RANSOMWARE AND EXTORTION REPORT

Table of Contents

Executive Summary

Threat actors are increasingly employing extortion techniques to gain leverage over targeted organizations and accomplish their goals. While much attention has been paid to ransomware in recent years, modern threat actors increasingly use additional extortion techniques to coerce targets into paying—or dispense with ransomware altogether and practice extortion on its own.

While in many cases the motivation is financial, Unit 42 also sees indications that extortion can happen in service of a group's larger goals—sometimes simply to fund other activities, but other times to distract from them.

Organizations, in turn, need to evolve defenses to address the various methods threat actors use to apply pressure. Incident response plans today need to involve not only technical considerations but also safeguards for an organization's reputation and considerations for how to protect employees or customers who may become targets for some of extortionists' more aggressive tactics.

In our review of incident response cases, as well as our threat intelligence analysts' assessment of the larger threat landscape, we noted some key points:

Multi-extortion tactics continue to rise. In Unit 42 ransomware cases, as of late 2022, threat actors engaged in data theft in about 70% of cases on average. Compare this to mid-2021, and we saw data theft in only about 40% of cases on average. Threat actors often threaten to leak stolen data on dark web leak sites, which are increasingly a key component of their efforts to extort organizations.

Harassment is another extortion tactic we see being used in more ransomware cases. Ransomware threat actor groups will target specific individuals in the organization, often in the C-suite, with threats and unwanted communications. By late 2022, harassment was a factor in about 20% of ransomware cases. Compare this to mid-2021, when harassment was a factor in less than 1% of Unit 42 ransomware cases.

Extortion gangs are opportunistic, but there are some patterns in the organizations they attack. Based on our analysis of dark web leak sites, manufacturing was one of the most targeted industries in 2022, with 447 compromised organizations publicly exposed on leak sites. Unit 42 believes this is due to the prevalence of systems used by this industry running on out-of-date software that isn't regularly or easily updated or patched—not to mention the industry's low tolerance for downtime.

Organizations based in the United States were most severely affected, according to leak site data, accounting for 42% of the observed leaks in 2022.

Large, multinational organizations can be lucrative targets for threat actors. Attacks on the world's largest organizations represent a small but notable percentage of public extortion incidents. In 2022, 30 organizations on the Forbes Global 2000 list were publicly impacted by extortion attempts. Since 2019, at least 96 of these organizations have had confidential files publicly exposed to some degree as part of attempted extortion.

Advanced threat groups may use extortion and ransomware to fund other activities—or hide them. Threat groups from countries under economic embargoes or sanctions have been observed using ransomware and extortion to fund their operations.

Other threat groups, including some from Iran or China, seem to have a different objective when using ransomware. Threat actors can gain more than money from deploying ransomware—it also has potential for both destruction and espionage.

Predictions for what to expect from extortion in the coming year. Unit 42 experts have put together predictions for what we expect to see from extortion groups in the coming year. Our predictions include:

- 2023 will be the year we see a large cloud ransomware compromise.
- A rise in extortion related to insider threats.
- A rise in politically motivated extortion attempts.
- The use of ransomware and extortion to distract from attacks aimed to infect the supply chain or source code.

Extortion Is on the Rise

The number one goal for many criminal threat actors is getting paid, and they'll do whatever they can to improve the chances of that happening. As such, we are seeing threat actors increasingly focus on extortion techniques—often layering them on top of each other.

Ransomware actors, for example, often use a variety of extortion techniques (called multi-extortion) to pressure organizations into making the difficult decision to pay ransom.

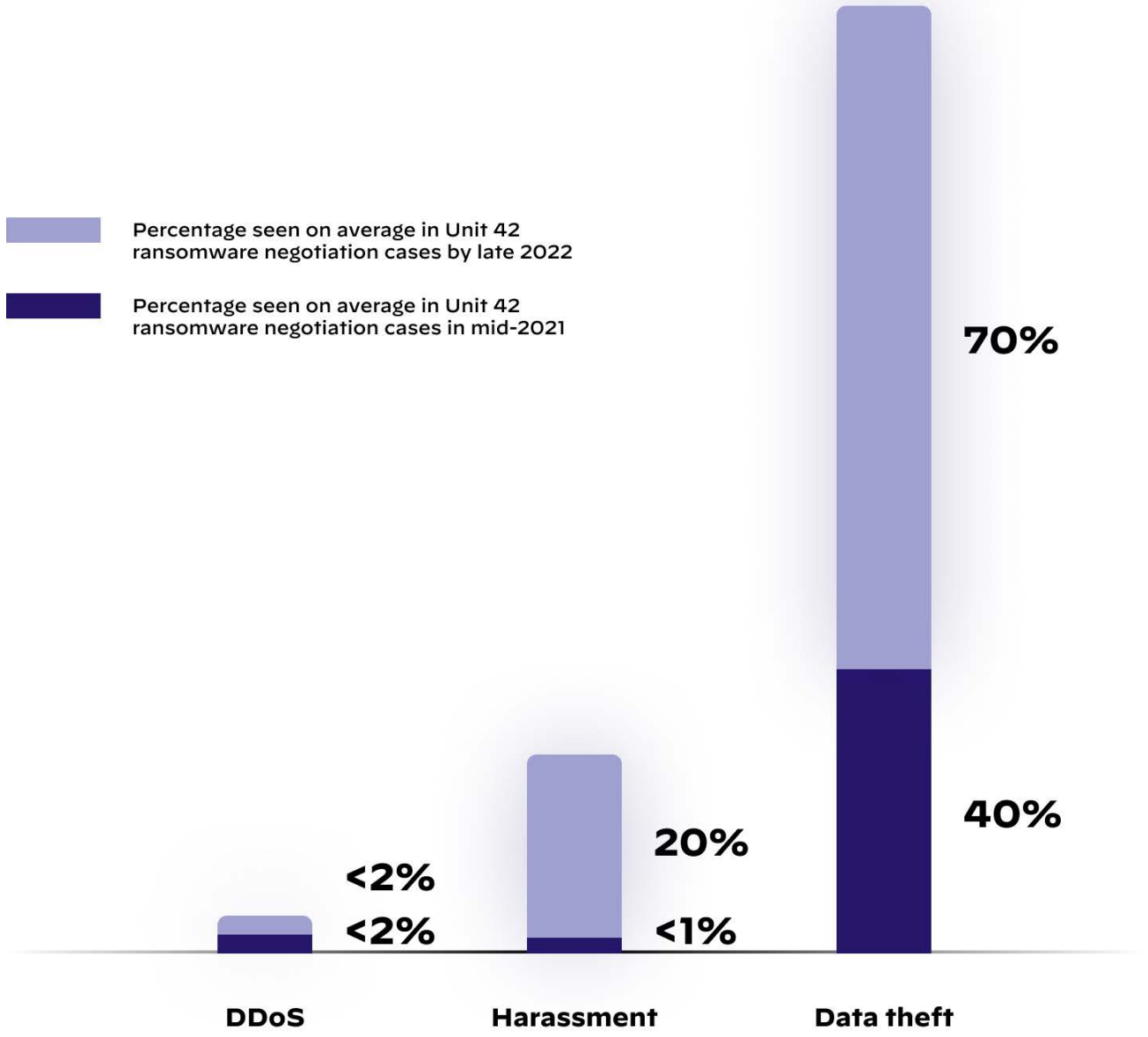
Unit 42 has observed the following extortion tactics employed and threatened by ransomware threat actors:

- **Encryption:**
  An organization's data and files are encrypted, and the threat actor demands payment in order to restore access to them. This has long been the primary extortion tactic of ransomware.
- **Data Theft:**
  Threat actors acquire an organization's data and threaten to disseminate it unless they are paid. This often involves dark web leak sites. Threat actors increasingly target information that may be particularly sensitive, such as files containing personally identifiable information (PII), customer financial data, protected health information (PHI), etc.
- **Distributed Denial of Service (DDoS):**
  Websites or other resources are targeted via a DDoS attack to disrupt operations and to get an organization's attention.
- **Harassment:**
  Threat actors may call, email, or otherwise contact an organization's employees or customers. They may also post on social media about the incident or contact journalists.

In a selected set of Unit 42 incidents involving ransomware, we have seen significant increases in threat actors' use of data theft and harassment.

Threat actors also simply use extortion. About 10% of the extortion incidents Unit 42 responded to in the period covered did not involve encryption.

Threat actor's use of additional extortion tactics



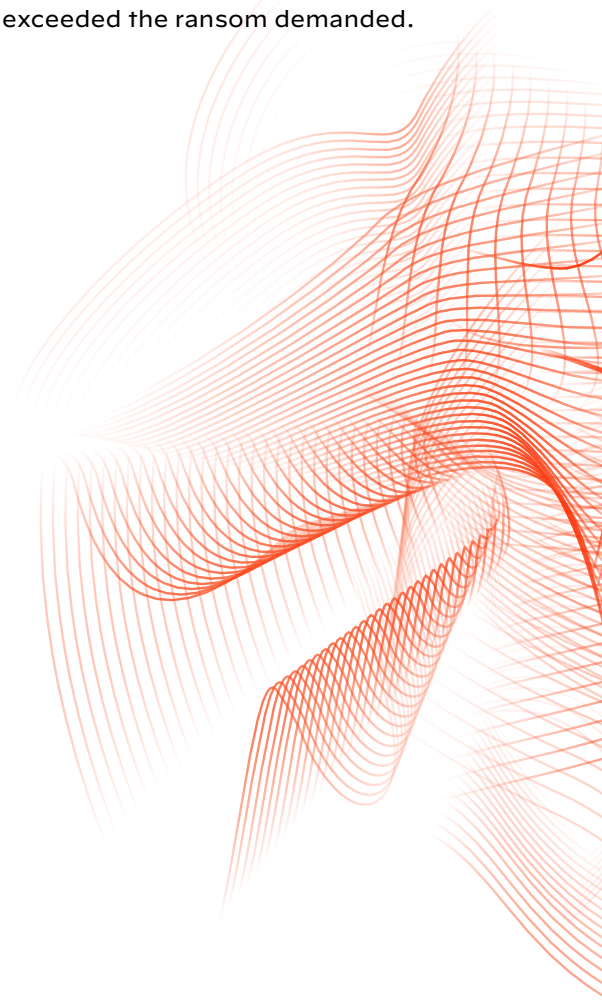
Why Having Backups Is No Longer Enough

With ransomware incidents grabbing attention of late—both in the news and within security teams—many organizations have absorbed the basic concepts of how to defend against them. Ransomware actors typically encrypt files to render them unusable and then demand ransom in exchange for a decryptor to recover encrypted data. The traditional advice for getting ahead of this type of attack is therefore to keep up-to-date backups, stored offline, and test them often, so that your data is never fully at the mercy of a threat actor.

This is still a vital safeguard. Unfortunately, many of today's threat actors have introduced such effective extortion techniques that they can coerce the victim to pay even if they've already backed up and protected their data and can minimize operational disruption from such attacks.

Often, the threat of disclosure of sensitive data is what coerces organizations to pay the ransom. Such leaks can cause reputational damage, loss of confidence from consumers and partners, and potential fines and sanctions from regulators and authorities—none of which can be prevented by backups.

We've also seen incidents in which organizations decided not to pay ransom because they had strong backups, but the threat actors followed up with harassment campaigns so intense that the resulting costs exceeded the ransom demanded.



RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Prepare a Playbook for Multi-Extortion

During an active extortion incident, rapid support from your incident response partner and outside legal counsel is critical. From a mitigation perspective, having a comprehensive incident response plan with corresponding crisis communication protocols will greatly reduce uncertainty. It's important to know which stakeholders should be involved and the process to make decisions promptly (e.g., whether or not to pay, or who is authorized to approve payments).

The crisis communication plan should also cover what to do (or avoid doing) in the event that employees or clients are being harassed. Ransomware harassment awareness training should be delivered to an organization's staff to equip them with tools and processes to follow during an active harassment incident.

Organizations should conduct a post-mortem compromise assessment to validate that any remnant backdoors or other indicators of compromise (IoCs) (e.g. scheduled tasks or jobs) have been removed. This ensures that the threat actor cannot easily conduct a follow-up attack after an initial breach.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

Common Extortion Tactics

Encryption

Encryption is a tactic commonly favored by ransomware threat actors. Criminal groups often tout the facility and speed of their encryption software as a means to recruit "affiliates." The typical approach, following an initial breach, is to deploy malware that encrypts files and delivers a ransom note. This note promises the delivery of a decryptor upon payment, provides instructions for how to contact the threat actor—and often warns against attempting to circumvent the attack.

However, threat actors are moving away from relying on encryption alone to extort payment. The majority of Unit 42's ransomware incidents involving negotiation also included at least one additional extortion tactic.

```
>> What happened?

Important files on your network was ENCRYPTED and now they have "[REDACTED]" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data

Sensitive data on your network was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Private financial information including:citizens data, courts data, bills,
budgets, annual reports, bank statements, etc
Samples are available on your personal web page linked below.

>> CAUTION

DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?

1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: [REDACTED]
```

Figure 2. An example of a BlackCat ransom note dropped on a compromised system

Data Theft and Multi-Extortion

Ransomware groups have threatened to leak data stolen from victims in about 53% of ransomware incidents involving negotiation between mid-2021 and late 2022. Due to the efficacy of this tactic, many threat actors target regulated data sets or highly commercially sensitive information for maximum leverage.

FOR JOURNALISTS

There are many journalists asking questions about us and our attacks.
If you are a journalist and want to ask some questions you should write:

1. Who are you?
2. Where are you from?
3. Where will you publish our answers?

We are trying to answer everyone in 24 hours.

#Frequently Asked Questions:
Why did you choose GTA as branding?
-Some old articles about us used GTA logo, so we decided to use it too.

How long have you beenn in operation?
-From January 2021.

Are you recruiting partners or are you closed?
-We have been closed from the beginning and we don't have affiliates.

How did you decide to team up and start a dedicated ransomware group? How was ViceSociety born?
-Group of friends that were interested in pentest. We decided to try.

What do you do if the law says that someone can't pay you? Does that matter? What happens if the customer doesn't respond?
-We don't care about laws. If someone doesn't pay or doesn't contact us, we will publish their documents.

Has Vice Society published all the data it took from "company name" or does Vice Society have additional data that still has not been published?
-We always publish everything.

Can you explain your decision to publish "company name" data?
-They didn't pay.

We DON'T answer questions like:
What country or region of the world are you from?
How old are you?
What vulns/eve do you use?

Figure 3. A page "for journalists" from Vice Society's leak site

Often known as multi-extortion, this tactic typically involves publicly posting information about breached organizations to a website maintained by the threat actors on the dark web.

These dark web leak sites sometimes threaten to sell data to third parties after the deadline for paying a ransom has passed. In other cases, threat actors simply threaten to post the data publicly.

The leak sites often include some version of a blog, or what appears to be a customer service portal, providing ways for affected organizations to view the status of their ransom demand and communicate with the threat actors. Some leak sites even have a section aimed at journalists seeking information about the ransomware group, a clear attempt by the cybercriminals to boost their notoriety in the cyber landscape.

During an 18-month span between May 2021 through October 2022, data theft leveraged as an extortion tactic grew by 30 percentage points. Unit 42 expects this upward trend of data theft and multi-extortion to continue.

Distributed Denial of Service (DDoS)

While DDoS remains an extortion tactic, Unit 42 has only observed this in less than 2% of ransomware cases. In these cases, threat actors have used DDoS to get an organization's attention if the victim chose to ignore them rather than communicate about payment of a ransom. While we continue to observe the tactic in use occasionally, we believe that it has not grown in popularity among threat actors because it is less effective at coercing payment than data theft and harassment.

Harassment

Unit 42 has observed threat actors leveraging harassment as an extortion tactic in at least 9% of our ransomware incidents involving negotiation overall. As with DDoS, threat actors generally employ this extortion tactic when trying to get an organization's attention. However, unlike with DDoS, threat actors seem to be turning to this extortion tactic more often.

Threat actors call and leave voicemails for corporate executive leaders and other employees, send emails to personnel, or disclose victims' identities on a leak site or social media. The purpose of these activities is to make it uncomfortable for an organization to avoid responding to the threat actors and their demands. Not only is the organization faced with responding to a ransomware incident, but now they also have a personnel public relations situation to deal with.

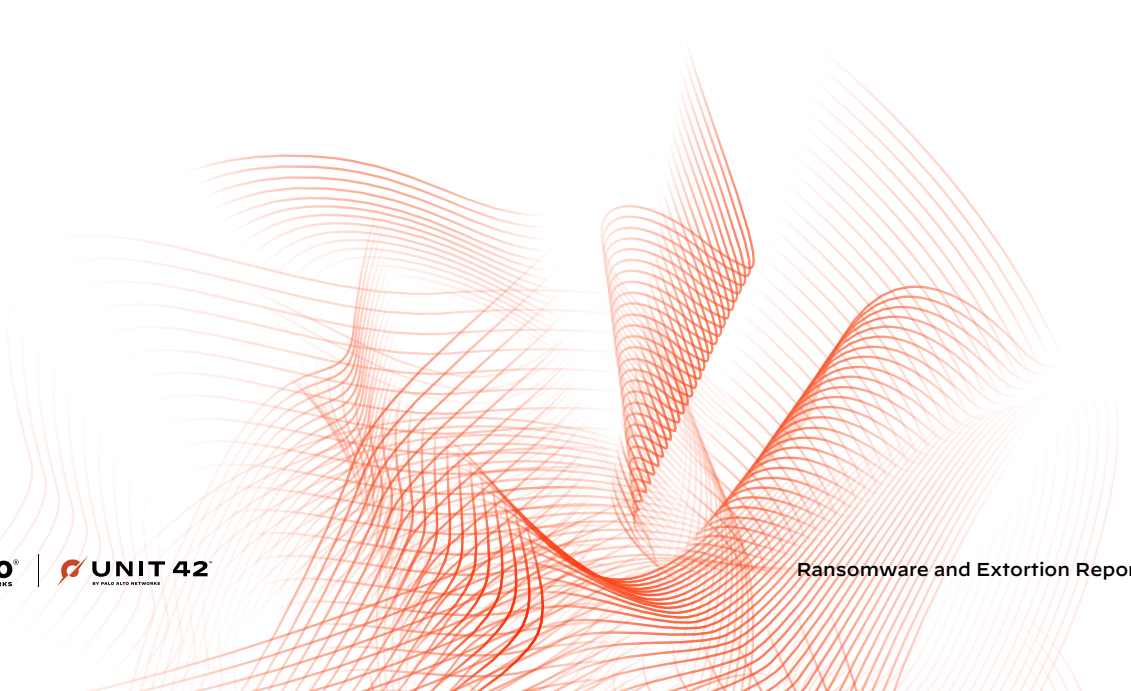
During an 18-month span between May 2021 through October 2022, harassment as an extortion tactic grew from an average of <1% of Unit 42's monthly ransomware cases to a monthly average of approximately 20%. While the available data and case information reflect an upward trend, the information available is limited and contains significant outliers. As such, while we believe this extortion tactic will continue to be used by threat actors, it is difficult to predict how frequently it will occur in the future. Unit 42 will be closely monitoring this trend.

Extortion Without Encryption

About 10% of Unit 42's incident response matters involving extortion do not involve encryption. Often, these extortion attempts rely on data theft.

However, in a small number of cases, threat actors have deleted organizations' data altogether. This is particularly prevalent in matters involving databases that were vulnerable and directly exposed to the internet. There are several automated threats that delete the database contents, claim to have exfiltrated them, and leave behind an extortion message in a new database table for the victims to find. Using data theft as an extortion tactic without encryption was most frequently seen in Unit 42 cases involving the Karakurt ransomware group.

We've also investigated several incidents related to the Luna Moth/Silent Ransom Group. These threat actors are known for an extortion campaign targeting businesses in multiple sectors, including legal and retail. Rather than encryption, the campaign relies on social engineering to convince targets to provide remote access to systems. They then use that access to exfiltrate data and follow up with extortion attempts.



RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Ensure Complete Visibility via Extended Detection and Response (XDR) Technology

When it comes to protecting your organization from threats, you must be able to see them. One of the greatest ways to protect your organization is to increase visibility of activity in your environments. Cortex XDR technology allows defenders to see activity on endpoints in near real time and respond to attacks quickly.

By empowering your defenders to isolate computers as malicious activity is detected, you can help reduce the likelihood of attackers spreading to other endpoints. This in turn reduces the impact of ransomware encryption. To increase protection, mature organizations move toward automating this isolation via Security Orchestration, Automation, and Response (Cortex XSOAR) technology. This can be important as attackers may operate when your team is not working.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident resonders.

Who Is Being Attacked?

Threat actors interested in extortion are frequently opportunistic, targeting whichever organizations they believe will pay. Because some criminals provide services to other threat actors, it can be difficult to discern the behavior of particular gangs. In part because of this, extortion can affect organizations large and small across various industries and regions.

However, many groups focus on profitable organizations—a practice sometimes known as "big-game hunting." Large, multinational organizations often have the means to pay larger sums of money and have the motivation to pay to avoid disruption of business operations. Although these organizations may be better prepared to withstand cyberattacks on a daily basis, they can still be vulnerable to extortion.

For example, less-protected subsidiaries, satellite offices, or remote workers could be impacted by ransomware in an attempt to move laterally to access an organization's crown jewels. We have observed ransomware groups focusing efforts on regional offices—a practice that could impact the larger organization.

Cybercriminals out to make a name for themselves may also seek to leak data from well-known organizations.

In some cases, threat actors display political motivations or regional preferences. For example, some samples of ransomware have been observed to check systems for Cyrillic characters, typical of Eastern European languages, and avoid encrypting files when they are found.

At times, extortionists do seem to favor targets in particular industries. For example, Vice Society has a reputation for targeting educational institutions.

Combining our observations from incident response cases and our ongoing monitoring of activity on dark web leak sites, we can provide a view of who criminal groups are attacking.

Insights From Dark Web Leak Sites

Every day, our threat researchers see information about seven new victims posted to dark web leak sites—averaging out to about one publicly posted new extortion target every four hours. In 2022, names and proof of compromise for 2,679 victims were posted on leak sites, about 4% higher than the number observed in 2021.

In 2022, the extortion group LockBit posted information about 801 breached organizations on their leak site, the highest victim count we have observed in the last two years from any one group. LockBit posted 409 victims in 2021, meaning that in 2022, we saw a 95% increase in victim count compared to last year's entries. By comparison, Conti posted 511 victims in 2021.

Attacks on the world's largest organizations represent a small but notable percentage of these incidents. In 2022, 30 organizations on the Forbes Global 2000 list were publicly impacted by extortion attempts from groups including LockBit, Conti, BlackCat, Hive, and Black Basta. Since 2019, at least 96 of these organizations have had confidential files publicly exposed to some degree as part of attempted extortion.

It's also worth mentioning that when we track organizations whose information was posted on a leak site, we are typically looking at those who chose not to pay the criminal group's original demand. Therefore, the actual global impact of gangs who maintain leak sites is higher than what we can observe there—presumably, some organizations choose to pay to keep their information off the dark web.

A few frequent practitioners of the multi-extortion strategy, such as Conti and REvil, dissolved in 2022. However, we expect other criminals to continue making heavy use of this approach to extortion. As noted above, cybercriminals threatened to leak stolen data in about 70% of ransomware cases involving negotiation in late 2022. The cybersecurity industry has also observed signs that individuals from the Conti and REvil groups continue to have an influence on the cybercriminal community, as former members of those gangs start new illicit endeavors and bring many of their tactics with them.

While they represent a body of evidence of the damage extortionists do to organizations, leak sites also provide visibility into these groups' resources, capabilities, and typical approaches. Unit 42 keeps tabs on them as part of our ongoing monitoring of the global threat landscape.

Data Extortionist Groups and the Global 2000

Karakurt, named the "Extortion Branch of Conti," was responsible for various notorious incidents in 2022. For example, they attacked one of the largest Chinese investment holding companies, allegedly stealing 320 GB of corporate data.

This group gains access to corporate networks either through their own expertise or by paying initial access brokers (who sell access to breached networks). Karakurt forgoes encryption in favor of other methods of extortion, such as contacting victims' employees, business partners, and clients with harassing emails and phone calls to pressure the victims to cooperate. They often exacerbate the situation by using the organization's own data against them.

Other groups try to make a name for themselves by attacking the world's most recognizable organizations. For example, Lapsus$, a cybercrime group that emerged in mid-2021, was responsible for compromising organizations such as NVIDIA, Samsung, Microsoft, and LG.

To accomplish this, Lapsus$ mostly used social engineering (including phishing and SIM swapping) for initial access. This group also tried to entice disgruntled employees to provide them with inside information in exchange for payment. Even well-defended organizations can struggle to prevent attacks targeted at insiders in this manner.

While the group extorted some victims, they sometimes appeared more interested in the notoriety of compromising high-profile targets.

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Implement a Threat Intelligence Program

Organizations can learn about the tactics, techniques, and procedures (TTPs) that threat actors use to successfully compromise their industry peers and conduct attacks. Organizations must have a chartered, funded, and staffed threat intelligence program in place.

The program will provide the blue team (their defenders) with net new, specific indicators sourced from the threat intelligence team. These can be used to monitor for the latest TTPs, enabling rapid detection and mitigation of a full-scale ransomware attack.

Unit 42 consultants can help with designing a modern, threat-informed security program or enhance the effectiveness of your existing program based on lessons learned from our incident response investigations.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

Industries Most Heavily Impacted

Based on both Unit 42's data and dark web leak site data, the manufacturing industry was one of the most impacted by extortion attacks in 2022, with 447 victims listed on various sites. Following this sector was the professional and legal services industry, with 343 victims.

Industries in which organizations often run on systems with out-of-date software can be more heavily impacted. When it's difficult for organizations to regularly update or patch, threat actors gain an opportunity to take advantage of old vulnerabilities to initiate their exploits.

This gives the threat actors a rapidly expanding attack surface through which they can deploy their attacks. The bigger the scale, the bigger the payout.

Criminals often seek targets in industries where it's critical for business operations to be able to provide certain products or services in a timely manner. The groups aim to take advantage of the pressure these organizations are under to meet deadlines and produce deliverables, hoping this will lead them to pay quickly and in full. Lost revenue streams from operational downtime can also push organizations to concede to threat actors' demands.

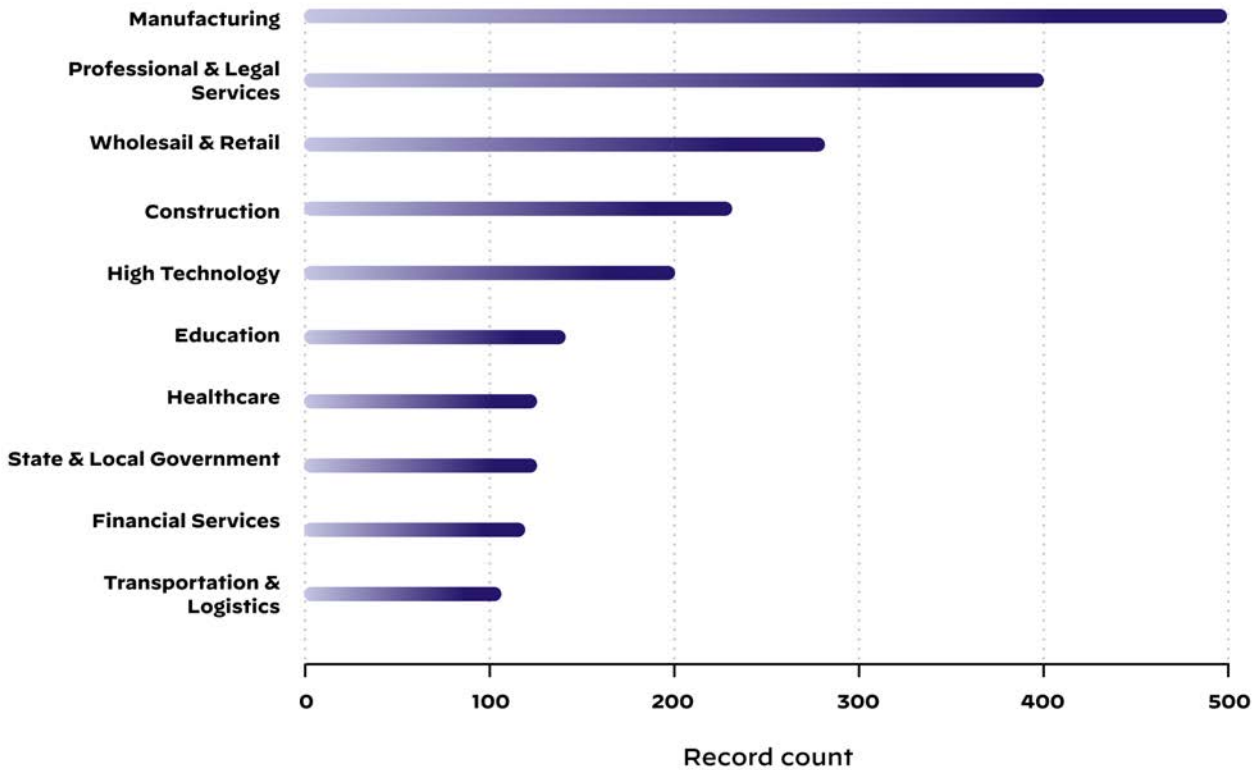


Figure 4. Industries most heavily impacted by extortion attacks (leak site data, 2022)

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Proactively Manage and Reduce Your Attack Surface Inventory

A staggering number (at least 75%) of ransomware attacks and breaches fielded by Unit 42's Incident Response team result from a common culprit: attack surface exposures. Organizations must continuously monitor the health, inventory, and accuracy of their external attack surface.

When using our Active Attack Surface Management (ASM) solution Cortex Xpanse with our clients in their environments, Xpanse continuously monitors all internet-connected assets and discovers unknown exposures. Once we receive the contextualized results from Xpanse, we can prioritize findings to align the security concerns with the organization's critical assets.

To illustrate, the analysis report from Xpanse shows all systems running Remote Desktop Protocol (RDP) that are directly accessible from the internet. Clients can then decide if Xpanse should automatically fix these exposures or not. RDP is the most common capabilities used by threat actors for initial access. Furthermore, RDP is the most impactful tool for lateral movement once attackers have a foothold inside targeted networks.

We also commonly see cybercriminals taking advantage of expired certificates, deprecated server operating system versions, and end-of-life email platforms, all items that are automatically discovered by Xpanse. All of these things were directly exposed to the internet, giving threat actors a path of least resistance.

It is strongly advised that you perform an Attack Surface Assessment if your organization does not have an accurate inventory of your external attack surface, including your cloud assets, or does not actively monitor changes to your external asset estate.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

Regions Most Heavily Impacted

Leak site data indicates the ● Americas region was hit the hardest by extortion attempts in 2022, followed by ● Europe, the Middle East, and Africa (EMEA), and the ● Asia Pacific region (JAPAC).

When looking at organizations posted on leak sites by country, the United States is still the most severely impacted, accounting for 42% of the observed leaks in 2022. This is followed by Germany and the U.K., accounting for nearly 5% each.

Threat actors, due to their financial goals, often focus on profitable organizations based in the United States. However, despite the concentration of attacks in the U.S., criminal gangs have a global presence and have been observed impacting organizations in 107 countries in 2022.

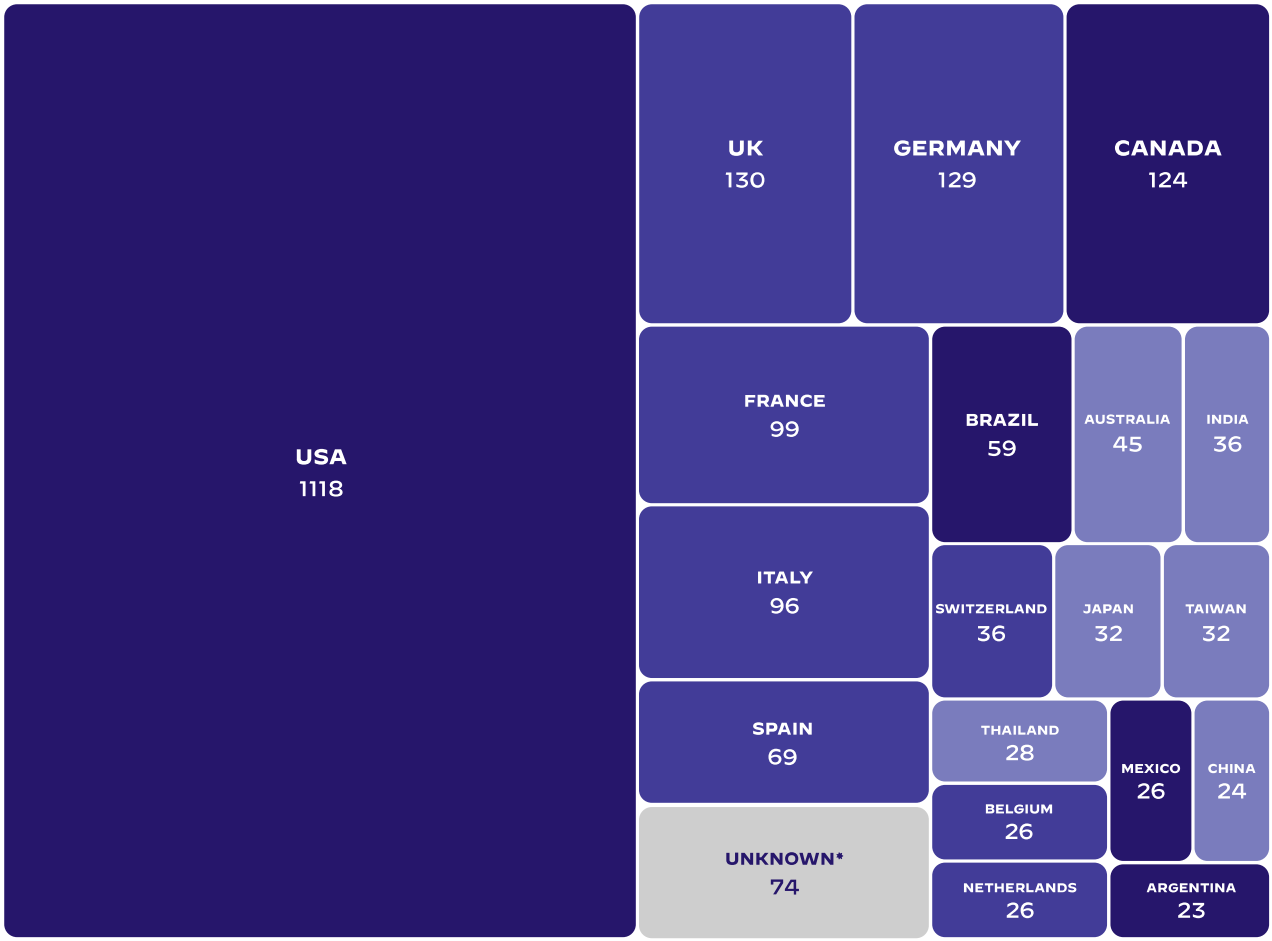


Figure 5. Top countries impacted by extortion attempts (leak site data, 2022)

What Are Extortion Threat Groups After?

While the obvious answer is "money," it can be helpful to take a look at what in your organization translates to financial gainfrom the perspective of a cybercriminal.

First and foremost, threat actors want you to feel pressured. The more you feel this way, the more likely you will pay what they demand. When cybercriminals use tactics such as harassment and urgency in addition to encryption, they're trying to make you feel out of control and under pressure so you'll do what they want.

Another way threat actors seek to amp up the pressure is to search your systems for information about any insurance policies or financial assets. Our incident responders have encountered threat actors who quote from these internal sources during negotiations and use this information to form an opinion about how high a ransom an organization can pay.

Today's threat actors, however, are also looking for ways to multiply their payday. This means they're not only looking for ways to halt the targeted organization's business operations—but they're also in pursuit of information that could be valuable to third parties.

This creates a win-win situation for the threat actor. If the targeted organization chooses to pay what is demanded, the threat actor makes a profit. If the organization chooses not to pay, the threat actor is still in possession of exfiltrated data they can sell. In some cases, cybercriminals may even try to double dip and make money both ways.

We often see evidence of threat actors searching systems for personal information such as identification numbers, passwords, and other credentials. They may seek documents such as passports and tax forms.

Threat actors know that many organizations are legally (and ethically) obligated to protect information of this type. Multinational organizations are bound by cyber regulation and data protection laws from various parts of the world—and failing to meet these requirements can result in fines, sanctions, the loss of operating licenses, and even the imprisonment of individuals. Threat actors can take advantage of these types of consequences to exert leverage on their targets.

Information that can be used in identity theft can often be sold to other criminals. And when threat actors search for passwords, they may be looking to sell initial access to a compromised network to other criminals—or they may be looking for ways to further the compromise and get deeper into an organization's systems.

These activities underscore the need to protect your systems beyond having backups. It's vital to be aware of what information is most sensitive and valuable to your organization and to be conscious of how that information is stored and who can access it. A Zero Trust approach can help minimize the damage a threat actor can do after an initial compromise.

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Implement Enterprise-Wide Zero Trust Architecture

Organizations that have the capabilities to rapidly contain the extent of their attack surface will reduce the impact that threat actors will have if they successfully circumvent other controls. Having an effective Zero Trust architecture mitigates the risk of a threat actor conducting lateral movement, which is a key indicator in advance of many types of attacks.

A huge part of winning the battle against cyberattacks is successfully making an attacker's job harder. Implementing Zero Trust Network Architecture (or ZTNA) is not an overnight journey, but is one of the more effective frameworks—specifically ZTNA 2.0, which is a refined version of ZTNA. This framework helps create the layers of security that slow down and prevent an attacker from successfully moving laterally around the network.

This framework helps force an attacker to make more noise to move around or through controls, while also slowing them down. Both of these things can provide more time for detection and response, giving you a better chance to properly contain and remediate the threat.

Taking it one step further, you can implement a Secure Access Service Edge (SASE) framework with Prisma SASE. Prisma SASE builds on the principals of ZTNA, but adds guidance on additional layers of control across web traffic and cloud platforms, in addition to other principles.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

What You Can Expect From an Attack: An Example Ransomware Incident

Attacks aren't a single malicious action. Breaching your network is only one step of a fairly complex process. The good news is that every time threat actors take an action in your network to further their criminal goals, it presents an opportunity for you to detect their presence or prevent them from having an impact.

Below, we tell the story of an example ransomware incident, which has been mapped to MITRE ATT&CK tactics and techniques. This provides a sample of how extortion groups may conduct themselves for maximum profit. When planning your organization's defense, it may be a useful exercise to assess how you might respond to a threat actor using these TTPs.

Financial Impact of Ransomware

In 2022 Unit 42 observed:

- Ransom demands as low as $3,000 and as high as $50 million.
- Ransom payments as low as $3,000 and as high as $7 million.
- The median demand was $650,000, while the median ransom payment was $350,000, a 46% decrease from the original median ransom demand.

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Pressure Test Your IR Plans and Program

Organizations that continuously review, update, and test their incident response plans are much more likely to effectively respond and contain an active attack. Organizations that conduct tabletop exercises, purple teaming tests, breach simulations (automated and manual), and partner with Unit 42 consultants strengthen their velocity and preparedness when responding to an active attack.

These exercises build the internal and external communication cadence, establish stakeholder relationships and foster environmental knowledge sharing in advance of an attack. This significantly increases the likelihood of early support and containment. Furthermore, these exercises will likely find opportunities or gaps that result in improved incident response posture once the gaps are mitigated.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

From First Campaign to Final Impact: A MITRE ATT&CK Flowchart

Note: *Certain actions in the narrative below are associated with multiple tactics and techniques, but only one has been listed for each row for the sake of brevity.*

RESOURCE DEVELOPMENT

T1608.006: Stage Capabilities: SEO Poisoning

The threat actor developed an extensive SEO poisoning and related malvertising campaign and placed malware disguised as legitimate software on numerous websites.

INITIAL ACCESS

T1189: Drive-by Compromise

An employee of the victim organization searched for "zoom" in a popular search engine to download the remote access software. Due to the threat actor's SEO poisoning campaign, the malicious website was displayed within the initial search results. The employee visited the malicious website to download Zoom, but unknowingly downloaded malware masquerading as legitimate software.

PERSISTENCE

T1546.016: Event Triggered Execution: Installer Packages

The employee ran the malicious installer, believing she was installing Zoom. The downloaded installer actually contained a legitimate PDF editor software program as well as a bundled malicious PowerShell script that served as a downloader for second-stage malware.

COMMAND AND CONTROL

T1105: Ingress Tool Transfer

The malicious PowerShell script downloaded Gozi, a variant of the Ursnif Trojan, and other malware. Within a few hours, Cobalt Strike was installed on this system, which established command and control (C2) communications with a malicious domain controlled by the threat actor.

COMMAND AND CONTROL | T1219: Remote Access Software

The threat actor downloaded and installed the Atera remote monitoring and management (RMM) tool onto the employee's computer.

EXFILTRATION | T1048: Exfiltration Over Alternative Protocol

The threat actor copied files from the victim organization's file server to a remote file transfer protocol (FTP) server using the rclone tool.

DEFENSE EVASION | T1562.001: Impair Defenses: Disable or Modify Tools

The threat actor remotely connected to a server via Splashtop (which it had installed) and executed a command to disable functionality of the Windows Defender antivirus solution: "Set-MpPreference -DisableRealtimeMonitoring $true"

IMPACT | T1490: Inhibit System Recovery

The threat actor used a batch script which, among other things, stopped various services and deleted all volume shadow copies in order to increase the effectiveness of its ransomware and to inhibit system recovery efforts.

LATERAL MOVEMENT | T1570: Lateral Tool Transfer

The threat actor deployed ransomware and the aforementioned batch script to hundreds of systems in the victim organization's network.

EXECUTION | T1569.002: System Services: Service Execution

The threat actor used PsExec to execute the aforementioned batch script and ransomware executable on hundreds of systems.

IMPACT | T1486: Data Encrypted for Impact

The ransomware encrypted files on hundreds of systems in the victim organization's network, including within shared folders and drives that were accessible from infected systems. The ransomware created copies of a ransom note in impacted locations and also physically printed the ransom note on networked printers within the victim's network environment.

Too Big—Nothing To See Here!

Unit 42 continues to see threat actors artificially increase the size of malicious scripts and utilities to evade automated scanning tools, which often have file size limitations for performance reasons (T1027.001: Obfuscated Files or Information: Binary Padding). By adding "junk data" to malicious utilities, these malicious files may evade detection by some antivirus and other security software solutions, depending on their configuration.

When APTs Use Ransomware

Security leaders at large organizations with mature security programs sometimes assign a lower risk level to ransomware incidents. These organizations generally have sufficient security tools, robust cyber liability insurance, and strong data recovery programs or operational redundancy. Instead of ransomware, these organizations are often more concerned about defending against nation-state attackers and advanced persistent threat (APT) groups.

While it makes sense to be concerned about determined and highly skilled threat groups—the sorts of threat actors who can circumvent even a mature organization's security controls—dismissing the threat of ransomware can overlook the infrequent but impactful ransomware attacks that are now run by APT groups.

Some APT groups use ransomware to raise money, either for individuals or for their organization. In other cases, threat actors use ransomware as a distraction from a larger and more impactful compromise.

APT Financial Motivation

Threat groups from countries that have been observed using ransomware in their attacks (including North Korea and Iran) are also among those currently under economic embargoes or sanctions by the United States government. This perhaps gives them extra motivation to seek financial benefit—and carries legal consequences that may eliminate an organization's ability to pay a ransom demand.

Threat groups from North Korea seem particularly interested in financial gain, as other tactics observed in their attacks (such as cryptocurrency theft and ATM cash-outs) also fit this pattern.

Ransomware payments could (in some cases) help fund these countries' domestic programs, which has led the U.S. Cybersecurity Infrastructure and Security Agency (CISA) to warn that paying ransomware operators could pose sanctions risks. They also noted that when organizations take proactive steps to prevent ransomware attacks, the U.S. Treasury's Office of Foreign Assets Control (OFAC) would be more likely to resolve apparent sanctions violations with a nonpublic enforcement response.

The British Office of Financial Sanctions Implementation (OFSI) issued sanctions in February against a number of individuals associated with ransomware groups. Guidance from the OFSI indicates that the purpose is to "disrupt and reduce the profitability of ransomware."

Paying ransoms will likely be even more heavily scrutinized by governments worldwide, especially as nations continue to sanction Russia, with which a number of well known ransomware groups are associated.

APT Smoke Screens and Red Herrings

Other threat groups, including some from Iran or China, seem to have a different objective when using ransomware. Threat actors can gain more than money from deploying ransomware—it also has potential for both destruction and espionage.

Some malware authors have taken steps to blur the lines between ransomware and wipers. Iranian attackers have specifically used wipers for destructive effect. Wipers could be very useful for getting rid of evidence of a threat groups' activities, while creating the appearance of a ransomware attack. If this approach is successful, organizations may not realize the true purpose of a threat group's intrusion.

Similarly, ransomware has been used as a way of disguising intellectual property theft or cyberespionage as something more banal. APT groups steal data from environments and attempt to pass it off as a multi-extortion scheme, promising to destroy the data if a ransom payment is made. In reality, the stolen data is not destroyed and is likely used to the threat actor's advantage.

Defending Against APTs and Cybercrime Groups

The TTPs used to deploy ransomware for either APT or cybercrime groups are often identical. Both groups exploit vulnerabilities to gain access to a target system, then compromise credentials and move laterally.

These common areas are where organizations must focus their defenses and visibility. Unfortunately, paying a ransom is not always the end of the story. With APT groups in the mix and ransomware groups using multi-extortion in the majority of the cases we see, apparent ransomware attacks are often related to data exfiltration. This can be especially concerning in light of a trend of cyber insurance providers stating that acts of war won't be covered. In some cases, a ransomware attack attributable to APT actors could be defined as such.

CONCLUSION

What to Expect From Extortion Groups in 2023

The most important information about the threat landscape is not where we have been, but where we are going. When we ask our incident responders and threat intelligence analysts what's coming for extortion, they make a few key predictions.

Prediction #1: Government involvement will be key to disrupting the operations of extortion groups.
Bans on payments to certain groups and countries have changed the landscape of the ransomware and extortion business. In some cases, concerns about sanctions may have influenced more organizations to refuse to pay threat groups, lowering revenue and causing affiliates to abandon known groups to work with unsanctioned groups instead.

Prediction #2: This will be the year we see a large cloud ransomware compromise.
Most of our cloud incident response cases thus far have shown threat actors reaching for low-hanging fruit. Organizations often neglect basic security controls and don't take advantage of security features offered by the major cloud service providers or additional enhanced cloud security tools. While threat actors know about these gaps, they've mostly chosen to not exploit these security issues for ransomware and extortion since there are still some complexities in cloud environments that they'll need to work through.

However, it's always been clear that ransomware actors will shift their focus to cloud environments and engage in attacks that require more skill but could have a larger payoff due to the potential operational impact to organizations. In recent years, Unit 42 has tracked cloud threat actors—individuals or groups posing a threat to organizations through directed and sustained access to cloud platform resources, services or embedded metadata. These threat actors have evolved their TTPs specifically to target cloud workloads.

While the shared responsibility model reduces users' burden in securing infrastructure, platform, and software in the cloud, we've also seen organizations—particularly the world's largest—transfer increasing amounts of valuable data and workloads to the public cloud. 2023 will be the year that this tempts threat actors to make the adaptations needed to deploy ransomware in cloud environments.

When this happens, it will raise new questions about the shared responsibility model—especially if ransomware deployed on a cloud service provider's platform manages to affect multiple clients.

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Protect Your Cloud Architectures

Threat actors will continue to weaponize and build attack payloads to compromise cloud workloads. As such, it is integral that a comprehensive cloud security program (from a governance perspective) and a cloud security platform (from a technical controls perspective) are both in place at the organization. The cloud security platform should be able to detect and prevent attacks to cloud workloads, network security, code (including infrastructure as code and source code), containers, identities and keys, and data.

Prisma Cloud is one example of a platform that offers comprehensive cloud native security.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

Prediction #3: Threat actors will identify novel means of initial access.

Our incident responders are seeing threat actors turning to different methods of initial access, including SEO poisoning (especially augmented by malvertising), callback phishing, and fake software installs and/or updates. This is because of the effectiveness of introducing social engineering elements, as well as the need to move away from other methods that are commonly detected.

Prediction #4: Threat actors will ramp up additional extortion methods.

Our data already shows an increase of data theft and harassment in conjunction with encryption. We expect this trend to continue as threat actors respond to lower success rates by attempting to increase the pressure to pay. This leads to our next prediction.

Prediction #5: Extortion without encryption will rise.

As threat actors have found success by adding extortion methods to ransomware, some groups have drawn the conclusion that extortion can be effective on its own. Forgoing the encryption step allows threat actors to reduce the technical complexity of an attack. We expect more groups to explore this approach.

What is SEO Poisoning?

Threat actors leverage search engine optimization (SEO) to infect potential victims. Unit 42 has often seen this take the form of (fake) software downloads, browser updates, or malicious document templates. For example, a threat actor compromises legitimate websites and shares supposed templates for common business document types, such as certain accounting or human resources forms, and these files contain malware. When a victim is searching for some kind of template (e.g., an invoice template), they find the malicious file via search results and upon downloading and opening it, are infected with malware. This malware gives the threat actor a foothold into the victim's environment. Unit 42 has repeatedly seen GootLoader and SocGholish in association with this technique.

Prediction #6: Politically-motivated ransomware incidents will rise.

Ransomware and extortion are most obviously carried out for financial gain. However, in some cases, these activities can be connected to political motivations. Groups may use ransomware to fund other politically-motivated activities. They may also use ransomware and extortion to disrupt the political process, destabilize critical infrastructure, create fear and anger at governments, and sow discord.

Prediction #7: Insider threats will lead to extortion attempts.

In 2023 alone, there have been more than 100,000 layoffs from more than 300 tech companies. Some of the people affected will hold a grudge—and have the skills to take revenge. Insider threats can be particularly dangerous because employees are more likely to know where the crown jewels are kept. In today's environment, an insider threat can cover their identity by selling access and other information to cybercriminal groups, making the act potentially more tempting.

Prediction #8: Attackers will infect supply chains and source code of victims before using ransomware to distract from the supply chain infection.

As more organizations learn how to deal with ransomware, they may begin to treat a ransomware infection as routine. Threat actors will take advantage of this by deploying ransomware to distract from the true purposes of their attacks. Taken to an extreme, this could allow threat actors to remain under the radar while orchestrating attacks that could affect large numbers of organizations worldwide.

Organizations should review incident response plans for ransomware and extortion with a view to the future landscape. We expect highly motivated threat actors to continue to seek additional layers of leverage to get what they want from their targets. We anticipate other types of threat groups taking advantage of known cybercrime techniques. Responsible security leaders should consider that dealing with today's extortion techniques goes beyond safeguarding data—as vital as that is. It is also a key responsibility to protect your organization's reputation, and the safety of employees, partners, and customers.

RECOMMENDATION

UNIT 42 EXECUTIVE RECOMMENDATION:

Talk to Your Board About Ransomware and Extortion

When it comes to ransomware, boards are most concerned with risk management and how effectively the organization is managing ransomware threats to the business. Boards frequently ask, after seeing in the news that one of their peers was significantly hit by ransomware or extortion, "Would we be able to prevent that type of attack?"

When the CISO is asked this type of question, they need to have defensible, objective data to respond with that maps directly to the risks that boards are most concerned with. These risks are often regarding the following categories:

- Strategic risk
- Reputational risks
- Compliance or regulatory concerns
- Operational issues
- Financial risks

The CISO's reponse should be able to link their ransomware and extortion readiness and prevention capabilities to those that would mitigate the risk areas that the board is focused on.

Organizations that are well prepared to engage in these discussions focus on proactively improving their security posture against known attacker tactics and techniques. Unit 42 consultants leverage the experience of responding to thousands of attacks into services that discover weaknesses for clients. Our consultants work with clients to build roadmaps and proactively secure gaps.

These trusted security advisors use Palo Alto Networks technology to accomplish

- Attack Surface Assessments
- Ransomware Readiness Assessments
- Incident Response Playbook Design and Review
- Incident Simulation Exercises
- SOC Transformations

Unit 42 consultants also partner with clients to discover and improve their capabilities to respond with a host of readiness and testing offerings aligned with the goals of the CISO and the needs of the board.

Read **Mitigating Cyber Risks with MITRE ATT&CK** for an in-depth set of recommendations by Unit 42 incident responders.

REACH OUT TO EXPERTS

Need help with a ransomware or extortion incident? Call in the experts.

If your files and applications are inaccessible due to a ransomware attack, please contact us. The Unit 42 Incident Response team is available 24/7, year-round, and can swiftly help investigate, contain, and eradicate the threat, so you can restore operations quickly. And while we hope you never need it, we can help negotiate ransom demands on your behalf.

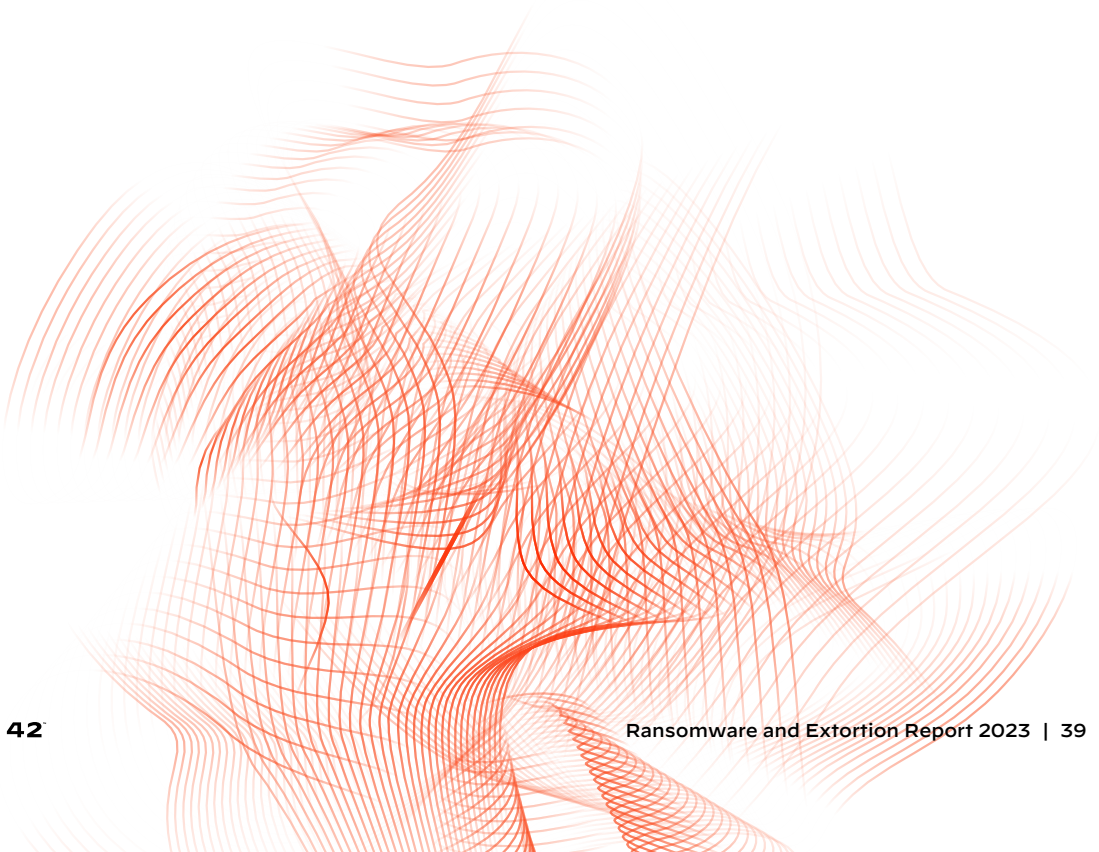
Additionally, with a Unit 42 Retainer in place, you can make our incident response experts an extension of your team—on speed dial. You can also choose to allocate your retainer credits for proactive Unit 42 cyber risk management services, such as a Ransomware Readiness Assessment.

Methodology

In creating this report, we reviewed the findings from a selection of approximately 1,000 incident response cases Unit 42 completed between May 2021 and October 2022. We reviewed a smaller subset (about 100 cases) for insights into ransomware and extortion negotiations. While the majority of cases were located in the U.S., the threat actors conducting attacks were located worldwide while targeting businesses, organizations, and IT infrastructure worldwide.

We also gathered information from our ongoing monitoring of dark web leak sites, as well as our threat intelligence analysts' work tracking cybercrime groups and APTs.

Finally, we supplemented our case data by conducting in-depth interviews with experienced security consultants to gather recommendations and predictions based on their work with clients in specific areas of expertise.



Unit 42 Incident Response Methodology

Every minute that an attack remains unresolved costs your organization money and can damage its reputation. With Unit 42 Incident Response team experts by your side, you will jump-start your investigation and take advantage of our experience responding to thousands of incidents similar to yours. With our threat-informed approach to incident response and advanced tools across endpoint, network, and cloud, we provide fast containment to minimize the impact on your business.

Unit 42's average response time—how long it takes us to make initial contact after receiving a request for assistance—is well under 15 minutes. Once called in, we work quickly to understand the full scope of the intrusion, which systems are impacted, and what security actions have already been taken so we can quickly contain the incident. We do this quickly, and remotely, to help you respond to an incident with speed. We follow the proven methodology outlined below.

We follow a proven methodology:

Scope
For an accurate understanding of the incident, it's critical to get the scoping phase right. This allows us to align the right resources and skill sets to get your organization back running as quickly as possible and accurately estimate the level of effort needed to assist you.

Investigate
We work to fully understand the incident as we investigate what happened, leveraging the available data and working alongside your team.

Secure
As the incident is contained and the threat actor and their tools are eradicated from your environment, we concurrently assist your organization with rapidly restoring operations.

Support and Report
Unit 42 will also assist you in understanding the root cause and potential impact of the incident, including any unauthorized access or acquisition of sensitive information that may trigger legal obligations.

Transform
We believe a key step in incident response is helping ensure an improved security posture going forward. We work with you to apply specific improvements and build out incident response plans that will help protect against future and similar attacks.

Learn more about Unit 42 Incident Response services

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 Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com