
2023

# MITIGATING CYBER RISKS WITH MITRE ATT&CK

## Expert Recommendations From Unit 42

# Recommendations to Mitigate Specific Attacker Capabilities Based Upon MITRE ATT&CK® Tactics

Modern threat actors behind ransomware and extortion incidents are coming up with new tactics, techniques and procedures (TTP) to more keenly impact their victims, coercing them to pay extortion fees. Although recovering from offline backups that have been tested can provide some protection against encryption-only ransomware attacks, organizations must take additional measures to prepare for threat actors who extort victims by stealing data, disrupting operations, and engaging in other forms of harassment.

To this end, the Unit 42 team has examined our incident response data from ransomware and extortion incidents to identify TTPs we see most commonly. We offer a detailed view of what we've observed, as well as a set of hand-crafted recommendations for addressing them. These have been split into strategy and practitioner-focused recommendations to help you put these insights into action.

To provide a common language for threat actor behavior, we've mapped these TTPs to the MITRE ATT&CK framework. While we've seen many additional tactics beyond what we've listed here, this report focuses on what we observed most frequently. Some techniques are mapped to multiple tactics within the framework, but only one is listed here for conciseness.

# WHAT IS MITRE ATT&CK?

The MITRE ATT&CK framework provides a common language for describing threat actor behavior. It organizes specific tactics and techniques into a taxonomy.

Throughout this report, various MITRE ATT&CK tactics and techniques are referenced by ID and name in association with threat actors' objectives, capabilities and methods. You can search for the referenced ID (e.g., tactic TA0003, technique T1486) and/or name in the MITRE ATT&CK knowledge base to learn more about specific adversary behaviors discussed in this report.

# Table of Contents

# Initial Access (TA0001)

Initial access techniques cover how threat actors get into networks in the first place. The approaches listed below are the most common ways we see threat actors sneaking into organizations' environments.

## Capabilities Most Commonly Used for Initial Access (TA0001)

- **T1210: Exploitation of Remote Services**
  Exploitation of remote services remains the most prevalent technique Unit 42 researchers see for initial access into organizations' environments by ransomware and extortion threat actors. Most commonly, we identified exploitation of software vulnerabilities related to initial unauthorized access in ransomware investigations. Once inside the victim's network, threat actors continued their exploitation activities to gain access to additional systems within the environment.

- **T1110: Brute Force**
  Unit 42 researchers have continued to see initial access to organizations' environments by threat actors via brute force attacks on internet-facing resources, often Windows systems with Remote Desktop Protocol (RDP) directly exposed to the internet, with only single-factor authentication. These attacks generally employ sub-techniques such as password guessing (T1110.001), password spraying (T1110.003) and/or credential stuffing (T1110.004).

- **T1566: Phishing**
  Phishing via malicious attachments remains a common initial access vector for ransomware and extortion incidents (especially sub-technique T1566.001: Phishing: Spearphishing Attachment).

- **T1078: Valid Accounts**
  Unit 42 researchers have observed threat actors using previously compromised and default valid account credentials to initially access organizations' environments.

- **T1608.006: Stage Capabilities: SEO Poisoning**
  *(This is technically associated with tactic TA0042: Resource Development, but has been included here because of its association with initial threat actor access into organizations' environments)*
  While not always clearly directly related to ransomware incidents, we have frequently observed SEO poisoning used as an initial access vector into victims' environments when investigating ransomware and extortion incidents.

# RECOMMENDATIONS

## INITIAL ACCESS (TA0001)

### Strategy Focused Recommendations

Looking critically at how most attacks we see start off, valid credentials are often a part of the initial access chain of events. Whether it be through brute forcing, phishing or default credentials, having exposed services in combination with compromised credentials launches a threat actor's path to success.

The risk of these access vectors can be reduced by establishing the following authentication sanitizing practices.

- Rotating user account passwords and removing expired accounts.
- Documenting procedures on how to handle accounts for newly deployed hardware and software.
- Having technical controls that address logins that put users in "impossible travel" scenarios, where login and MFA attempts appear to place them in two places at once.

There are also well-established processes for finding exposed remote services, like scanning your external networks and keeping an inventory of the devices and services that are exposed. You can also leverage software that helps identify unsanctioned remote access solutions installed on endpoints. These tools are sometimes installed by threat actors to gain unauthorized remote access to systems.

## Practitioner Focused Recommendations

The bigger the environment and more diverse the systems and infrastructure, the bigger the overall challenge in managing employee access. Protecting an organization from external attacks starts with understanding what you're protecting in the first place.

Attack Surface Management (ASM) is key to keeping a handle on what services a threat actor could target with stolen credentials, or what risky exposures could hit you the hardest, including software vulnerabilities.

When the Unit 42 team investigates ransomware and extortion incidents, we leverage Cortex Xpanse to help understand an organization's external attack surface. This helps us make informed decisions about where to focus our investigative efforts, since risky exposures or vulnerabilities might have served as the initial access vector for compromise. We also use ASM to find areas where a threat actor could attempt to regain access to the environment, ensuring full and effective containment.

Endpoint security tools (e.g., EDR or XDR) are effectively becoming standard in every organization the Unit 42 team works with. However, these tools are not always fully deployed or configured appropriately.

It is critical that endpoint security solutions are properly connected to—and leveraging—threat intelligence and behavioral analytics in the battle against phishing attacks. The dynamic nature of phishing payloads in most successful attacks means default XDR configurations won't stop all threats.

As a fail-safe, the Unit 42 team deploys Cortex XDR in ransomware and extortion incidents. This platform is connected to a comprehensive threat intelligence library including behavioral IoCs to help detect and shut down payloads that have made it onto compromised systems.

# Discovery (TA0007)

Once inside a network, threat actors will attempt to understand what's there. Techniques used for discovery allow threat actors to gain a sense of the systems and assets that they can access after gaining unauthorized entry.

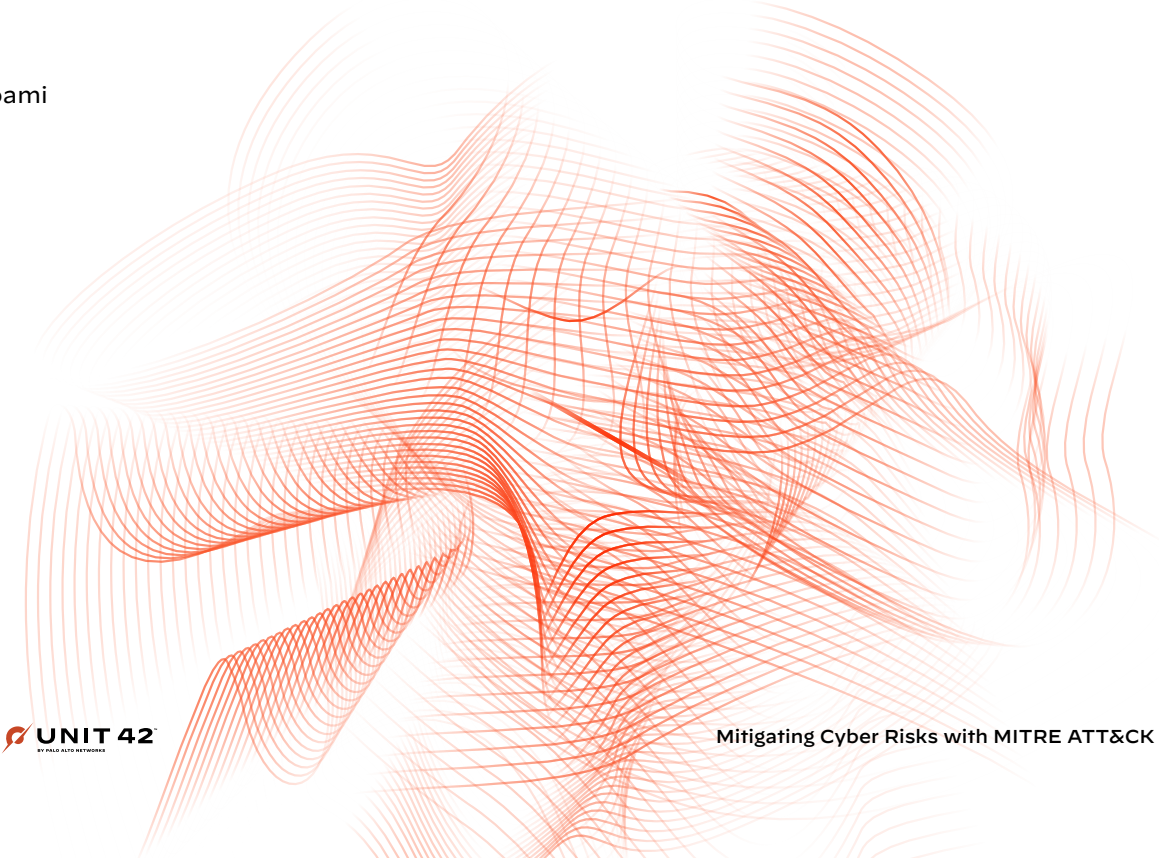
## Capabilities Most Commonly Used for Discovery (TA0007)

- **T1018: Remote System Discovery**
  Unit 42 researchers frequently observe threat actors enumerating remote systems, whether by hostname or IP address, for lateral movement opportunities.
- **T1033: System Owner/User Discovery**
  Threat actors in ransomware and extortion incidents attempt to discover the currently and/or recently logged in user(s) on a system. This tactic is particularly prevalent on hosts related to the initial unauthorized access vector, and is frequently automated by various types of malware.
- **T1046: Network Service Discovery**
  Threat actors use tools to identify open ports and services on hosts in a victim's network.
- **T1069: Permission Groups Discovery**
  Threat actors commonly enumerate users and groups to identify those that have administrative privileges, including local (T1069.001) and domain (T1069.002) groups.
- **T1087: Account Discovery**
  Threat actors routinely attempt to identify administrative accounts for privilege escalation, whether local (T1087.001) or domain (T1087.002) accounts.
- **T1135: Network Share Discovery**
  Threat actors enumerate shared folders and drives to identify information sources for later Collection (TA0009).

- **T1482: Domain Trust Discovery**
  We routinely observe threat actors gathering information about domain trust relationships to identify opportunities for lateral movement (and eventual privilege escalation).

Unit 42 researchers have most commonly seen these tools used by threat actors for discovery:

- Advanced IP Scanner
- Advanced Port Scanner
- AdFind
- BloodHound (and related variants, e.g. SharpHound)
- Cobalt Strike
- Net
- Nltest
- Nmap
- Ping
- Whoami



# RECOMMENDATIONS

## DISCOVERY (TA0007)

### Strategy Focused Recommendations

Even in situations where attackers already know significant information about their target, they will often perform additional discovery techniques once inside the network. This allows them to gain an understanding of what additional resources they could gain access to.

This discovery phase is a great opportunity for organizations to discover early signs of post-exploitation activity. However, it can be challenging to find the right balance of detection to avoid overwhelming your security operations center (SOC) with false-positive alerts.

Noisier and less stealthy attackers could be easier to detect, since they often bring in tools from outside of the environment (such as scanning tools and Active Directory enumeration tools). These tools could trigger existing security systems as anomalous activity. Strong software policies—like using Windows AppLocker or platforms that bring in controls for banned/approved software—can help alert on and shut down early discovery activity.

More savvy attackers prefer to use tools that already exist in the environment to avoid detection. These are often referred to as "living off the land" binaries (LOLBins). Leveraging built-in utilities such as whoami, net and nltest enables attackers to hide among the noise of legitimate activity executed by system administrators and trusted applications.

In order to detect this activity, leverage security tools with the ability to develop a baseline of normal activity in the environment. This allows you to ensure that anomalous activity that could be associated with threat actor discovery is detected and prevented.

## Practitioner Focused Recommendations

Since threat actors often leverage LOLBins to perform internal discovery, endpoint security tools like Cortex XDR can help detect anomalous activity by establishing a baseline of normal user activity in your environment. This can include the types of applications people run on a daily basis, or the resources accessed to perform tasks. This means that if a normal user account attempts to run a network scanning utility they've never executed before, the SOC will be notified of the activity.

When the SOC needs to triage an alert, it is important that they have quick access to the data they need to piece together a potential security incident. This sometimes requires quickly analyzing artifacts on multiple systems. Leveraging Cortex XDR with forensic data collection and analysis capabilities can help expedite this process.

However, if threat actor discovery activity is detected, it's too late. The threat actor already has the information needed to plan their next steps. This is one of many areas where proper segmentation in an environment is critical.

Leveraging network segmentation with SD-WAN capabilities that can tightly control and (better yet) inspect traffic between network segments means you're confining the threat actor to a smaller footprint. If they cannot see systems during discovery, they're less likely to target those systems in their attack. Furthermore, implementing Prisma secure access service edge (SASE) in your environment means slowing down (or potentially stopping) a threat actor from discovering the targets of greatest interest.

# Persistence (TA0003)

In matters of malware, persistence means maintaining access. To accomplish their illicit goals over a period of time, threat actors use techniques to stay in the network even if passwords change, systems restart or defenders begin trying to evict them.

## Capabilities Most Commonly Used for Persistence (TA0003)

- **T1053.005: Scheduled Task/Job: Scheduled Task**
  Unit 42 researchers have identified scheduled tasks being created by threat actors to recurrently execute malicious code.
- **T1098: Account Manipulation**
  Threat actors often modify account permissions and/or credentials. Numerous domain administrators have informed the Unit 42 team that upon their discovery of a security incident, they were unable to log in using their administrative credentials because the threat actor changed them.
- **T1136: Create Account**
  Threat actors create accounts, including local (T1136.001) or domain (T1136.002) accounts, in order to retain persistent access to systems or other resources in victims' environments.
- **T1505.003: Server Software Component: Web Shell**
  We observe threat actors leveraging web shells as a means of obtaining persistent, backdoor access to victims' internet-facing servers—particularly Microsoft Exchange servers. We frequently identify web shells in cases involving exploitation of Microsoft Exchange vulnerabilities.
- **T1543.003: Create or Modify System Process: Windows Service**
  Threat actors commonly install malicious services or modify existing processes on Windows systems.
- **T1547.001: Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder**
  Windows Registry run keys are frequently modified to automatically launch malicious programs or scripts.

# RECOMMENDATIONS

## PERSISTENCE (TA0003)

### Strategy Focused Recommendations

Most of the tactics we see used for persistence have been around for well over a decade. We see ransomware threat actors using time-tested tactics such as creating new scheduled tasks, leveraging autostart services, and both creating and manipulating existing user accounts.

As new techniques are deployed by threat actors, new methodologies are continuously created to detect and prevent tactics used by threat actors, such as new persistence mechanisms or execution techniques. However, Unit 42 researchers continue to see instances where over-permissioned accounts are able to create persistence mechanisms by changing registry keys or other system settings.

Endpoint security solutions that evaluate the entire process execution tree and associated system actions can help detect or prevent persistence mechanisms from being created on compromised systems. Beyond XDR sweeps, looking into and thinking critically about how to change user and application group permissions and structures can often add significant hurdles to make an attacker's job harder.

## Practitioner Focused Recommendations

Even with XDR technologies helping to remove the burden of identifying common persistence mechanisms, it's still useful to consider detecting them at the next level up. This further reduces the likelihood of threat actor success, and protects network segments unable to take full advantage of XDR technology.

This is where we zoom in on the significant advantages of Palo Alto Networks Next-Generation Firewalls (NGFW) that are paired with high fidelity threat intelligence. Both NGFWs and cloud-delivered security services (CDSS) with inline SSL decryption, provide visibility into malicious actions as they are in flight from threat actors to endpoints. They also provide the chance to trigger on binaries and malicious code and/or scripts before they even make it to the endpoint.

# Defense Evasion (TA0005)

Most organizations have some form of cybersecurity measures set up to prevent threat actors from achieving their goals. Threat actors have also developed techniques to avoid, bypass or disable these defenses. These are the approaches we see most commonly in ransomware and extortion incidents.

## Capabilities Most Commonly Used for Defense Evasion (TA0005)

- **T1027: Obfuscated Files or Information and T1140: Deobfuscate/Decode Files or Information**
  Threat actors routinely encode or otherwise obfuscate commands, variables, file names as well as other information to evade detection and make it more challenging to determine the functionality of malicious commands (TA1059: Command and Scripting Interpreter) and scripts. Base64 encoding, XOR and compression (often combined) are common obfuscation techniques observed by Unit 42 researchers. Binary padding is also a semi-prevalent technique.
- **T1055: Process Injection**
  We routinely identify evidence of various sub-techniques of process injection in ransomware and extortion incidents, often associated with post-exploitation tools such as Sliver or Cobalt Strike.
- **T1218.011: System Binary Proxy Execution: Rundll32**
  Threat actors often use rundll32.exe to execute malicious payloads in ransomware and extortion incidents. This is commonly seen in association with post-exploitation tools such as Cobalt Strike.
- **T1562: Impair Defenses**
  Threat actors routinely modify victims' environments to impair or entirely disable security measures. Most commonly, this takes the form of disabling or removing antivirus or other endpoint security tools (T1562.001), but it can also include adding exceptions to the host firewall (T1562.004) and leveraging older versions of PowerShell to limit defender visibility (e.g. T1562.010: Downgrade Attack).
- **T1620: Reflective Code Loading**
  We often identify code that has been reflectively loaded into a process to hide malicious payload execution. This is particularly seen in association with post-exploitation tools such as Cobalt Strike.

# RECOMMENDATIONS

## DEFENSE EVASION (TA0005)

### Strategy Focused Recommendations

Cortex XDR solutions leveraged by experienced analysts are helpful in combating common defense evasion techniques leveraged by threat actors. It's certainly true that threat actors will find their way to systems that allow them to change or outright remove endpoint protections, so keep close watch on those systems. Be sure to leverage privileged access workstations (PAWS) when working with sensitive systems like those that control endpoint security solutions.

It's important to keep your team well trained, ensuring that they have access to the right threat intelligence feeds to facilitate hunting and detections. The specific threat actor tradecraft changes rapidly in this space.

Even when looking at core concepts like obfuscation and process injection, you need a strong combination of a quality XDR to help find atypical events as they're occurring, and a well-versed team that knows when to dig deeper into those events.

## Practitioner Focused Recommendations

Defense evasion is demanding when competing with modern day post-exploitation frameworks like Cobalt Strike or Brute Ratel C4. These frameworks are designed with specific purposes, one of which is bypassing defenses to carry out attacks.

Offensive security teams are constantly working to build and enhance the scripts that plug into PowerShell-based post-exploitation frameworks to find new ways to stay ahead of defensive teams. Unfortunately, innovation in defense evasion techniques is something threat actors take advantage of when they use these tools to carry out ransomware and extortion attacks.

The chain of events around process injection, reflective code loading and system binary proxy execution often makes it difficult to follow and determine whether what is taking place is bad, or really bad. When the Unit 42 team investigates more complex ransomware incidents, having access to a full causality chain in Cortex XDR is invaluable for cutting down on the time it takes to fully understand and stop an attack.

# Credential Access (TA0006)

Threat actors can do more damage if they have more access, so one of their key goals after breaching a system is to obtain credentials and escalate privileges to take them deeper into the network they are targeting.

Imagine a burglar trying to rob a bank. Accessing the front door is only the first step. The criminal's true goal is accessing the bank vault. Similarly, cybercriminals seek the credentials that will give them more access to more valuable assets and enable greater impact.

## Capabilities Most Commonly Used for Credential Access (TA0006)

- **T1003.001: OS Credential Dumping: LSASS Memory**
  Unit 42 researchers frequently observed threat actors accessing the Windows Local Security Authority Server Service (LSASS) process memory to obtain credential data.

We have most commonly seen these tools used by threat actors for credential access:

- Mimikatz
- LaZagne
- Impacket secretsdump
- Procdump targeting the LSASS process
- Multifunctional post-exploitation tools (e.g. Cobalt Strike)

# RECOMMENDATIONS

## CREDENTIAL ACCESS (TA0006)

### Strategy Focused Recommendations

A number of the tools that we observe in engagements rely heavily on PowerShell to achieve success in organizations' environments. Modern implementations of tools like Mimikatz and Impacket frequently leverage PowerShell to compromise and use credentials.

Unfortunately, in incident response engagements, we frequently find that PowerShell is not appropriately controlled to limit risk. Consider implementing PowerShell's constrained language mode, and blocking the binaries themselves from executing on systems that have no valid use cases for PowerShell. The combination of these two actions via group policy alone can significantly reduce overall risk.

## Practitioner Focused Recommendations

Cortex XDR leverages heuristic detections and behavioral indicators to trigger on both the atypical use of PowerShell in an environment, as well as on the security tools themselves when they are leveraged. That is to say, your team has a chance to catch a threat actor both when they bring a tool into the environment and again when the tool is executed.

While the signatures for the tools themselves change, the behavioral actions tend to be more consistent. This allows your enterprise to catch Mimikatz and Impacket as well as general post-exploitation frameworks leveraging PowerShell.

# Lateral Movement (TA0008)

To achieve their goals, threat actors often need to move through multiple systems and accounts within a network. Lateral movement refers to the techniques they use to move within a victim's environment.

## Capabilities Most Commonly Used for Lateral Movement (TA0008)

- **T1021.001: Remote Services: Remote Desktop Protocol**
  Lateral movement via the RDP remains the most prevalent technique used by ransomware threat actors for lateral movement in victims' networks between Windows systems.

# RECOMMENDATIONS

## LATERAL MOVEMENT (TA0008)

### Strategy Focused Recommendations

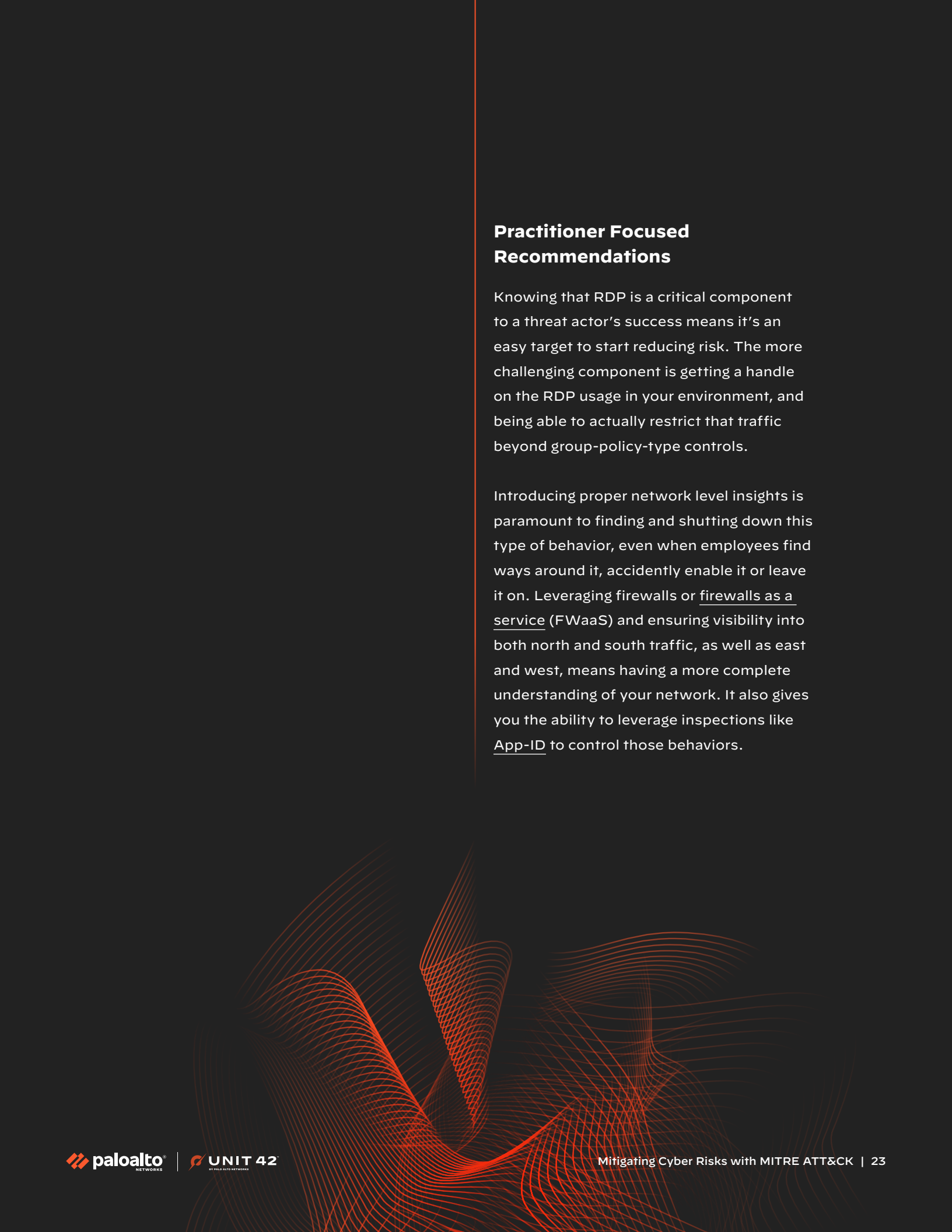
RDP continues to be the most impactful method used by threat actors for lateral movement once inside a network. This method tends to be so prevalent inside of organizations' environments that the attackers can go undetected while still having a significant range of capabilities.

These capabilities include tunneling the RDP back outside of the environment to easily move around, while easily taking screenshots and copying back data via the clipboard. Limiting RDP use can be a daunting project, but starting with an initial focus on leveraging PAWS along with trusted routes between critical and sensitive systems dramatically reduces the efficacy of unauthorized lateral movement inside of a network.

## Practitioner Focused Recommendations

Knowing that RDP is a critical component to a threat actor's success means it's an easy target to start reducing risk. The more challenging component is getting a handle on the RDP usage in your environment, and being able to actually restrict that traffic beyond group-policy-type controls.

Introducing proper network level insights is paramount to finding and shutting down this type of behavior, even when employees find ways around it, accidently enable it or leave it on. Leveraging firewalls or firewalls as a service (FWaaS) and ensuring visibility into both north and south traffic, as well as east and west, means having a more complete understanding of your network. It also gives you the ability to leverage inspections like App-ID to control those behaviors.



# Command & Control (TA0011)

Command and control (C2) techniques allow threat actors to communicate with the systems they're trying to control.

## Capabilities Most Commonly Used for Command & Control (TA0011)

- **T1219: Remote Access Software**
  Threat actors often leverage desktop support and other administrative tools to remotely access victims' systems. Such tools are not inherently malicious and therefore are not generally prevented. They are not typically detected by traditional antivirus solutions.
- **T1572: Protocol Tunneling**
  Unit 42 researchers have observed threat actors repeatedly using post-exploitation tools to tunnel network traffic in order to conceal it and evade detection, most commonly disguising it as legitimate web traffic. We have also observed comparable activity in conjunction with the Proxy (T1090) and Data Obfuscation (T1001) techniques. Beyond multi-functional post-exploitation tools, we have also observed the use of simpler tools such as Chisel and GO Simple Tunnel (GOST).

We have most commonly seen these tools used by threat actors for C2:

**Post-exploitation tools:**

- Cobalt Strike
- Metasploit
- Sliver
- Brute Ratel

**Administrative tools (abused by threat actors)**

- AnyDesk
- ConnectWise/ScreenConnect
- LogMeIn
- PuTTY
- Splashtop
- TeamViewer
- TightVNC

# RECOMMENDATIONS

## COMMAND & CONTROL (TA0011)

### Strategy Focused Recommendations

There is a reason that remote access software and protocol tunneling are so prevalent in the ransomware incidents investigated by Unit 42. These tactics simply work and are easy for threat actors to leverage.

When looking at the use of remote access software, threat actors are living in a grayware world of using legitimate remote access toolkits for malicious purposes. Having a strong sense of your software inventory and what is and isn't allowed can help make these tools quickly stick out when installed on an endpoint.

As it relates to protocol tunneling, we often find that all a threat actor needs to do is send their C2 traffic over a legitimate HTTPS channel, and it can easily pass undetected. Decrypting and inspecting traffic on at least the most sensitive parts of your network will enable you to identify malicious traffic that is traversing over a legitimate-looking protocol.

## Practitioner Focused Recommendations

Most environments that we work with are incredibly diverse, including on-premise data centers and cloud service providers to provide services for both distributed offices and an employee population that works remotely. As a result, network visibility as a whole is challenging, leading to gaps that offer attackers opportunities to maintain strong footholds.

A focus on the benefits of a SASE model is a worthwhile investment. Prisma SASE takes an approach that places emphasis on securing all data and all platforms, no matter where they reside.

Adding in visibility for cloud data, provided via cloud access security brokers (CASB), allows stronger insight into what kind of data is at risk and what your normal access patterns look like. Focus on getting all user traffic into an environment with more comprehensive SD-WAN capabilities.

The benefits of adding in a platform such as Prisma SASE enables you to have greater visibility into daily user connections. It also allows you to have controls over sanctioned and unsanctioned traffic, and it pulls in the ability for you to inspect HTTPS traffic across the organization. This ultimately leads to quicker detection—if not prevention—of C2 activity.

# Exfiltration (TA0010)

Exfiltration is the step threat actors take to steal data. We see this increasingly in ransomware matters due to gangs' growing reliance on double extortion, data theft, and dark web leak sites.

## Capabilities Most Commonly Used for Exfiltration (TA0010)

- **T1567.002: Exfiltration Over Web Service: Exfiltration to Cloud Storage**
  Unit 42 researchers routinely observe threat actors who acquire victims' data (often associated with the data theft extortion tactic) and upload it directly to cloud storage services. Sometimes threat actors have even used an alternative account with a cloud storage provider already used by the victim to evade detection (T1537: Transfer Data to Cloud Account).

We have seen these tools and cloud storage services used by threat actors for exfiltration:

**Services**

- MEGA
- Google Drive
- Dropbox
- pCloud
- OneDrive
- DropMeFiles
- Sendspace
- Files.io
- Web-based email services (e.g., ProtonMail, Gmail)

**Tools**

- Rclone
- WinSCP
- FileZilla
- Cloud-service-specific tools (e.g., MEGAsync, pCloud App, Google Drive for desktop, etc.)

# RECOMMENDATIONS

## EXFILTRATION (TA0010)

### Strategy Focused Recommendations

Cloud storage is by far and away the chief method for data exfiltration. While we still observe instances of clipboard-style data theft, the volume of data in exfiltration has increased significantly. To accomplish this shift, threat actors have turned to cloud-based methodologies.

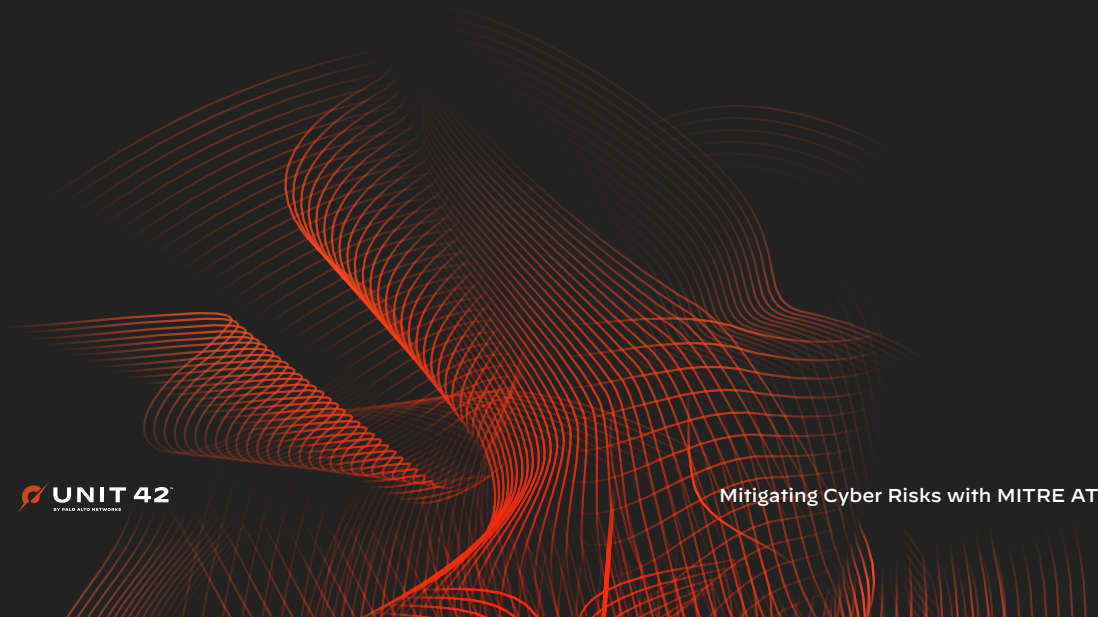
Establishing clear visibility into all sanctioned cloud data storage providers your organization uses is a critical first step in ensuring you are staying ahead of mass data exfiltration. The second core step is ensuring proper visibility into traffic across your organization.

During the time of traditional on-premise data centers and centralized offices, it was much easier to sustain visibility throughout the organization by controlling flows through a handful of known exit points. In modern networks, the need for always-on VPN connections and visibility into traffic moving between cloud service providers is fundamental to catching ransomware and exploit actors early on in attempts to exfiltrate data.

## Practitioner Focused Recommendations

Threat actors have no shortage of cloud platforms to push data to. Having visibility across your organization with firewalls that offer granular insights Into communicating applications is the best way to track down unsanctioned data movement.

Most modern networks require a combination of traditional firewalls and FWaaS implementations to gather appropriate visibility. Beyond visibility alone, being able to inspect traffic and sort it into categories (e.g., sanctioned, unsanctioned and tolerated) provides you with an opportunity to be flexible, but also to shut down cloud providers that your organization doesn't do business with.



# Impact (TA0040)

Impact techniques refer to the approaches threat actors use to achieve their outcomes. An organization won't decide to pay a ransom fee without feeling an impact from the threat actor's actions. These techniques cover some of the core features of ransomware and extortion activities.

## Capabilities Most Commonly Used for Impact (TA0040)

- **T1486: Data Encrypted for Impact**
  Encryption of victims' data is the primary extortion tactic associated with ransomware.

- **T1490: Inhibit System Recovery**
  Ransomware threat actors delete volume shadow copies on impacted Windows systems.

  Many threat actors explicitly encrypt (or delete) online backups to inhibit victims' ability to restore operations without paying the ransom demand.

# RECOMMENDATIONS

## IMPACT (TA0040)

### Strategy Focused Recommendations

While trends with ransomware have shifted over time to include models around double, triple and even quadruple extortion, the encryption of file components remains a strong constant. Most XDR platforms leverage canary files to help detect and alert on this activity.

One of the biggest challenges that Unit 42 researchers still see in detecting encryption activity is insufficient XDR coverage. It's worth routinely reviewing your XDR asset inventory and comparing it against your other forms of asset inventory.

Also, be sure to enable anti-tamper protections in your XDR and leverage strong uninstallation passwords. It's common for threat actors to remove an agent, or to find systems without an agent and attack them, thus creating a more significant impact.

Beyond the XDR component, ensuring you have both high-quality and tested backups will continue to be critical when any impact does take place.

## Practitioner Focused Recommendations

Canary files as a part of XDR have been helping detect and shut down malicious ransomware binaries for years. Turning to detections that can help earlier in the process, and at scale, is an area worth evaluating more closely.

While all ransomware binaries and groups have some variation, many of them use proven tactics like deleting volume shadow copies from systems just prior to encryption. This helps decrease your ability to easily recover files.

XDR solutions that leverage behavioral detection can stop this behavior before any encryption takes place. However, it's crucial that the XDR has enough intelligence driving it to know the difference between a malicious action or a routine process.

Beyond detecting and shutting down a ransomware binary, it's worth assessing how well you are able to hunt down and destroy other copies of the threat across your network. Unit 42 researchers observe threat actors placing their binary in different locations and with different file names, depending on their group tradecraft.

Ensure that your XDR has a quality search and destroy process to remove any lingering binaries from delayed or accidental detonation after the immediate threat is contained. The Unit 42 team prefers to utilize Cortex XDR, as it encompasses the necessary technology and the integrated threat intelligence to be successful against these adversaries.

# Prevention is Key to Mitigating Ransomware Attacks

Having gathered information from the Unit 42 team to determine the most crucial TTPs for security practitioners and strategists to focus on, we hope these recommendations can help you streamline preparations for the current ransomware and extortion landscape. Legitimate businesses have taken the message to heart that paying criminals is bad for everyone, and threat actors are now hitting victims harder to continue to motivate them to pay.

As defenders, you need to continue building more robust processes for maximum protection against an increasingly hostile threat actor community. Relying on backups alone will not protect you against extortion tactics. You need a combination of detection and visibility techniques in place to identify problems before they become so unmanageable that extortion payments seem like a feasible solution.

## Achieve a Target State of Ransomware Readiness

As ransomware attacks continue to hold organizations hostage, you can't afford to be unprepared. By partnering with Unit 42 for a Ransomware Readiness Assessment, you will develop a comprehensive understanding of your ability to prevent and respond to these threats. Our security consultants work with you to assess your current defenses, develop control enhancements and remediation recommendations, and update existing playbooks or help you develop a new one based on best practices and the latest ransomware trends. This will empower you to communicate with your key stakeholders and board of directors, so they understand the ransomware threat risk and how prepared you are to drive better security outcomes for your organization.

**Read the datasheet**

# UNDER ATTACK?

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team.

- Fill out the form at start.paloaltonetworks.com/contact-unit42.html.
- Call North America Toll-Free: 866.486.4842 (866.4.UNIT42), EMEA: +31.20.299.3130, UK: +44.20.3743.3660, APAC: +65.6983.8730, or Japan: +81.50.1790.0200.
- Email unit42-investigations@paloaltonetworks.com.

## Approved by Cybersecurity Insurance Plans

Unit 42 is on the approved vendor panel of more than 70 major cybersecurity insurance carriers. If you need to use Unit 42 services in connection with a cyber insurance claim, Unit 42 can honor any applicable preferred panel rate in place with the insurance carrier. For the panel rate to apply, just inform Unit 42 at the time of the request for service.

## About Palo Alto Networks

Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably's Best Companies for Diversity (2021), and HRC's Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

## About Unit 42

Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. Visit paloaltonetworks.com/unit42.

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clary, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com