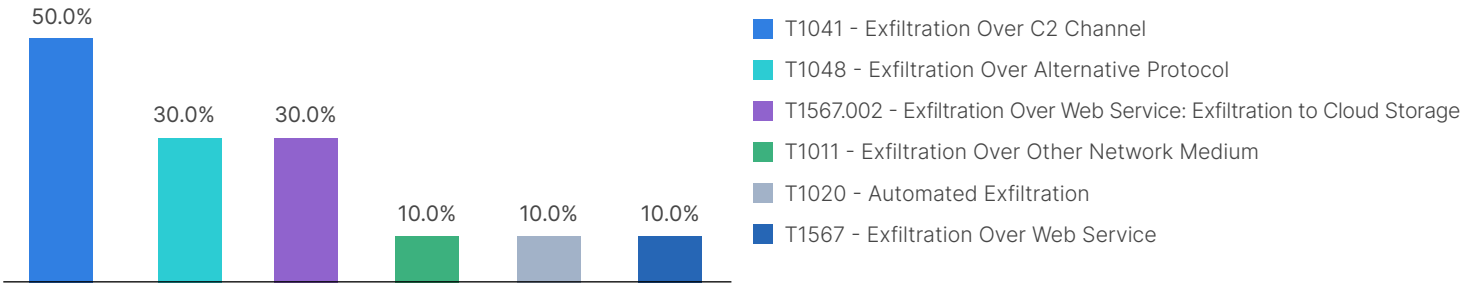


Figure 14: Most prevalent observed Exfiltration techniques

The most common technique for exfiltration was Exfiltration Over C2 Channel (T1041). In cases where exfiltration was observed, the C2 frameworks employed by various actors included the capability to retrieve files remotely, hence the prevalence of this technique. In cases where threat actors mostly employed valid accounts and RDP for accessing an environment, we observed the threat actor manually opened files to confirm contents via their RDP connection. In these cases, it is assumed that once the adversary verified the files of interest, they exfiltrated these files by direct copy from client to host.

The second most prevalent Exfiltration technique was Exfiltration Over Web Service (T1567), which was observed in a full third of incidents where exfiltration was observed. In several cases adversaries used rclone[22] with MEGA[23] cloud storage services to exfiltrate data to cloud storage (T1567.002). This replicates techniques explicitly outlined in the Conti playbooks from 2021.

Exfiltration of sensitive data is a core component of financially motivated cybercriminal activity for the majority of organizations across the globe. Exfiltration is a key part of ransomware, supporting the double-extortion method of encryption of workable data on victim's systems, then threatening to release stolen data unless a ransom is paid.

Recommendations

- Block direct access to web and cloud storage services if they are not critical to core business functions.
- Filter network traffic for DNS and web requests for related subdomains to prevent most methods for accessing the service.
- Filter network traffic based on known indicators of the service.
- Use endpoint telemetry, specifically Process Creation metadata (DS0009) to detect potential execution of file transfer software like rclone.
- Collect Process Creation telemetry with either a modern EDR solution or an open-source tool like Sysmon, then centralize this data and take advantage of existing crowd-sourced detection logic.[24,25]

Impact

The Impact tactic relates to techniques adversaries employ to manipulate, disrupt, or damage systems, data, or operations within a targeted environment. This includes actions such as data destruction, resource hijacking, and system or service disruption, aiming to impact a target's normal functioning.

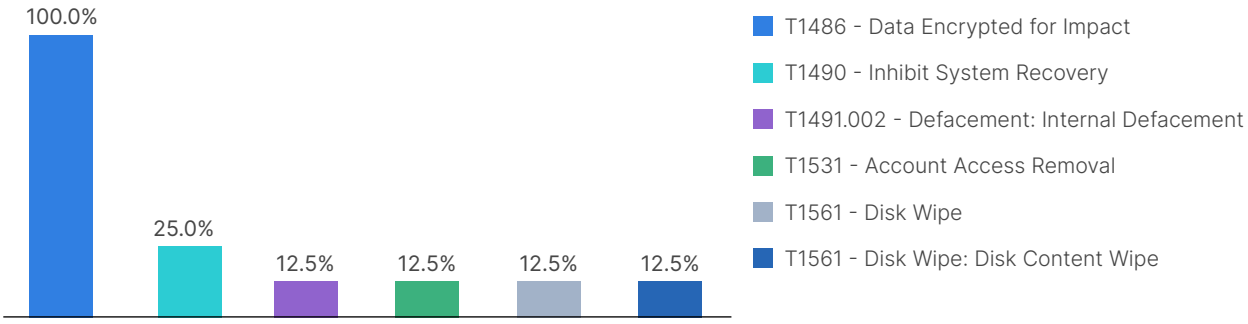


Figure 15: Most prevalent observed Impact techniques

Techniques observed for this tactic all correspond to investigated ransomware attacks. While the team investigated a range of different types of intrusions, those related to ransomware were the only ones where Impact techniques were observed.

Recommendations

Techniques employed at the Impact stage indicate an adversary has progressed significantly through their kill chain and likely has freedom of maneuver within a victim's environment.

- Take advantage of TTP crossovers shared by many threat actors for tactics usually employed earlier in an intrusion, such as initial access, execution, persistence, and lateral movement.

Where ransomware and wipers are considered a threat, organizations should follow best-practice advice in preparing to respond to such attacks.[26]

- Understand and document assets, including their configuration information.
- Prepare and maintain offline encrypted backups of critical data.
- Create, maintain, and exercise a formal incident response plan (IRP), playbooks, and incident communications plan.
- Apply patches to all external-facing applications and devices as a priority.
- Implement application allow listing and install of a capable EDR tool.
- Apply the principles of least privilege when configuring user permissions.
- Harden infrastructure associated with the management of hypervisors.

Overall Observed Technique Heatmap

The following figure provides a visualization of the top five previously identified most prevalent techniques for each tactic. Organizations can use this to identify techniques relevant to their environments and prioritize investment in improving security posture.

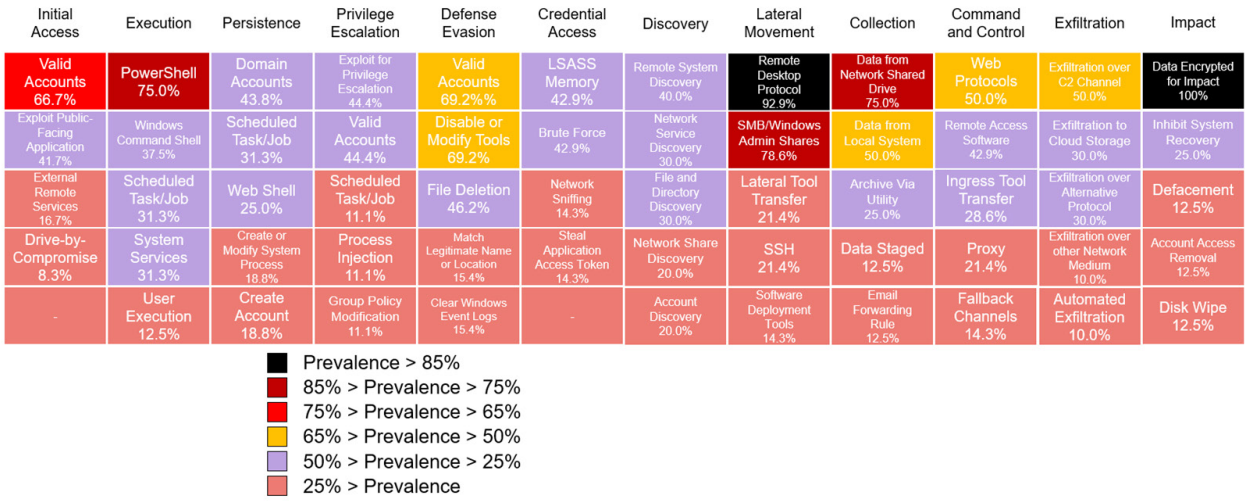


Figure 16: Heatmap of observed technique prevalence from investigated intrusions

Contributing Factors

Part of the FortiGuard IR team's investigation is to work with the customer to determine what the contributing factors were to the intrusion.

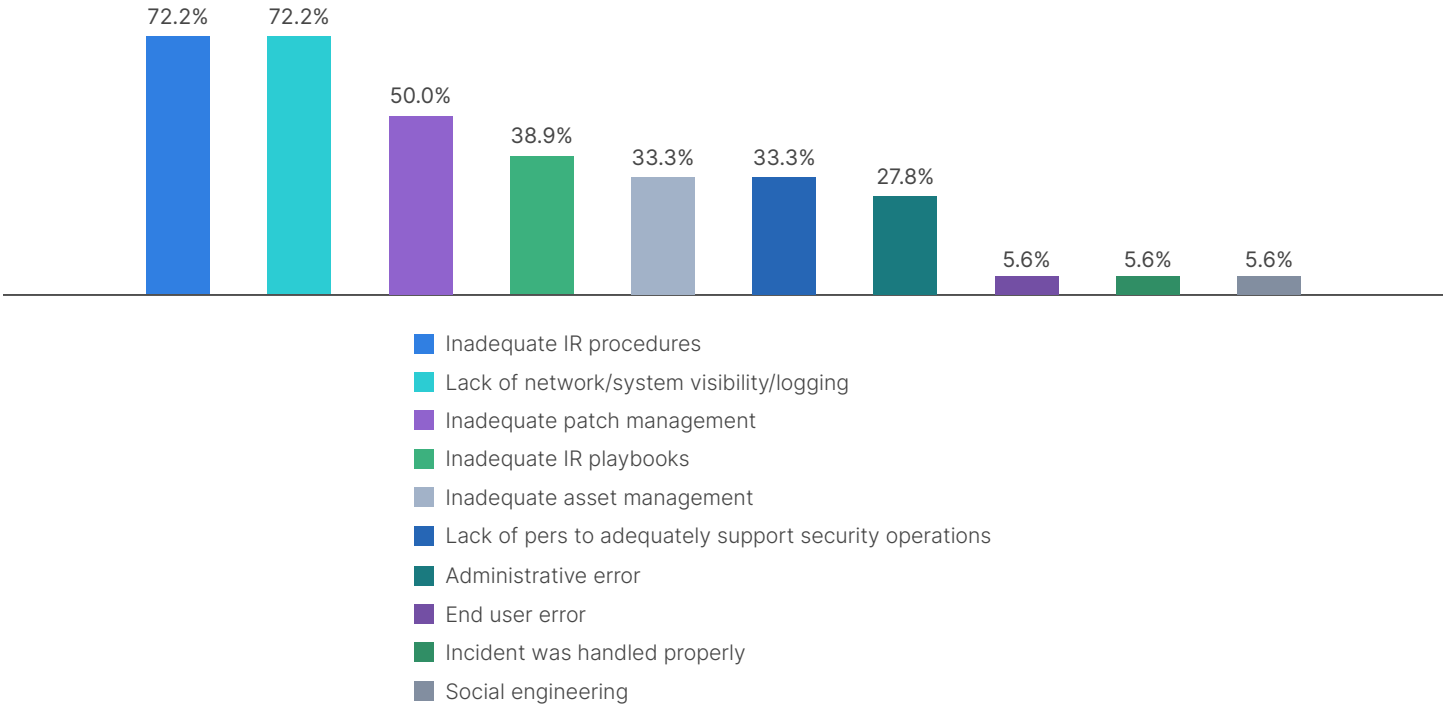


Figure 17: Contributing factors to observed incidents

This data gives insight into situations where the existing security solutions, procedures, and people were ineffective at detecting, mitigating, or responding to a security incident. Unlike metrics that may have a bias toward earlier stages of the kill chain where incidents may have been stopped, IR investigations give greater insight into contributing factors throughout the whole kill chain.

To best understand the main contributing factors observed by the team, let's outline the definitions of the top four contributing factors:

- Inadequate IR procedures: 72.2%
  - Organization knew what they needed to do but could not execute as desired. The victim organization did not know how to appropriately respond to an identified incident at the tactical level. This often resulted in incomplete mitigations or failing to adequately conduct triage during the early stages of an intrusion.
- Lack of network or system visibility or logging: 72.2%
  - The victim organization failed to adequately collect, centralize, or monitor known data sources that would have enabled them to detect an intrusion earlier than it was detected.
- Inadequate patch management: 50.0%
  - A known vulnerability with a readily available patch was exploited as part of the intrusion.
- Inadequate IR playbooks: 38.9%
  - Organization did not know if the activity they observed was an incident or did not know what to do when one was identified. The victim organization did not know how to appropriately respond to an identified incident at the operational level. This often resulted in a complete failure to identify a security incident and a lack of understanding of responsibilities in responding to an incident.

Top Four Contributing Factors

- Inadequate IR procedures (72.2%)
- Lack of network or system visibility or logging (72.2%)
- Inadequate patch management (50.0%)
- Inadequate IR playbooks (38.9%)

Despite it making investigations difficult from a digital forensics perspective and making investigation findings frustrating for victim organizations to hear, the lack of network or system visibility or logging is a conquerable problem. In many cases the team investigated, the victim organizations existing security or logging solutions had captured evidence of compromise weeks and months before engaging our team, but the victim organization did not have the centralization or monitoring capabilities setup that would have allowed them to respond to this evidence. The simple solution in these cases was to recommend a focus on growing visibility using existing resources to incorporate existing capabilities into the security team's workflows.

In other cases, organizations had invested in security solutions that had alerted them to indicators of compromise, but their response was inconsistent at scale or not commensurate with the threat they identified. For example, in one case we saw an organization respond to the initial detection of late-intrusion command and control indicators solely by implementing IP firewall blocks and hash-based AV blocks with no root cause investigation. In that example, the adversary responded with a fresh set of techniques and an increased operational tempo. In this case, our most important recommendation to the customer was to develop and formalize playbooks and procedures that would allow them to use their existing tools to more effectively and cohesively respond to a future incident rather than being forced into implementing mitigations for the first time during an incident.

As highlighted earlier in this report, the exploitation of known vulnerabilities with available patches continues to provide pathways for initial access. Additionally, the IR team observed known unpatched vulnerabilities being used to support lateral movement and privilege escalation. In many cases, these unpatched vulnerabilities were known by victim organizations at the time of the compromise and had been earmarked for decommissioning, but this decommission had never occurred. It is strongly recommended that organizations in a similar situation prioritize the decommissioning of legacy systems, especially when these systems contain vulnerable software known to be actively exploited. For reference, CISA maintains a database of known exploited vulnerabilities available here: Known Exploited Vulnerabilities Catalog. For new vulnerabilities, organizations should look at leveraging tools like FIRST EPSS to assist with prioritizing patches for their software.

Combatting Valid Account Abuse

The use of valid credentials was increasingly prevalent among IR engagements accounting for about 67% of Initial Access methods. This refers to investigations where the earliest adversary activity that could be linked to an intrusion is a logon with legitimate credentials. This can occur for several reasons, but the most likely are:

- Credentials were collected by the adversary through an earlier activity that could not be linked to an intrusion. For example, a credential harvesting campaign that went unreported prior to the incident.
- Credentials were purchased by the adversary from an access broker who gained victim credentials through a previous compromise.

The use of valid accounts gives adversaries a head-start as they bypass detection opportunities for early kill chain techniques that are often easier to detect. The use of valid accounts is also a Defense Evasion technique as it can be difficult to discern the legitimate use of legitimate credentials from threat actor use of legitimate credentials. This issue is exasperated where legitimate and adversary activities with the same valid account overlap. As highlighted in the above data, the use of Valid Accounts supports not just Initial Access (about 67% prevalence) and Defense Evasion (about 69% prevalence), but it also is used for Privilege Escalation (about 44% prevalence) and Persistence (about 56% prevalence). Additionally, the use of Valid Accounts enables the use of the most prevalent Lateral Movement techniques, T1021.001, Remote Desktop Protocol (about 93% prevalence), and T1021.002, SMB/Windows Admin Shares (about 79% prevalence).

The FortiGuard IR team has worked with the FortiRecon team to identify situations where an organization's credentials were for sale on the dark web prior to an intrusion. The use of services to perform external monitoring of an organization's attack surface, including leaked credentials associated with an organization for sale on the dark web, allows organizations to get ahead of access brokers and reset compromised credentials before they result in breaches.

The typical view of a cyber intrusion is that a threat actor will gain access to an environment by exploiting a vulnerability somewhere in the attack surface, drop some form of malware to maintain access, progress through the kill chain sequentially, and then perform their actions on objectives. As highlighted in the data contained in this report, when Valid Account access is made available to an adversary, this progression remains much less interesting. The typical intrusion observed by the FortiGuard IR team in this first half of 2023 looked more like this: The adversary logged in to a remote network device using Valid Account, laterally moved using RDP to endpoints within the victim environment, moved to endpoints hosting key data, and exfiltrated over RDP via direct copy, manually deployed ransomware on critical servers. As expected, this type of intrusion sidesteps many of the detections a SOC team may rely on to identify malicious behavior by hiding alongside benign behavior.

To better combat this, look to better understand and monitor standard user behavior. This understanding, combined with the segmentation of user privileges, can provide an effective way of detecting anomalies in user activity and minimizing impact when accounts inevitably get compromised. Typically, log aggregation and analysis present great opportunities for detecting anomalous user behavior and is even more effective when applied through a SIEM solution, like FortiSIEM, that supports custom visualization of user activity within a network. Some common anomalies that could be used to identify the majority of illegitimate use of valid accounts investigated by the FortiGuard IR team includes:

- Geographical anomalies, for example, a small U.S.-based organization won't likely have logins from overseas IP addresses.
- Temporal anomalies, for example, remote logins outside of business hours or the same user logging in to multiple endpoints within a short period of time.
- Behavioral anomalies, for example, standard end-users performing administrative tasks or remoting into production servers.

Building and Exercising Robust IR Playbooks (Operational Response) and Procedures (Tactical Response)

As highlighted in the contributing factors data, many organizations are still struggling to implement the correct countermeasures and validate the effectiveness of any countermeasures they do employ. Many organizations appear to see the pathway to improving their security posture as investing in more security solutions rather than building the processes and frameworks around optimizing the use of resources they already have within their environment.

Often organizations do not have the resources or the expertise within their internal SOC teams with the security team having specializations in a few key solutions but often a lack of experience or understanding of the bigger picture. Where this is the case, it's unrealistic to expect a security team to have the capacity to simultaneously maintain secure operations, integrate new technologies, and build a larger strategy for sequentially growing the security posture of their organization. In addition to this, security teams understandably have limited budgets as cybersecurity expenditure is often considered 'insurance' and rarely directly linked to an organization's profitability. Where organizations lack the internal knowledge, skillsets, or experience to build robust incident response plans, playbooks, and procedures, it is recommended they seek external help to ensure they are getting the most out of their existing resources and to shape future investment. When looking for external advice on this, organizations should ensure that provided advice is:

- Customized for their operating environment
- Built around industry best practices
- Actionable, with recommendations and tangible work products that fill an organization's gaps and work with existing internal processes

FortiGuard Labs offers a range of proactive services to meet the above needs, including support in the development of incident response plans (IRP), incident response playbooks, and incident response procedures. The team also offers security posture assessments and incident response readiness assessments (IRRA), when organizations are not aware of where they should prioritize investment in growing and formalizing their processes. The team's guidance follows best practices outlined in NIST 800-61 with additional local guidance where applicable. Strategic readiness services are also provided, such as network vulnerability assessments and penetration testing. Learn more here.

Understanding Collection Data Sources

Alongside descriptions of ATT&CK techniques, MITRE also provides a set of detections defined in terms of "data sources" composed of "data components." Organizations can assess their ability to detect a particular technique by determining if they are monitoring corresponding data sources. These data sources define key artifacts that contain characteristics that can indicate the use of a technique. Organizations should prioritize the collection, centralization, and monitoring of the data sources outlined in the table below as these correspond to majority of the techniques outlined in Figure 16 above:

Data Source ID	Data Source	Data Source Name
DS0002	User Account Creation	Windows Event Logs
DS0002	User Account Authentication	Windows Event Logs
DS0003	Scheduled Job Creation	Windows Event Logs
DS0009	Process Creation	Windows Advanced Auditing, Sysmon, EDR
DS0009	Process Metadata	Windows Advanced Auditing, Sysmon, EDR
DS0009	Process Termination	Windows Advanced Auditing, Sysmon, EDR
DS0009	Process Access	Sysmon, EDR
DS0011	Module Load	Sysmon, EDR
DS0012	Script Execution	Windows Command Line Auditing, EDR
DS0013	Host Status	RMM, Windows Event Logs, Sysmon, EDR
DS0015	Application Log Content	Windows Event Logs, Application Logs
DS0017	Command Execution	Windows Command Line Auditing, Sysmon, EDR
DS0019	Service Creation	Windows Event Logs, EDR
DS0019	Service Modification	Windows Event Logs, EDR
DS0019	Service Metadata	Windows Event Logs, EDR
DS0022	File Modification	Windows Advanced Auditing, EDR

Data Source ID	Data Source	Typical Data Source Provider
DS0022	File Creation	Windows Advanced Auditing, Sysmon, EDR
DS0022	File Deletion	Windows Advanced Auditing, Sysmon, EDR
DS0022	File Metadata	Windows Advanced Auditing, Sysmon, EDR
DS0022	File Access	Windows Advanced Auditing, Sysmon, EDR
DS0024	Windows Registry Key Modification	Windows Advanced Auditing, Sysmon, EDR
DS0024	Windows Registry Key Creation	Windows Advanced Auditing, Sysmon, EDR
DS0024	Windows Registry Key Deletion	Windows Advanced Auditing, Sysmon, EDR
DS0027	Driver Load	Windows Advanced Auditing, Sysmon, EDR
DS0028	Logon Session Creation	Windows Event Logs, EDR
DS0028	Logon Session Metadata	Windows Event Logs, EDR
DS0029	Network Connection Creation	Firewall Logs, Windows Advanced Auditing, Sysmon, EDR
DS0029	Network Traffic Flow	Firewall Logs, Windows Advanced Auditing, Sysmon, EDR
DS0029	Network Traffic Content	Firewall Logs, Windows Advanced Auditing, Sysmon, EDR
DS0033	Network Share Access	Firewall Logs, Windows Advanced Auditing, Sysmon, EDR

While these data sources don't protect against all techniques observed, they detect the majority and will allow organizations to prioritize consolidation of data sources already available in their environments.

Reframing defensive effectiveness: an alternative perspective

This helps organizations to build detection capabilities. But how can organizations plan to harden their networks from these techniques or evict an adversary employing one of these techniques? That role is better performed by using the lesser-known MITRE D3FEND framework in combination with the ATT&CK detection data sources.

MITRE D3FEND countermeasures are grouped into defender tactics; Model, Harden, Detect, Isolate, Deceive, and Evict. Countermeasures are described in terms of their relationship with the components of computer networks. MITRE ATT&CK techniques can also be described in terms of their relationships with these same computer network components. This common model aims to provide organizations with a finite list of D3FEND countermeasures that can support the detection and mitigation of an effectively infinite list of implementations of ATT&CK techniques.

The table below shows the MITRE D3FEND countermeasures that the FortiGuard IR team has identified as being relevant to the most prevalent techniques summarized in Figure 16 above.

D3FEND ID	D3FEND Tactic	D3FEND Technique	Typical Implementation
D3-FA	Detect	File Analysis	Logging, AV, EDR, Sandbox
D3-FR	Evict	File Removal	AV, EDR, SOAR, SOC
D3-AZET	Detect	Authorization Event Thresholding	Logging, SIEM, SOAR, SOC
D3-NTCD	Detect	Network Traffic Community Deviation	Logging, IPS, NDR, SIEM, SOC
D3-NTF	Isolate	Network Traffic Filtering	IPS, NDR, NAC, SOC
D3-PHDURA	Detect	Per Host Download-Upload Ratio Analysis	Logging, IPS, NDR, SIEM, SOC
D3-PMAD	Detect	Protocol Metadata Anomaly Detection	IPS, NDR, SIEM, SOC
D3-RTSD	Detect	Remote Terminal Session Detection	Logging, EDR, SIEM, IPS, NDR, SOC
D3-UGLPA	Detect	User Geolocation Logon Pattern Analysis	Logging, IPS, NDR, SIEM, SOC
D3-EAL	Isolate	Executable Allow listing	AV, EDR, AppLocker

D3FEND ID	D3FEND Tactic	D3FEND Technique	Typical Implementation
D3-EDL	Isolate	Executable Deny listing	AV, EDR, AppLocker
D3-PSA	Detect	Process Spawn Analysis	Logging, EDR, SIEM, SOC
D3-DA	Detect	Dynamic Analysis	EDR, Sandbox
D3-FCA	Detect	File Creation Analysis	Logging, AV, EDR, SIEM
D3-CAA	Detect	Connection Attempt Analysis	Logging, AV, EDR, IPS, NDR, SIEM, SOC
D3-PLA	Detect	Process Lineage Analysis	Logging, EDR, SIEM
D3-PSMD	Detect	Process Self-Modification Detection	EDR
D3-PS	Evict	Process Suspension	AV, EDR, SOAR, SOC
D3-PT	Evict	Process Termination	AV, EDR, SOAR, SOC
D3-SCA	Detect	System Call Analysis	EDR, Sandbox
D3-SCF	Isolate	System Call Filtering	EDR
D3-AL	Evict	Account Locking	SOAR, NAC, SOC
D3-DAM	Detect	Domain Account Monitoring	Logging, NAC, SIEM, SOC

Organizations should maintain the ability to implement these countermeasures to ensure they are in the best position to combat the majority of observed techniques. Alongside these techniques is a rough indicator of the technologies that organizations may already have that can likely be leveraged to employ each countermeasure. Different vendor solutions may have varying capabilities so organizations should seek advice from their vendors to determine their solution capabilities.

Summary Recommendations

Organizations should prioritize understanding the countermeasure capabilities provided by their existing security solutions and focus on optimizing the use of existing resources rather than patching apparent gaps with new technologies. At the more tactical level, organizations should also ensure they can identify anomalies in the use of valid accounts to both access and operate within their environments.

As highlighted in this report, most of the contributing factors to incidents we responded to could have been mitigated through the consolidation of existing solutions and a bigger investment in the procedures that support incident response and network monitoring. Formalizing and exercising playbooks and tactical procedures to ensure response to an incident is swift and efficient would contribute more to an organization's response effectiveness than the inclusion of another underutilized security solution. A refocus on collecting data sources associated with detecting relevant techniques using existing solutions or free alternatives would also put organizations in good stead to take the fight back to the threat actors we have observed.

Conclusion

The first half of 2023 has been a busy year for defenders across the globe, with waves of critical vulnerabilities in network devices, public-facing applications, and desktop applications highlighting holes in organizations' defenses and testing our responses. While these vulnerabilities and the subsequent threat intel reporting provide timely tactical intelligence that allows us to take action against immediate threats, we should ensure that we don't lose focus on opportunities to make lasting improvements to our defenses.

In addition to the waves of vulnerabilities, we have continued to see the maturing of the ransomware and extortion ecosystem. As this ecosystem matures, we can expect to see the TTPs employed throughout the ecosystem homogenize. This is the same phenomenon we see in other industries, where the most efficient approaches to scaling a business are adapted by other businesses. As this scaling and standardization occurs, we need to identify trends used at scale as part of this standardization to prevent us from fitting into the standard victim profile.

This report has provided a number of broad recommendations that organizations can take to improve their approach to shoring up potential gaps in their defenses. While these changes mostly paraphrase industry best practices, they aim to provide approachable recommendations that can be iteratively implemented and built upon using an individual organization's existing solutions, rather than recommending investment in something new.

Appendix

This appendix includes additional information to add context to the data depicted in this report. It provides demographics of the victims whose incidents we investigated and outlines some biases associated with the provided data.

Demographics

Industry

The FortiGuard IR team provides support to organizations across a broad range of industries.

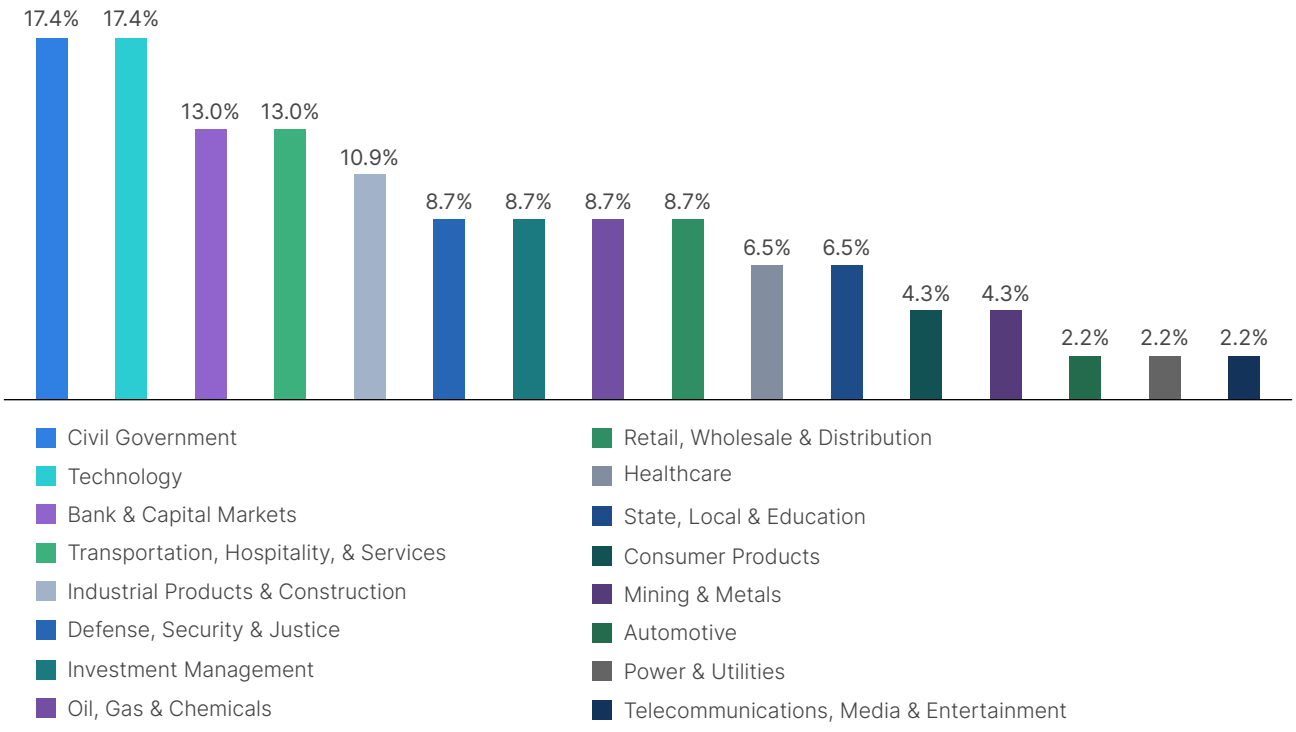


Figure 18: Victim industry for investigated incidents

Tracking industries gives the FortiGuard IR team insight into emerging trends across industries rather than those focused on just one industry. While looking at threats targeting an individual industry can provide additional scope for narrowing the focus of a defensive approach, many of the threats observed by the FortiGuard team bridged industries. This was especially evident when looking at financially motivated threat groups (such as ransomware and extortion groups) that appear to mostly select opportunistic targets based on available initial access options rather than targeting a particular industry.

Note: Given that this data is only taken from IR investigations performed by the FortiGuard IR team, generalizations cannot be applied to year-on-year changes in industry victimology. For example, the fact that there were more intrusions investigated by the FortiGuard IR team targeting civil government organizations in H1 2023 than H2 2022 does not necessarily indicate that these organizations were more targeted in this half of the year than last year.

Region

The FortiGuard IR team supported victims from all major regions across the globe.

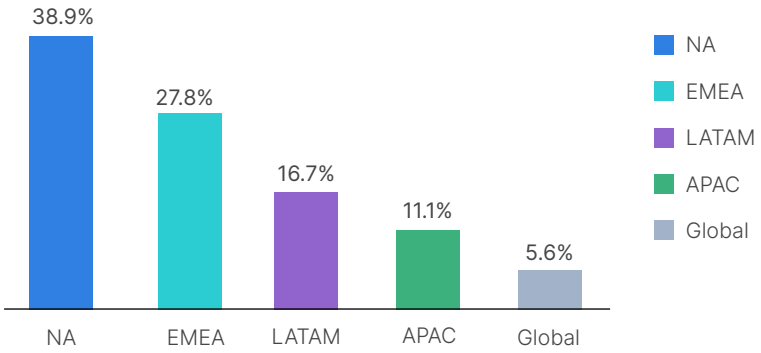


Figure 19: Victim region for investigated incidents

Note: This data should not be used to conclude that EMEA received 21% more cyber intrusions than LATAM, but simply that the FortiGuard IR team investigated more incidents in EMEA-based organizations than LATAM-based organizations.

Data Biases

The data contained in this report regarding the most prevalent techniques observed and the contributing factors to victim organizations' compromises over the last six months is based entirely on direct observation by the FortiGuard IR team. As a result, the insights taken from this data only represent a subset of all global intrusions over this period.

Additionally, not all IR engagements performed by the team involved a complete forensic investigation and many investigations could not be completed due to lack of forensic evidence (inhibiting detection of early kill chain evidence). It is for this reason that technique data is provided in the form of a prevalence. This prevalence reflects how often a particular technique was observed where at least one technique within a particular tactic was observed. For example, the Persistence technique T1505.003 – Server Software Component: Web Shell was considered 25.0% prevalent, meaning that it was observed in 25.0% of investigated intrusions where a Persistence technique was observed. Presenting the data in this format aims to reduce the bias caused by incomplete investigations.

[1] FortiGuard Labs, "SolarView Compact Command Injection Vulnerability," FortiGuard Outbreak Alerts, accessed September 10, 2023.

[2] FortiGuard Labs, "Zoho ManageEngine RCE Vulnerability," FortiGuard Outbreak Alerts, accessed September 10, 2023.

[3] FortiGuard Labs, "Progress MOVEit Transfer SQL Injection Vulnerability," FortiGuard Outbreak Alerts, accessed September 11, 2023.

[4] FortiGuard Labs, "Oracle WebLogic Server Vulnerability," FortiGuard Outbreak Alerts, accessed September 10, 2023.

[5] FortiGuard Labs, "PaperCut MF/NG Improper Access Control Vulnerability," FortiGuard Outbreak Alerts, accessed September 10, 2023.

[6] FortiGuard Labs, "Apache RocketMQ Remote Command Execution Vulnerability," FortiGuard Outbreak Alerts, accessed September 10, 2023.

[7] CISA, "Malicious Actors Exploit CVE-2023-27350 in PaperCut MF and NG," Cybersecurity Advisory, accessed September 09, 2023.

[8] Microsoft, "Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets," Threat intelligence, accessed September 09, 2023.

[9] Ibid.

[10] "SigmaHQ/sigma/powwershell," GitHub, accessed September 10, 2023.

[11] "Sysmom v15.0," Microsoft, accessed September 10, 2023.

[12] Defender Control, softonic, accessed September 10, 2023.

[13] Asaf Gilboa, "LSASS Memory Dumps are Stealthier than Ever Before," deep instinct, January 24, 2021.

[14] Advanced Port Scanner, Famatech, accessed September 10, 2023.

[15] Advanced IP Scanner, Famatech, accessed September 10, 2023.

[16] "Implementing Application Control," Australian Cyber Security Centre, October 6, 2021.

[17] "What is a Port Scan?" Fortinet, accessed September 10, 2023.

[18] "Allow log on through Remote Desktop Services," Microsoft, accessed September 10, 2023.

[19] Yuval Lazar, "135 is the new 445," Pentera, September 13, 2022.

[20] FortiGuard Labs, Premium Services, accessed September 10, 2023.

[21] Fortinet, FortiRecon – Adversary Centric Intelligence, accessed September 11, 2023.

[22] "About rclone," Rclone, accessed September 10, 2023.

[23] MEGA, accessed September 10, 2023.

[24] "SigmaHQ/sigma/process creation," GitHub, accessed September 10, 2023.

[25] "SigmaHQ/sigma/rclone execution," GitHub, accessed September 10, 2023.

[26] "Stop Ransomware," CISA, accessed September 10, 2023.

October 17, 2023 2:52 PM

2322955-0-0-EN