UNIT 42™
BY PALO ALTO NETWORKS

Ransomware Threat Report

2021

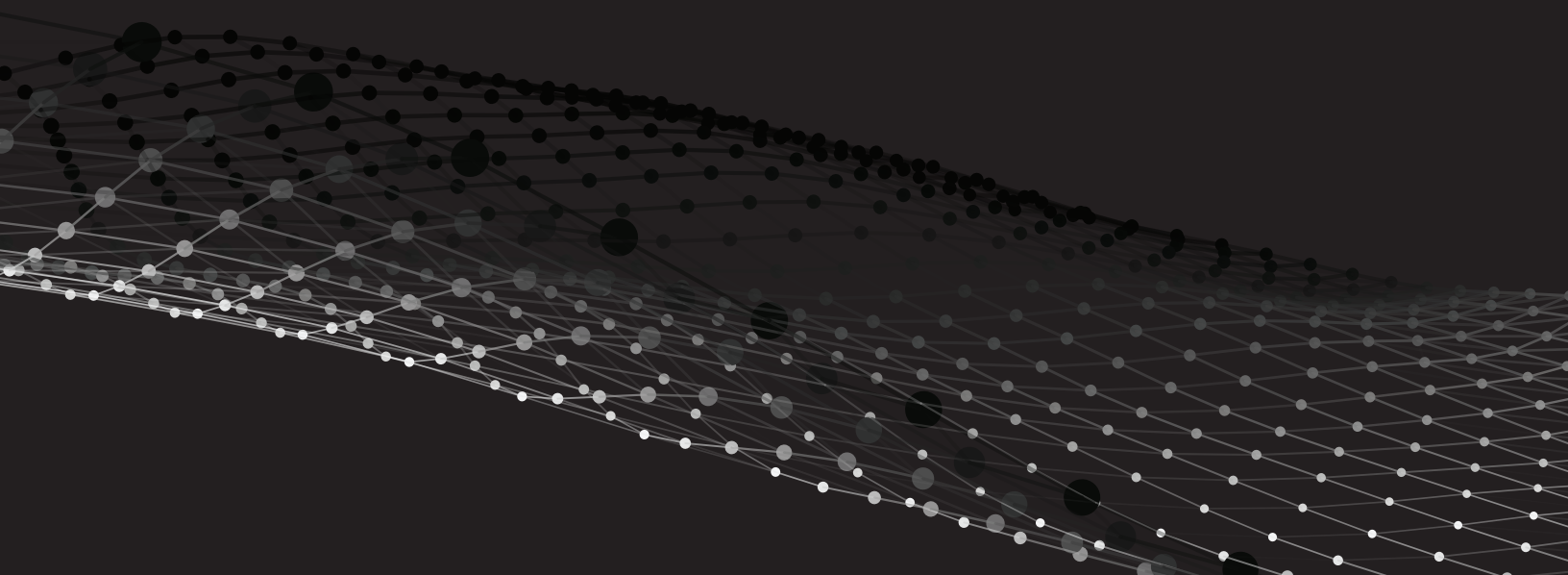


Table of Contents

Foreword

Before joining Palo Alto Networks, I served 35 years in the US military, with the last 10 of those years devoted to cyber-related assignments. During my tenure, I was able to see firsthand how ransomware was a major threat to national security—and we're still seeing it today.

Ransomware is one of the top threats in cybersecurity. According to the Identity Theft Resource Center, there were 878 cyberattacks in 2020, 18% of which were recorded as ransomware.[1] This threat is a focus area for Palo Alto Networks. Our Unit 42 global threat intelligence and incident response teams worked together to create the 2021 Unit 42 Ransomware Threat Report to provide the latest insights on the top ransomware variants, ransomware payment trends, and security best practices so we can best understand and manage the threat.

Put simply: ransomware is a lucrative business. The average ransom paid by organizations in the US, Canada, and Europe increased from US$115,123 in 2019 to $312,493 in 2020—a 171% year-over-year increase. With new tactics like double extortion, this number will only continue to rise.

Organizations around the world are being held hostage by ransomware, and many are being forced to pay cybercriminals because they're not equipped to combat the threat for varying reasons, from a lack of recoverable backups to the cost of downtime outweighing the cost of paying the ransom.

We need to significantly reduce this criminal enterprise, which is why I'm proud that Palo Alto Networks is a member of the Institute for Security and Technology's Ransomware Task Force (RTF), in which I serve as a co-chair.

The RTF is focused on developing a suite of recommendations for a comprehensive strategy to mitigate the ransomware threat. To develop a set of solutions that will attack all sides of the ransomware scourge, the RTF has recruited a large and diverse set of experts who are currently investigating a broad array of avenues for recommendations—acknowledging all of the good work that has already been done in this space.

This means exploring questions like:

- What can we do to better prepare organizations for a ransomware attack?
- How can organizations understand and best respond to a ransomware attack?
- What are the greatest barriers for ransomware security adoption?
- How can we make it more difficult for ransomware actors to carry out an attack?
- How can we make the outcome of a ransomware attack less destructive?
- How can we create solutions tailored to the many different victims of ransomware attacks?

As these discussions progress, the task force aims to provide clear and actionable recommendations for both public and private sector decision-makers internationally in spring 2021.

I believe resources like the 2021 Unit 42 Ransomware Threat Report will help us in this effort to learn everything we can about this threat, enabling us to work across the public and private sectors to collaboratively reduce the ransomware problem to something more manageable than the significant threat we face today.

John Davis
Retired US Army Major General
Vice President of Public Sector at Palo Alto Networks

1. "2020 Data Breach Report," ITRC, January 28, 2021, https://notified.idtheftcenter.org/s/2020-data-breach-report.

Executive Summary

To evaluate the current state of the ransomware threat landscape, the Unit 42 threat intelligence and incident response teams collaborated to analyze the ransomware threat landscape in 2020 using their global data.

This report details the top ransomware variants (with links to threat assessments for each variant), average ransomware payments, ransomware predictions, and actionable next steps to immediately reduce ransomware risk.

Cybercriminals Are Making, and Demanding, More Money Than Ever

Note: The following data is from the US, Canada, and Europe.

The average ransom paid for organizations increased from US$115,123 in 2019 to $312,493 in 2020, a 171% year-over-year increase. Additionally, the highest ransom paid by an organization doubled from 2019 to 2020, from $5 million to $10 million. Meanwhile, cybercriminals are getting greedy. From 2015 to 2019, the highest ransomware demand was $15 million. In 2020, the highest ransomware demand grew to $30 million.

Of note, Maze ransom demands in 2020 averaged $4.8 million, a significant increase compared to the average of $847,344 across all ransomware families in 2020. Cybercriminals know they can make money with ransomware and are continuing to get bolder with their demands.

Healthcare Organizations in the Crosshairs

The world changed with COVID-19, and ransomware operators took advantage of the pandemic to prey on organizations—particularly the healthcare sector, which was the most targeted vertical for ransomware in 2020. Ransomware operators were brazen in their attacks in an attempt to make as much money as possible, knowing that healthcare organizations—which needed to continue operating to treat COVID-19 patients and help save lives—couldn't afford to have their systems locked out and would be more likely to pay a ransom.

Ryuk ransomware stood out from the pack. In October 2020, a joint cybersecurity advisory was issued by the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS), warning healthcare organizations against Ryuk attacks.

The Rise of Double Extortion

A common ransomware attack consists of the ransomware operator encrypting data and forcing the victim to pay a ransom to unlock it. In a case of double extortion, ransomware operators encrypt and steal data to further coerce a victim into paying a ransom. If the victim doesn't pay the ransom, the ransomware operators then leak the data on a leak site or dark web domain, with the majority of leak sites hosted on the dark web. These hosting locations are created and managed by the ransomware operators. At least 16 different ransomware variants are now threatening to expose data or utilizing leak sites, and more variants will likely continue this trend.

The ransomware family that leveraged this tactic the most was NetWalker. From January 2020 to January 2021, NetWalker leaked data from 113 victim organizations globally, far surpassing other ransomware families. RagnarLocker was second, leaking data from 26 victims globally. It's worth noting that the US Department of Justice announced in January 2021 it had coordinated international law enforcement action to disrupt the NetWalker ransomware gang. The dark web domain managed by the NetWalker operators, which hosted leaked data, is no longer accessible.

01

2020 Top Ransomware Observations

COVID-19 Pandemic

Adversaries take advantage of current events to lure victims into opening phishing emails, visiting fake websites, or downloading malicious files. Case in point: with the global impact of the COVID-19 pandemic, ransomware attackers heavily exploited it as a theme in ransomware attacks targeting a variety of industries. While the healthcare sector was a top target throughout 2020 due to the coronavirus, many industries suffered deeply from ransomware incidents.

Battling with a more fragile financial outlook throughout the year as well as the added challenges of employees working from home, many businesses have had to make do with less. With fewer staff and budget cutbacks, cyberthreat awareness and cybersecurity protections may be more difficult to implement.

Shifts in Approach

Ransomware has become increasingly easy to get hold of and is available in many formats targeting multiple platforms. We've observed shifts from high-volume and spray-and-pray models to a more focused "stay-and-play" model, where operators take their time to learn the victims and their networks, following a more traditional network penetration approach.

Platforms Targeted

In addition to ransomware being observed on Microsoft Windows®, Apple macOS®, and mobile operating systems, we are now seeing Linux being targeted as well.

Ease of Use and Availability

Adversaries understand that ransomware, specifically the ransomware as a service (RaaS) subscription-based model, is simple to execute, exceptionally effective, and potentially profitable—both from direct payments and sale of valuable information. The RaaS model allows affiliates to utilize existing ransomware software to carry out attacks, thereby earning a percentage of each successful ransom payment.

Ransomware operators continue to gain access to victim environments through traditional methods, including phishing, weak or compromised Remote Desktop Protocol (RDP) credentials, and exploiting application/software vulnerabilities. Despite 2020's larger remote workforce, these entry techniques remained the same. Many operators are also combining commodity malware such as Dridex, Emotet, and Trickbot for initial access. Once inside a network, adversaries use native tools such as PSExec and PowerShell to enumerate the network and move laterally.

The Rise of Double Extortion

Several ransomware families—NetWalker, RagnarLocker, DoppelPaymer, and many others, as shown in figure 1—have displayed their ability to exfiltrate data and use double extortion techniques. Instead of only encrypting files on the victim host(s), operators exfiltrate files first to further coerce the victim into paying the ransom. Exfiltrated files are then posted, or threatened to be published, on a public or dark web leak site, with the majority of leak sites hosted on the dark web. These hosting locations are created and managed by the ransomware operators. Some ransomware operators will further prove their knowledge of a victim's network environment by displaying the data in the form of directories or file trees.

Figure 1 gives a high-level overview of victims impacted by leak sites that were still live in January 2021. This gives us an understanding of the enormous scale of the damage these ransomware operators are doing. Most notably, NetWalker ransomware leaks lead the list at a staggering 33%, and other groups account for 7% or lower each. It is also important to highlight that a coordinated international law enforcement action was conducted to disrupt the NetWalker ransomware gang on January 27, 2021. The dark web domain managed by the NetWalker operators is no longer accessible.

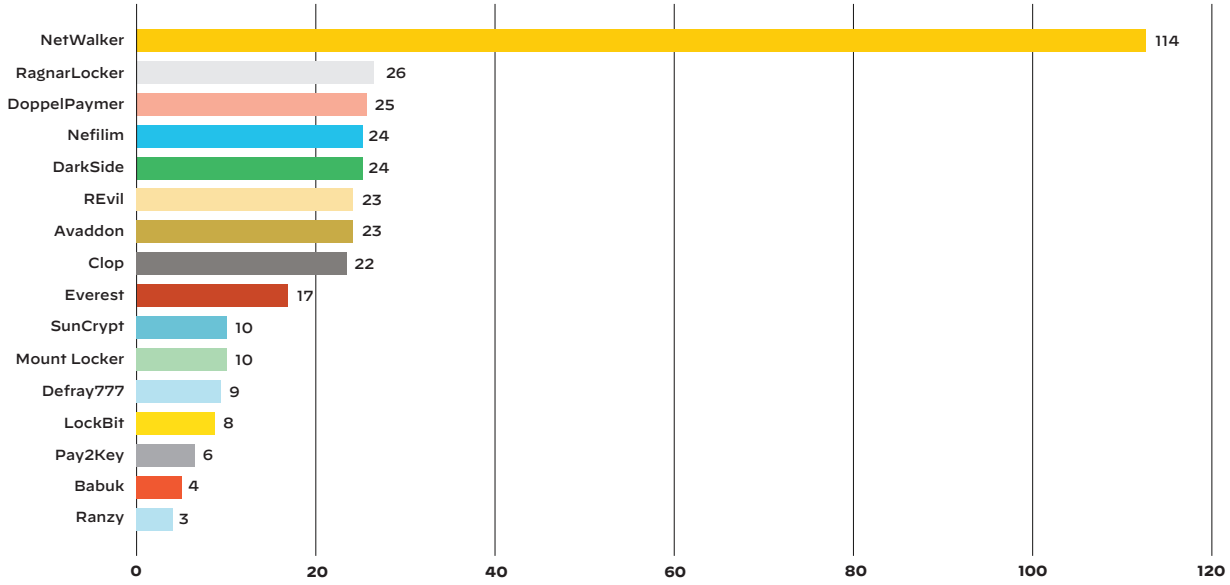


Figure 1: Number of victim organizations globally, by ransomware family, with data published on leak sites, Jan. 2020 – Jan. 2021

We also looked into the number of victim organizations with data published on leaked sites by region. As seen in figure 2, the Americas region was hit the hardest, followed by EMEA (Europe, the Middle East, and Africa) and JAPAC (Japan and Asia-Pacific).

Of the victim organizations with data published on leak sites, the top three countries impacted globally were the United States (47% of organizations), Canada (12%), and Germany (8%). If these percentages are parallel to how many organizations actually pay the ransom, this could mean organizations in the US are more profitable for ransomware operators to target than others. Also, given the increasing acceptance of cyber insurance solutions in countries like the US, Canada, and Germany, many companies may decide to pay the ransom if they are already covered by their respective insurance providers. Figure 3 provides a breakdown of figure 2 from a global perspective.

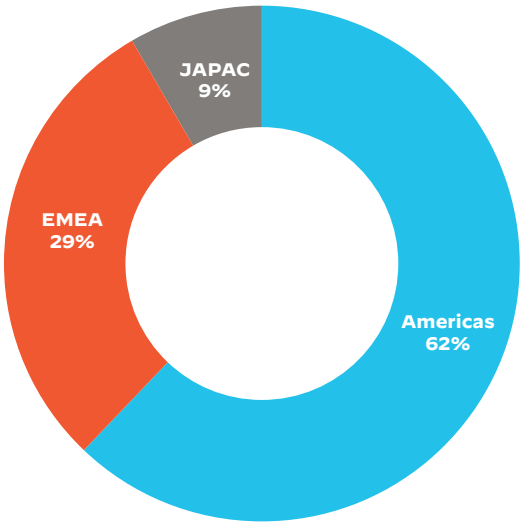
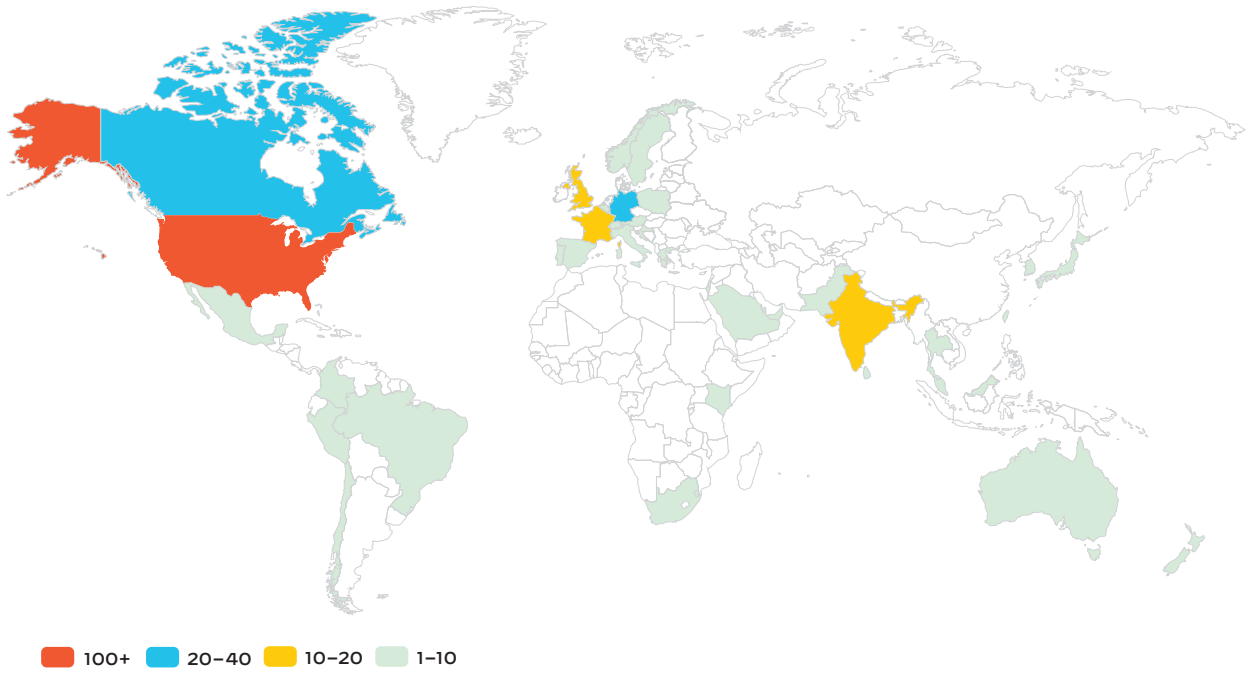


Figure 2: Percentage of total victim organizations with data published on leak sites by region, Jan. 2020 – Jan. 2021



Number of victim organizations with data published on leak sites by country							
United States	151	Belgium	4	Chile	1	Pakistan	1
Canada	39	Sweden	4	Colombia	1	Peru	1
Germany	26	South Africa	3	Croatia	1	Poland	1
United Kingdom	17	Spain	3	Greece	1	Portugal	1
France	16	Japan	2	Hong Kong	1	Saudi Arabia	1
India	11	Mexico	2	Jamaica	1	Singapore	1
Australia	7	New Zealand	2	Kenya	1	Sri Lanka	1
Brazil	5	South Korea	2	Luxembourg	1	Taiwan	1
Israel	5	Switzerland	2	Malaysia	1	Thailand	1
Italy	5	Austria	1	Norway	1	United Arab Emirates	1

Figure 3: Numbers of victim organizations with data published on leak sites by country, Jan. 2020 – Jan. 2021

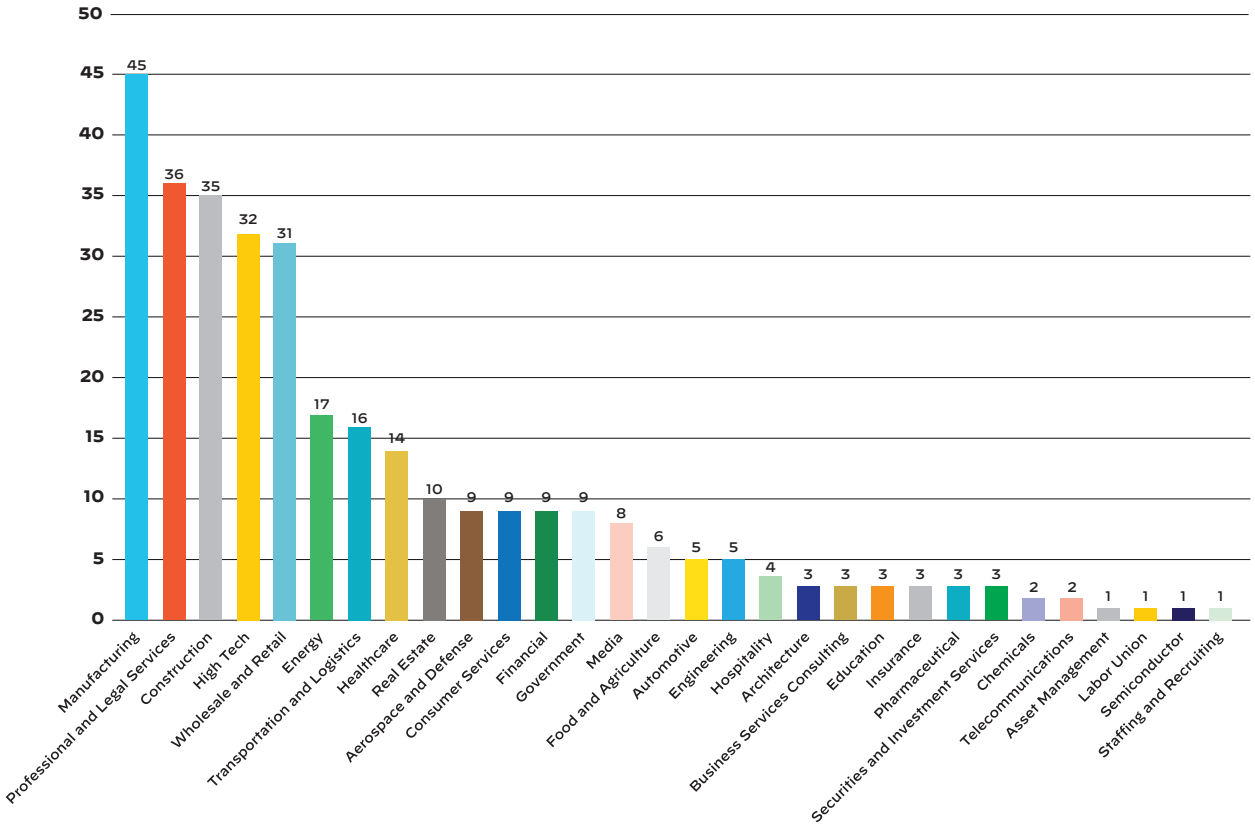


Figure 4: Numbers of victim organizations with data published on leak sites globally by sector, Jan. 2020 – Jan. 2021

Figure 4 breaks down the victim organizations by their respective industries, showing the number of organizations per industry where data was exposed to a leak site controlled by the ransomware operators. Many of the operators have staged leaks of each organization's data, likely in an effort to pressure victim organizations into paying the ransom by a deadline, failing which the operators decide to leak the full data. Published data from each organization ranged anywhere from 30 MB to more than 1000 GB.

The Reintroduction of DDoS Campaigns

Several ransomware families were identified using distributed denial-of-service (DDoS) against victim websites as additional leverage. For example, the Avaddon ransomware operators have begun employing DDoS attacks against victim organizations that do not cooperate with the actors during the negotiation period. This concept is not new. In 2016 and again in 2019, operators were emailing DDoS threats to ransom victims if they did not pay. However, 2020 reintroduced this destructive strategy.

Ransomware Incident Costs

Organizations of all sizes across many industries have been impacted by ransomware. Compared to 2019, we observed an increase of ransomware incident response cases across several industries in the US, Canada, and Europe, as displayed in figure 5. While this figure depicts a summary of overall industry targeting, it is not representative of the known increase in incidents across sectors such as healthcare, manufacturing, and education. Ransomware engagements throughout 2020 were more complex than in prior years, leading to longer, more in-depth breach response times.

Most notably, the information technology sector saw a 65% increase in ransomware incident response cases from 2019 to 2020. As organizations shifted to remote workforces due to the COVID-19 pandemic, ransomware operators adapted their tactics accordingly, including the use of malicious emails containing pandemic-based subjects and even malicious mobile apps claiming to offer information about the virus.

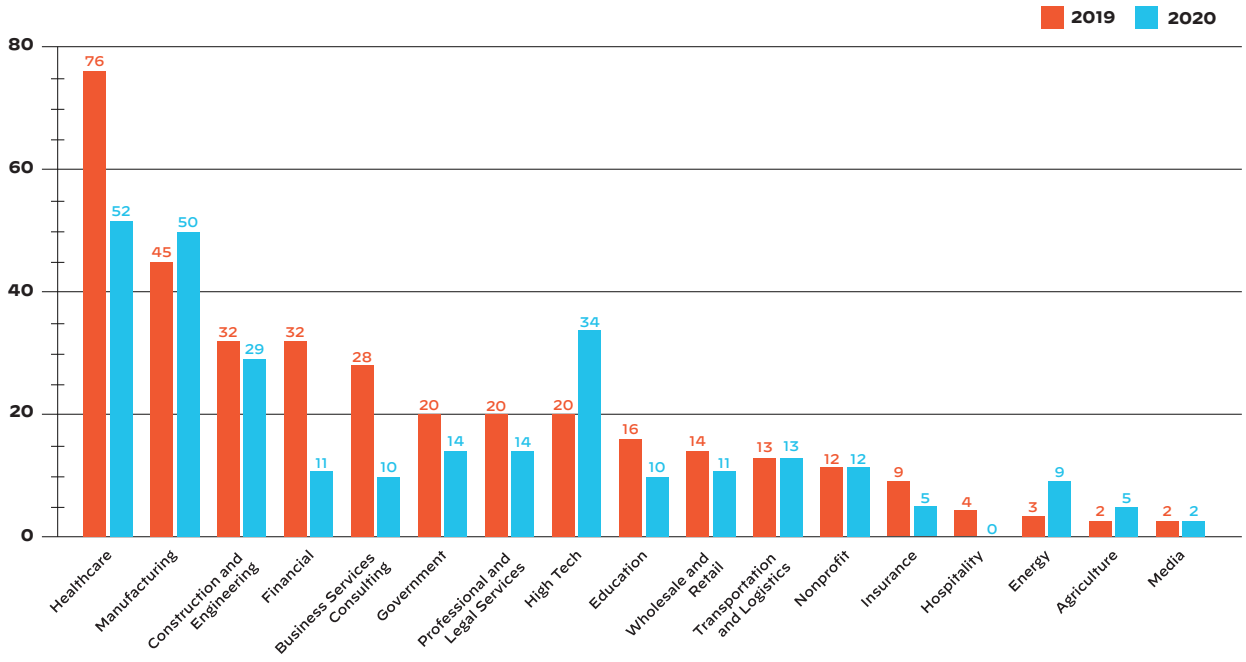


Figure 5: Ransomware incident response cases by industry in 2019 and 2020 in the US, Canada, and Europe

Additionally, ransomware actors are demanding more money year over year in the US, Canada, and Europe. In 2020, ransom demands were an average of US$847,344, often requested in the form of bitcoin or Monero cryptocurrency. This amount can vary dramatically depending on the ransomware family.

The total cost of a ransomware incident is also typically much more than the demand itself. In 2020, the average cost of a forensic engagement (or incident response investigation) was US$73,851, even when backups were considered a viable option for the organization. This number does not account for other costs potentially accrued, monetary or otherwise, bringing the total average cost overall to a number that would incapacitate many businesses.

Table 1 shows a breakdown of ransomware costs.

Table 1: Costs Associated with Ransomware Incidents in 2020 in the US, Canada, and Europe (US$)

	2020 Data	Earlier Data (Where Available)
Avg. ransom demand	$847,344	–
Avg. ransom paid	$312,493	$115,123 (2019)
Highest ransom demand	$30,000,000	$15,000,000 (2015–2019)
Highest ransom paid	$10,000,000	$5,000,000 (2015–2019)
Lowest ransom demand	$1,000	–
Avg. cost of forensic engagement	$73,851	$62,981 (2019)
Avg. cost of forensic engagement, small and midsize business	$40,719	–
Avg. ransom demand, small and midsize business	$718,414	–
Avg. cost of forensic engagement, large enterprise	$207,875	–
Avg. ransom demand, large enterprise	$2,923,122	–

02

2020 Top Ransomware Variants

2020 was a big year for ransomware. We saw both old and new families wreaking havoc on industries globally. Ransomware operators took advantage of widespread COVID-19 concerns by conducting phishing attacks containing pandemic-related themes and heavily targeted already overwhelmed industries such as healthcare. While the following is not an all-inclusive list, Palo Alto Networks observed these families during the 2020 calendar year.

Ryuk

Since August 2018, numerous industries, including government, healthcare, energy, and high tech, have been targeted by Ryuk ransomware. Throughout 2020, we saw a significant increase in Ryuk ransomware attacks targeting education, healthcare, and government/military organizations primarily within the US, but also in the UK and Canada. A heavy focus was put on hospital systems, likely due to the necessity for uptime, as these systems were overwhelmed with handling the ongoing COVID-19 pandemic. We observed initial Ryuk ransom requests ranging from US$600,000 to $10 million across multiple industries. Most often, these payments were communicated using a ProtonMail account and requested in the form of bitcoin.

To gain access to a target system, Ryuk has successfully compromised hosts through malicious macros in phishing documents, utilized commodity malware such as Trickbot, BazaLoader, and Emotet, and used exploit techniques that allow malicious software to evade endpoint security products. In some cases, Ryuk was installed weeks or even months after backdoor malware, such as Trickbot, was observed on that victim's host. In at least one instance, it was deployed after business hours using backup service accounts. Once they gain access to a system, Ryuk operators will leverage RDP connections to deploy the Ryuk payload or move laterally through the network. During active infection, Ryuk will close and encrypt all files, including their own malicious document that resulted in the initial download. A file named "RyukReadMe" is placed onto the system, and tools such as PowerShell and Windows Management Instrumentation (WMI) are used to enumerate the network while evading detection. Ryuk ransomware is believed to be associated with the threat group Wizard Spider.

Visit the Unit 42 blog for more information on Ryuk ransomware.

Maze (ChaCha)

Maze ransomware, a variant of the ChaCha ransomware family, was first observed active around May 2019 and increased activity exponentially at the beginning of 2020. Using malicious Microsoft Word and Excel phishing documents, Maze targeted organizations globally across many industries, exploiting vulnerable external services using exploit kits such as Spelevo to gain access to victim environments. Industries impacted by Maze include finance, healthcare, transportation and logistics, high tech, telecommunications, construction and engineering, media and communication, and many others in the US, UK, Canada, France, and Switzerland.

In late 2020, Maze began delivering its ransomware payload from within a virtual machine (VM) as a means to evade detection. This novel technique was first observed in RagnarLocker and allows the ransomware to deploy itself as a VM on nearly every targeted device it infects. The Maze file-encrypting payload was delivered on a VirtualBox virtual disk image identified within a Windows MSI file. Also included in the MSI file was a VirtualBox hypervisor used to run the VM. In some cases, the operators deployed the payload days after establishing persistence on the network. Maze also uses various tools, including Cobalt Strike, Mimikatz, PowerSploit, and ProcDump, during campaigns.

Before file encryption, Maze operators could exfiltrate files for further leverage to get their desired ransom payment. These files, or threats to expose these files, were posted to a leak site. In 2020, Maze ransom demands averaged US$4.8 million, a significant increase compared to the average ransom demand of $847,344 across all ransomware families in 2020. Direct communication with the operators was through a Tor website.

In November 2020, the Maze actors announced their retirement from the ransomware scene. However, their legacy appears to live on in the Egregor ransomware, which began to emerge just before this announcement. These actions follow a similar pattern to that of the GandCrab ransomware group, which announced retirement in May 2019, only to return under the REvil umbrella.

Visit the Unit 42 blog for more information on Egregor ransomware or Maze ransomware.

Defray777

Defray777, also known as RansomEXX and Target777, was first discovered in 2017. Run entirely in memory, it is the first ransomware to have standalone executable files for both Windows and Linux, where the Windows version will encrypt all files and the Linux variant will only encrypt directories specified via a command line argument. Toward the end of 2020 and into 2021, Defray777 operators began to display their ability to exfiltrate data. Data associated with victims of this ransomware began appearing on the dark web. Defray777 is associated with the threat group PyXie and has targeted the healthcare, education, manufacturing, government, construction and engineering, and high tech sectors in the US, Canada, Australia, Japan, France, and Brazil.

Between February and October 2020, we observed Defray777 alongside commodity malware such as Trickbot and IcedID. Like many other ransomware families, Defray777 is delivered most commonly via phishing emails containing malicious Microsoft documents or abusing software vulnerabilities. Defray777 is executed using Cobalt Strike after installation of backdoor malware, such as Vatet, and upon encryption renames files using a file extension such as .[unique ID][eight-digit hexadecimal number] or containing 777 or .txd0t. Ransoms for this variant were recorded between US$16,000 and $42,000, demanded via bitcoin.

Visit the Unit 42 blog for more information on Defray777 ransomware.

WastedLocker

One of the newest names in the ransomware game is WastedLocker. Since at least May 2020, WastedLocker has been actively used against numerous industry verticals—primarily those with a perceived large number of assets, which ultimately results in larger ransom requests that could be US$10 million or more. WastedLocker is associated with the threat group referred to as Evil Corp, the same group responsible for Dridex and BitPaymer activities.

Between June and September 2020, Unit 42 observed WastedLocker targeting the information technology, legal, pharmaceutical, manufacturing, and transportation and logistics sectors in the US and UK. These operators have been extremely successful with their ransomware infections thanks to some of the malware features, including the ability to mask itself as a fake browser or other software update. WastedLocker was developed with defense evasion in mind, as it contains the ability to bypass behavior-based malware detection capabilities in anti-malware security software and transparently encrypts cached documents in memory. The operators have also been observed using standard off-the-shelf tools (e.g., Cobalt Strike and PSExec) not only for initial access, but also for system enumeration, lateral movement, and command and control (C2) communications.

Visit the Unit 42 blog for more information on WastedLocker ransomware.

GandCrab + REvil

Launched in January 2018, the GandCrab ransomware put a considerable dent in the pockets of many organizations. Despite a retirement announcement in May 2019 and the arrest of a significant distributor in July 2020, as well as a publicly available decryptor for multiple versions of the ransomware, we continued to see GandCrab infection attempts at numerous organizations throughout 2020. In fact, through November 2020, GandCrab made up approximately 45% of observed ransomware variants collected from Unit 42 telemetry.

In April 2019, REvil ransomware (also known as Sodinokibi) began to emerge, targeting the professional and legal services, manufacturing, media and communication, wholesale and retail, construction and engineering, and energy sectors in the US, Australia, Canada, Finland, and Hong Kong. This ransomware variant, likely developed by the same creators as GandCrab, continued to follow the traditional ransomware-as-a-service model with a preference for RDP vulnerabilities or phishing for initial access. Once in a system, the malware will attempt to initiate DNS requests to multiple domains followed by a TLS 1.0 connection after DNS resolution.

In January 2020, the threat operators began to utilize double extortion methods, informing victims that they would publicly expose stolen data if the ransom were not paid. Ransom demands were requested in bitcoin and Monero, ranging from US$18,000 to $1.3 million.

Visit the Unit 42 blog for more information on GandCrab and REvil ransomware.

NetWalker

NetWalker (sometimes referred to as MailTo) is yet another ransomware variant that has exposed compromised victim data on the dark web, leaking data from more than 100 organizations heading into 2021. NetWalker has been actively deployed since August 2019, targeting the government, healthcare, manufacturing, transportation and logistics, and energy sectors in the US, Canada, Saudi Arabia, France, Germany, Australia, New Zealand, Sweden, Pakistan, India, Thailand, UK, United Arab Emirates, Colombia, and South Africa. Victim organizations found themselves with ransom demands ranging from US$100,000 to $2 million in bitcoin.

NetWalker is PowerShell-based and executed directly in memory via reflective loading. It has been delivered to organizations via phishing emails, weak RDP credentials, or exposed VPN and web applications, and often spread via Server Message Block (SMB) remote execution using PSExec.

In January 2021, Tor sites used to communicate with NetWalker victims were taken down through a coordinated effort with international law enforcement. NetWalker is a supporter of the ransomware affiliate model. While many of the infected victims were asked to communicate with the operators through Tor, in at least one case, the victims received communication through standard email. The primary communication site may have been taken down. However, the malware still exists, and so does the capability to stand up new ways to engage with victims. NetWalker is associated with the threat group Circus Spider.

Visit the Unit 42 blog for more information on NetWalker ransomware.

DoppelPaymer

Another ransomware variant that emerged in 2019 and carried strong into 2020 is DoppelPaymer, a known descendant of BitPaymer ransomware.

For its initial infection vector, DoppelPaymer has been observed using fake software updates. Once downloaded and executed, the fake update will then download and execute second-stage malware such as Dridex onto an infected system. Off-the-shelf post-exploitation tools such as Cobalt Strike, PowerShell Empire, and Mimikatz have also been observed during DoppelPaymer infections, as has PSExec (specifically to facilitate lateral movement within compromised environments). Additionally, a tool called Process Hacker, which can be used to terminate security services and processes, has also been observed in these incidents.

Where approaches to victimization are concerned, the DoppelPaymer operators have hopped onto the double extortion trend. In February 2020, they launched a leak site, threatened to sell data on the dark web, and even created a Twitter account for general exposure. Additionally, according to the FBI, the DoppelPaymer operators have been known to call victims to pressure them into paying ransoms.

In terms of victims themselves, DoppelPaymer operators have targeted state and local governments in addition to industries including wholesale and retail, manufacturing, finance, insurance, transportation and logistics, high tech, hospitality, and real estate within the US, Canada, Mexico, South Africa, Belgium, Italy, Norway, and Germany. DoppelPaymer ransom demands for 2020 were relatively high, ranging from US$50,000 to $1.5 million, initially requested in bitcoin. DoppelPaymer is possibly associated with the threat group Indrik Spider.

Visit the Unit 42 blog for more information on DoppelPaymer ransomware.

Dharma

One of the oldest ransomware families we still see actively deployed today, Dharma (also known as CrySIS and Wadhrama) was first identified publicly in 2016. This ransomware typically spreads via fake software installer files or phishing emails and leverages unsecured or weak RDP servers. Dharma attempts to escalate privileges through the use of SMB. Files are often encrypted using the .cezar extension. However, many other file extensions have been observed post-encryption. Dharma's source code has been offered for sale on hacking forums for as little as US$2,000. Available source code for malware such as Dharma could mean more customization with other malware, resulting in more successful and damaging infections.

Dharma targeted the insurance, transportation and logistics, high tech, healthcare, and government sectors around the US, Italy, Japan, and India with a focus on small and medium-sized businesses. Ransom demands vary tremendously, having been observed as low as US$1,000 and as high as $150,000, requested in bitcoin. These operators appear to prefer communicating with victims through standard email. Instead of using an anonymizer service such as Tor like many other ransomware families, Dharma uses various free email services, such as Tutanota, Gmail, Foxmail, and ProtonMail.

Visit the Unit 42 blog for more information on Dharma ransomware.

Phobos

Another offender that came into the ransomware scene around December 2019 is Phobos ransomware. It is a likely variant of Dharma ransomware that leverages phishing using malicious Word documents or URLs, and compromised or weak RDP credentials for system access. Phobos has utilized SMBv2 for lateral movement. Files are often encrypted using the extension .phobos, but other file extensions have been observed over time using the format .[ID][Email].[extension]. Phobos operators may also offer to decrypt one or more files as proof of decryption capability and will do so for free as a good faith gesture.

Throughout 2020, Phobos targeted small and medium-sized businesses in the finance, education, manufacturing, professional and legal services, insurance, high tech, construction and engineering, healthcare, and energy sectors around the US, Portugal, Brazil, Seychelles, Romania, Indonesia, Germany, and Japan. Ransom demands were requested in bitcoin and varied from US$8,000 to $50,000.

Visit the Unit 42 blog for more information on Phobos ransomware.

Zeppelin

Zeppelin ransomware, a possible variant of Buran/VegaLocker, has been actively used since at least November 2019. This ransomware can be deployed in multiple configurations and creates two distinct registry keys to store the encryption key. These keys are fairly distinct and quite prominently contain the string "Zeppelin" within them.

In 2020, Zeppelin targeted the healthcare, high tech, manufacturing, finance, and real estate sectors in the US, Canada, Bulgaria, Japan, South Korea, France, and Taiwan. Primarily, Zeppelin was deployed through the use of weak RDP servers, malicious web advertisements, and invoice-themed phishing emails with malicious macros. Also of note, this ransomware variant specifically checks a system's IP address on execution and will not fully execute if a given system appears to be located in Belarus, Russia, Ukraine, or Kazakhstan. This indicates that the operators may be in or around these regions.

Like other ransomware families, Zeppelin has shown double extortion capability and interest in exfiltrating documents prior to, or in lieu of, encryption to be sold on the dark web. Zeppelin ransom demands appeared relatively consistent in their amounts across each targeted industry sector, ranging from US$13,000 to $35,000 requested in bitcoin.

Visit the Unit 42 blog for more information on Zeppelin ransomware.

2020 Ransomware Summary

Table 2 collects key details from the "2020 Top Ransomware Variants" section.

Table 2: 2020 Ransomware Summary

Name (+Variants/ Aliases	Mode of Operation	Typical Delivery (Besides Phishing)	Common Industries	Common Countries	Ransom Demand (US$) + Payment Type	Double Extortion Witnessed	Threat Assessment
Ryuk	Spray and pray	Commodity malware, (e.g., Trickbot, BazaLoader, Emotet); used exploit techniques against endpoint software	Govt., Healthcare, Energy, High Tech	US, UK, Canada	$600K–10M, bitcoin	No	Click here
Maze (ChaCha)	Targeted	RDP; vulnerable external services; exploit kits such as Spelevo	Finance, Healthcare, Transportation/ Logistics, High Tech, Telecom, Const./ Engr., Media/ Comms, et al.	US, UK, Canada, France, Switzerland	Avg. $4.8M, bitcoin	Yes	Click here
Defray777 (RansomEXX, Target777)	Targeted	Software vulnerabilities	Healthcare, Education, Mfg., Govt., Const./ Engr., High Tech	US, Canada, Australia, Japan, France, Brazil	$16K–$42K, bitcoin	Yes	Click here
WastedLocker	Targeted	Masquerading as legitimate software updates	High Tech, Professional/Legal, Pharma., Mfg., Transportation/ Logistics	US, UK	$10M+, bitcoin	No	Click here
GandCrab + REvil (Sodinokibi)	Targeted	RDP	Professional/ Legal, Mfg., Media, Wholesale/Retail, Const./Engr., Energy	US, Australia, Canada, Finland, Hong Kong	$18K–$1.3M, bitcoin and Monero	Yes	Click here
NetWalker (MailTo)	Targeted	RDP; exposed VPN and web applications	Govt., Mfg., Healthcare, Transportation/ Logistics, Energy	US, Canada, Saudi Arabia, France, Germany, Australia, New Zealand, Sweden, Pakistan, India, Thailand, UK, United Arab Emirates, Colombia, S. Africa	$100K–$2M, bitcoin	Yes	Click here
DoppelPaymer (BitPaymer)	Targeted	Fake software installers; Dridex	Govt., Wholesale/ Retail, Mfg., Finance, Insurance, Transportation/ Logistics, High Tech, Hospitality, Real Estate	US, Canada, Mexico, S. Africa, Belgium, Italy, Norway, Germany	$50K–$1.5M, bitcoin	Yes	Click here

Table 2: 2020 Ransomware Summary (continued)							
Name (+Variants/ Aliases	Mode of Operation	Typical Delivery (Besides Phishing)	Common Industries	Common Countries	Ransom Demand (US$) + Payment Type	Double Extortion Witnessed	Threat Assessment
Dharma (CrySIS, Wadhrama)	Spray and pray	RDP; fake software installers	Insurance, Transportation/ Logistics, Healthcare, Govt.	US, Italy, Japan, India	$1K–$150K, bitcoin	No	Click here
Phobos (Dharma)	Spray and pray	RDP	Finance, Education, Mfg., Professional/ Legal, Insurance, High Tech, Const./ Engr., Healthcare, Energy	US, Portugal, Brazil, Seychelles, Romania, Indonesia, Germany, Japan	$8K–$50K, bitcoin	No	Click here
Zeppelin (Buran/ VegaLocker)	Spray and pray	RDP	Healthcare, High Tech, Mfg., Finance, Real Estate	US, Canada, Bulgaria, Japan, S. Korea, France, Taiwan	$13K–$35K, bitcoin	Yes	Click here

The Future of Ransomware

Reviewing activities throughout 2020 and looking back over the last several years, it's easy to see the ongoing trends with ransomware and which components have picked up more quickly than expected.

Ransomware-as-a-Service Model

The ease of success with ransomware attacks tells us that more financially motivated operators will continue appearing on the scene. Adversaries of all kinds are continually looking for organizations to target, and they know that ransomware is not only effective, but can also be low-effort, especially if using the ransomware-as-a-service model. We expect more and more operators will follow this model for all sums of money.

Increase in Variants and Capabilities

Some of the most prevalent ransomware families we observed throughout 2020 were less than a year old. New and updated ransomware variants will continue to be developed and deployed for use as standalone malware or alongside commodity malware. Additionally, with Linux being targeted more often, it is clear that adversaries will continue to build out the capability to target all kinds of systems.

More to Adopt Double Extortion

Proof of compromise and double extortion techniques were also less than a year old heading into 2020, but they have now exploded in popularity. At least 16 different ransomware variants are now threatening to expose data or utilizing leak sites, and more variants will likely continue this trend. In this vein, the use of Tor and other anonymous services will also continue to grow. The use of anonymized services makes it more difficult for security researchers and law enforcement to track activities and identify indicators that can be used for network defense.

Increasing Ransom Demands

The highest ransom demand has increased from US$500 to more than $30 million in just a few years (doubling from $15 million in 2019 to $30 million in 2020). As long as attackers keep getting paid, these demands will continue to rise. Very few operators make ransom demands in forms other than virtual currency, generally favoring bitcoin, though Monero was also requested in several incidents we observed.

Continued Use of What's Familiar

Much of the success of these operators lies in their ability to evade detection. Adversaries will continue to infiltrate networks using traditional phishing and weak credentials, alongside tools native to the targeted environments. This includes using post-exploitation frameworks such as Cobalt Strike, PowerShell Empire, and PowerSploit.

03

Conclusion and Recommendations

Defending against ransomware attacks is similar to protecting against other malware. However, it represents a much higher risk to the organization.

Initial Access

Initial access is relatively consistent across all ransomware variants. Organizations should maintain user awareness and training for email security as well as consider ways to identify and remediate malicious email as soon as it enters an employee's mailbox. Organizations should also ensure they conduct proper patch management and review which services may be exposed to the internet. Remote desktop services should be correctly configured and secured, using the principle of least privilege wherever possible, with a policy in place to detect patterns associated with brute-force attacks.

Backup and Recovery Process

Organizations should continue to back up their data and keep an appropriate recovery process in place. Ransomware operators will target on-site backups for encryption, so organizations should ensure that all backups are maintained securely offline. Recovery processes must be implemented and rehearsed with critical stakeholders to minimize downtime and cost to the organization in the event of a ransomware attack.

Security Controls

The most effective forms of protection from ransomware are endpoint security, URL filtering or web protection, advanced threat prevention (unknown threats/sandboxing), and anti-phishing solutions deployed to all enterprise environments and devices. While these will not outright guarantee prevention, they will drastically reduce the risk of infection from common variants and provide stopgap measures, allowing one technology to offer a line of enforcement when another may not be effective.

Palo Alto Networks Capabilities

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—our services eliminate the coverage gaps generated by disparate network security tools:

- WildFire® malware prevention service detects activity associated with known and unknown ransomware variants as well as other file-based threats.
- URL Filtering can be configured to block access to URLs in suspicious categories, preventing a host from reaching out via HTTP to a web server Palo Alto Networks has seen host suspicious content/malware.
- Threat Prevention leverages the firewall's visibility to inspect all traffic and automatically prevent known threats regardless of port, protocol, or SSL encryption, confronting threats at each phase of the attack. This service can also detect brute-force attacks when the Vulnerability Protection profile is enabled.
- Enterprise Data Loss Prevention prevents an organization's sensitive data from leaving the enterprise network.

Cortex® XDR™ contains an anti-ransomware module as well as an exploit prevention and anti-malware module that targets encryption-based activities associated with ransomware and other commodity malware in addition to detecting lateral movement. Local analysis detection and behavioral threat protection identify anomalous activities and malicious files.

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.

Visit Palo Alto Networks Cyberpedia to read more about ransomware prevention.

About

Unit 42 Threat Intelligence and Incident Response

Unit 42 brings together an elite group of cyber researchers and incident responders to protect our digital way of life. 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 will serve as trusted partners to rapidly respond to and contain threats so you can focus on your business.

Cortex

Cortex® is the Palo Alto Networks security operations suite, offering extended detection and response through Cortex XDR, expert data breach response with Unit 42, and more.

Cortex XDR™ is an AI-powered, behavior-based endpoint security solution that fuses data from the endpoint, network, and cloud for full host situational awareness.

Cortex XSOAR is the industry's most comprehensive security orchestration, automation, and response (SOAR) platform, helping you automate investigation and response to quickly shut down ransomware and limit its impact on your network.

Strata

Cloud-Delivered Security Services seamlessly integrate with Palo Alto Networks industry-leading Next-Generation Firewall platform to coordinate intelligence and provide protections across all attack vectors.

Methodology

The Unit 42 threat intelligence and incident response teams collaborated to create this ransomware threat report. The information in this report was derived from analysis of available threat data for the 2020 calendar year and a look back to 2015–2019 where relevant.

Unit 42 researchers analyzed ransomware leak site data available on the dark web and public websites, global threat data available via internal and external sources, and breach response data provided by the Unit 42 incident response team for the US, Canada, and Europe.

AutoFocus

AutoFocus™ contextual threat intelligence service provides the intelligence, analytics, and context required to understand threat data on your network.

The following dataset was used to determine 2020's top ransomware variants as detailed herein by Unit 42:

Network sessions analyzed

19,568

Unique malware samples

164

Unit 42 Incident Response

Unit 42 data breach response services are available for any cybersecurity incident, including ransomware infections. In a ransomware attack, Unit 42 investigators conduct expert forensic analysis to quickly contain the attack and provide victims with key response information to ensure operations are restored quickly and efficiently.

For the calendar years 2019 and 2020, the following dataset—which includes businesses of all sizes in many industry verticals, with select data dating back to 2015—was used to review trends in ransomware activities across the US, Canada, and Europe:

Ransomware investigations

252

Ransomware Leak Sites

Unit 42 reviewed data between January 2020 and January 2021 available on public leak sites and the dark web to gauge an understanding of the organizations being extorted by ransomware operators. The data analyzed for this report is a summary of the following dataset:

Victims	Victim industries	Victim regions	Victim countries
337	**56**	**5**	**39**

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