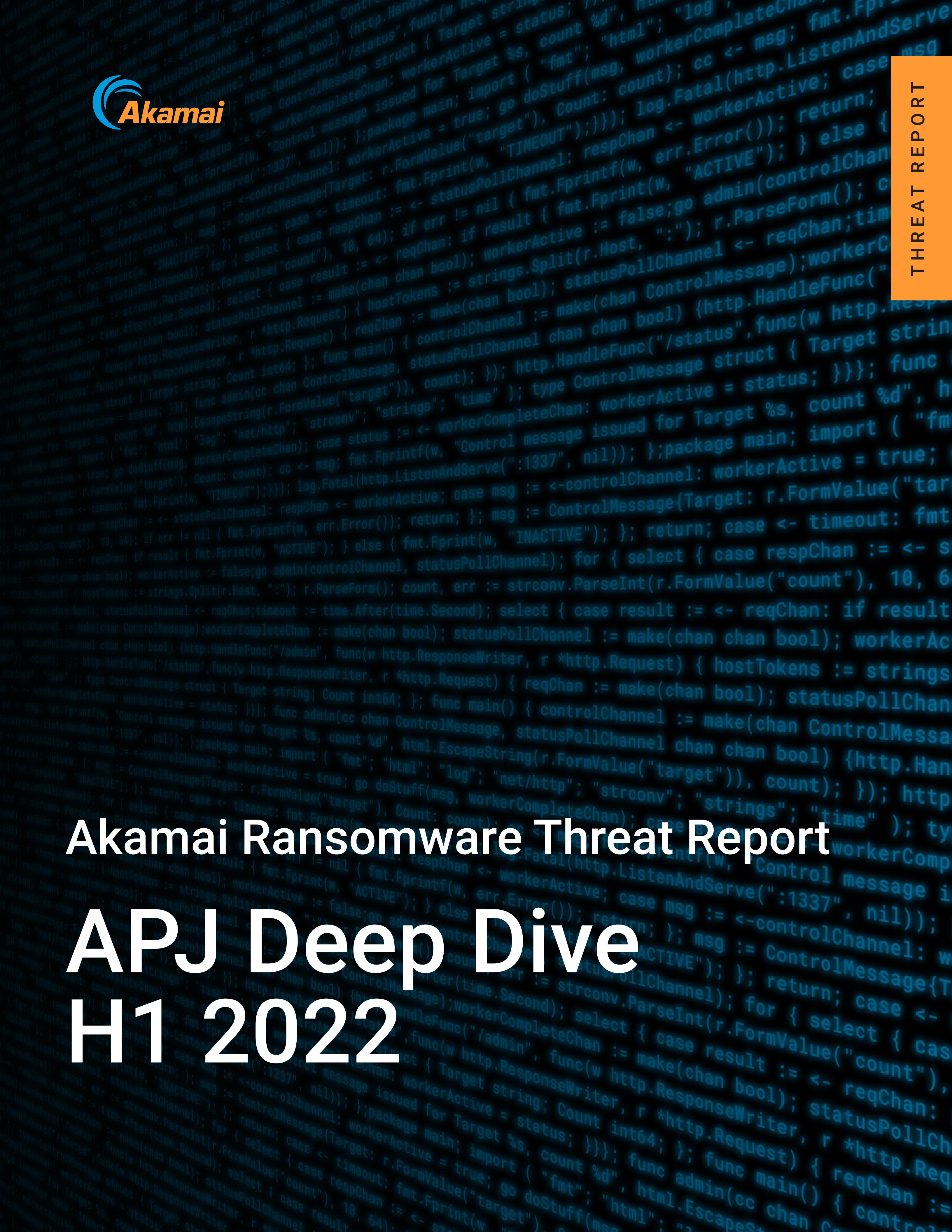


THREAT REPORT

Akamai Ransomware Threat Report

APJ Deep Dive H1 2022

Table of Contents

Highlights

In recent years, ransomware has become ubiquitous in cybersecurity attacks, costing more than US$20 billion globally in damages in 2021. The advent of high-profile ransomware attacks, starting with 2017's WannaCry global attack, has significantly elevated ransomware awareness. Recent years have seen ransomware attackers strike at schools, government, healthcare, and infrastructure, among other targets.

Since the beginning of the COVID-19 pandemic, the Asia-Pacific and Japan (APJ) region has seen a surge in cyberattacks. Organizations across all industries are 80% more likely to be a target for a cyberattack in APJ than in other regions globally. Australia, India, and Japan are reportedly seeing the brunt of attacks in the APJ region.

This report will focus on the organizations that execute these attacks, and the ways in which they operate, with an emphasis on APJ activity. Ransomware as a service (RaaS) groups have grown into businesses, with structures mimicking the very companies they seek to extort — customer service representatives, new employee training, and more. A recent leak of documents from Conti, one of the world's most prolific RaaS providers, revealed some of its inner workings, providing researchers and reporters with insight into how these organizations operate.

Akamai researchers have been analyzing and researching RaaS providers to reveal some of the underlying mechanisms that have contributed to their success. The results provide a thorough reporting of attack trends, tools, and the mitigation that must follow.

The report finds:

- The majority of Conti attacks in APJ are on Australian and Indian organizations.
- The business services industry is highest on the list of Conti victims in APJ, emphasizing the potential for supply chain cyberattacks via third parties.
- Critical infrastructure accounts for 13.6% of overall victims in APJ.

- Attacks on retail and hospitality combine to make up 27% of Conti victims in APJ, highlighting the increase in attacks on commerce verticals in the APJ region; this is echoed by a recent Akamai Web Application and API Threat Report.

- The overwhelming majority of Conti victims in APJ are businesses with US$10 million to US$250 million in revenue.

- Approximately 20% of Conti victims in APJ are businesses that earn more than US$1 billion in yearly revenue. This is unlike the overall global trend, which shows much lower impact on high-revenue organizations.

- Attack scenarios are multifaceted and detail-oriented, with a strong focus on "hands on keyboard" network propagation.

- Tactics, techniques, and procedures (TTPs) hint at the need for strong protections against lateral movement and their critical role in defending against ransomware.

- TTPs are well-known, but highly effective, and help reveal the tools commonly used by other groups. Studying these TTPs offers security teams insights into attackers' modus operandi in order to better prepare against them.

- Conti's emphasis on hacking and hands-on propagation, rather than encryption, should drive network defenders to focus on those parts of the kill chain as well, instead of focusing only on the encryption phase.

The effects of Conti in APJ

There are many ways to analyze ransomware activity online, from conducting surveys to examining product data. Each method has some inherent advantages and limitations in providing a holistic view of global ransomware activity. The research conducted for this report strives to focus on one group in particular to provide an accurate account of one of the world's leading RaaS groups.

We chose to focus on an analysis of victims of the Conti RaaS group to establish the relevance of Conti's tools and techniques, which will be explored later in the report. The data is gathered from Conti's dark marketplace, where victim data and information is bought and sold. Conti's goal is to extort their victims into paying ransom, and to do so, they share information that helps us create an analysis of the attack preferences, successes, and failures of the infamous group. The data we report reflects the past year of activity and is fully anonymized.

For context, Conti is a notorious RaaS group that was first detected in 2020 and appears to be based in Russia. It is believed that the group is the successor to the Ryuk ransomware group, and is also known as Wizard Spider. According to Chainalysis, Conti was the highest-grossing ransomware group in 2021, with an estimated revenue of at least US$180 million. Notably, the group has recently successfully attacked the Costa Rican government, Irish Department of Health, and others (see U.S. FBI Flash CP-000147-MW: Conti Ransomware Attacks Impact Healthcare and First Responder Networks).

Recent news has indicated that Conti has disbanded. This, in our mind, implies an even greater relevance to this analysis. A large number of new ransomware organizations are expected to pick up operatives from the Conti group, and share information about the tools and tactics that made it so successful. As the information spreads among many ransomware organizations, so does the chance that these tools will be used against victims worldwide.

Ransomware attack trends in APJ

To understand Conti's victim preference in APJ, we will begin with an examination of the top targeted countries in the region. It is worth noting that Conti is a group that primarily targets Western countries, such as the United States and Europe. This deep dive into APJ attacks is provided as an acknowledgment of Conti's impact in APJ, but we find that other groups who are primarily focused on APJ will display different attack patterns.

Top 5 Countries by Attack Count
(May 1, 2021 – April 30, 2022)

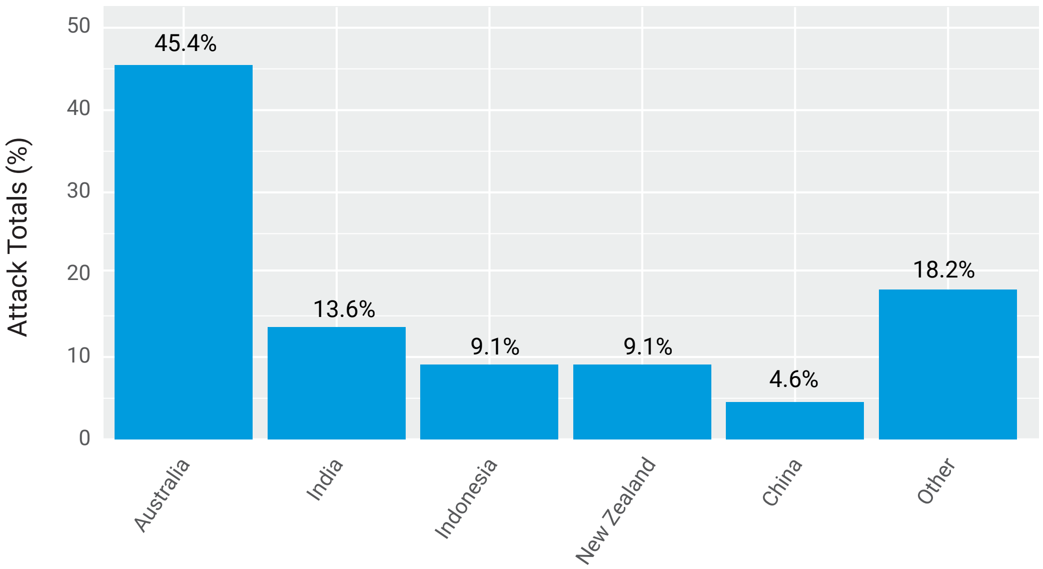


Fig. 1: The top five countries targeted in APJ include Australia, India, Indonesia, New Zealand, and China

Distribution of victims by country (Figure 1) shows that 45% of Conti victims come from Australia, followed by India, Indonesia, New Zealand, and China. Other countries that did not make the top five, but have been the victims of Conti attacks, are Japan, Pakistan, South Korea, and Vietnam.

This could be examined several different ways, but primarily, it is known that Conti is a Russian attack group, and as such it shows a heavy slant toward the North American and European regions in terms of target selection. During our research we found that 93% of Conti victims are organizations in North America and the region composed of Europe, the Middle East, and Africa (EMEA).

The large number of victims in Australia and New Zealand might therefore be an extension of Conti's selection bias for Western countries. Additionally, it is possible that the reuse of materials in English, such as phishing emails, contributes to this trend. Through our research of Conti victims we've found that English-speaking countries are more likely than other countries around the globe to become Conti victims.

India and Indonesia follow on that list, with the second and third largest pools of victims. India, in particular, has been experiencing a tremendous amount of cyberattacks, according to reporting in the region, with a recent article reporting that the number of attacks in India have grown by approximately 25% year over year. Despite this trend, and despite the general success the Russian attack group has found in the region, it seems that Conti does not gravitate particularly toward non–English-speaking countries in APJ.

Top Regions by Attack Count
(May 1, 2021 – April 30, 2022)

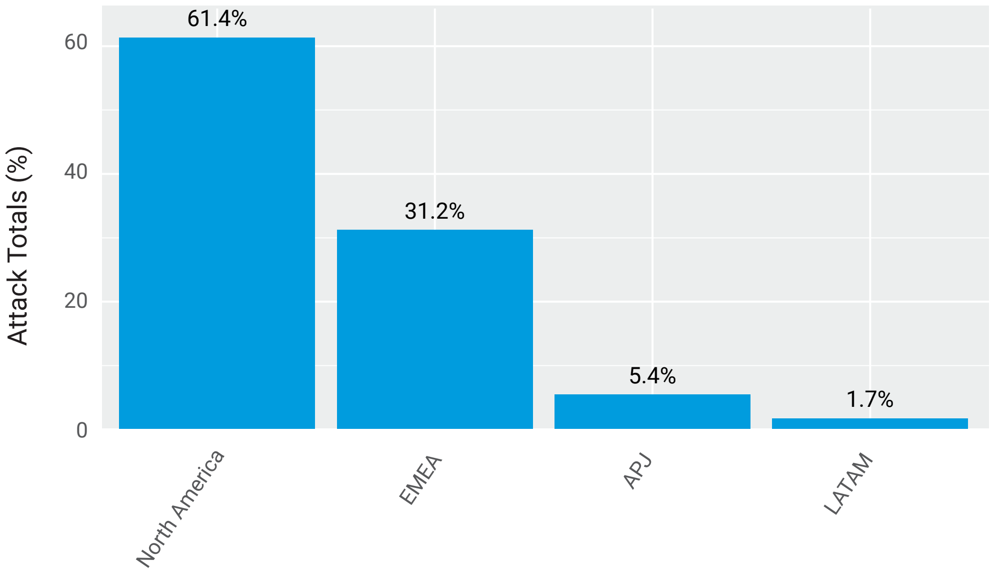


Fig. 2: The APJ region has been targeted less than North America and EMEA

A high-level examination of victim trends by region (Figure 2) shows North America and EMEA as the first and second largest attacked regions, followed by APJ and Latin America (LATAM). Despite the low victim count of the APJ and LATAM regions in relation to North America and EMEA, it's important not to disregard the significance of these attacks, as the impact of each individual attack can vary within regions. A notable example is Conti's recent successful attack on the Costa Rican government, which has caused widespread disruption in the region.

Overall, however, Conti's focus on specific regions over others is not surprising. Its attack on Costa Rica is an example of how its alignment with Russian state goals may cause it to hit unexpected targets in many parts of the world. However, outside of that, there seems to be a "regionalization" of ransomware threat actors, who show a language, region, and country preference.

Industry and vertical trends in APJ

Next, we analyze the vertical distribution of victims of Conti attacks in APJ. Industry and vertical analyses play an important role in cybersecurity. Although attack groups don't necessarily target some industries over others, the data in Figure 3 indicates how the success rate of Conti's attacks differs among industries and verticals. There are similarities and differences among industries that may be important to analyze and note.

Top Industries by Attack Count
(May 1, 2021 – April 30, 2022)

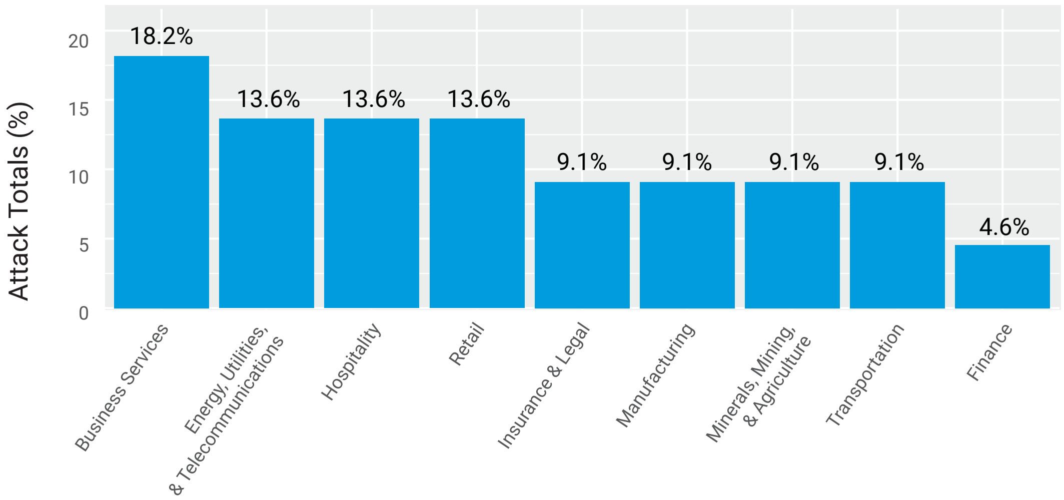


Fig. 3: The top targeted industries in APJ were business services and energy, utilities, and telecommunications

As we break down the list of victims by industry, we find a number of interesting trends to consider. To observe these trends, we need to look beyond the direct financial impact of these attacks, and examine the broader impacts of business disruption brought about by ransomware attacks. As demonstrated with the Colonial Pipeline attack, attacks on some verticals may cause a longer-lasting and more critical impact than others.

Three important findings arise from our analysis of victims by industry; chiefly, the high potential for supply chain attacks through the vulnerability of third parties, the high number of critical infrastructure victims, and the focus on commerce.

A major concern arising from this analysis is the possibility of supply chain cyberattacks, such as the recent SolarWinds and Hafnium attacks. This is indicated by the large number of victims in the business service vertical. A supply chain cyberattack might breach a third party, such as these business services organizations, to get to a larger, more lucrative victim. The high number of business services victims points to the risk of supply chain cyberattacks, not only from the ransomware operators themselves (although that is indeed possible), but also via leaked documents. Companies providing services to organizations may have access to sensitive information, which could potentially be used in attacks against affiliated companies. A notable example is a 2013 attack on a large retail company, which put 40 million credit and debit cards at risk, and was made possible through a third-party HVAC company. Similar attacks have been reported in the APJ region, some with far-reaching impact.

The utilities, energy, and telecommunications industries represent 13.6% of the total victims. Attacks on these verticals can cause an immediate disruption to large populations, and can have catastrophic, real-world implications. The collateral consequence of ransomware's impact could be considered a cyber-kinetic impact. One example of this is the healthcare vertical, in which ransomware attacks have caused significant disruptions to vital care and have even caused a number of deaths around the world.

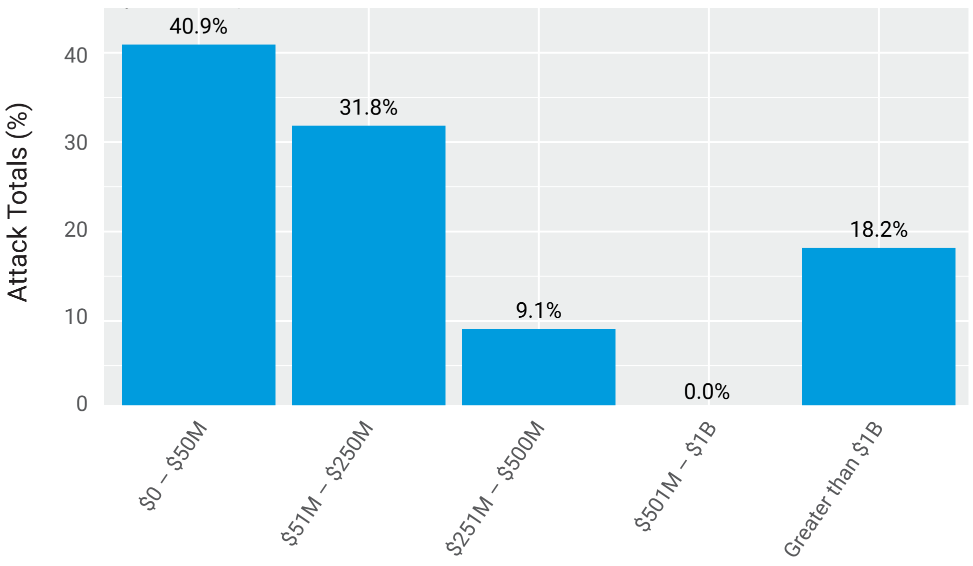
In comparison with other global regions, the APJ region shows a significantly larger number of critical infrastructure victims — nearly twice the relative number of critical infrastructure victims compared with the global average. This may hint at the need for a more detailed focus on critical infrastructure defense in the APJ region. Recent incidents in Australia and India seem to support these findings and highlight this overarching trend.

The final emphasis is on the large number of retail and hospitality organizations on the list. The number of attacks on commerce verticals in APJ has seen significant growth in recent years. We find this not only in this ransomware report, but also in our analysis of web application and API threats, which sees commerce as one of the most targeted verticals for these types of attacks. It is worth noting that these numbers do not represent the number of targeted organizations, but rather the number of organizations who have fallen victims to an attack. This highlights a potential cause for concern for organizations classified as retail and hospitality.

Revenue trends

Ransomware as an attack vector is largely financially motivated, which, in part, is one of the reasons it has gained so much attention in recent years. An analysis of attacks by revenue allows us to examine the motivations and success rates of RaaS groups' attacks against different sizes of companies. It is often assumed that RaaS groups target only the largest organizations; however, a closer observation reveals a somewhat different picture of victim distribution through revenue groups.

Figure 4 displays RaaS victim distribution by revenue range. It is important to note these are not the ransom figures, but the overall revenue of each company.



Total Attacks by Revenue Range
(May 1, 2021 – April 30, 2022)

Fig. 4: The largest revenue range targeted in APJ were companies with overall revenues of less than $50 million

In APJ, we see a large portion (73%) of affected organizations have up to US$250 million in revenue. More than 40% of victims make revenue up to US$50 million, and 32% make US$50 million to US$250 million. This is very much in-line with global averages for the Conti ransomware group. The analysis reveals an interesting trend in the success pattern of RaaS groups like Conti. Although the hardest-hitting attacks are often the ones that are widely publicized, it seems that the majority of successful ransomware attacks happen in the lower revenue brackets.

It is possible that these companies represent an optimal range for these ransomware groups — companies that make enough revenue to pay a substantial ransom, but are not yet mature enough to defend themselves successfully against Conti and other RaaS groups.

In sharp contrast, however, to the global trend, we find that a large portion of victims in APJ are in the US$1 billion revenue bracket. Nearly one in five of Conti victims in APJ are found in this bracket, which is three times the global average. It also appears that the majority of these high-revenue victims are found outside native-English-speaking countries in APJ, and represent victims in Japan, South Korea, and China.

This could be viewed a few different ways, but it is likely to do with the fact that Conti's diminished focus in the APJ region provides us with a smaller sample size, more likely to show statistical anomalies. Alternatively, it is possible that a diminished focus on non–native-English-speaking countries in the region leads Conti to less proactively pursue small and medium businesses in those countries, and rather find its way to the larger corporations through their global presence, or through a similar selection of victims in this region.

Understanding the attackers' toolkit

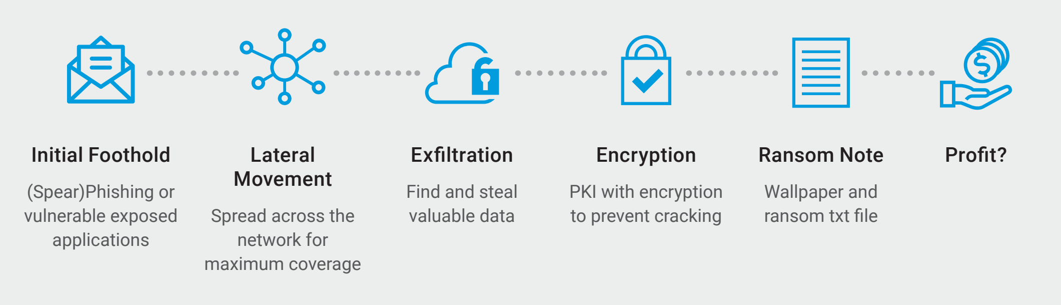
To devise proper mitigation strategies for Conti in particular, and ransomware attacks in general, we first have to look at the arsenal of tools that are used by ransomware operators. Fortunately, there is a lot of similarity between the various ransomware groups regarding the TTPs that they use. This means that we can discuss strategies that should mitigate, or at least hinder, most ransomware attacks.

For our analysis of ransomware attacker TTPs, we turn to the recent Conti leak of documents. On February 27, 2022, the Twitter handle @ContiLeaks was created and began leaking internal documents and chat logs of the group, as well as the addresses of some of their internal servers and source code. This leak of documentation and source code reveals the most commonly used TTPs. The research below focuses on the tools and techniques, and the appropriate mitigation strategies.

The kill chain

To begin examining the ransomware attack methodology, we look to the ransomware kill chain as illustrated in DFIR reports. While leaks can give us a nice overview of the attackers' entire toolset and the thought process behind the inclusion/usage of each tool, DFIR reports tell us how those TTPs were used in actuality. They both paint a similar picture.

A typical ransomware kill chain looks something like this:


Initial Foothold
(Spear)Phishing or vulnerable exposed applications
Lateral Movement
Spread across the network for maximum coverage
Exfiltration
Find and steal valuable data
Encryption
PKI with encryption to prevent cracking
Ransom Note
Wallpaper and ransom txt file
Profit?

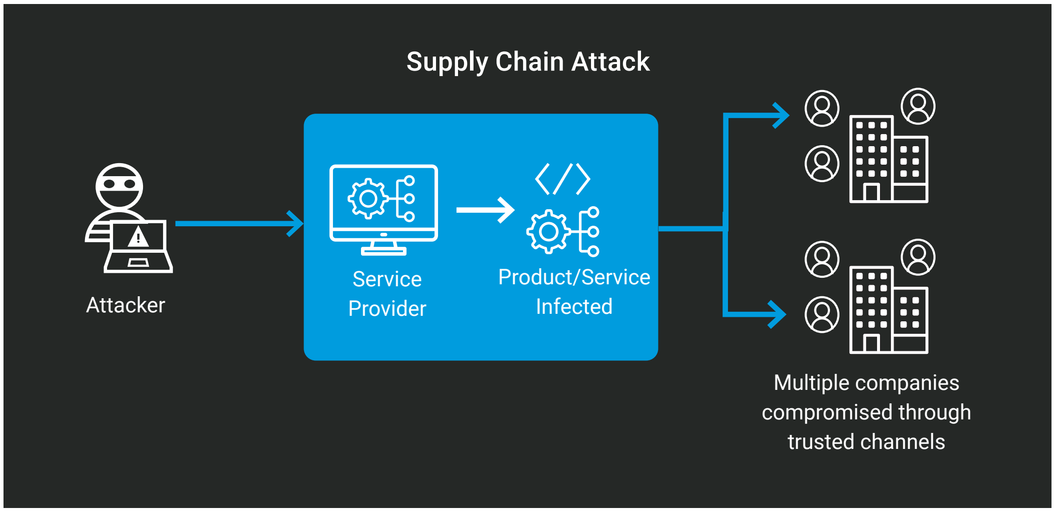
Ransomware attacks are multifaceted — an initial breach is not enough. An attacker or malware must also spread across the network before beginning encryption to maximize the damage. If only a single computer is encrypted, they will not have enough leverage to demand a ransom. This fact makes the lateral movement stage the "make or break" part of a successful ransomware operation.

While the tools used for lateral movement (and other stages in the kill chain) can be extracted with DFIR, the thought process behind using them is harder to glean. For that, we can use the recent Conti leak to look at how a network attack progresses.

The RaaS attackers' cookbook

The first thing to note when discussing Conti is their manual, hands-on approach to attacks. Conti's attack doctrine is not a novel one, but is still highly successful. The use of effective tools and the consistency of operation seems to do the trick. They do utilize some automated or scripted functions, but operators are generally expected to do the work of obtaining credentials and making cognizant decisions on spreading in the network.

Conti's methodology can be summarized as "harvest credentials, propagate, repeat." This occurs after the initial access stage, so an operator is assumed to have access to a machine in the network. At that point, their goal is to begin propagating through the network, first either by attempting to dump and decrypt passwords or by using brute force. The operator is then instructed to use the harvested credentials on the next machine which expands their reach, then to repeat step one. Likewise, operators are taught that encryption doesn't start until network dominance has been reached, which ensures the impact is maximized.



Network propagation goals

First and foremost, Conti's goal is to reach the domain controller (DC). Operators are instructed to work their way to the DC via the aforementioned process of stealing credentials and expanding. Since the process seems to be largely manual, this allows Conti operators a level of discretion in choosing targets. Once the domain admin credentials are found, Conti operators will have gained access to a number of critical assets:

- Login logs for most of the network to analyze user behavior
- DNS records for most of the domain, which can be used to infer usage
- Password hashes
- Focal points for lateral movement

CERT NZ's lifecycle of a ransomware incident (Figure 5) is a useful illustration of Conti's interest in the DC, along with the path they take that allows them to target it. Conti makes their way via myriad infection vectors. Once a vulnerable attack surface is identified, an operator is called in. The operator works through the initial access layers, laterally moving

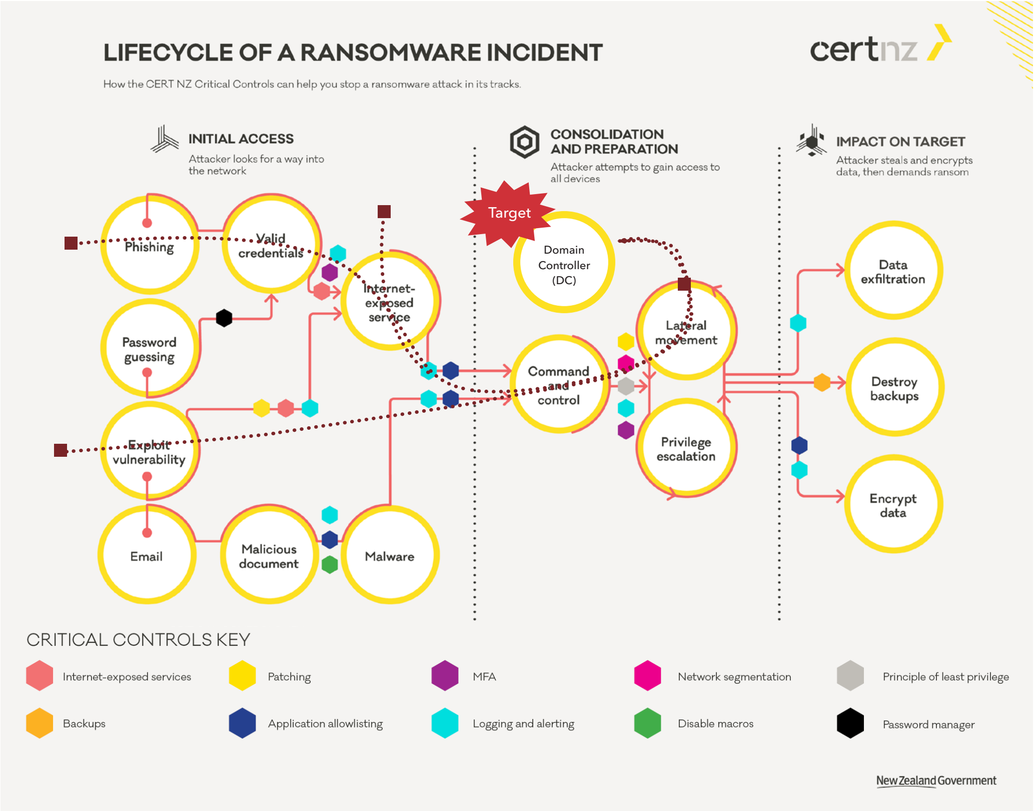


Fig. 5: CERT NZ's lifecycle of a ransomware incident

This focus on the DC bolsters the idea that the network propagation phase is crucial to the attack. From the DC, the attackers can extract most (if not all) the credentials they need to access the entire network. Also, as more domain configuration is usually stored there, the attackers usually gain a lot of intel about the network itself and its crown jewels.

Interestingly, Conti discourages leaving backdoors and persistence on the DC, and instead encourages backdooring outward-facing servers since a DC is (in their words) much more heavily monitored. This tells of a strong OPSEC mindset that precedes the attack, likely contributing to their success.

Conti defines *crown jewels* as network file shares and other machines that hold data that can be exfiltrated, including:

- Emails, address lists, contact information
- Databases
- Source code
- Accounting information
- Design documents
- Passwords/credentials for other networks
- Digital wallets

A step-by-step guide to network dominance

Also extracted from Conti's leaked manuals is a step-by-step technical guideline on gaining network dominance. Figure 6 is an almost literal translation of their method, but a bit more organized than the original text. It requires some technical understanding of the tools and processes used. However, for those concerned with defending their organization against similar attacks, or those looking to emulate a ransomware attack, valuable information can be gathered about the type of telemetry that should appear during the lateral movement and privilege escalation phases.

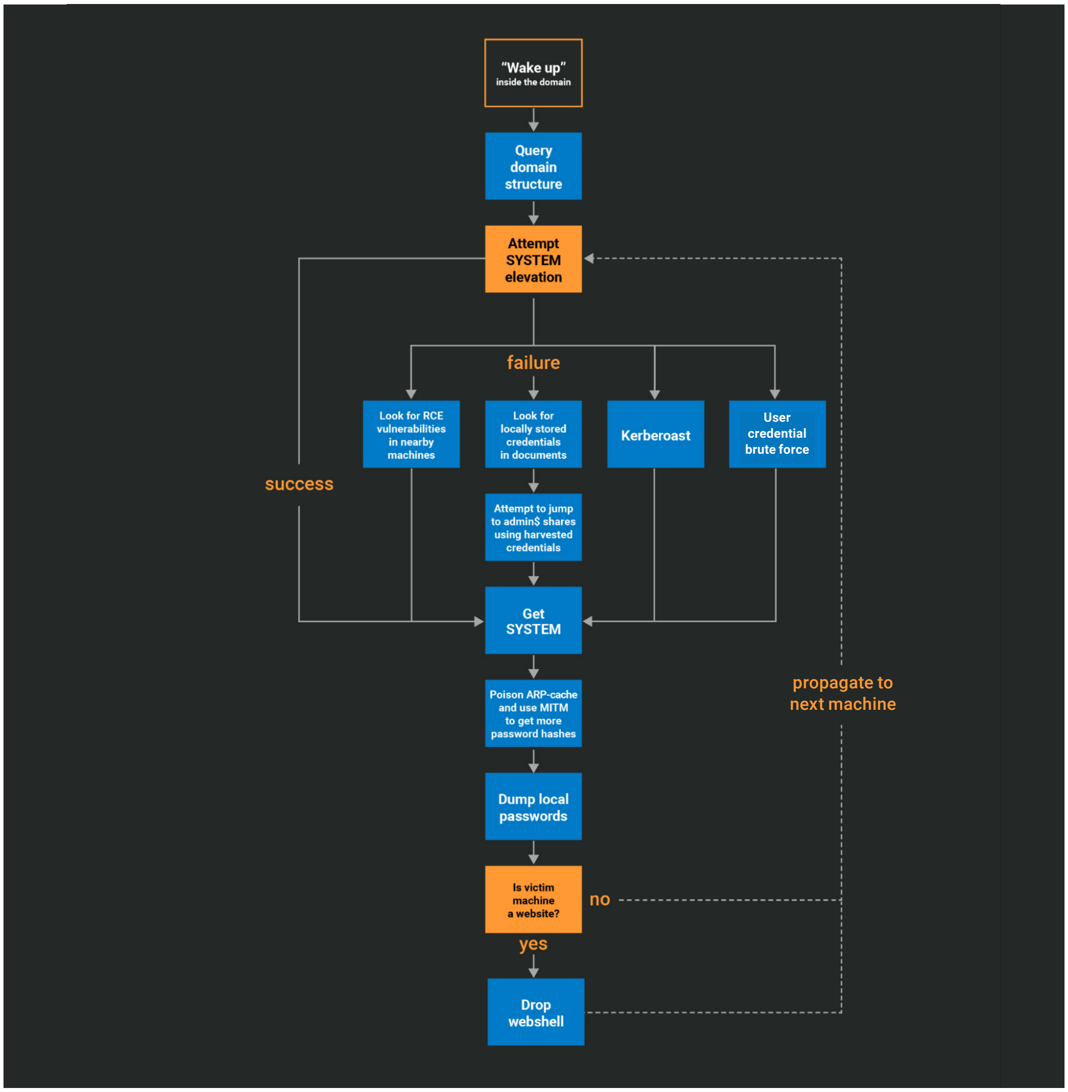

"Wake up" inside the domain
Query domain structure
Attempt SYSTEM elevation
failure
success
Look for RCE vulnerabilities in nearby machines
Look for locally stored credentials in documents
Kerberoast
User credential brute force
Attempt to jump to admin$ shares using harvested credentials
Get SYSTEM
Poison ARP-cache and use MITM to get more password hashes
Dump local passwords
Is victim machine a website?
no
yes
Drop webshell
propagate to next machine

Fig. 6: Step-by-step guidelines

1. Query domain structure (using adfind, net view, etc)
    - a. Sometimes passwords will appear in those tools' output immediately, under some comments
2. Try to elevate to SYSTEM rights
3. If possible:
    - a. Poison ARP-cache and intercept password hashes from other machines in the network
    - b. Dump local password hashes
4. If not:
    - a. Try to see if other machines in the network are accessible, specifically if their admin$ share is accessible
        - i. If it is, jump there to obtain SYSTEM rights
    - b. Look for RCE vulnerabilities in the network
    - c. Attempt Kerberoast to obtain more password hashes
    - d. For small networks, also possible to attempt brute forcing user passwords
        - i. There's a special emphasis on testing the lockout limits for brute force before attempting it
5. For any server with a writable inetpub directory, drop an aspx webshell
6. Scan the network for further spread paths

The toolset

To achieve their network infiltration and propagation goals, ransomware groups employ various tools, most of which are well known and heavily used in the industry. In fact, usually only the crypter (and sometimes the trojan) seem to be proprietary and differ between the various ransomware groups. But the lateral movement, propagation, and exfiltration TTPs should be familiar to anyone on both red and blue teams: Cobalt Strike, Mimikatz, and PsExec, to name a few.

Initial access

For most ransomware, it seems that the most common breach vector is phishing, causing the user to open a weaponized document or archive. Other common methods include breaching VPN or RDP servers by "guessing" the correct credentials.

Conti's leak provided design documentation for internet crawlers that implement other less commonly seen methods of infection:

Service	Crawler logic
Apache Tomcat	Scan for Tomcat servers, and attempt to exploit the cgi-bin vulnerability
Outlook Web Access (OWA)	Internet crawler and credential brute forcer
SQL	Scan websites that have user inputs and attempt to use SQL injection on them
Printers	Scan for printers accessible from the internet and attempt to exploit them using PRET

Lateral movement

The common lateral movement techniques that are used by ransomware are the same ones that MITRE covers, namely:

- WMI — used for triggering payloads remotely using */node:.. process call create*
- PsExec — both the Sysinternals tool itself and its Cobalt Strike implementation are used for remote payload execution
- Remote scheduled task — using the command line utility *SCHTASKS* with the */s* flag to create a remote task to execute a dropped payload
- RDP
- WinRM

In addition to those, zero-day exploits are also sometimes used:

- EternalBlue — exploiting a remote code execution vulnerability in SMB
- BlueKeep — exploiting a remote code execution vulnerability in RDP

Persistency and backdoors

The most common persistence method we've seen in reports and leaks is scheduled tasks.

Conti's leaked manuals also describe less commonly seen persistence methods:

- Registry run keys
- Office application startup
- Windows services
- Image file execution options
- WMI event subscription
- AppInit DLLs
- Winlogon userInit
- LSASS notification packages
- Netsh helper DLL

In addition to the above, which are used to launch their beacons/reverse shells, the manuals also mention installing **AnyDesk** and **Atera**, as well as changing the RDP port (and enabling it to pass through Windows' firewall) — all presumably to have another entry point in case communication is lost.

Credential harvesting

Credential harvesting is usually done by accessing LSASS or the SAM. The most common tool for this purpose (which also has a lot of other credential dumping utilities) is Mimikatz.

There are also other attacks and recent zero-day vulnerabilities that can be employed to get credentials over the network:

- DCSync
- Zerologon — exploiting a netlogon vulnerability to get an authenticated session to the DC and reset the krbtgt password
- Kerberoast — used to crack Kerberos service user passwords from service tickets
- PetitPotam — exploiting an Encrypting File System (EFS) vulnerability to get NTLM hashes from vulnerable machines

Mitigation

A ransomware resiliency architecture covers multiple entry, exploitation, lateral movement, and targeting. The materials exposed by Conti's leaks illustrate some of their favored approaches.

Resisting Conti's favored initial infection vectors

As highlighted in Figure 5 (the CERT NZ illustration), credential harvesting, exploit vulnerabilities, targeted internet exposed entry points, lateral movement, and privilege escalation are all in the "Conti Playbook." While ransomware operations certainly rely on (spear)phishing, it's important not to neglect securing internet-exposed services, as they are similarly at risk. Using the TTPs for initial access, we recommend reducing the internet visibility for the following applications:

1. Remote access services (e.g., RDP, SSH, TeamViewer, AnyDesk, VPNs)
2. Potentially vulnerable services (e.g., Apache, IIS, Nginx)
3. Potentially vulnerable machines (detect machines with an unpatched operating system using Guardicore Insight)
4. Unwanted exposed services (e.g., databases, DCs, internal web or file servers)

The existence of public service tools like Shadowserver's Network Reporting tool allows security teams to get an "outsider's view of their organization's vulnerabilities and exposures." These daily reports help any organization see exposures and risks that miscreant organizations like Conti are likely to exploit.

Expected penetration

A mature organization will know that a persistent attacker will relentlessly look for ways to succeed. Despite implementing all the proper defenses, there always exists a chance that your network will be breached eventually. This could be due to a user infected by a spear-phishing campaign or a server running a vulnerable service that was not mitigated properly. With this mindset, we should be prepared and have proper mitigations set beforehand. Lateral movement detection and prevention is one of the neglected areas that Conti favors in their exploitation. In fact, the March 21, 2022, U.S. President's Security Advisory called out lateral movement as a critical area of focus used by threat actors:

> **"Develop software only on a system that is highly secure and accessible only to those actually working on a particular project. This will make it much harder for an intruder to jump from system to system and compromise a product or steal your intellectual property."**

We are going to focus on detecting and preventing lateral movement in organizations. The advice and tools here use the lessons gleaned from the Conti data dumps, along with our own experiences, to help organizations reduce lateral movement risk.

Detect and cut threat actors' lateral movement

Assuming a machine has been breached, and the attackers have a foot in the door, we would want to limit them from propagating inside the network. This can be done in two ways:

- **Segmentation** and application **ringfencing**
- Restricting **lateral movement** across the network

Segmentation is key

You want to separate the network into operational segments — by application, usage, or environment — and not allow unnecessary connections both between and within those segments.

Consider the following guidelines:

1. Block any communication between laptops/workstations
2. Block communication from processes running with "powerful" domain users' privileges, like domain administrators
3. Limit users that can execute processes on your servers
4. Limit access from laptops/workstations to data center servers and cloud instances

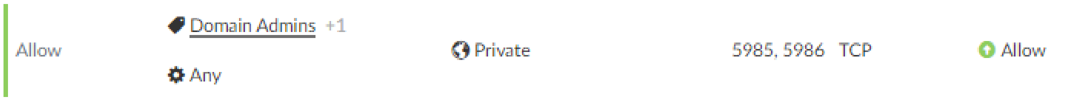
Preventing lateral movement with protocol-restricting rules

Below are general guidelines for specific protocols and behaviors. Because of these protocols' inherent usage in normal day-to-day operations, we cannot account for all usages and use cases. Consider the rules demonstrated below as examples and rules of thumb, and adjust them to your network and operational model.

In all the scenarios, we finish by adding a general “block any” rule. You might want to first use a similar rule in alert mode, and — after a monitoring period to see if there are more exceptions that you didn’t cover with allow rules — move the rule to block mode.

WinRM

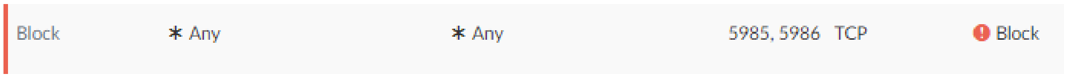
Windows Remote Management (WinRM) is the remote management infrastructure in Windows. It serves both remote WMI and remote PowerShell, two tools that attackers can (and do) utilize for their own purposes. Because of the administrative nature of this protocol, we suggest you create an exception for domain admins and IT personnel that use it, but block it otherwise.



Allow	Domain Admins +1 Any	Private	5985, 5986 TCP	Allow

Add an exception to your domain administrators and IT personnel that might use it

If you do not see WinRM (TCP ports 5985, 5986) usage in your network, there is no need to allow it, but there is still need to block it, in case it is enabled and simply not in use normally. An attacker can still utilize it if it is not blocked explicitly. Blocking WinRM, along with RPC (covered next), will ensure that attackers can’t utilize WMI for their malicious needs.



Block	* Any	* Any	5985, 5986 TCP	Block

Finish by blocking any access over WinRM — WMI remote management protocol

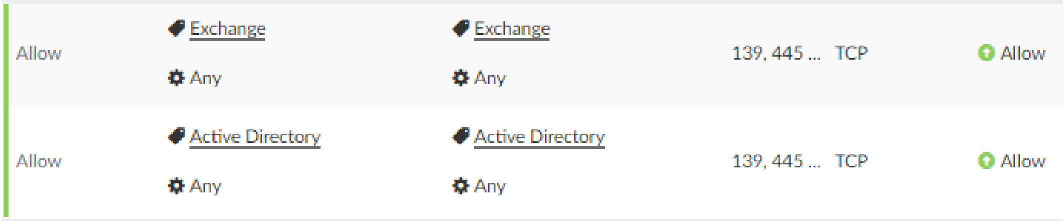
SMB and RPC

SMB (TCP port 445, 139) and RPC (TCP port 135 for the portmapper and a dynamic port range for each service that utilizes it) are very important protocols in the Windows domain system. They are used for various communications against the DCs (authentication and group policy, for example), and for accessing file shares and network drives. SMB is also used for replication between various servers (e.g., exchange servers and DCs).

Consider the following guidelines — first, add exceptions that ensure normal operations can continue unhindered:

Replication allowance

Allow internal communication in application's assets that require replication, like DCs or exchange servers.

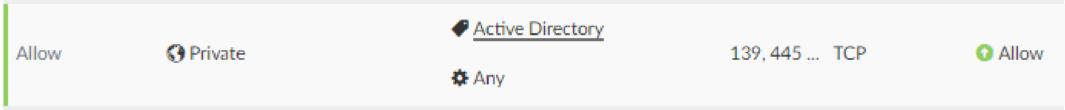


Allow	Exchange Any	Exchange Any	139, 445 ...	TCP	Allow
Allow	Active Directory Any	Active Directory Any	139, 445 ...	TCP	Allow

Allow SMB and RPC communication inside various applications for replication

Domain user authentication

Allow internal assets to access the DCs, to allow them to authenticate normally and not hamper the domain.

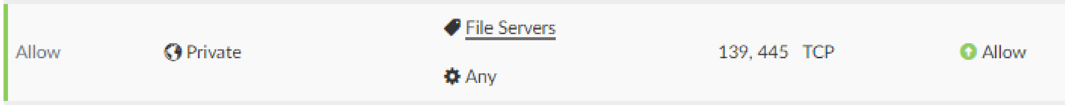


Allow	Private	Active Directory Any	139, 445 ...	TCP	Allow

Allow internal assets to access the domain controllers normally

File servers

Allow internal assets to access your file servers over SMB — that is what they're for, after all.

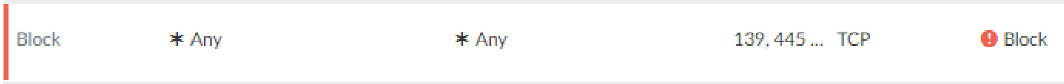


Allow	Private	File Servers Any	139, 445	TCP	Allow

Allow internal assets to access your file servers over SMB

If possible, refine the internal access restriction further, to not allow assets that don't need file servers to access them.

For finishers, drop any other SMB and RPC communication that wasn't specifically allowed.



Block	∗ Any	∗ Any	139, 445 ...	TCP	Block

Finish by blocking RPC and SMB across the network

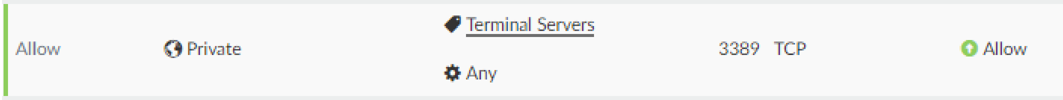
RDP

Remote Desktop Protocol (RDP) is another tool that is frequently used. Unless absolutely necessary, we recommend you block it, and perhaps allow exceptions as they occur. If possible, deploy terminal servers to funnel all the connections to a central location for easier, and more secure, monitoring.

Consider the following scenarios and guidelines:

Terminal servers

Use terminal servers to make all users RDP to a single place — this allows for easier monitoring across the network of RDP usage, and also lets you configure stricter security policies on those servers.

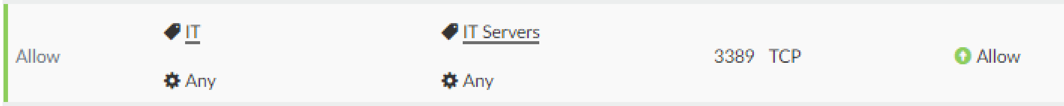


Allow	Private	Terminal Servers Any	3389	TCP	Allow

Allow internal assets to access your terminal servers over RDP

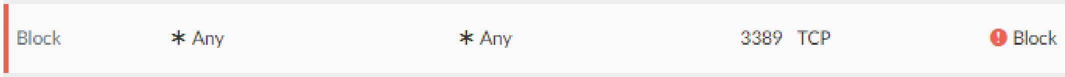
__Internal department access__

You might also want to allow RDP inside departments, or specific environments — sometimes users need regular remote desktop access to their servers, and that's okay.



Allow	IT Any	IT Servers Any	3389 TCP	Allow

For example, perhaps your IT department needs to access their servers regularly over RDP



Block	* Any	* Any	3389 TCP	Block

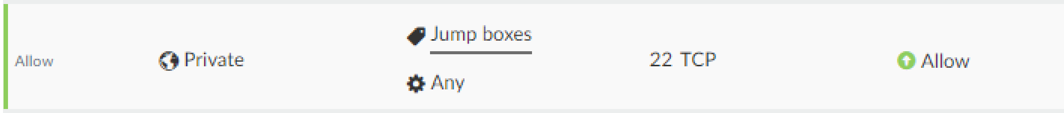
Finish by blocking any access over RDP

SSH

While SSH is useful for remote administration, and also serves to make other protocols secure (like sFTP), it is also a tool for attackers to breach machines and propagate around the network. You'll want to restrict network-wide SSH as much as possible. We recommend you create jump boxes from which users can use SSH, and give access to them only to users who need them.

__Jump boxes__

Use jump boxes and make users connect to other servers only through them. This will allow for easier monitoring on all connections as they come from a central place. Use security controls on the jump box to ensure who can access what.

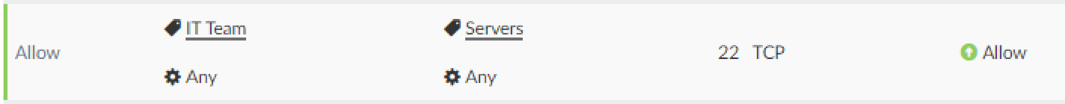


Allow	Private	Jump boxes Any	22 TCP	Allow

Allow internal assets to access your jump boxes over SSH

Domain admins

IT personnel and domain administrators are more likely to need SSH access for their day-to-day operations. Consider adding special exceptions to them, in case they absolutely need it.

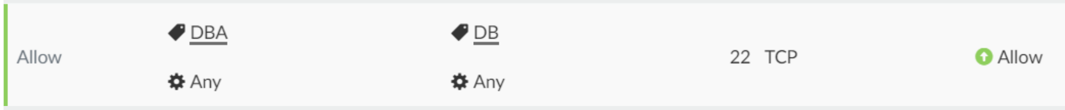


Allow	IT Team Any	Servers Any	22 TCP	Allow

Consider allowing your IT personnel and domain administrators SSH access to internal servers

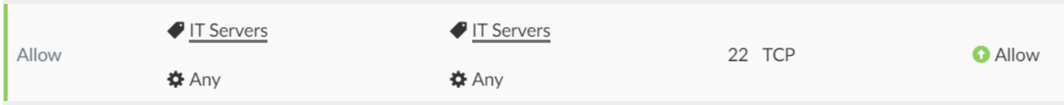
Internal environment access

Some applications need SSH communication, so you shouldn't explicitly block them — it will hinder your operational continuity. Consider adding allow rules according to existing network flows, or simply inside an application or department segment.



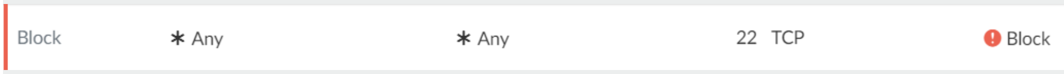
Allow	DBA Any	DB Any	22 TCP	Allow

For example, your DB architects might need access to their servers



Allow	IT Servers Any	IT Servers Any	22 TCP	Allow

Or (for example), some of the IT servers might need to use SSH tunnels on each other



Block	* Any	* Any	22 TCP	Block

Finish by blocking any access over SSH

Protecting backups

To maximize damage, ransomware campaigns usually target the organization’s backup application to encrypt the stored backup data. Use extra segmentations on your backup servers to further separate them from the rest of the network. Minimize communication to/from them using custom process-level microsegmentation policy rules.

Segment critical data services

Your data services and servers are targets. Use segmentation and ringfencing on critical data services such as your databases and file servers, and limit access to them from outside the network and from regions in your network that do not need to access them. Limiting your data services’ exposure to only the operational minimum will reduce the risk factor to those services and mitigate ransomware exposure and propagation paths.

Detailed response plans

Create and plan your breach mitigation policies in advance to reduce response time once malware is detected.

Consider the following guidelines for your mitigation policy:

- Consider cutting off file servers and SMB from desktop machines — ransomware usually looks for network shares on the victim machine and encrypts them first. Don’t let your file server be compromised by cutting it off from any machine that mustn’t have it for operational continuity.
- Restrict lateral movement even more — while you may need to leave some remote control channels open for your IT department, block the rest. For the channels that you do leave open, restrict them heavily with both machine and user policies.

You can also create plans for the recovery process — consider which applications and sections you need to bring online first, and create policies accordingly to keep them secure while you restore the rest of the network.

Credits

Authors

Eliad Kimhy Stiv Kupchik

Editorial

Barry Greene Ophir Harpaz Tricia Howard

Data analysis

Chelsea Tuttle