UNIT 42™

RANSOMWARE THREAT REPORT 2022

paloalto® NETWORKS

TABLE OF CONTENTS

Foreword

Ransomware attacks commanded headlines around the world in 2021, and show no signs of slowing down. In fact, cybercriminals are doubling down by finding additional ways to extort victims in conjunction with ransomware. Double extortion first took off in 2020 with the rise of dark web leak sites that cybercriminals used to identify ransomware victims and threaten to leak sensitive corporate data. In 2021, ransomware gangs took these tactics to a new level, popularizing multi-extortion techniques designed to heighten the cost and immediacy of the threat. For example, we've seen gangs make threatening phone calls to employees and customers and launch denial of service (DoS) attacks to shut down a victim's website in an effort to incentivize payments.

In 2021, we also saw ransomware-as-a-service (RaaS) operators grow. RaaS operators offer a wide array of easy-to-use tools and services that make launching ransomware attacks almost as simple as using an online auction site. These operators have been making investments during these past few years to optimize their businesses – they have perfected their malware, developed marketing strategies to recruit more affiliates, and even built up technical support operations to help victims get back online once they pay their ransoms.

All these innovations have made it harder for organizations to defend against ransomware, forcing some to make the hefty sorts of payments that are documented in this report. The average ransom demand on cases worked by Unit 42 consultants last year climbed 144% to $2.2 million, while the average payment rose 78% percent to $541,010.

As these ransomware gangs and RaaS operators find new ways to remove technical barriers and up the ante, ransomware will continue to challenge organizations of all sizes in 2022. As a result, ransomware has become one of the top threats in cybersecurity and a focus area for Palo Alto Networks. This report provides the latest insights on established and emerging ransomware groups, payment trends, and security best practices. I hope these insights will help you better understand and manage the threat to your organization.

Ryan Olson
VP of Threat Intelligence,
Unit 42, Palo Alto Networks

Executive Summary

Ransomware was a headliner in 2021, with a series of high-profile attacks disrupting businesses, governments and schools around the globe. The attacks interfered with a number of everyday activities people take for granted: seeing a doctor, getting gas, buying groceries, watching the local news on TV, paying bills, booking travel, and even calling for emergency assistance.

Unit 42 has compiled the 2022 Ransomware Threat Report to help put all this ransomware activity into context and offer a better understanding of the scope of the ransomware landscape and where it is headed. **To generate the report, our researchers and security consultants pulled data from two sources:**

1. The cases handled by Unit 42, which provide an on-the-ground view of the diverse range of threat actors out there.
2. The analysis of leak sites, where ransomware operators provide snippets of stolen information as part of their name-and-shame (multi-extortion) tactics designed to coerce victims to pay ransom demands, as well as general underground forums where cybercriminals discuss the tools of their trade.

One key takeaway is that ransoms keep rising – both demands and payments. Among our incident response cases in 2021, which were predominantly in the U.S., the average ransom demanded was approximately $2.2 million. This represents about a 144% increase from the average demand of $900,000 from the cases our consultants handled in 2020. The average payment in cases worked by Unit 42 consultants climbed to $541,010, which is 78% higher than the previous year.

144%

AVERAGE DEMAND IN 2021

78%

AVERAGE PAYMENT IN 2021

The tactics employed by these cybercriminals mirror the growing sophistication and maturity of the ransomware landscape. **In 2021 we increasingly saw:**

Multi-extortion techniques where attackers not only encrypt the files of an organization, but also name and shame the victims and/or threaten to launch additional attacks (e.g., distributed denial of service, known as DDoS) to encourage victims to pay more quickly. In 2021, the names and proof of compromise for 2,566 victims were publicly posted on ransomware leak sites, marking an 85% increase compared to 2020.

Extremely prolific ransomware-as-a-service (RaaS) business models, which offer "startup kits" and "support services" to would-be cybercriminals, significantly lowering the technical barrier to entry and accelerating the speed with which attacks can be introduced and spread.

Rapid weaponization of vulnerabilities. For example, major ransomware gangs quickly exploited CVE-2021-44228, commonly referred to as Log4Shell. It is highly likely that as long as organizations fail to patch known critical vulnerabilities, attackers will exploit them to their advantage.

It seems no one is immune to ransomware attacks – organizations in almost every country and industry were targeted in 2021. Our analysis of ransomware leak sites identified the Americas region as the most impacted – 60% of the victims listed were attributed to this region, while 31% and 9% were attributed to the Europe, Middle East, and Africa (EMEA) and Asia Pacific regions respectively. Professional and Legal Services, followed by Construction, were the most targeted sectors, with 1,100 and 600 victims respectively named on leak sites.

Most targeted countries

60% AMERICAS

31% EUROPE, MIDDLE EAST AND AFRICA

9% ASIA PACIFIC

Most targeted sectors

1,100 PROFESSIONAL AND LEGAL SERVICES

600 CONSTRUCTION

The long-term effects of these ransomware attacks can be devastating, going beyond the actual cost of the ransom to include a number of ancillary costs associated with downtime, remediation, and disruptions to the business.

It's our hope that shining a light on the tactics, techniques, and procedures (TTPs) of ransomware groups will help defenders turn the tables on ransomware gangs and start to change the narrative. In that spirit, this report provides actionable insights that can be used to address the ransomware problem. The ultimate objective of this report is to help organizations understand the ransomware landscape and become better able to bolster defenses and determine the best course of action, if (or when) undergoing a ransomware attack.

01 | Ransomware 101

Ransomware comes in many varieties.

Different ransomware groups are known for the types of attacks they launch – the files, methods, tactics, and notes they use – and the targets they go after. Recent headlines have been dominated by ransomware gangs such as Conti and REvil. These groups actively recruit affiliates (cybercriminals) to carry out their attacks. Sometimes, ransomware groups maintain an online presence, such as a leak site, "support" site, and/or social media profile to help them with their affiliate recruitment and overall success rates.

Ransomware is a type of malware used by cybercriminals for financial gain. It is delivered in the same way any type of malware makes its way onto victim systems. For example, attackers will exploit known vulnerabilities, take advantage of systems that have already been compromised, and/or use social engineering tactics, such as phishing emails that attempt to trick users into downloading infected files or clicking on malicious links, to get a foothold into an organization that they can use to carry out their attack.

Once in, the ransomware will take over the victim's files or systems and encrypt key information to render it unusable to the organization. The attacker will demand a ransom be paid in exchange for a decryption key, which will presumably return the files to their original state.

Typically, a ransom note is installed on a victim's system at the same time the files/systems are encrypted. The note will include information on the ransomware gang's demands; it will detail the amount of the ransom demand, a deadline for payment (sometimes including a discounted offer for early payment), and instructions on how to reach and pay the group demanding the ransom, providing details on the cryptocurrency wallet or other wiring information the victim will need to complete the transaction. Occasionally, groups include more colorful information in their notes, such as critiques of the victim organization's security posture or offers to help secure the victim in the future – for a price.

Sometimes, a group will offer victims a way to test the decryption key on certain files or provide other forms of proof that the attack is real and dangerous – e.g., posting a sampling of data on the ransomware gang's leak site. In recent years, the definition of ransomware has been extended to include double or multi-extortion attacks, which combine additional threats and tactics, on top of holding a victim's data hostage.

These tactics pressure victims to pay the ransom fast and in full, as well as make it so that offline backups aren't sufficient for organizations. It used to be that if organizations had (and tested) offline backups, it was enough to recover from a ransomware attack. With multi-extortion, those backups can't prevent all the negative effects that ransomware groups can leverage.

Double extortion is the practice of exfiltrating data during a ransomware attack that is used to blackmail victims into paying. The idea is victims won't want their information posted on a leak site (typically hosted on the dark web) or put up for sale through other illicit forums, so they will be incentivized to conclude the incident as fast as possible. Multi-extortion includes even more pressure tactics, such as launching distributed denial-of-service (DDoS) attacks that shut down public-facing websites belonging to targeted organizations.

02

The Ransomware Landscape

After analyzing ransomware activity in 2021 and comparing it to the activity of the past several years, we have seen some recurring techniques and tactics that attackers rely on, as well as some emerging trends that are shaping the ransomware landscape. The following are the observations that you need to be mindful of — both old and new — when building strategies to bolster your defense.

How Ransomware Actors Behave

Attackers Take Shortcuts

Using an initial access broker, who sells ready access to corporate networks to anyone who will pay for it, is becoming standard for many ransomware gangs. While many in the cybercrime world want this kind of access, ransomware operators are particularly interested because it saves their affiliates a lot of effort and time. The cooperation is very profitable for both the ransomware operators and the access brokers. It also enables less sophisticated threat actors, who lack the skills to find an unobtrusive way into a network, to quickly and easily carry out attacks by simply dropping ransomware into an already compromised environment. Organizations should remain vigilant and do all they can to uncover attackers hiding in their environment, looking for lateral movement and dormant executable files that could indicate the presence of an attack foothold.

Attackers Will Use Any Tricks They Can

Attackers are increasingly using anonymized services, which makes it more difficult for security researchers and law enforcement to track activities and identify indicators of compromise (IoCs) that can be used for network defenses. Tor, short for The Onion Router, and other anonymous services are very popular with ransomware groups and will likely continue to be a critical part of their tactics to make it as hard as possible to defend against their attacks.

Attackers Are Innovative

Ransomware threat actors continue to invest in their own tooling to keep compromising victims, developing new and updated ransomware variants for use as standalone malware or alongside commodity malware. More ransomware groups are developing variants to target additional operating systems, such as Linux (e.g., HelloKitty), or leveraging highly customizable programming languages, such as Rust (e.g., BlackCat), to create attacks more easily. It is clear that adversaries will continue to create new variants and build out their capabilities to target all kinds of systems, which will widen the scope of possible victims in the process. Organizations need to do the same with defenses, adapting and adding capabilities to minimize the attack surface.

Three Ransomware Trends to Know for 2022

1 Victim Shaming Is on the Rise

Increasingly, ransomware gangs are using multi-extortion techniques in an effort to strong arm the victim organization to pay the ransom demand. They not only encrypt an organization's files, but also leverage leak sites and threaten follow-on attacks (e.g., DDoS) to incentivize a swift payout. Releasing samples of the victim's stolen/compromised data on the dark web or their gang's leak site is a way for the perpetrator to prove they have the information and the threat is serious – they may even include details on the total amount of data they have – to name and shame the victims into payment. These tactics prevent offline backups from stopping all the negative effects of a ransomware attack.

Multi-extortion techniques were less than a year old heading into 2020, but exploded in popularity last year. At least 35 new ransomware gangs, such as Black Matter, Hive, and Grief emerged and threatened to expose data or utilized leak sites in 2021. Suncrypt and a new player, BlackCat, began executing triple extortion attacks, siphoning a victim's data before deploying their ransomware and then threatening to release the information and launch a DDoS attack if the ransom was not paid. In 2021, the names and proof of compromise for 2,566 victims were publicly posted

35
NEW RANSOMWARE GANGS IN 2021

2,566
VICTIMS PUBLICLY POSTED ON LEAK SITES IN 2021

85%
INCREASE IN VICTIMS COMPARED TO 2020

on ransomware leak sites, marking an 85% increase compared to 2020. Be prepared to see more multi-extortion attack tactics in 2022 and beyond.

2 Ransomware-as-a-Service Is Quickly Lowering the Technical Bar

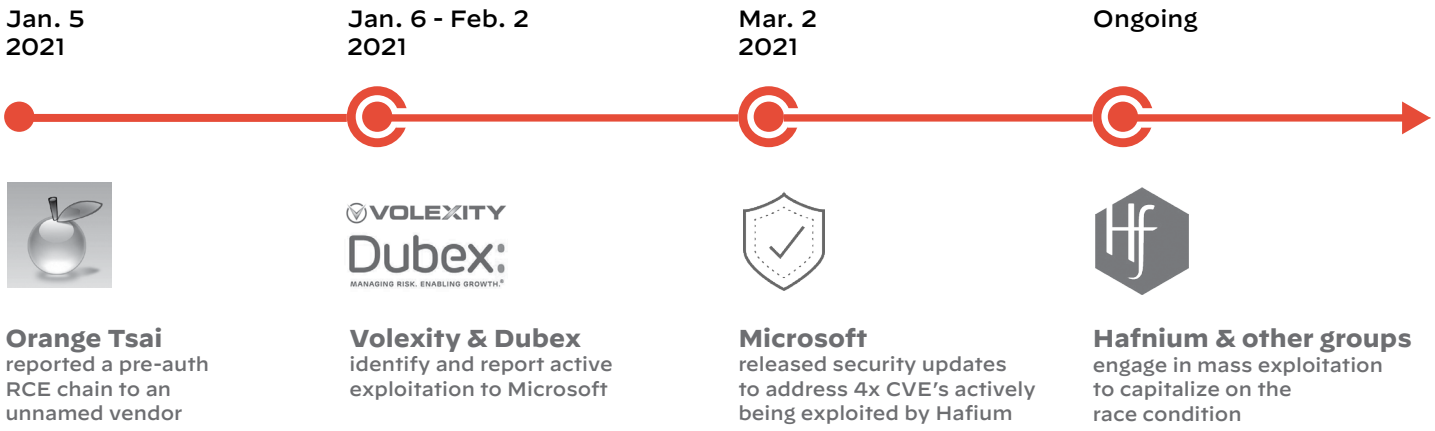
Ransomware has proven to be an effective mechanism for cybercriminals to hit it big, in terms of both payouts and notoriety. This has led to an evolution of the ransomware scene with "entrepreneurial" threat actors looking to capitalize on a growing number of cybercriminals who want in. These entrepreneurs have started offering RaaS. This is a business for criminals, by criminals, with agreements that set the terms for providing actual ransomware to affiliates, often in exchange for monthly fees or a percentage of ransoms paid. RaaS makes carrying out attacks that much easier, lowering the barrier to entry and expanding the reach of ransomware. We are actively tracking at least 56 active RaaS groups, some of whom have been operating since 2020. Due to the success of these groups, we expect activity of this type to continue to grow.

3 Attackers Are Making Increasing Use of Zero-Days

Ransomware attacks often leverage a wide variety of vulnerabilities as an initial vector of compromise. In 2021, we observed at least 42 vulnerabilities across different technologies being used by ransomware operators.

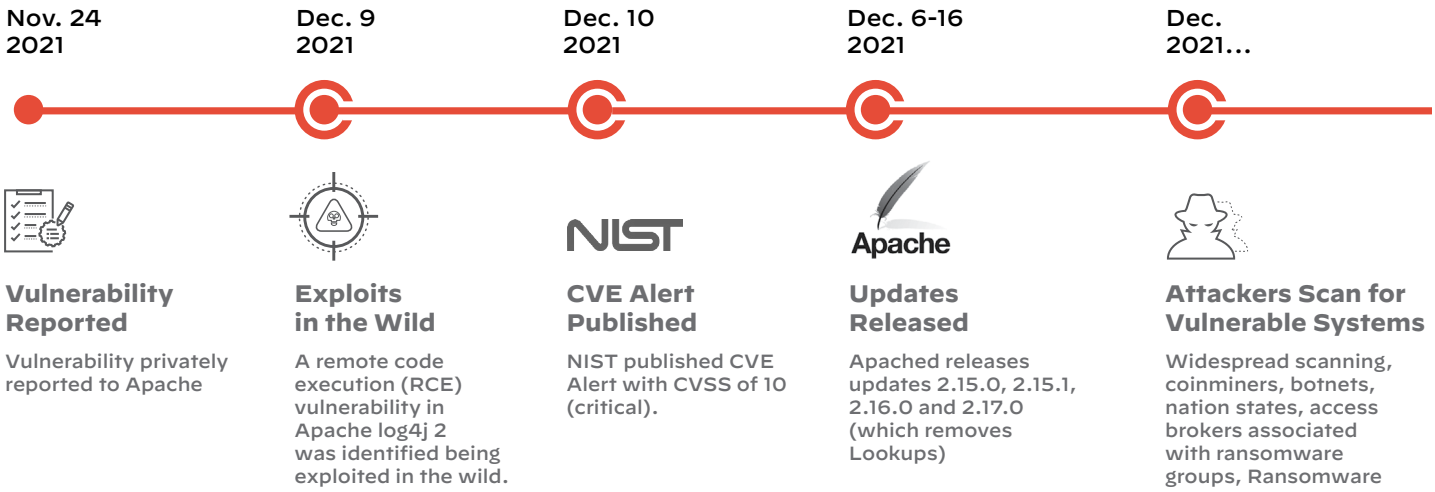
Figure 1: Vulnerabilities that have been observed being used by ransomware affiliates in 2021

Figure 2: Microsoft Exchange Server vulnerabilities timeline



While there is some reliance on older, unpatched vulnerabilities, we believe threat actors are increasingly tracking high-profile vulnerabilities and exploiting them to gain an initial foothold in an organization. The timeframe from vulnerability to exploit is getting shorter – it can practically coincide with the reveal if the vulnerabilities themselves and the access that can be achieved by exploiting them are significant enough. We saw this with Hafnium's advanced persistent threat against Microsoft Exchange Server vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065), where various attacks were launched by multiple threat groups to capitalize on vulnerable systems.

Figure 3: Log4j timeline



Another example came at the beginning of September when Conti used CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 (ProxyShell) in their ransomware attacks and then, in December, started exploiting the recent vulnerability CVE-2021-44228, known as Log4Shell, as a way to gain entry to victims as well as to move laterally across internal devices.

As long as vulnerabilities are available (unpatched), attackers will take advantage of them to further their objectives. It's important to keep in mind that attackers may also take advantage of vulnerabilities in third-party software or attack supply chain elements, which can introduce risks for many organizations down the line. We saw this with REvil in the Kaseya attacks.

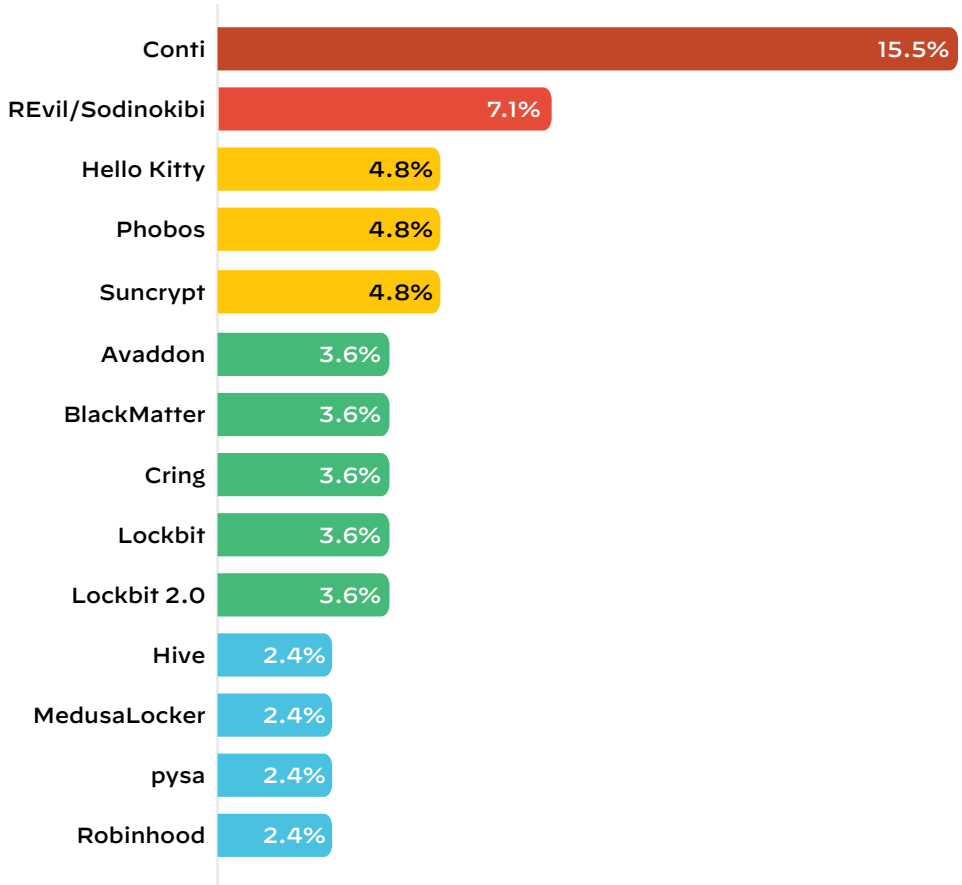
Organizations may have previously grown used to taking time between the disclosure of a vulnerability and patching it, but while it's still necessary to perform due diligence on a patch, attackers' ability to scan the internet in search of vulnerable systems means it's more important than ever to shorten the time it takes to patch. Organizations need to ramp up patch management and orchestration to try to close these known holes as soon as possible.

03

Ransomware Group Behavior

In 2021, we saw the emergence of many new ransomware gangs, as well as the re-emergence of a number of established players who had gone quiet for a period of time. Most of these ransomware groups proceeded to be very active, increasingly employing multi-extortion tactics to improve the likelihood of a payout.

Figure 4: Most active ransomware variant in 2021 – Unit 42 incident response data



Most Active Ransomware Groups

Conti was by far the most active of the ransomware groups among the incident response cases handled by Unit 42 in 2021, making up 15.5% of ransomware activity; REvil/Sodinokibi was the second at 7.1%, followed by Hello Kitty and Phobos at 4.8% each.

15.5%
CONTI

7.1%
REVIL/SODINOKIBI

4.8%
PHOBOS

4.8%
HELLO KITTY

Conti

As noted, Conti was the most active ransomware group among the incidents handled by Unit 42 in 2021. They impacted large victims asking for very high ransom demands. We first observed them in March with an initial ransom amount of $50,000. This was the lowest request reported during the year for this group. They quickly and significantly increased their demands, averaging around $1.78 million for the year – their top initial payment request was $3 million. Given their initial (only observed) ransom demand in 2020 was $187,114, it is fair to say they have been quickly growing in numbers and confidence.

Conti stands out as one of the most ruthless ransomware gangs since their emergence in 2020. They operate without a "code of honor" that some other threat actors claim to observe when it comes to targeting vital or particularly vulnerable victims. Conti carries out attacks against hospitals, emergency services, and law enforcement agencies, using double extortion techniques to shame victims into paying a ransom. From leak site data, which includes victims beyond those handled by our incident response team, we found that Conti has leaked the information of more than 600 organizations since 2020.

600+
ORGANIZATIONS AFFECTED SINCE 2020


HOSPITALS


EMERGENCY SERVICES


LAW ENFORCEMENT

Conti is also opportunistic, exploiting known vulnerabilities as an initial vector of compromise. In 2021, they used CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 (ProxyShell) in their ransomware attacks, and then started successfully exploiting CVE-2021-44228, known as Log4Shell, in December, as a way to move laterally across internal devices.

In February 2022, a large amount of data associated with Conti was leaked, including internal chat messages, screenshots, and raw data files. Much of the information was originally in Russian. Here we show screenshots of translated versions of some of what was leaked – providing a view into how Conti operates when conversing with their victims.

Conti stands out as one of the most ruthless ransomware gangs since their emergence in 2020.

$118,114
2020 INITIAL (ONLY OBSERVED) RANSOM DEMAND

$50K
MARCH 2021 INITIAL RANSOM DEMAND

$1.78M
AVERAGE 2021 RANSOM DEMAND

$3M
TOP 2021 REQUEST

```
  { "ts": "2021-11-06T11:27:44.059579",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "bio@q3mcco35auwcstmt.onion",
  "body": "hi"
}
{
  { "ts": "2021-11-06T11:27:51.064723",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "bio@q3mcco35auwcstmt.onion",
  "body": "are you there ?"
}
{
  { "ts": "2021-11-06T11:28:02.267373",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "body": "I did not mean to step on your toes seems I did not get my message over
to you. We do understand the consequences of the situation. That is why we want to
negotiate a solution with you! All I was trying to deliver is the message that we
are in a tough economic situation and simply cannot pay your demand. I have spoken
to my management. They understand the situation and are willing to pay. The money
we can afford is 500,000.00 USD. This is a huge amount for us. Please let us fix a
deal."
}
{
  { "ts": "2021-11-06T11:28:19.202666",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "Here are the guys you wrote the bigger letter to yesterday."
}
{
  { "ts": "2021-11-06T11:28:40.724324",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "body": "he Price to unlock is
  $2,000,000."
}
{
  { "ts": "2021-11-06T11:29:02.278040",
  "from": "tramp@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "body": "we need to raise their price to 1.5kk at least"
}
```


Figure 5: Translation of Conti communications, November 2021

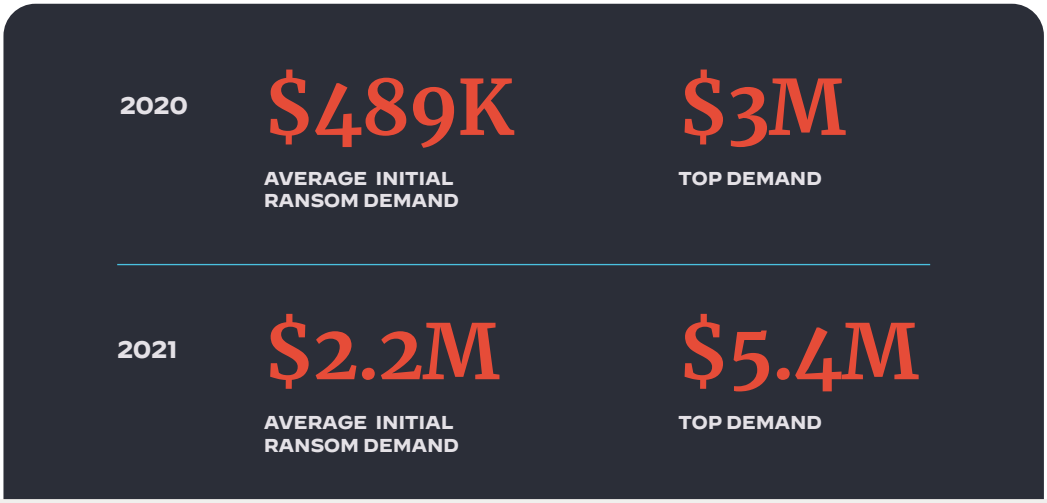

```
{
  { "ts": "2022-02-23T12:50:43.214428",
  "from": "pumba@q3mcco35auwcstmt.onion",
  "to": "skippy@q3mcco35auwcstmt.onion",
  "body": "We are very upset that you don't believe in the fulfillment of our
conditions. First of all, we appreciate and value our reputation (about us and
on the fulfillment of our agreements you can find a lot of information in the
Internet). This is the main thing. But you will understand this when we make the
deal. The second one, we will explain you a little bit deeper about amount: The
Conti has a big legal department and it checks all the possible data and sources to
establish an appropriate amount. We check your annual income, the value of
materials (you have a lot of SENSETIVE and PRIVATE files, Military bufget and so
on), etc.
Also, please don't forget about the decryption software and our expenses.
Therefore, basing on all the info, we set a 5% amount for a payment. FYI, every our
client is asked to pay this sum, you are not unique. But considering your situation
we can give you very big disount - 20%. Now our price for you is $8kk."
}
```


Figure 6: Translation of Conti communications, February 2022

REvil - also known as Sodinokibi

REvil/Sodinokibi was the second most active ransomware group during 2021, dropping slightly from being the most active in 2020. From our 2021 incident response data, they averaged an initial ransom demand of approximately $2.2 million. This was significantly higher than what was observed during 2020, when their average ransom demand was $488,928.52. In 2020, their top initial ransom demand was $3 million; in 2021 their highest demand was $5.4 million.

The operator behind this ransomware, PINCHY SPIDER, switched its GandCrab operations to REvil/Sodinokibi in mid-2019. This was probably due to recent arrests of affiliates suspected of about 7,000 infections. The switch, however, did nothing to lower their profile; in fact, thanks to the Kaseya VSA and other big headline attacks, they are one of the world's most notorious ransomware operators.



REvil/Sodinokibi is also one of the most prominent providers of RaaS, taking a percentage of the negotiated ransom price as their fee. The size of specific ransoms depended on the size of the organization and type of data stolen. Further, when victims failed to meet deadlines for making payments via Bitcoin, the attackers often doubled the demand. Eventually, they posted stolen data on leak sites if the victim didn't pay up or enter into negotiations.

BlackCat

BlackCat (aka ALPHV) is notable because of the group's meteoric rise – just one month after surfacing, in November 2021, BlackCat had the seventh-largest number of victims listed on their leak site among ransomware groups tracked by Unit 42. Operating a RaaS business model, BlackCat was observed soliciting affiliates in known cybercrime forums. They offered to allow affiliates to leverage the ransomware and keep 80-90% of the ransom payment, paying the remaining 10-20% to the BlackCat author. The largest number of the group's victims so far are U.S. organizations, but BlackCat and its affiliates have also attacked organizations in Europe, the Philippines, and other locations. Victims include organizations in the following sectors: construction and engineering, retail, transportation, commercial services, insurance, machinery, professional services, telecommunication, auto components, and pharmaceuticals.

80–90%

RANSOM PAYMENT TO AFFILIATES

10–20%

RANSOM PAYMENT TO THE BLACKCAT AUTHOR

BLACKCAT VICTIMS INCLUDE ORGANIZATIONS IN THE FOLLOWING SECTORS:

- construction and engineering
- retail
- transportation
- insurance
- commercial services
- professional services
- machinery
- telecommunication
- auto components
- pharmaceuticals

BlackCat ransomware is one of the first, if not the first, to be coded in the Rust programming language (though other malware has used Rust). Rust has numerous native options and is highly customizable, which makes it easier for malware authors to pivot and individualize attacks. By leveraging this programming language, ransomware attacks can be easily compiled against various operating system architectures, which could account for BlackCat's fast, prolific nature.

AvosLocker

AvosLocker is RaaS that started operations in late June, using a blue beetle logo to identify itself in communications with victims and "press releases" aimed at recruiting new affiliates. AvosLocker was observed promoting its RaaS program and looking for affiliates on dark web discussion forums and other forums. Like many of its competitors, AvosLocker offers technical support to help victims recover after being attacked with encryption software that the group claims is "fail-proof," has low detection rates, and is capable of handling large files. This ransomware also has an extortion site, which claims to have impacted six organizations in the following countries: the U.S., the U.K., the U.A.E., Belgium, Spain, and Lebanon.

Hive Ransomware

Hive Ransomware is double-extortion ransomware that started operations in June. Since then, Hive has impacted 66 organizations that are now listed on the group's extortion site, including a European airline company and three U.S.-based organizations. Hive uses all tools available in the extortion tool set to create pressure on the victim, including publishing the date of initial compromise, a countdown, the date the leak was actually disclosed on their site, and even providing the option for visitors to the leak site to share the disclosed leak on social media.

HelloKitty

HelloKitty is not a new ransomware group – it can be traced back to 2020, when it mainly targeted Windows systems. However, in July, we observed a Linux variant of HelloKitty targeting VMware's ESXi hypervisor, which is widely used in cloud and on-premises data centers. We also observed two clusters of activity. Across the observed samples, some threat actors preferred to communicate with victims via email, while others used the peer-to-peer anonymous instant messenger service, TorChats. The observed variants impacted five organizations in Italy, Australia, Germany, the Netherlands, and the U.S.

LockBit 2.0

LockBit 2.0 (previously known as ABCD ransomware) changed their name to LockBit in July 2021 and launched a slick marketing campaign to recruit new affiliates. It appeared to work, since the three-year-old RaaS operator was linked to some high-profile attacks in 2021 across multiple industries. Their success prompted the Federal Bureau of Investigation to publish a warning on them in early 2022. **The group claims to offer the fastest encryption on the ransomware market.** To date, there are 406 victims listed on the group's leak site, including organizations in the U.S., Mexico, Belgium, Argentina, Malaysia, Australia, Brazil, Switzerland, Germany, Italy, Austria, Romania, and the U.K.

Mespinoza

Mespinoza was observed targeting real estate, manufacturing, and education organizations. Through research and analysis, Unit 42 researchers have concluded that Mespinoza has a large global reach, with victims in the U.S., Canada, South America, Europe, South Africa, and Australia. **Mespinoza uses the remote desktop protocol as an initial intrusion vector and exfiltrates files for exposure on leak sites.**

eCh0raix

eCh0raix has been active for about a year targeting Synology network-attached storage (NAS) and Quality Network Appliance Provider (QNAP) NAS devices used in small offices and home offices (SOHOs). To date, the attacks have resulted in modest payouts. **SOHO users are attractive to ransomware operators because they typically don't employ dedicated IT or security professionals, which makes them less prepared to block ransomware attacks.** They also offer a potential way into larger enterprises, if attackers can use the SOHO NAS devices as a stepping stone of supply chain attacks on an enterprise.

Initial Ransom Amount versus Payment Amount

While many ransomware families made ransom demands that were substantial, for the most part, actual payments in incident response cases we handled tended to be less significant. There are always outliers, such as BlackCat getting one payout of $8.5 million, which was pretty close to the initial $9 million demand, but the majority of payments ended up being significantly less than initial demands.

For instance, in one case, Suncrypt received a final payout of $200,000, which was 1.67% of the initial demand of $12 million. From a case by case viewpoint, we calculated that victims on average paid 42.87% of the initial ransom amount. Figure 8 shows the difference between actual ransom payouts and initial ransom demands for those incidents where the ransomware gang wanted $3 million or more and the victim chose to pay the ransom. With one exception, all payouts in the graph were at least 50% less than the demand, which indicates just how much room there is for negotiation when a victim is attacked.

On average, we calculated that actual payments ended up being

42.87%

OF THE INITIAL RANSOM AMOUNT

Figure 7: Average ransom demands compared to average ransom payments in 2020 and 2021, according to Unit 42 incident response data

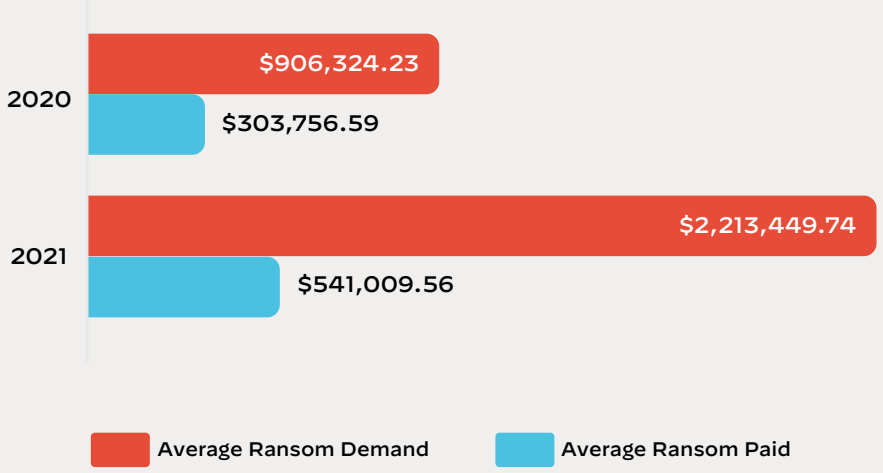
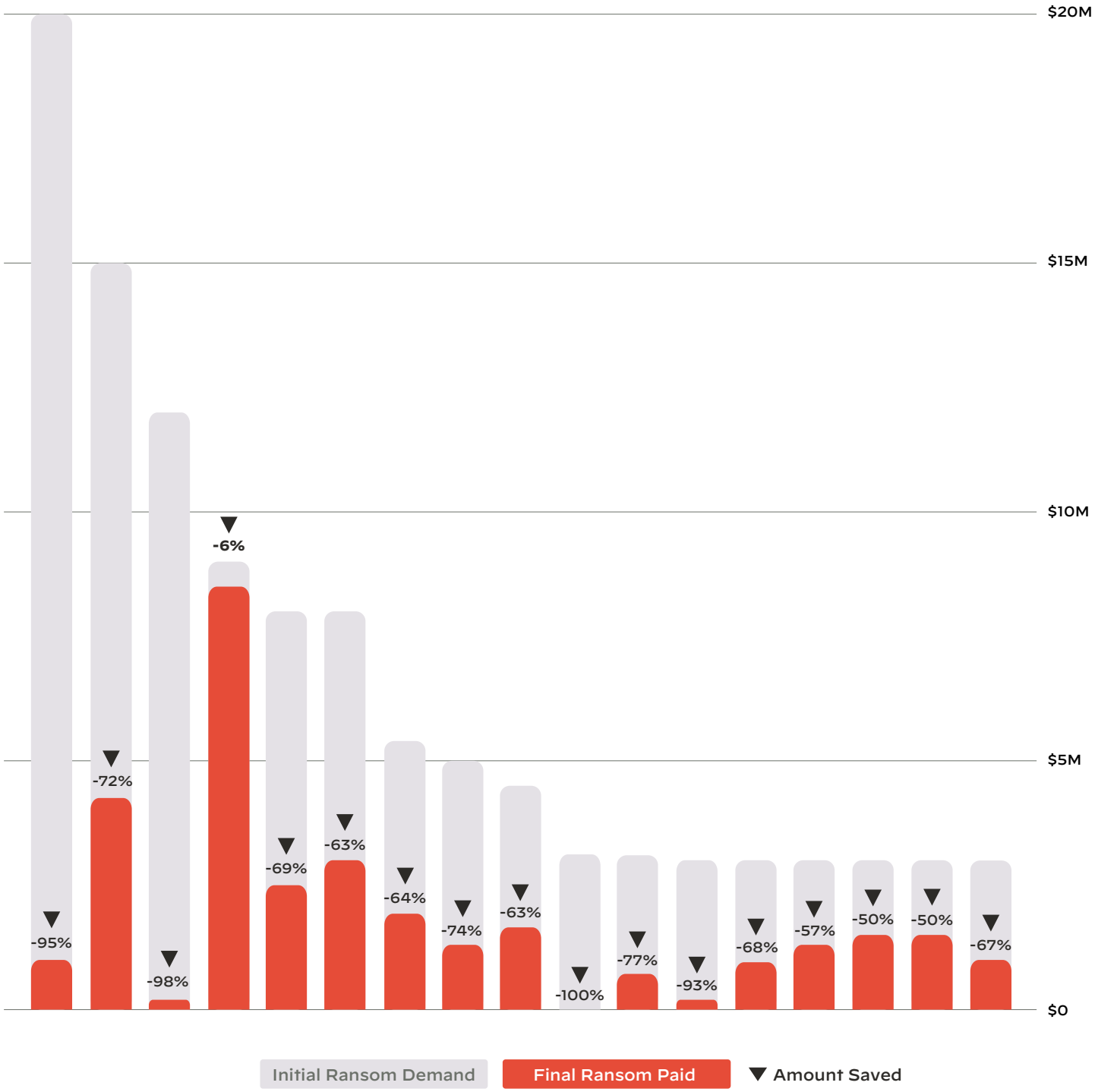


Figure 8: Final ransom paid versus initial ransom requests over $3 million in 2021, for cases in which the victim chose to pay a ransom, according to Unit 42 incident response data



The Rise of Double (and Multi) Extortion Techniques

Maze popularized the double extortion tactic in 2019, laying the path for future ransomware operators. With double extortion techniques, adversaries demand a ransom and then inform victims that they will publicly expose the stolen data if the ransom is not paid, presumably to incentivize swift payment in full. In 2021, we observed 35 new groups emerge using the same extortion model.

We also started to see ransomware groups apply triple extortion techniques. Suncrypt, originally seen in October 2019, was one of the first, along with BlackCat, to apply these triple extortion tactics. This means that, along with data encryption and theft, the gang and its affiliates further extort their victims by threatening to launch a DDoS attack on the organization's infrastructure or network should ransom demand negotiations fail. If negotiations don't go well, not only do they leak victim data, they initiate the DDoS attacks to render their victims inoperable, with the hope that the victim will contact them to restart negotiations.

Should triple extortion not pan out, Suncrypt is also one of the first, if not the first, ransomware group to use multi-extortion. This includes escalating to additional tactics, such as threatening to expose the breach to employees, stakeholders, and the media. Suncrypt operators have gone so far as to leave voicemails for employees of victim organizations in an effort to wear down any remaining resistance to their demands.

Figure 9: Ransomware families that emerged using the double extortion technique in 2020 versus 2021 based on analysis of ransomware group leak sites

04

Insights from Ransomware Leak Sites

In 2021, names and proof of compromise for 2,566 victims were publicly posted on ransomware leak sites, which marked an 85% increase compared to 2020. The following are some key insights we gathered from collating, analyzing, and enriching the information on these sites.

2,566

VICTIMS PUBLICLY POSTED ON LEAK SITES

85%

IN PUBLICLY POSTING VICTIMS ON LEAK SITES COMPARED TO 2020

Most active ransomware groups leveraging double extortion techniques

511

PUBLICLY POSTED BREACHES BY CONTI

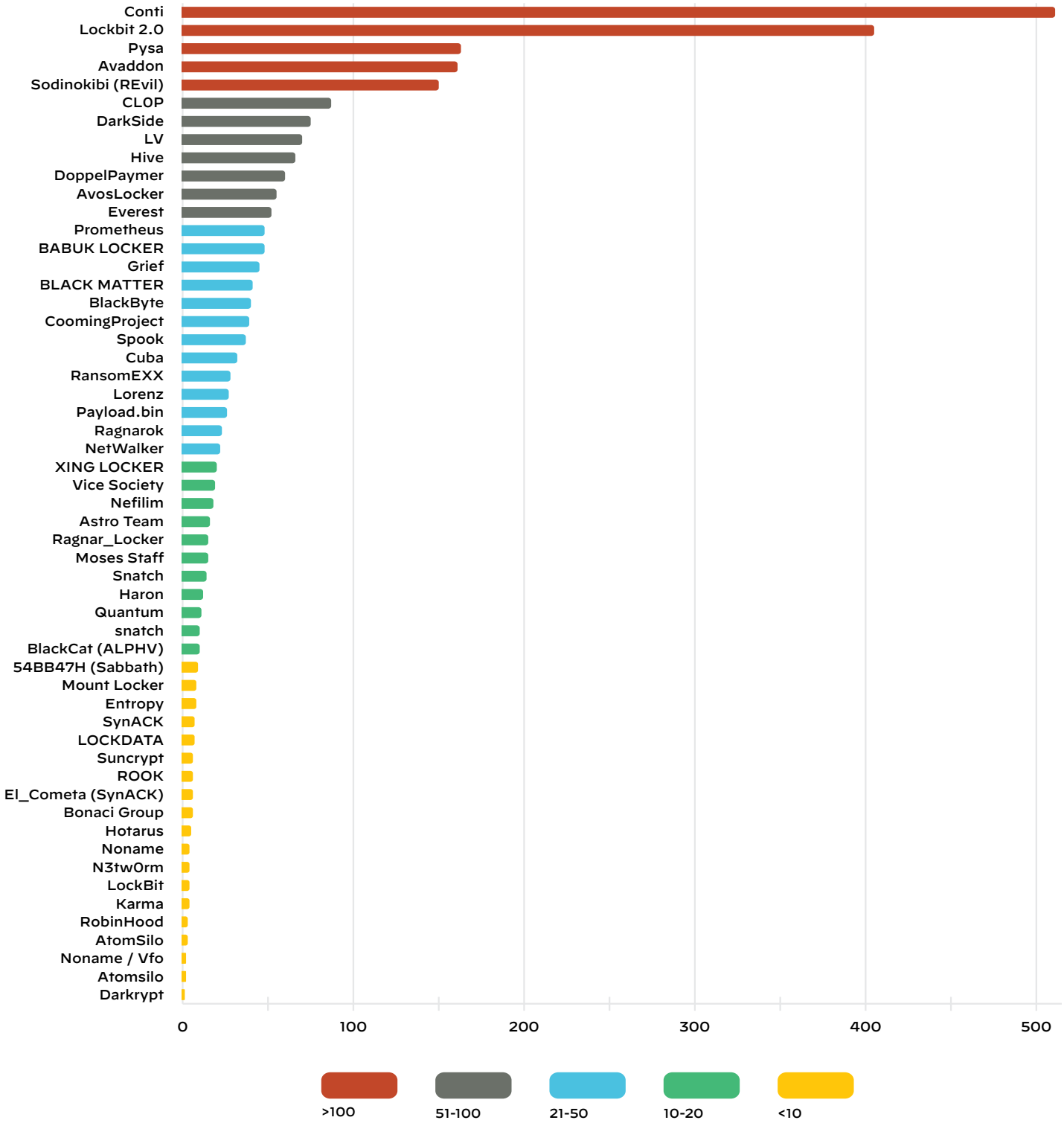
406

PUBLICLY POSTED BREACHES BY LOCKBIT 2.0

Conti Is the Most Prolific on Leak Sites

Analysis of leak sites found that Conti and LockBit 2.0 are the most active ransomware groups leveraging double extortion techniques. Conti is the ransomware family with the most publicly posted breaches in 2021 with 511, closely followed by LockBit 2.0 at 406, which also has been actively leaking data since their rebrand in July 2021.

Figure 10: Victim count per ransomware family, 2021



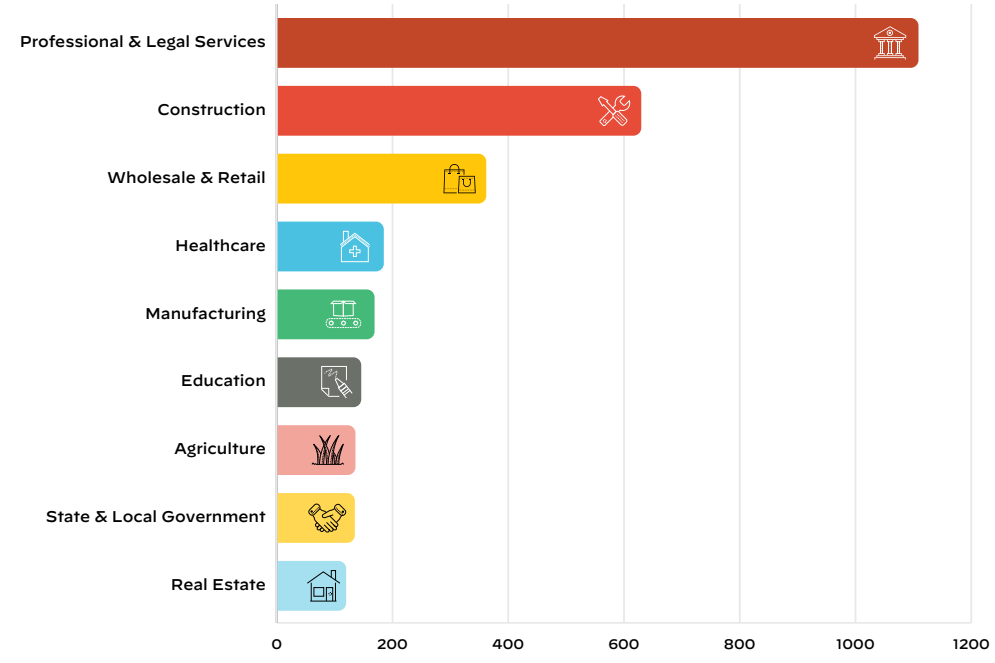
Sectors and Industries Most Heavily Targeted

Based on ransomware leak site data, the Professional and Legal Services industry was the most targeted by ransomware breaches in 2021, with more than 1,100 victims listed on various sites. Following this sector was the Construction industry, which included more than 600 victims.

These organizations may be prone to cyberattacks because they often run on systems with out-of-date software that isn't easily or regularly updated/patched – ransomware operators can take advantage of these old vulnerabilities to initiate their exploits. Add in the rapid adoption of IoT, and attackers have a rapidly expanding attack surface through which they can deploy their ransomware (e.g., WannaCry).

Another reason these industries could be a popular target is that attackers know if the victim's operations are disrupted, it means they can't provide their products or services. Many organizations within these sectors use their own technologies to provide their services, if impacted by a ransomware attack, productivity stops and processes slow down, which could impact business and generate significant costs and damages. Ransomware groups hope the pressure these organizations are under to meet deadlines and produce deliverables will lead them to quickly pay in full, so they can get back up and running as fast as possible.

Figure 11: Sectors and industries most heavily targeted by ransomware (leak site data)



Regions and Countries Most Heavily Targeted

Leak site data indicates the Americas region was hit the hardest by ransomware attacks in 2021, followed by EMEA and Asia Pacific.

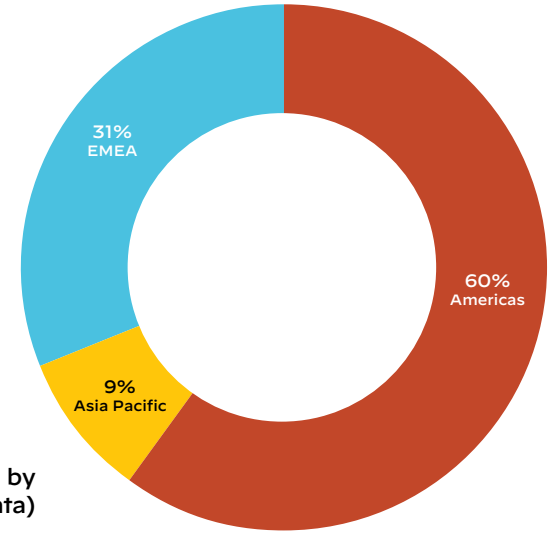
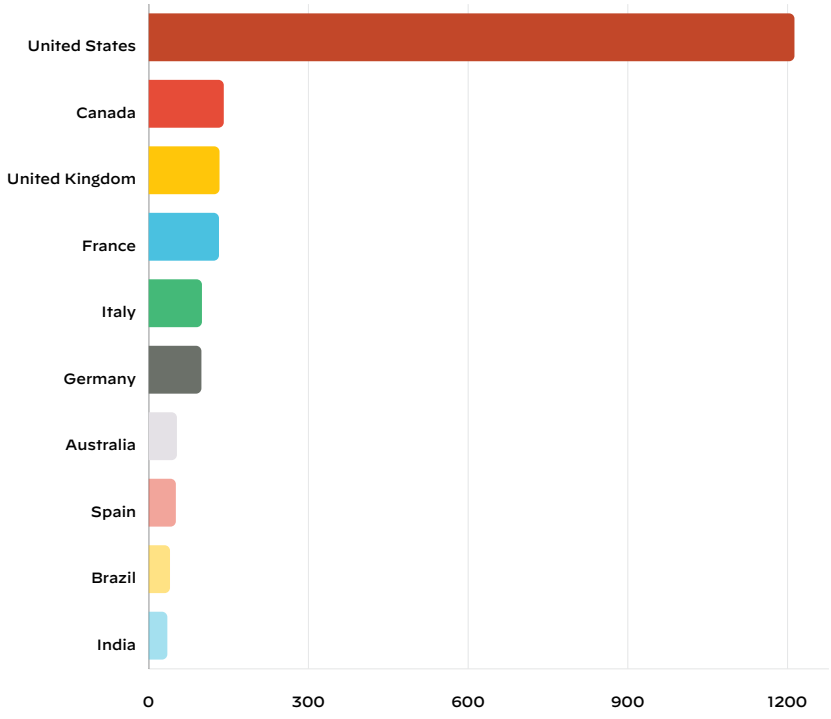


Figure 12: Regions affected by ransomware, 2021 (leak site data)

Figure 13: Top countries impacted by ransomware (based on the number of victim organizations within each country)



When we look for trends by country rather than region, the United States was the most severely impacted by data breaches, with U.S. organizations accounting for 49% of the leak site data, followed by Canada and the United Kingdom, accounting for 5% each. Since many ransomware threat actors are highly financially motivated, they often focus on profitable organizations in the United States. That said, ransomware is a global issue; we have observed at least one victim impacted in more than 90 different countries.

49% UNITED STATES

5% CANADA

5% UNITED KINGDOM

The Ebbs and Flows of Ransomware Gangs

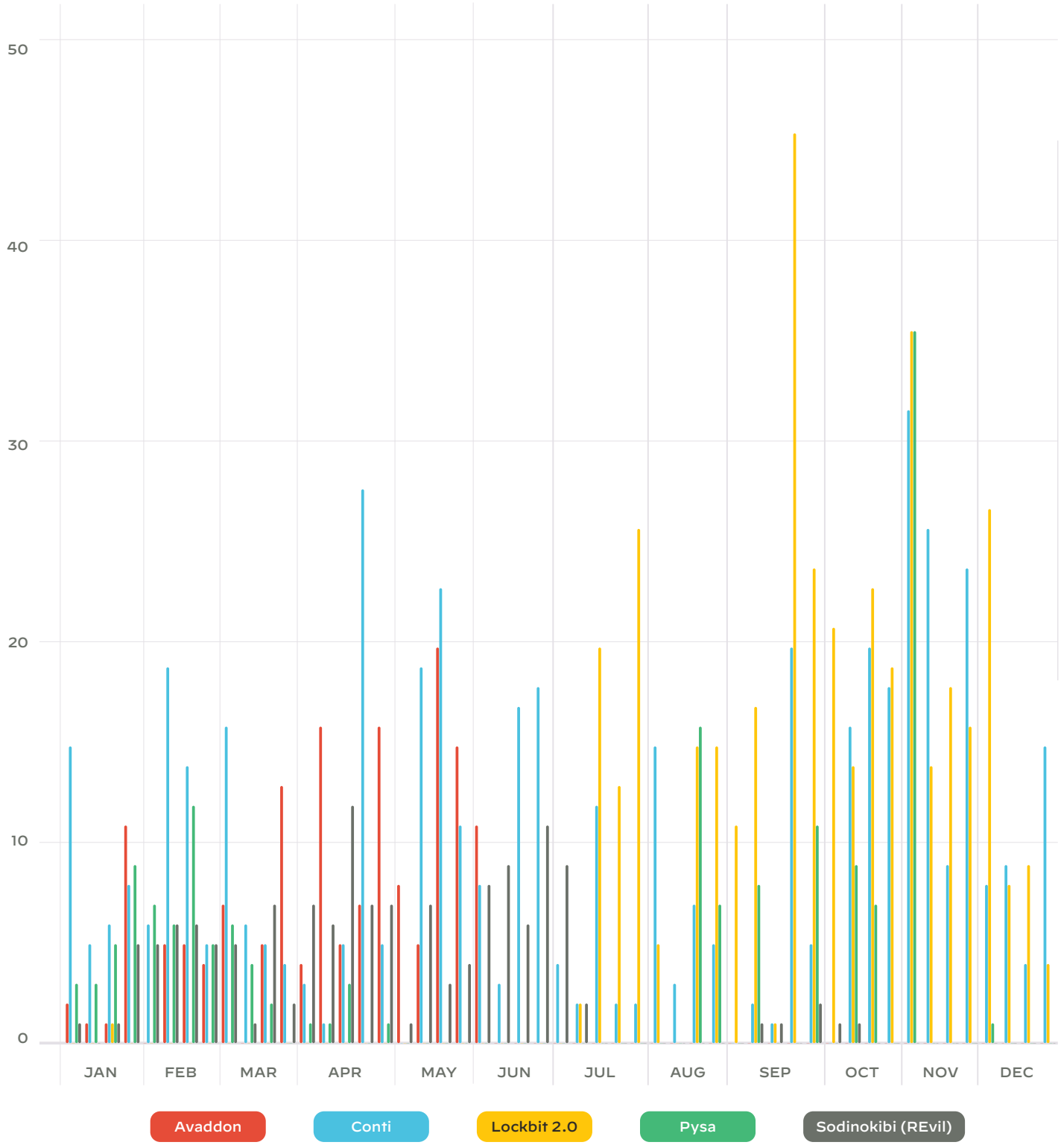
The activity of individual ransomware groups tends to go up and down – a group that's prominent and active one month may seem to disappear altogether the next month. These ransomware groups shut down or go quiet for various reasons. For instance, they may be under pressure or scrutiny from law enforcement, sorting out internal struggles (between operators and affiliates), or dealing with competition (e.g., a new RaaS with better rates that incentivize affiliates to switch).

Sometimes a group may simply rebrand or re-launch their product. Operators need people (affiliates) who are willing to use their ransomware – if they can't sell it, they may try to retool and rebrand. One interesting use case is the **critical flaw that Emsisoft researchers found** in DarkSide and BlackMatter ransomware, which enabled victims to decrypt and recover their files without having to pay a ransom. This cost the ransomware groups millions of dollars in ransom payments and is likely related to why they went offline. It is presumed they went quietly to work on a better version (it's suspected they are the BlackCat group, which suddenly came on the scene and made waves in November 2021, but Unit 42 researchers have not yet confirmed this).

Examples of some swings in ransomware group activity seen in 2021:

- **LockBit** successfully pulled off a rebrand last year with their launch of LockBit 2.0. After their initial debut in July 2021 they added victims at a very stable rate for a few months, peaking in September 2021.
- **Avaddon** decreased submissions to their sites in early June, and then halted operations altogether mid-June, when they released decryption keys for all of their 2,934 victims. (It's worth noting that this activity shows how challenging it is to get visibility into ransomware operations – their site only had 180 victims publicly listed.)
- **REvil/Sodinokibi** activity was noticeable throughout the year, but due to their attack against Kaseya, they stopped submitting victims after July 2021. The group re-emerged in September as displayed on the chart, but went back to being offline for the remainder of the year, most likely as a result of law enforcement action against the group.
- **Pysa** re-emerged at the end of the year with lots of activity, after no activity during the summer of 2021.
- November was a very active month for **Conti**, **LockBit 2.0**, and **Pysa**, with more than 30 submissions into their respective leaksites.

Figure 14: Snapshot of the ebbs and flows of leak site activity for ransomware families in 2021



05

Ransomware in Cloud Environments

In general, we believe public clouds that follow cloud security best practices have the potential to be more resilient to ransomware than on-premises environments. The shared responsibility model significantly reduces the burden on any one organization to secure infrastructure, platform, and software. API-driven cloud services make monitoring, automation, and centralized access control easier, and cloud-native backup services provide reliable ways to recover cloud resources. Nevertheless, it is an organization's responsibility to securely configure, operate, and monitor cloud workloads.

As the IT infrastructure grows with the business, securing thousands of dynamic workloads in a multi-cloud and hybrid cloud environment can be challenging. However, DevOps security automation practices allow IT and security teams to maintain security over highly dynamic environments.

Given the amount of valuable data in the cloud, it is only a matter of time before we see ransomware groups target cloud environments. However, to launch ransomware attacks in cloud environments, threat actors will likely use new TTPs, which means organizations will need to be prepared to adjust their defensive approaches in turn.

Hardening Cloud Workloads from the Image Down

The Log4J vulnerabilities highlight the need for a good vulnerability management program and compensating controls where updates aren't possible. A majority of attacks on cloud workloads are known vulnerabilities. That's why it's critical to ensure that vulnerabilities are patched and misconfigurations, like privileged containers, are remediated before and through runtime. For zero-days and unpatchable workloads, it's necessary to have compensating controls in place, such as virtual patching and anomolous process, network, and file access. Cloud resource segmentation via tightly controlled IAM policies can also help ensure that if a workload is compromised, the infection is contained to a single or at least small number of workloads.

Securing Cloud APIs through IAM Best Practices

Threat actors seeking to deploy ransomware in the cloud will not be able to simply infect more hosts and encrypt the files they find there. Instead, they will use cloud APIs to access and encrypt data, which means that organizations will need to secure access to those APIs.

This is one of the ways that following cloud security best practices is key. All API communications require identity and access management (IAM) access keys and sufficient permissions for the cloud resource the user is trying to interact with. Threat actors seeking to abuse cloud APIs would have to steal access keys and then test their permissions, which means that organizations can defend against this type of attack by closely monitoring IAM permissions. First, organizations should check for misconfigurations, overly broad permissions, and other weaknesses in IAM access. Next, organizations should institute procedures to identify exposed IAM access keys and continuously monitor IAM access keys to cloud resources.

Threat Actors Face Barriers in the Cloud, Which Buys Time for Organizations to Prepare Now

For now, various barriers will likely slow threat actors seeking to attack organizations through the cloud. The supported APIs for each cloud service are different, and each cloud service provider offers a number of different data storage services. This doesn't mean organizations should assume they're immune to ransomware in the cloud. The time to institute best practices, especially regarding identity and access management, is now, so those protections are in place before threat actors focus their efforts on deploying ransomware in this manner.

This can include the use of a Cloud Security Posture Management tool to help ensure the deployment of proper compliance frameworks and perform valid asset control over cloud environments. A Cloud Infrastructure Entitlement Management tool can assist with IAM security monitoring. Other tools such as Cloud Code Security and Cloud Workload Protection can be configured automatically to ensure that security teams can scale as the cloud scales.

06

Costs of Ransomware

As ransomware gangs become bolder, they are having a bigger impact on the organizations they target. While it is generally advised not to pay the ransom, the prolonged effects of a shutdown can force organizations to consider other options to restore operations.

The long-term effects of a ransomware attack can pose a substantial challenge for organizations. A Canadian study found that of the businesses hit by ransomware, a majority (58%) of IT decision-makers say their organization paid the ransom, with 14% saying their organization paid more than once.

In addition to the ransom—whether or not the organization decides to pay it—there are other ancillary costs that need to be factored into the damage inflicted by an attack:

- Costs associated with any downtime or disruptions to the business
- The impact of the breach on a company's brand reputation
- Time spent by IT staff dealing and recovering from the incident
- Legal expenses incurred addressing regulatory and compliance considerations
- Most notably, any data loss that triggers any number of follow-on impacts

The Canadian study found that, while 41% of businesses hit with a ransomware attack were able to recover in less than a month, 58% took more than a month. As more time passed, some businesses were still working on recovery – 29% of surveyed businesses attacked by ransomware took more than three months, and 9% said it took them more than five to six months to return to normal.

To minimize the impact of a successful attack or, ideally, prevent it altogether, preparation is key. This includes ensuring both backup systems and proactive defenses are in place to accelerate an organization's recovery.

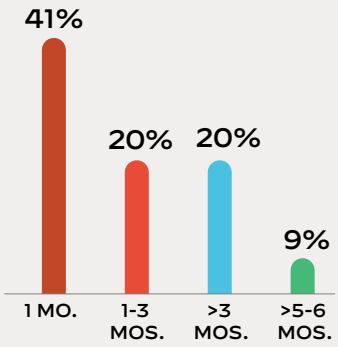
58%

ORGANIZATIONS PAID THE RANSOM

14%

ORGANIZATIONS PAID MORE THAN ONCE

RANSOMWARE ATTACK RECOVERY TIME



07

Conclusion and Recommendations

As ransomware actor activity continues to rise worldwide, preparation is key to thwarting attacks. Because double extortion and leak sites are the new normal for emerging ransomware families, the ante has been raised – it's no longer just access to data that's at stake, as significant as that can be, but also a victim's reputation and the trust a customer has in an organization that is on the line. While maintaining good cyber hygiene and implementing security awareness training is a foundational starting point, Unit 42 makes the following recommendations to help you become more resilient against ransomware.

1 Stay Up to Date on the Evolving Threat Landscape

The ransomware threat landscape will undoubtedly continue to evolve, as threat actors leverage new creative techniques to stifle business operations. Keep your security team and key executive stakeholders better informed of the current state of ransomware threats, their potential impact to your business, and actionable steps your organization can take to prevent attacks. This means educating your key C-level stakeholders and the board by speaking the language of the business and leveraging threat briefings to strategically inform your risk profile and security strategy. You must also educate your technical security team on the latest ransomware threats, including attack vectors, TTPs, ransom demands, and top safeguards to prevent attacks.

2 Analyze the Business Impact of Losing Critical Data

To understand the impact of losing access to critical data, you must first gain full visibility into your assets and understand where critical data lives, how it's accessed, and how it's used across your organization. We recommend completing a data mapping exercise, ensuring that access to confidential information is on a need-to-know basis. Next, conduct

a business impact analysis to fully understand the risks associated with not having access to that data – both from an upstream and downstream perspective. For example, if you're a retail organization, what is the downtime that is going to occur at your headquarters, in your stores, and in the supply chain if your point-of-sale system is down and you can't do manual processing?

3 Assess Internal and External Readiness

You run the increased risk of a successful – and highly damaging – ransomware attack if you don't consistently assess your security posture. Assess the most significant ransomware risks ahead of you within the context of your unique combination of people, processes, technology, and governance capabilities. You will also need to look across the business to identify any third-party elements, partner elements, or supply chain elements that could introduce risks. With this knowledge, you can establish a prioritized mitigation roadmap detailing the requirements to reach your organization's security goals aligned with strategic business objectives.

4 Review and Test Your Incident Response Plan

Pressure test and update your incident response plan on a regular basis leveraging the latest ransomware threat intelligence to conduct tabletop exercises and purple team testing simulations. By conducting mock incident response walkthroughs, you can measure your ability to respond to a ransomware attack before it happens and evaluate your ability to counter the tactics, techniques, and procedures used by common ransomware groups. These types of exercises can help you identify gaps and areas for improvement to help bolster your readiness and strengthen your overall cyber defense capabilities to combat ransomware.

As a part of these exercises, leaders should ensure that decision trees are formally defined and socialized with key stakeholders to facilitate discussion and buy-in. When a change in stakeholder personnel occurs, these decision trees should be revisited and updated as required. Having the tough conversations before an incident occurs will save valuable time

and enable organizations to focus on what matters most – maintaining critical operations and recovering to a state of normalcy.

- Under what circumstances would you pay a ransom?
- How would you maintain customer trust if the media was swirling with rumors and your stock price was sinking?
- What would happen if your CISO was incapacitated when an incident was discovered?
- Who would you call to stop an active incident from spreading like wildfire?

5 Implement Zero Trust

Zero Trust, a strategic approach to cybersecurity to secure an organization, eliminates implicit trust and continuously validates every stage of digital interaction. The Zero Trust Model has become increasingly top of mind for executives who need to keep up with digital transformation and adapt to the ever-changing security landscape. Many organizations still struggle with a poorly integrated, loose assembly of point products that do not align with the strategic approach expected by board members and C-level executives. Deployed properly, Zero Trust simplifies and unifies risk management by making security one use case across users, device, source of connection, or access method.

6 Identify Your Exposed Assets

Implement a system of record to track every asset, system, and service you own that is on the public internet. This includes tracking across all major cloud service providers and dynamically leased (commercial and residential) Internet Service Provider (ISP) space, using comprehensive indexing and spanning common, and often misconfigured, port/protocols (i.e., not limited to the old perspective of only tracking HTTP and HTTPS websites). For example, Remote Desktop Protocol (RDP) is the most popular initial ransomware attack vector, accounting for the majority of ransomware infections, since attackers can easily uncover this protocol thanks to working from home now being a common norm. M&A, supply chain, and IoT also bypass change controls, making them another popular vector. M&A activity, for example, has reached an all-time high during the COVID-19 pandemic, changing the face of networks almost overnight.

While security teams are doing a good job, it's no longer sufficient to protect a static IP address – infrastructure changes quickly.

An attack surface management (ASM) platform can provide a complete and accurate inventory of an organization's global internet-facing assets and misconfigurations to continuously discover, evaluate, and mitigate security issues on an external attack surface, flag risky communications, evaluate supplier risk, find RDP instances, or assess the security of acquired companies.

7 Prevent Known and Unknown Threats

To prevent known threats, you need to stop known exploits, malware, and command-and-control traffic from entering your network. Once those have been stopped, the cost of executing an attack rises and, subsequently, reduces its likelihood, by forcing attackers to create new malware variants and launch new exploits against lesser-known vulnerabilities.

You also need to prevent users from inadvertently downloading a malicious payload or having their credentials stolen by preventing access to known malicious and phishing URLs. Blocking these threats removes them from the equation entirely. Once these known threats have been blocked, you need to scan for known malware on your SaaS-based applications, as they are increasingly leveraged to deliver threats. Any identified malware and exploits from the scan should be blocked. The same should be done for known malware and exploits on the endpoint.

Once the known threats have been blocked, it is imperative to identify and block any unknown threats, as attackers continue to deploy new zero-day exploits and develop new ransomware variants. Identify all traffic on the network and block unknown, potentially high-risk traffic (e.g. macros downloaded from the internet) at the edge, ensuring you have coverage of web and non-web traffic. Next, detect unknown threats in files and URLs. As new files are submitted, it is essential to detonate, analyze, and look for malicious behavior.

Additionally, you need to automatically push the protections to different parts of the security infrastructure as fast as possible in order to prevent threats from becoming successful. These protections should include an

understanding of the context of the attacker, malware, campaign, and IoCs associated with the attack. Once unknown threats or trends of suspicious behavior have been identified and blocked, block unknown malware and exploits on the endpoint to ensure that all access points are secure.

The ultimate goal of this process is to turn the unknown into the known and improve the security posture with new protections at a faster pace than attackers can develop their malware and exploits – across the entire attack lifecycle.

8 Automate Where Possible

Consider implementing tools that support the automated remediation of events that leverage pre-made playbooks to respond and recover from incidents. Incident response (IR), SecOps, and threat intelligence teams can save many hours of manual labor trying to piece disparate sources of information together from multiple tools. Security orchestration, automation, and response (SOAR) products can automate the whole process of user investigation, endpoint isolation, notifications, enrichment, and threat hunting by orchestrating across security information and event management (SIEM), firewalls, endpoint security, and threat intelligence sources so that response teams can quickly shut down the ransomware, minimize the risk of losing data, and limit the financial impact of ransom demands.

9 Secure Cloud Workloads

Securing cloud workloads for ransomware defense begins with a secure posture. Ensure that all cloud infrastructure, Kubernetes, and container images are securely configured and steps have been taken to minimize vulnerabilities. Check that standard policies, like encryption, MFA delete, versioning, and backups that are built into cloud provider offerings, but off by default, are turned on and properly configured. Check open source packages and libraries for vulnerabilities that can be patched. Identify and remove overly permissive or unused IAM entitlements. This is best checked throughout the development lifecycle, making sure the code is secure before it turns into cloud applications and infrastructure. At runtime, check for known bad and anomalous activities that indicate a compromise.

Track and block bad behavior at a process, file, and network level. Isolate services to just their intended dependencies and block lateral and external access that isn't required to operate. Blocking threat behaviors at all of these levels creates a layered approach that maximizes security.

10

Reduce Response Time with Retainers

It's critical to take swift action once a potential breach has been identified. With an IR retainer in place, you can make IR experts an extension of your team, having them on speed dial whenever you require assistance. You won't engage in a frantic search for resources when there is a problem – instead, you know the correct specialist will show up within hours. And because IR consultants will already understand your environment, they can respond faster and more accurately should an incident occur. You won't experience the anxiety of answering baseline questions from uninformed third-party investigators when all you want to do is get on with eliminating the problem. You're able to create a predictable incident response budget and take faster action to minimize the impact of an attack.

Want to Be Prepared for a Ransomware Attack? Call in the Experts.

If you think you may have been impacted by any of these ransomware families, please contact us.

The Unit 42 Incident Response team is available 24/7/365. If you have cyber insurance, you can request Unit 42 by name. You can also take preventative steps by requesting a Ransomware Readiness Assessment.

Methodology

This report is based on data from multiple sources, both internal and external. The objective is to expose threat actors, not their victims, so all case data has been anonymized and only categorized by topics, such as industry, geography, and attack vector. The source of specific data referenced in the report is noted throughout.

Internal data for this report (referenced primarily in Section 2) was anonymized information collected during security consulting and incident response engagements from clients predominantly based in the U.S. One service that Unit 42 Security Consulting performs is ransomware negotiations on behalf of clients. For the subset of clients who use this service and elect to pay the ransom, Unit 42 tracks key information, including the ransomware variant, initial demand, amount paid, and whether or not the threat actor provided the decryption utility upon payment for the initially agreed-upon amount. Additional data for this report comes from managed threat hunting, product security telemetry, and threat research organically developed during the course of business.

External data (referenced primarily in Section 3) was collated and analyzed from ransomware leak sites to identify ransomware families performing double extortion. Most of the time these ransomware notes include onion links, which direct victims to their site – these sites are hosted in a repository and monitored by the team to understand their activity throughout the year. The majority of the sites are publicly available and found on the "dark web," which allows the team to scrape victim names, dates, and the sites where the data is hosted. After the data is collected, it is enriched by the team with the victim's industry, sector, location, and any other details that can be discerned.

We recently revised the methodology we use to calculate average ransom demands and payments. As a result, we're restating the 2020 average payment to $303,757 (from $312,493 published in the 2021 Ransomware Threat Report).

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance members. CTA members use this intelligence to rapidly deploy protections to their customers and systematically disrupt malicious cyber actors. Visit the Cyber Threat Alliance for more information.

About Unit 42

Palo Alto Networks' Unit 42 brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk. With a deeply rooted reputation for delivering industry-leading threat intelligence, Unit 42 has expanded its scope to provide state-of-the-art incident response and cyber risk management services. Our consultants serve as your trusted advisor to 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. Visit paloaltonetworks.com/unit42.

Palo Alto Networks Ransomware Capabilities

Many Palo Alto Networks products include comprehensive functionality specific to stopping ransomware. Learn more about Unit 42's research into ransomware actors and the product protections that Palo Alto Networks offers for specific situations on the Unit 42 blog.

Network Security

Cloud-delivered security services bring the network effect of thousands of customers across various security technologies to coordinate intelligence and provide consistent protection across all attack vectors. Deployed across our range of ML-Powered Next-Generation Firewalls – hardware PA-Series, software VM-Series and CN-Series, and cloud-delivered Prisma® Access along with Cloud-Delivered Security Services – our services help eliminate coverage gaps. To read in-depth on each product and service, please visit the links.

WildFire® malware prevention service is natively integrated into all Palo Alto Networks products and blocks activity associated with known and unknown ransomware variants as well as other file-based threats.

Advanced URL Filtering blocks access to known and new unknown malicious URLs, preventing a host from reaching out via HTTP to a web server Palo Alto Networks has deemed to host suspicious content/ malware.

Advanced Threat Prevention leverages the firewall's visibility to inspect all traffic and automatically prevent known exploits, malware, and spyware regardless of port, protocol, or SSL encryption.

DNS Security blocks command and control and data exfiltration attempts that specifically exploit the DNS protocol, found in over 85% of breaches, including ransomware.

IoT Security provides visibility into all IoT, OT, IT, and Bluetooth devices and recommends least- privilege (Zero Trust) policies, which minimizes the risk of an adversary using an unmanaged device as a jumping off point to deliver ransomware or other malicious files.

Enterprise Data Loss Prevention automatically detects and prevents unsafe transfers of sensitive data against corporate policies and minimizes overexposure of sensitive data throughout the entire enterprise, across remote users, and on cloud applications.

CORTEX

Cortex® XDR™ is the industry's first extended detection and response platform that integrates data from any source to stop ransomware and countless other dangerous attacks. The Cortex XDR agent automatically blocks exploits, malware, and fileless attacks targeting endpoints. Analysts can quickly stop the spread of ransomware, restrict network activity to and from devices, and update threat prevention lists like bad domains through tight integration with enforcement points. Cortex XDR allows you to:

- Block ransomware attacks at every step in the attack lifecycle with a complete endpoint protection stack, including exploit prevention, behavioral threat protection, AI-driven local analysis, and an anti-ransomware module.
- Find stealthy attacks such as lateral movement and exfiltration with cross-data analytics across endpoint, network, cloud, and identity data.
- Quickly investigate incidents with root cause analysis.
- Contain any threat with coordinated and flexible response.

Cortex XSOAR helps you speed discovery and remediation when ransomware is detected by automating the whole process of user and host data enrichment, blocking malicious indicators, and isolating/ quarantining infected endpoints and users.

PRISMA®

Prisma® Cloud is a comprehensive cloud native security platform with the industry's broadest security and compliance coverage – for applications, data, and the entire cloud native technology stack – throughout the development lifecycle and across hybrid and multi-cloud deployments. Prisma Cloud's integrated approach enables security operations and DevOps teams to stay agile, collaborate effectively, and accelerate cloud native application development and deployment securely.

Cloud Security Posture Management – Segments services to prevent lateral movement, limiting the impact of a successful breach.

UNIT 42
BY PALO ALTO NETWORKS

Unit 42 brings together world-renowned threat researchers with an elite team of incident responders and security consultants to create an intelligence-driven, response-ready organization passionate about helping customers more proactively manage cyber risk.

Ransomware Readiness Assessment – Using the latest threat intelligence, Unit 42 can help you assess your current state of readiness and develop a ransomware playbook to expertly manage ransomware attacks leveraging real-world simulations, compromise assessments, and board advisory consulting.

Incident Response – When your files and applications are inaccessible due to a ransomware attack, call in our elite Unit 42 incident response team to step in to investigate, contain, and eradicate the threat, so you can restore operations quickly.

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