zscaler™ | ThreatLabz

2022 ThreatLabz State of Ransomware Report

Contents

Introduction

If it feels like ransomware is always in the news, it isn't just media bias: the Zscaler ThreatLabz research team has found that ransomware attacks increased by yet another 80% between February 2021 and March 2022 compared to the previous year, setting new records for both the volume of attacks and the cost of damages.

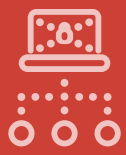
Ransomware is more and more attractive to attackers, who are able to wage increasingly profitable campaigns based on three major trends:

Supply chain attacks

that exploit trusted vendor relationships to breach organizations and multiply the damage of attacks by enabling threat actors to hit multiple (sometimes hundreds or thousands) of victims at the same time.

Ransomware as a service

that uses affiliate networks to distribute ransomware on a wide scale, allowing hackers who are experts in breaching networks to share profits with the most advanced ransomware groups.



Multiple-extortion attacks

that utilize data theft, distributed denial of service (DDoS) attacks, customer communications, and more as layered extortion tactics to increase ransom payouts.

These tactics add up to be very damaging. Industry experts predict that ransomware will be the top tactic used in third-party breaches and supply chain attacks in 2022, and that the global cost of ransomware damages will grow to $42 billion by 2024.

These trends have pushed ransomware even further up the list of cybersecurity priorities for organizations across industries. Aimpoint's "The CISOs Report," 2022 found that ransomware is the single highest threat that CISOs around the world are most concerned about.

How can you identify and defend against the latest ransomware variants? This report should help.

ThreatLabz analyzes data from more than 200 billion daily transactions and 150 million daily blocked attacks across the Zscaler Zero Trust Exchange along with Zscaler ThreatLabz threat intelligence to track prevalent threat families, identify emerging trends, and improve protections for Zscaler customers. In this report, ThreatLabz looked at ransomware data from February 1, 2021, through March 31, 2022, to identify the most prolific ransomware families and their tactics. We will share our findings, predictions, and best practices guidance to help inform your ransomware defense strategies.

Key findings

Ransomware attacks increased by 80% year over year, accounting for all ransomware payloads observed in the Zscaler cloud.

Double extortion ransomware increased by 117%, indicating that more and more attacks include data theft in their strategies. Some industries saw particularly high growth of double extortion attacks, including healthcare (643%), food service (460%), mining (229%), education (225%), media (200%), and manufacturing (190%).

Manufacturing was the most targeted industry for the second straight year, making up almost 20% of double extortion ransomware attacks.

Supply chain ransomware attacks are on the rise, as are supply chain attacks in general. Exploiting trusted suppliers lets attackers breach a large number of organizations all at once, including organizations that otherwise have strong protections against external attacks. Supply chain ransomware attacks of the past year include damaging campaigns against Kaseya and Quanta as well as a number of attacks exploiting the Log4j vulnerability.

Ransomware as a service is driving more attacks. Ransomware groups continue to recruit affiliates through underground criminal forums. These affiliates compromise large organizations and deploy the group's ransomware, typically in exchange for about 80% of the ransom payments received from victims. Most (8 out of 11) of the top ransomware families of the past year have commonly proliferated via ransomware-as-a-service models.

Law enforcement is cracking down. A number of last year's top ransomware families—particularly those targeting critical services—attracted attention from law enforcement agencies around the world. REvil (responsible for famous attacks on Kaseya and JSB), DarkSide (responsible for the attack on Colonial Pipeline), and Egregor (a rebranding of Maze, last year's top ransomware family) all had assets seized by law enforcement in 2021.

Ransomware families aren't going away—they're just rebranding. Feeling increased heat from law enforcement, many ransomware groups have disbanded and reformed under new banners, where they use the same (or very similar) tactics. DarkSide rebranded as BlackMatter, DoppelPaymer rebranded as Grief, and Avaddon rebranded as Haron and Midas. Evil Corp, sanctioned by the US government, has consistently rebranded their ransomware operations.

The Russia-Ukraine conflict has the world on high alert. There have been several attacks associated with the Russia-Ukraine conflict, including multiple wipers including HermeticWiper and PartyTicket ransomware. So far, most of this activity has targeted Ukraine. However, government agencies have warned organizations to be prepared for more widespread attacks as the conflict persists.

Zero trust remains the best defense. To minimize the chance of a breach and the damage a successful attack can cause, your organization must use defense-in-depth strategies that include reducing your attack surface, enforcing least privileged access control, and continuously monitoring and inspecting data across your environment.

The evolution of ransomware

Ransomware is a type of malware cybercriminals use to disrupt a victim's organization. Ransomware encrypts an organization's important files into an unreadable form and demands a ransom payment to decrypt them. Ransom demands are often proportional to the number of systems infected and the value of the encrypted data: the higher the stakes, the higher the payment.

In late 2019, attackers evolved their ransomware tactics to include data exfiltration, commonly referred to as a "double extortion" ransomware attack. In these attacks, if victims choose not to pay the ransom to decrypt the data and, instead, attempt to restore the data from a backup, the attackers threaten to leak the stolen data. In late 2020, some ransomware attackers added another attack layer with DDoS tactics that bombard the victim's website or network, creating even more business disruption, thus pressuring the victim to negotiate.

In 2021 and going into 2022, the most damaging ransomware trend involves supply chain attacks, in which a breach of a vendor (typically a software or other technology provider) opens the door for second-stage attacks on organizations that rely on their products. Supply chain attacks are estimated to have jumped 51% in the back half of 2021. Threat actors have made headlines through exploits of popular software products such as SolarWinds, Kaseya, and Log4j, and we expect this trend to escalate in the coming years.

Ransomware attack sequence

Today's ransomware attacks typically have the following stages:

1. **Initial compromise:** Attackers use a variety of intrusion vectors to gain access to systems, including phishing emails, exploiting vulnerabilities in remote administrator or virtual private network (VPN) tools, and using brute force or stolen credentials to access Remote desktop protocol (RDP) connections. Supply chain attacks are yet another method to infiltrate an organization.

2. **Lateral movement:** After gaining initial access, threat actors proceed to gather victims' infrastructure information and move laterally across network systems, escalating privileges and establishing persistence mechanisms as needed, cataloging key data to steal or encrypt, and depositing ransomware payloads for later execution.

3. **Data exfiltration:** In the case of a double extortion attack, attackers will next steal sensitive data to use as a secondary extortion tactic so they can demand higher ransom payments. This reduces the victims' leverage: even if they can recover the encrypted data from backups, they still must face the threat of the cybercriminals leaking the stolen data.

4. **Ransomware execution:** Next, attackers deploy and execute the ransomware, encrypting targeted files on systems connected to the network. Ransomware typically terminates processes related to security software and databases to maximize the number of files it can encrypt. Shadow copy backups are also usually deleted from the system to hinder file recovery. Some ransomware families will also reboot the compromised system in Windows Safe Mode to bypass security endpoint software prior to file encryption. After file encryption, victims are provided with a ransom note that provides instructions for paying the ransom and decrypting their files.

5. **DDoS:** If the victim does not negotiate, some hacking groups will wage a DDoS attack against the victim's network or website, disrupting their business operations to gain additional leverage.

Figure 1 displays the typical attack chain of a multi-extortion ransomware attack.

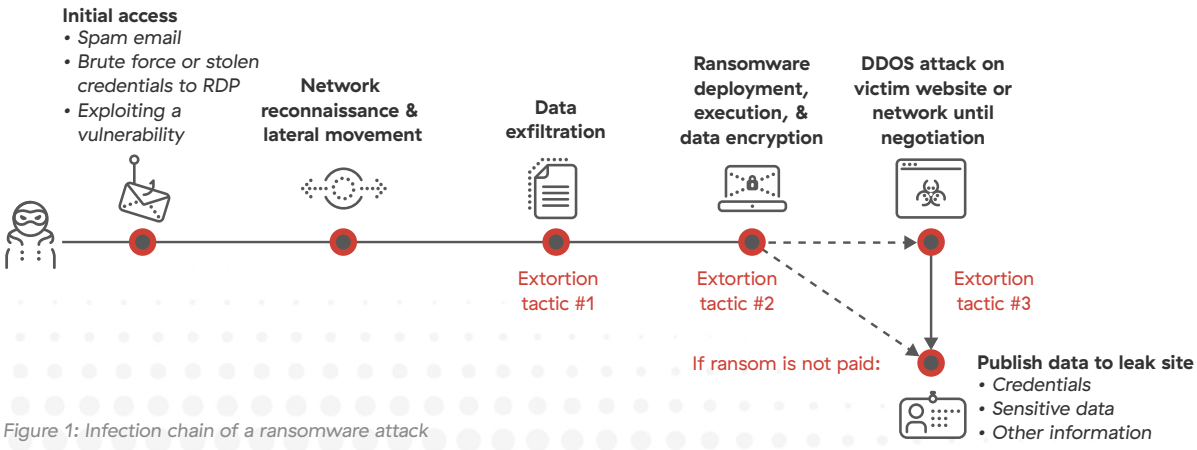


Figure 1: Infection chain of a ransomware attack

2021–2022 ransomware attack statistics

The high volume of transaction data on the Zero Trust Exchange provides a unique look into the tactics and victims of cybercriminals. From February 2021 through March 2022, ThreatLabz observed an 80% increase in ransomware payloads compared to the previous year. Further, we saw a 117% increase in double extortion ransomware victims based on data published on threat actors' data leak sites.

Industry verticals affected by ransomware

Manufacturing was already the most targeted vertical in 2020, making up 12.7% of double extortion ransomware attacks between November 2019 and January 2021. This year, the percentage of attacks on manufacturing organizations rose even further to 19.5%, followed by services (9.7%), construction (8.1%), retail and wholesale (7.5%), and high tech (6.7%).

Ransomware infections by industry

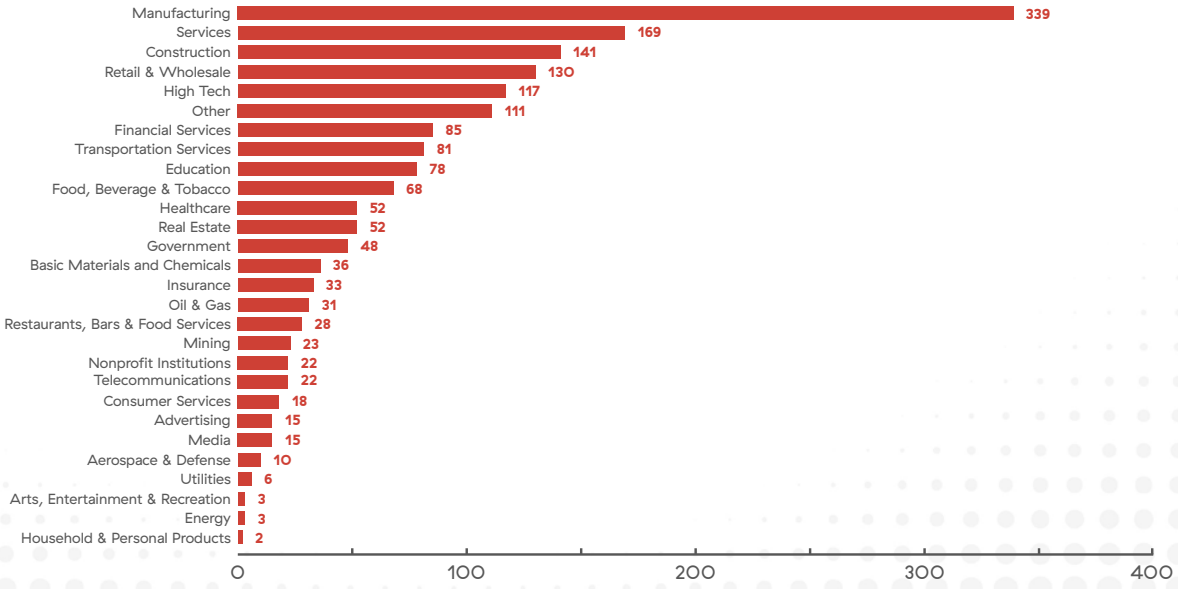


Figure 2: Ransomware infections by industry

Growth in double extortion ransomware attacks varied widely by industry. In last year's report, we noted a particularly low number of attacks against healthcare organizations, driven by increased scrutiny from law enforcement as well as pledges from several prevalent ransomware families that they would not target healthcare during the COVID-19 pandemic.

This year's data tells a different story. Double extortion ransomware attacks against healthcare grew by 643% in 2021, though it started with a very low baseline of attacks in 2020. Several other verticals with higher starting points also saw triple-digit growth in attacks, including education (225%), manufacturing (190%), construction (161%), financial services (130%), and services (109%).

Percent change in double extortion attacks: 2021 vs 2020

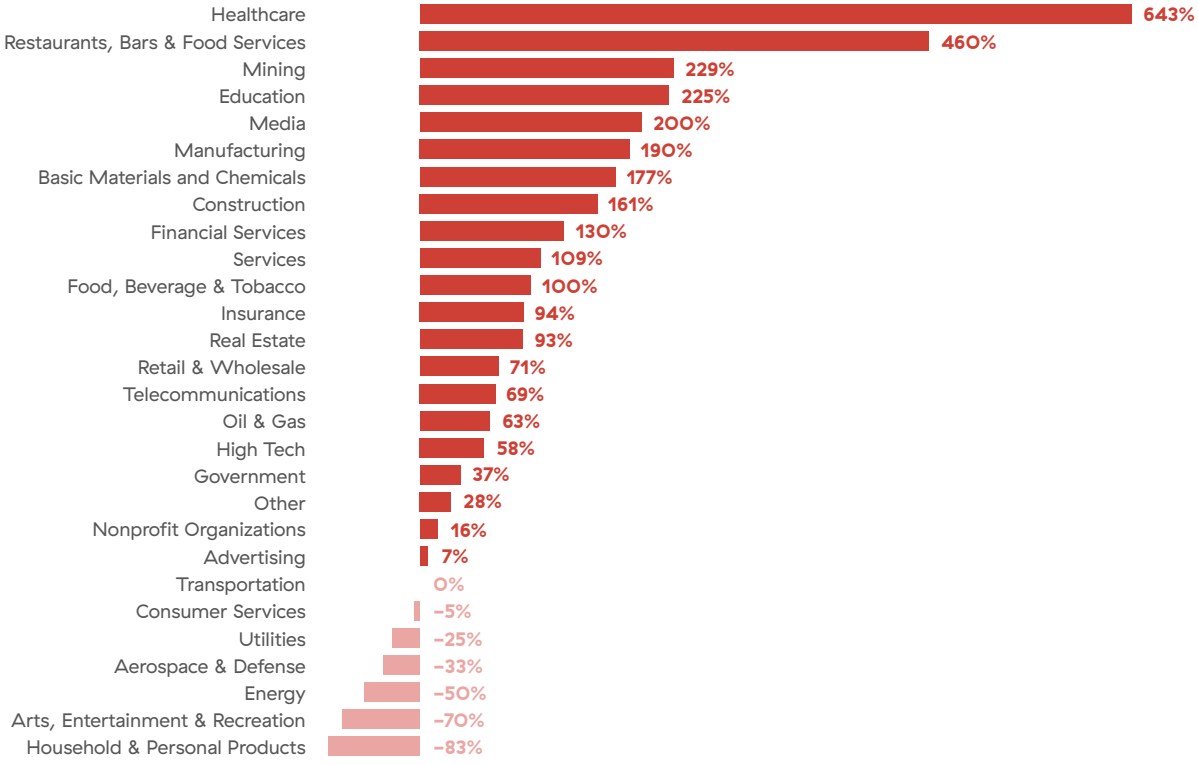


Figure 3: Percentage change in double extortion attacks by industry

Top ransomware families

Conti and LockBit were the most prevalent double extortion ransomware families in 2021, joined by a range of new entrants that emerged over the course of the year.

Figure 4 shows when each of the most active ransomware families of the past several years first emerged and began publishing data on leak sites or hacking forums.

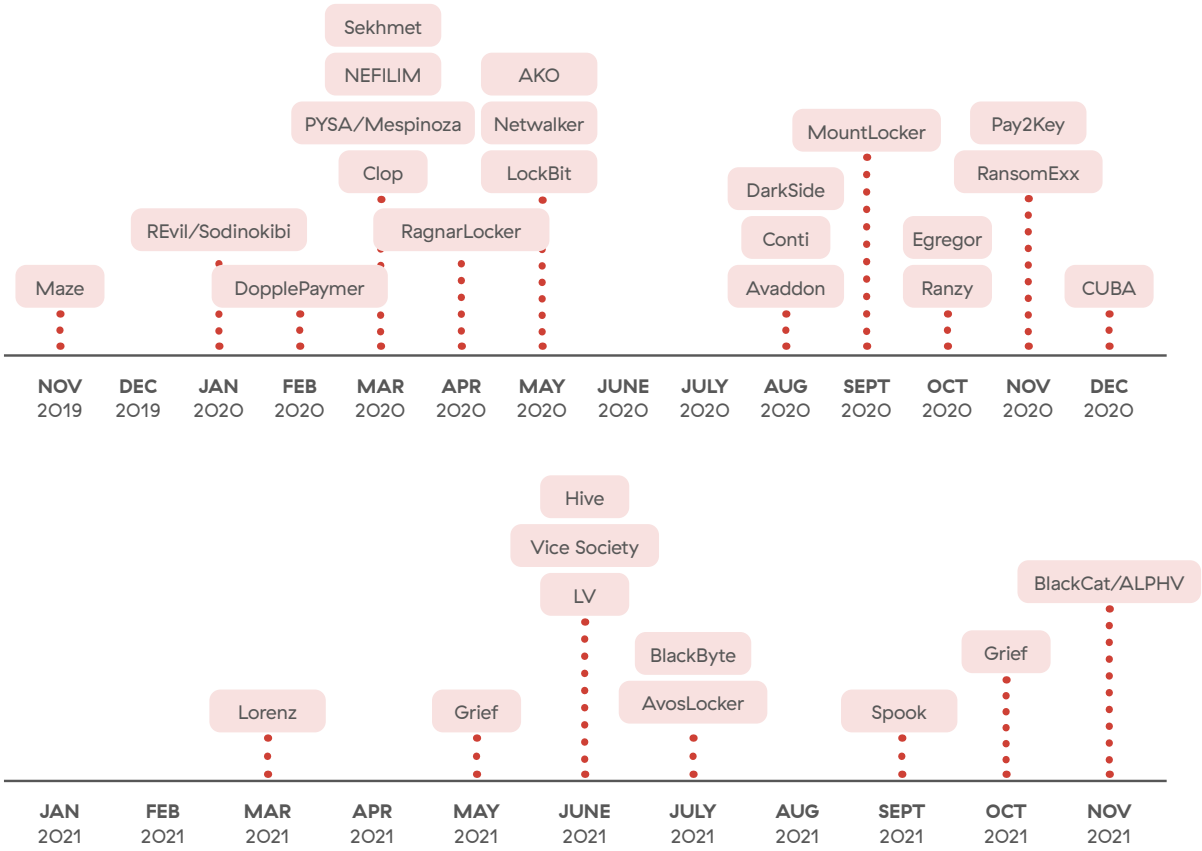


Figure 4: Timeline of ransomware families publishing on data leak sites or hacking forums

Many of the active ransomware families in 2021—2022 are ransomware-as-a-service (RaaS) models, increasing their distribution through affiliate networks. In 2021, we also saw the rebranding of several popular ransomware families, such as DoppelPaymer rebranding as Grief, DarkSide rebranding as BlackMatter, and Avaddon rebranding as Haron followed by Midas (the latter two using the Thanos ransomware builder).

Conti has been the most active ransomware group of the last two years and the costliest of all time: The FBI estimates that as of January 2022, there were more than 1,000 victims of attacks associated with Conti ransomware, with total victim payouts exceeding US$150 million (not including related damages or remediation costs). Conti victims have included a range of critical services organizations from financial services, IT, energy, and government sectors, including Ireland's public healthcare services and the government of Costa Rica. In May 2022, the US Department of State offered a $10 million reward for information on leaders of the group.

LockBit, formerly known as ABCD ransomware, tends to attack small- to medium-size businesses, thus mostly avoiding the headlines, with the exception of their attack on Accenture in August 2021. LockBit is a widely used RaaS that is attractive to attackers due to its speed and performance.

Figure 5 shows the ransomware families that affected the highest number of organizations with double-extortion attacks between February 2021 and March 2022, based on information from data leak sites.

Percent change in double extortion attacks: 2021 vs. 2020

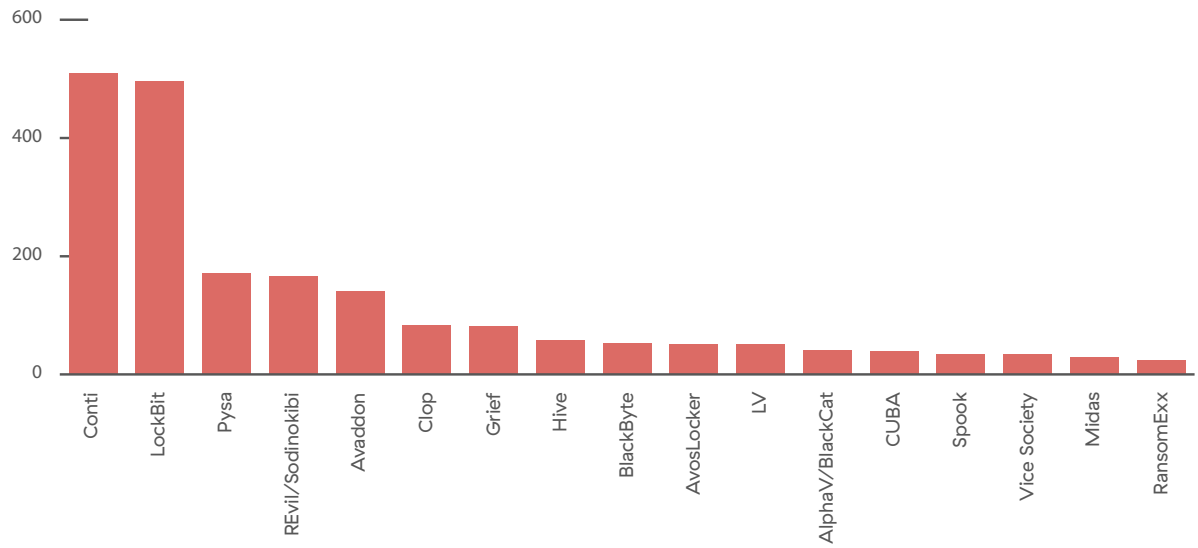


Figure 5: Ransomware attacks by family, February 2021–March 2022

2022—23 predictions

Ransomware as a service will continue to increase

RaaS has proven to be valuable for all parties involved. New ransomware developers and affiliates will increase their use of this model to wage rapidly changing attacks on vulnerable organizations.

Changing ransomware models will lead to changing targets

With ransomware builders and organizational intel available for sale on the dark web, attackers have the advantage of filtering through company profiles to narrow down the ideal targets for specific vulnerabilities, profits, and types of ransomware. As a result, you should expect to see a shift toward easier targets, including small to medium enterprises with fewer security controls and organizations with internet-visible applications that have known vulnerabilities along with previously phished credentials.

Dwell time will continue to decrease

Now that threat actors have easy and cheap access to company profiles and compromised credentials for sale on the dark web, the days of attackers sitting on targets for months or even years and then taking extra time to look around before launching an attack are coming to an end. With more public reports of ransomware attackers reducing dwell times to just days, the criminals are savvy to increased detection techniques, realizing time is of the essence for a successful attack. As a result, security teams need to close the gap and speed up detection—to days, hours, or just minutes—to prevent worst-case scenario breaches in 2022 and beyond.

Supply chain attacks will increase as adversaries compromise partner and supplier ecosystems

The world's top organizations often have the best security in place—but the same may not be true for their suppliers and partners, with third-party access to supporting networks, systems, and information. We saw this in the recent compromise of Okta by the rogue hacker group Lapsus$, and in REvil threatening Apple via Quanta Computer, a top manufacturer of Apple products. These groups and many others used supply chain attacks to access sensitive upstream information using supplier access without ever having to breach the hardened security measures of their final targets.

Ransomware may be used as, or in conjunction with, a wiper to destroy data

In early 2022, publicized attacks on Ukraine featured multiple types of wiper attacks, including HermeticWiper alongside a decoy ransomware known as PartyTicket. This is not the first time ransomware has been used in geopolitical attacks, with NotPetya and Bad Rabbit being deployed in 2017 to attack Ukrainian organizations. Geopolitical tensions bring with them the threat of masked ransomware, wipers, and other tactics that afford threat actors an elevated degree of anonymity and plausible deniability.

Old (and new) vulnerabilities will continue to cause damage

There have been some major vulnerabilities discovered in the past year (e.g., Log4j, PrintNightmare, ProxyShell/ProxyLogon) that organizations will be dealing with for years to come. Attackers will continue to search for and exploit unpatched and out-of-date software and servers to bypass security controls.

Ransomware families will continue rebranding

We saw this cycle throughout 2021: a ransomware group pulls off a major attack, earns attention and sanctions from law enforcement, and then disappears and reforms later under a new name. With ransomware very much on the radar of law enforcement, this cycle will continue throughout 2022 and beyond.

Organizations will need to beef up security beyond endpoint protection

Ransomware groups will increase use of tactics to bypass antivirus and other endpoint security controls. Organizations will have an even greater need for defense-in-depth rather than relying solely on endpoint security to prevent and detect intrusions.

Ransomware developers will add more malware obfuscation

Malware authors implement malware obfuscation techniques to hinder reverse engineering and bypass static signature detection. The malware obfuscation complexity will continue to increase with advanced techniques, including control flow flattening, polymorphic string obfuscation, and the use of virtual machine-based packers.

Leaked ransomware source code will lead to forks

There have been several source code leaks for ransomware in the past year, including two versions of Conti and Babuk. Zscaler ThreatLabz has already observed both ransomware families' source code being forked by third parties and used in attacks. The release of source code will undoubtedly lead to abuse by other criminal groups that do not have the expertise to design and build their own ransomware from scratch.

Prevention guidance

Whether a simple ransomware attack, a double- or triple-extortion attack, a self-contained threat family, or a RaaS attack executed by an affiliate network, the defense strategy is the same: employ the principles of zero trust to limit vulnerabilities, prevent and detect attacks, and limit the blast radius of successful breaches. Here are some best practices recommendations to safeguard your organization against ransomware.

1 Get your applications off of the internet.

Ransomware actors start their attacks by performing reconnaissance on your environment, looking for vulnerabilities to exploit, and calibrating their approach. The more applications you have published to the internet, the easier you are to attack. Use a zero trust architecture to secure internal applications, making them invisible to attackers.

2 Enforce a consistent security policy to prevent initial compromise.

With a distributed workforce, it is important to implement a security service edge (SSE) architecture that can enforce consistent security policy no matter where your users are working (in office or remotely).

3 Use sandboxing to detect unknown payloads.

Signature-based detection is not enough in the face of rapidly changing ransomware variants and payloads. Protect against unknown and evasive attacks with an inline, AI-powered sandbox that analyzes the behavior rather than the packaging of a file.

4 Implement a zero trust network access (ZTNA) architecture.

Implement granular user-to-application and application-to-application segmentation, brokering access using dynamic least-privileged access controls to eliminate lateral movement. This allows you to minimize the data that can be encrypted or stolen, reducing the blast radius of an attack.

5 Deploy inline data loss prevention.

Prevent exfiltration of sensitive information with trust-based data loss prevention tools and policies to thwart double extortion techniques.

6 Keep software and training up to date.

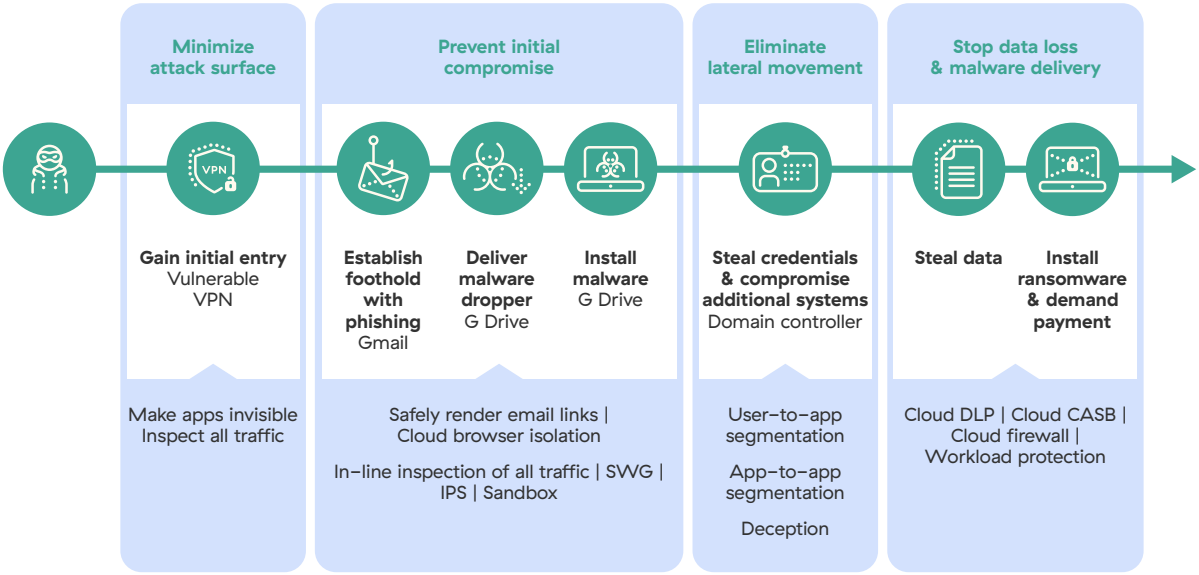
Apply software security patches and conduct regular security awareness employee training to reduce vulnerabilities that can be exploited by cybercriminals.

7 Have a response plan.

Prepare for the worst with cyber insurance, a data backup plan, and a response plan as part of your overall business continuity and disaster recovery program.

To maximize your chances of defending against ransomware, you must embrace layered defenses that can disrupt the attack at each stage—from reconnaissance to initial compromise, lateral movement, data theft, and ransomware execution.

Stopping ransomware with zero trust



Key ransomware trends

Supply chain Aattacks

What is a Supply Chain Attack?

Supply chain attacks—sometimes called value chain or third-party attacks—are attacks against the suppliers of an organization as a means for gaining access. Most large organizations have sophisticated security controls that make infiltration difficult, so attackers have found a way in through the suppliers to these organizations.

Supply chain attacks exploit the trust between legitimate organizations that exists in normal business operations. Attackers plant a backdoor into a product that they know their target uses, which allows the attacker to infiltrate the target's network without detection—typically gaining entry via automated patches or software updates, called "trojanized" updates. Once inside, the attackers can spy, steal data, implant other malware, and disrupt operations.

Such attacks involve a high degree of planning and sophistication, and they can have a devastating impact on organizations within the blast radius of the original compromise.

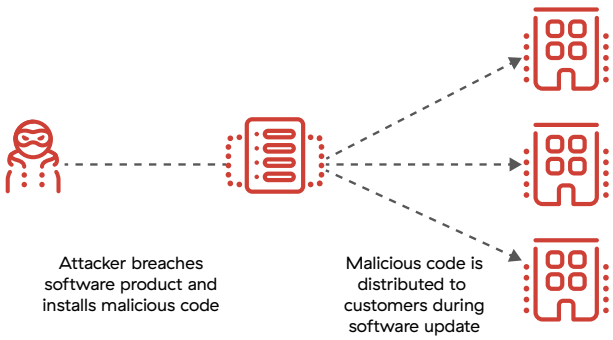


Figure 6: Supply chain attack

Kaseya supply chain ransomware

On July 2, 2021, IT management software firm Kaseya disclosed a security incident impacting their on-premises version of Kaseya VSA software, a platform that allows managed service providers (MSPs) to perform patch management, backups, and client monitoring for their customers. Roughly 70 MSPs are believed to have been breached in this attack, with downstream impacts to as many as 1,500 small and medium businesses.

The threat actor behind this attack identified and exploited a zero day vulnerability in the Kaseya VSA server that allowed them to send a malicious script to all clients that were managed by that server. The script was used to deliver REvil/ Sodinokibi ransomware that encrypted files on the affected systems.

Quanta computer supply chain

In April 2021, REvil attacked Quanta Computer, the world's largest laptop manufacturer and a top manufacturer of Apple products. Quanta refused to pay a $50 million ransom demand, leading to REvil targeting Apple and other Quanta customers for the ransom instead. REvil leaked 21 screenshots of MacBook schematics and threatened to publish more data from Apple and other companies until Apple or Quanta paid the ransom demand.

Log4j ransomware

In December 2021, the Apache Software Foundation released a security advisory regarding a remote code execution vulnerability (CVE-2021-44228) in their popular Log4j logging library. This vulnerability allows an attacker to download and execute a malicious payload by submitting a specially crafted request to the vulnerable system. The attacker can then control log messages or log message parameters to execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. Log4j is incorporated into many popular websites, applications, and frameworks, making the impact widespread. Several ransomware attacks have emerged exploiting this vulnerability:

NightSky ransomware

On January 4, 2021, attackers exploited the Log4j vulnerability in an internet-facing system running VMware Horizon, dropping the NightSky ransomware.

Khonsari

Multiple attacks have been observed using Log4j exploits on Windows systems to deploy Khonsari ransomware.

Conti

The Conti group has also leveraged the Log4j vulnerability to execute ransomware attacks. AdvIntel discovered the group scanning and targeting vulnerable Log4j VMware vCenter versions, moving laterally from existing Cobalt Strike sessions to US and European victim networks.

TellYouThePass

Attackers have exploited the Log4j vulnerability to deploy and execute the TellYouThePass ransomware in Windows and Linux systems.

Ransomware as a service

The dark web has become a very popular place for threat groups to sell their wares to would-be criminals. We've detailed the impact of these marketplaces for other attack types, such as the growth of phishing as a service in the 2022 ThreatLabz State of Phishing report.

RaaS has become incredibly popular, and it now drives the bulk of modern ransomware attacks. In fact, 8 of the top 11 ransomware families from the past year utilize RaaS ecosystems.

The RaaS model requires two parties: operators and affiliates. Operators are the threat groups that develop the ransomware. Affiliates target their victims, execute the ransomware, and set demands.

Operators recruit affiliates and provide them with the ransomware and tools required to execute it, access to a data leak site, negotiation assistance, and other support, in exchange for approximately 70—80% of the profit from the attacks.

This model is beneficial to both parties. Affiliates get everything that they need to execute highly effective ransomware attacks without needing to develop any of it themselves. This is attractive both to skilled criminals who save development time and resources as well as low-skilled criminals who otherwise would not be able to execute such an attack. Ransomware operators can dramatically increase the scale of their operations and, consequently, their profits.

RaaS has increased both the volume and damage of attacks:

- **Increase in volume of ransomware attacks:** More affiliates begin executing ransomware as it now requires less time and skill to develop.
- **Increase in ransom amounts due to double extortion:** RaaS includes a double extortion component in which threat actors steal data and threaten to publish it on a data leak site if the ransom is not paid. This increases the ransom amount and the rate of successful payment.

Geopolitical attacks

Security leaders around the world are on guard for an increase in ransomware attacks as a result of the Russia-Ukraine conflict.

In March 2022, US President Joe Biden issued a statement warning of the potential for malicious cyber conduct against the United States as a response to economic sanctions against Russia. His statement urged immediate action to harden cyber defenses among both public and private sector organizations.

8 of the top 11 ransomware families of 2021 utilize RaaS ecosystems.

As of the writing of this report, there have been several ransomware attacks against Ukraine and/or associated with this conflict:

1. **PartyTicket ransomware:** This Go-based ransomware has been used in conjunction with the HermeticWiper malware to target organizations in Ukraine. PartyTicket is unsophisticated and contains flawed encryption that can be decrypted and reversed, leading us to suspect that it was developed as a decoy to distract from HermeticWiper.
2. **Conti ransomware:** The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the United States Secret Service have rereleased an advisory on Conti, a Russia-linked ransomware group. Their advisory warns that "Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000." In late February, Conti posted two statements on their leak site, pledging support to the Russian government in response to "Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation."

Law enforcement takedowns

Law enforcement agencies around the world are paying increased attention to ransomware families, particularly those causing widespread damages. There have been several successful takedowns of high-impact ransomware families through 2021 and early 2022.

REvil takedown

REvil is one of the most infamous ransomware families of the last two years, in the news after major attacks against Kaseya and JSB. Following the Kaseya attack, the FBI planned a takedown of the REvil servers. However, they never got their chance: shortly after this critical attack in July 2021, REvil shut down its operations and the hackers disappeared. This turned out to be brief, as Kaseya's operations restarted in September 2021.

In January 2022, the Russian government apparently dismantled the REvil hacking group, arresting members at the request of the United States. The Russian Federal Security Service (FSB) searched 25 addresses, detaining 14 group members of REvil as well as seizing 426 million rubles, US$600,000, 500,000 euros, 20 luxury cars, and computer equipment. However, REvil reemerged in April 2022, attacking organizations with an updated ransomware version.

DarkSide takedown

On May 6, 2021, the DarkSide ransomware group executed a high-profile ransomware attack on Colonial Pipeline, the largest oil pipeline in the United States. Federal agencies took action, and within two weeks of the attack, a threat actor known as UNKN announced that DarkSide had been shut down, as they had lost access to servers and their cryptocurrency had been transferred to an unknown account. The Department of Justice announced that they had seized 63.7 bitcoins valued around US$2.3 million.

Egregor takedown

The Egregor ransomware group—formerly known as Maze—was taken down by cooperative law enforcement efforts on February 9, 2021. Agencies from Ukraine, France, and the United States shut down the Egregor leak website, arrested group members, and seized computers

that were linked to ransomware attacks. Egregor had extorted approximately US$80 million from more than 150 victim companies.

Ransomware rebranding

Ransomware operators have been rebranding their ransomware at a high rate in the past year. Rebranding is commonly due to unwanted attention from law enforcement and the media, as well as due to sanctions that limit the groups' abilities to collect ransom payments.

DoppelPaymer rebranded as Grief
In early May 2021, DoppelPaymer ransomware activity dropped significantly. Although the DoppelPaymer leak site still remains online, there has not been a new victim post since May 6, 2021. In addition, no victim posts have been updated since the end of June. This lull is likely a reaction to the Colonial Pipeline ransomware attack that occurred on May 7, 2021. However, the apparent break is due to the threat group behind DoppelPaymer rebranding the ransomware under the name Grief. Both ransomware variants share malware code, and the leak sites are very similar. The Grief ransom portal has some differences from the DoppelPaymer portal. In particular, the ransom demand payment method is made in Monero (XMR) instead of bitcoin (BTC). This switch in cryptocurrencies may be in response to the FBI recovering part of the Colonial Pipeline ransom payment.

Darkside rebranded as BlackMatter
After DarkSide's shutdown in May 2021, a new ransomware family named BlackMatter emerged in late July. The encryption routine used in the ransomware and text in the data leak site indicated that BlackMatter was a rebranding of DarkSide.

BlackMatter ceased its operations in November 2021. The group posted a shut down operation message on its RaaS portal that said, "Due to certain unsolvable circumstances associated with pressure from the authorities (part of the team is no longer available, after the latest news) — the project is closed."

Thanos based ransomware rebranding
Advertised on the dark web as RaaS, Thanos ransomware was first identified in February 2020. The Thanos builder was leaked, and in the following two years, a series of new variants have been developed. The Prometheus ransomware variant emerged in February 2021. In September, Prometheus was rebranded as Spook. Both have similar ransom notes and data leak sites and contain Thanos's signature Key Identifier.

In July 2021, another Thanos derived ransomware called Haron was discovered. Haron ransomware has striking similarities with Avaddon ransomware. Haron and Avaddon share commonalities in their ransom notes, negotiation sites, and data leak sites. In October 2021, another variant called Midas was discovered that is a rebranded version of Haron ransomware.

Ransomware groups rebrand to bypass sanctions and reduce attention from law enforcement.

Evil Corp rebranding

The Evil Corp gang, also known as Indrik Spider, is known for a range of malicious activity. They created banking trojans such as Dridex, the latter of which was used to distribute their BitPaymer ransomware.

The Office of Foreign Assets Control (OFAC) of the US Treasury Department sanctioned members of Evil Corp for damages caused by their Dridex malware, claiming that they inflicted more than $100 million in damages across banks and financial institutions in more than 40 countries. Following these sanctions, ransomware negotiation firms refused to facilitate ransom payments for Evil Corp for fear of fines or legal action from the US Treasury Department. To bypass sanctions, Evil Corp discovered a simple loophole through rebranding their ransomware.

Evil Corp distributed WastedLocker ransomware in June 2020, Hades ransomware in December 2020, and Phoenix ransomware in March 2021. In May 2021, they continued to rebrand their ransomware as PayloadBin, impersonating another threat actor who was not subject to the same sanctions.

Rook rebranding

Rook ransomware was spotted in November 2021, based on leaked source code from Babuk ransomware. In December 2021, a variant of Rook was rebranded as Night Sky, which has been used by the China-based threat actor group DEV-0401 to target corporate networks in double extortion ransomware attacks leveraging the Log4Shell vulnerability. In January 2022, both Rook and Night Sky shut down, and Pandora ransomware emerged. Based on code similarities, Pandora is also a rebranded version of Rook.

Major vulnerabilities used in ransomware attacks

ProxyLogon vulnerabilities

BlackKingdom and DearCry ransomwares have combined four different ProxyLogon vulnerability exploits to gain entry and encrypt their victims' networks. This tactic has been used to access the Microsoft Exchange servers, steal email, and deploy other backdoors. The ProxyLogon vulnerabilities include CVE-2021-26855 (server-side request forgery [SSRF] vulnerability in Exchange), CVE-2021-26857 (insecure deserialization vulnerability in the Unified Messaging service), CVE-2021-26858 (post-authentication arbitrary file write vulnerability in Exchange), and CVE-2021-27065 (post-authentication arbitrary file write vulnerability in Exchange). Microsoft patched these vulnerabilities in March 2021.

A typical attack chain that allows an attacker to execute remote code over exposed port 443: Attackers use the CVE-2021-26855 vulnerability to bypass Microsoft Exchange authentication and impersonate a user. The attacker sends a modified POST request for any file in the directory that is readable without authentication, where the file in the directory is not required. The attacker authenticates into the Exchange control panel (ECP) and overwrites any file in the targeted system using CVE-2021-26858 or CVE-2021-27065 vulnerabilities. After these exploits, an attacker can execute remote code using web shell on the Exchange server.

ProxyShell exchange vulnerability

Conti ransomware exploits Microsoft Exchange Server's vulnerability to enter into the victim's

network. ProxyShell exchange vulnerabilities are a combination of CVE-2021-34473 (Microsoft Exchange Server remote code execution vulnerability), CVE-2021-34523 (Microsoft Exchange Server elevation of privilege vulnerability), and CVE-2021-31207 (Microsoft Exchange Server security feature bypass vulnerability) vulnerabilities. Microsoft has patched these vulnerabilities between April and May 2021, but Conti continues to target unpatched servers to execute remote code. The infection chain for this ransomware can be seen in this report, in the breakdowns of BlackByte, AvosLocker, and Hive ransomware gangs. LockFile ransomware also targets these vulnerabilities to deploy the ransomware.

PrintNightmare

Ransomware actors exploit the PrintNightmare vulnerabilities to target Windows systems. PrintNightmare vulnerabilities are a combination of CVE-2021-34527 and CVE-2021-34481, remote code execution vulnerabilities in the Windows print spooler service that improperly performs privileged file operations and allows attackers to execute remote code with SYSTEM privileges.

The vulnerability exists in the point-and-print capability on Windows systems, and allows nonprivileged users to update or install remote printers. Microsoft released updates for PrintNightmare in July and August 2021 addressing the vulnerabilities.

In one attack, a ransomware group exploited PrintNightmare vulnerabilities and dropped Vice Society ransomware. In another campaign, attackers exploited PrintNightmare and dropped Magniber ransomware.

SonicWall SMA 100

In January 2021, SonicWall confirmed a SQL injection vulnerability in their Secure Mobile Access SMA 100 Series product that allowed attackers to access login credentials and sessions and breach vulnerable appliances by using unauthenticated, specially crafted queries. It was patched by SonicWall in February 2021.

This was discovered after the UNC2447 threat group used this flaw to attack a targeted network and deploy FIVEHANDS double extortion ransomware into victims' systems. The threat actor used the zero-day vulnerability to gain entry and drop the SOMBRAT backdoor along with additional tools to gain a foothold, perform reconnaissance, and exfiltrate data, including Cobalt Strike beacons, Adfind, BloodHound, Mimikatz, PC Hunter, and Rclone. At the end of attack, UNC2447 dropped and executed FIVEHANDS ransomware to encrypt the data of the targeted system, and then attempted to extort money under threat of publishing the data on hacker forums.

QNAP NAS device

A new variant of eChOraix ransomware targeted Quality Network Appliance Provider (QNAP) network-attached storage (NAS) devices and Synology NAS devices. In the attack chain, the attacker exploited the vulnerability CVE-2021-28799 in QNAP NAS devices. The improper authorization vulnerability has been reported in QNAP NAS running HBS 3 (hybrid backup sync) devices and allows the attacker to log in to a device remotely.

Top 11 prevalent ransomware families

What follows is an overview of 11 different ransomware families and their attack sequences. These ransomware families claimed the most victims in 2021 and into 2022, and best represent the current state of ransomware that your organization must defend against. For each family, we'll provide a bit of history, a summary of their tactics (including MITRE ATT&CK mappings), and some statistics on their target industries.

Conti

Conti ransomware was first spotted in February 2020. Conti is sometimes classified as RaaS, but their affiliates are essentially employees, rather than affiliates who sign up, use a portal to manage the page, and receive a cut of the profits. Conti and Ryuk share similar code, indicating that Conti is likely the successor of Ryuk ransomware. Conti has been the most prevalent ransomware in 2021.

Infection chain:
Conti has used a range of initial access mechanisms across various campaigns:

1 It has been distributed through spam emails containing malicious attachments or links that further download TrickBot, IcedID, BazarLoader or Cobalt Strike to get a foothold into the system.

2 Initial access is also done by exploiting known vulnerabilities such as Log4j, ProxyShell, or using weak RDP (Remote desktop protocol) credentials.

After compromise, Conti uses Cobalt Strike, Mimikatz, and other post-exploitation tools to steal credentials and establish a foothold on the network. Conti threat actors are known to use Metasploit, Netscan, and other red team tools to obtain network and domain controller information. After acquiring the necessary information, the threat actors may use AnyDesk, PsExec, or other remote utilities for lateral movement. Conti threat actors exfiltrate data using Rclone or other tools, and finally deploy and execute Conti ransomware to encrypt data as shown below in Figure 7.

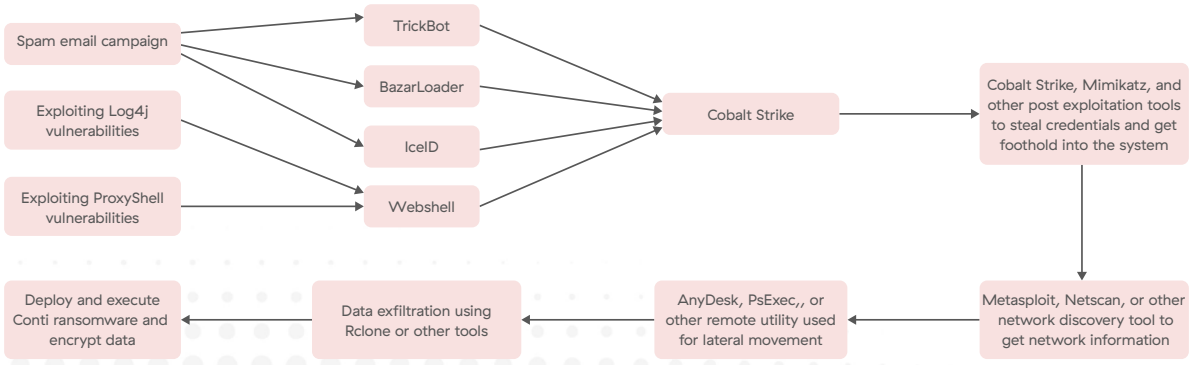


Figure 7: Anatomy of a Conti ransomware attack

The first version of Conti used RSA and AES algorithms in the encryption process. However, AES was later replaced with ChaCha encryption.

In late January 2022, ThreatLabz identified an updated version of Conti ransomware as part of our global ransomware tracking efforts. This update was released prior to a massive leak of Conti source code and chat logs on February 27, 2022, which was published by a Ukrainian researcher after the invasion of Ukraine. The new version of Conti added new command line arguments that allow Conti to reboot the system in Windows Safe Mode with networking enabled, and then start encryption. By booting in Safe Mode, Conti can maximize the number of files that are encrypted, because business applications such as databases are likely not running. Conti also updated the encrypted file extensions to include uppercase and lowercase characters and numbers. It also sets the victim's desktop wallpaper after file encryption.

Figure 8 displays the industry verticals targeted by double extortion attacks using Conti.

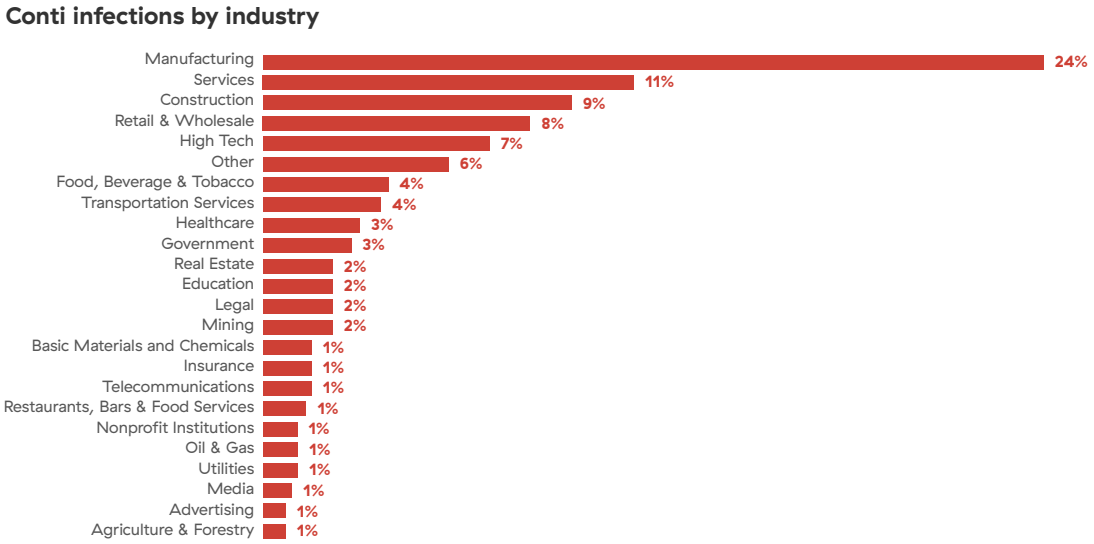


Figure 8: Conti infections by industry

Conti created its own data leak site in August 2020. If a ransom demand is not paid by an organization, Conti will publish its stolen data.

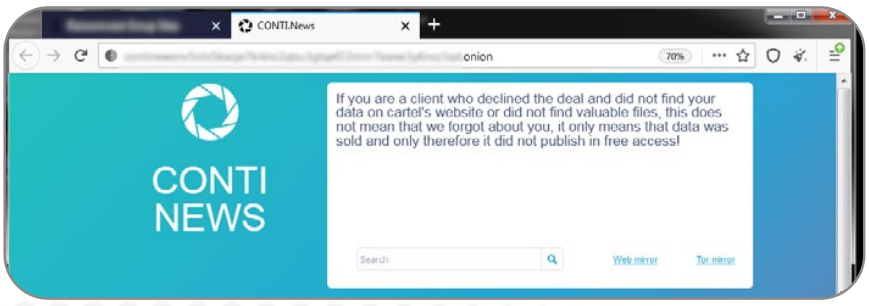


Figure 9: Conti data leak site

Conti: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Spear phishing link	Command-line interface	Boot or logon autostart execution	Access token manipulation	Deobfuscate/ Decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Automated exfiltration	Data encrypted for impact
Spear phishing attachment	Execution through module load		Exploitation for privilege escalation	Impair defenses	Remote system discovery	Remote services	Data from local system	Exfiltration over web service	Inhibit system recovery
Exploit public-facing application	Shared modules			Process injection	File and directory discovery				System shutdown/ reboot
Valid accounts	User execution				Security software discovery				Defacement
Supply chain compromise					Query registry				

LockBit

LockBit ransomware first emerged in September 2019 as ABCD ransomware, named after its extension ".abcd". A new version emerged at the start of 2020 that appends the extension ".lockbit" to encrypted files. In 2020, LockBit joined the Maze cartel and began publishing victims' data on Maze's data leak site. In September 2020 when Maze shut down their operations, LockBit started their own data leak site as shown in figure 10.

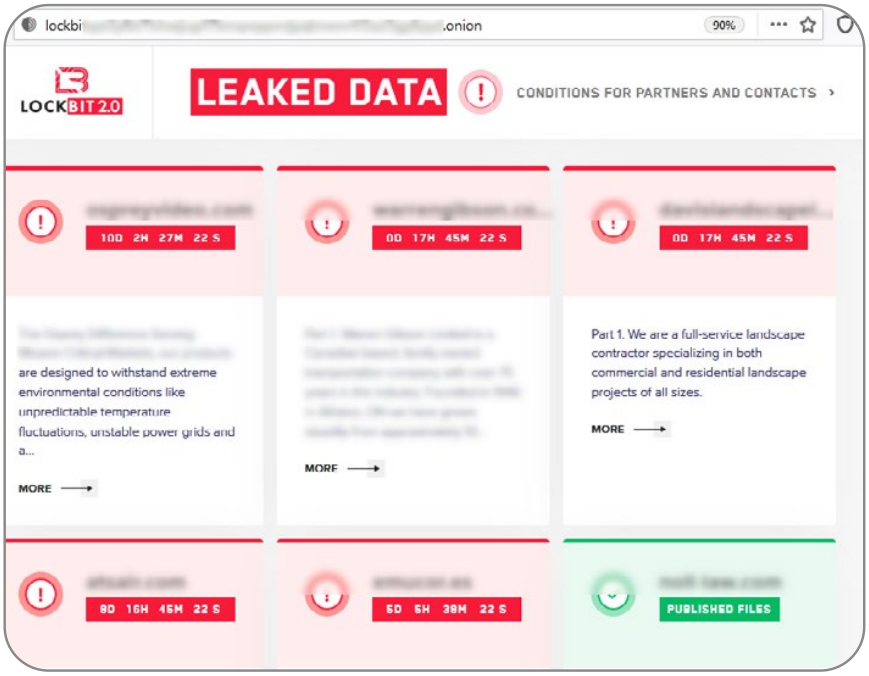


Figure 10: LockBit data leak site

In June 2021, LockBit released a new version called LockBit 2.0. In July 2021, LockBit 2.0 started publishing victim companies' data on their data leak site. It uses the RaaS model. LockBit has solicited affiliates who were employed by their target organizations and had legitimate network access. LockBit has been distributed through spam email campaigns that contain malicious attachments or links.

LockBit has also been seen to gain access by brute forcing RDP or VPN credentials, via compromised RDP accounts, and exploiting Fortinet VPN's CVE-2018-13379 vulnerability.

Infection chain:
In the first observed LockBit 2.0 attack, the attacker used a hacked RDP account to access the targeted system. They then used a network scanner to recover network information and locate domain controllers. The threat actor used StealBit to exfiltrate the data, Process Hacker and PC Hunter to terminate processes and services related to the database, and other tools. A batch file was used to uninstall security products and disable Windows event logs and Windows Defender features. Finally, LockBit used Windows group policies to distribute and execute the LockBit 2.0 ransomware.

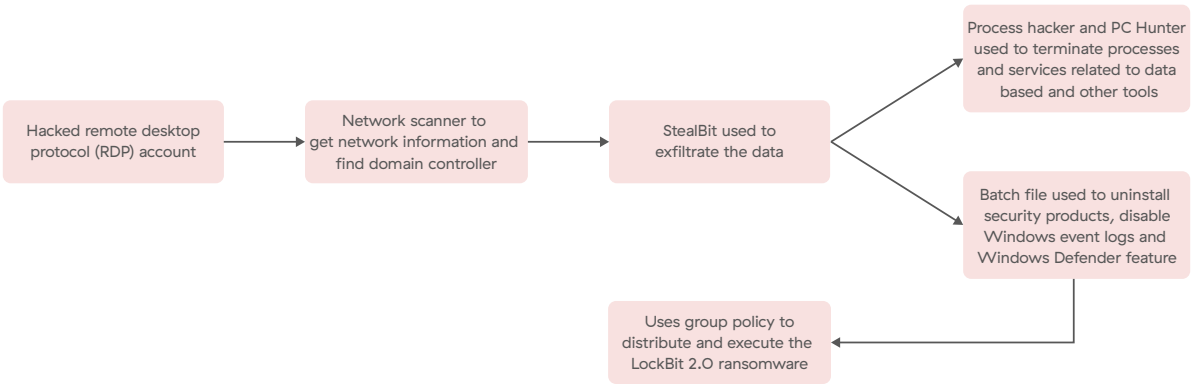


Figure 11: Anatomy of a LockBit ransomware attack

Part of what makes LockBit so popular is its efficiency: LockBit has the fastest encryption method as it uses a multi-threaded encryption approach and encrypts only 4 KB of data for each file. It uses a combination of RSA and AES algorithms to encrypt files. LockBit released a Linux and VMware ESXi variant in October 2021. This uses a combination of Advanced Encryption Standard (AES) and elliptic-curve cryptography (ECC) algorithms for data encryption.

Figure 12 displays the industry verticals targeted by double extortion attacks using LockBit.

Lockbit infections by industry

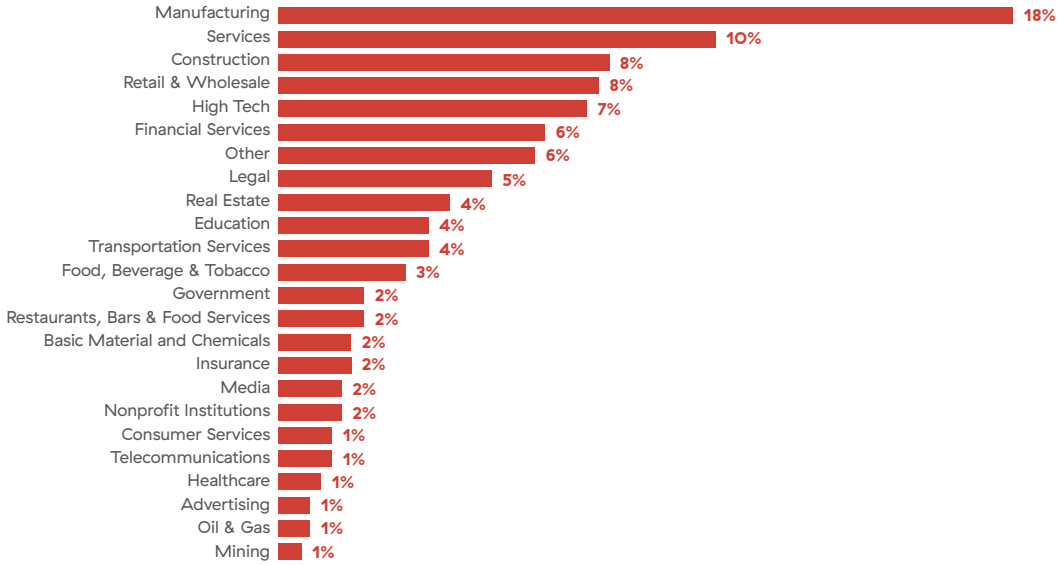


Figure 12: LockBit infections by industry

LockBit: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Spear phishing link	Command-line interface	Boot or logon autostart execution	Abuse elevation control mechanism: Bypass user account control	Deobfuscate/ Decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Exfiltration over web service	Data encrypted for impact
Spear phishing attachment				Impair defenses: disable or modify tools	Remote system discovery	Remote services	Data from local system		Inhibit system recovery
Valid accounts				Indicator removal on host: Clear windows event logs	File and directory discovery				Defacement
Exploit public-facing application				Domain policy modification: group policy modification	Security software discovery				
Supply chain compromise									

PYSA/Mespinoza

PYSA ransomware, also known as Mespinoza, was first spotted in October 2019. They attack a wide range of industries around the world, but are known in particular for attacks on “soft targets” such as education and hospitals.

Infection chain

PYSA achieves initial compromise through spam email or compromised RDP credentials. Next, the threat actors collect network information through scanning tools such as Port Scanner and the Advanced IP Scanner developed by Famatech Corp. The attackers use post exploitation tools like Mimikatz, PowerShell Empire, Koadic, and PsExec to steal credentials and move laterally. The WinSCP tool has been used to exfiltrate the data from victims’ systems. A PowerShell script disables security software and deletes shadow copies and system restore points, preventing victims from restoring their data. Finally, the attacker deploys and executes the PYSA ransomware and encrypts the victim’s data.

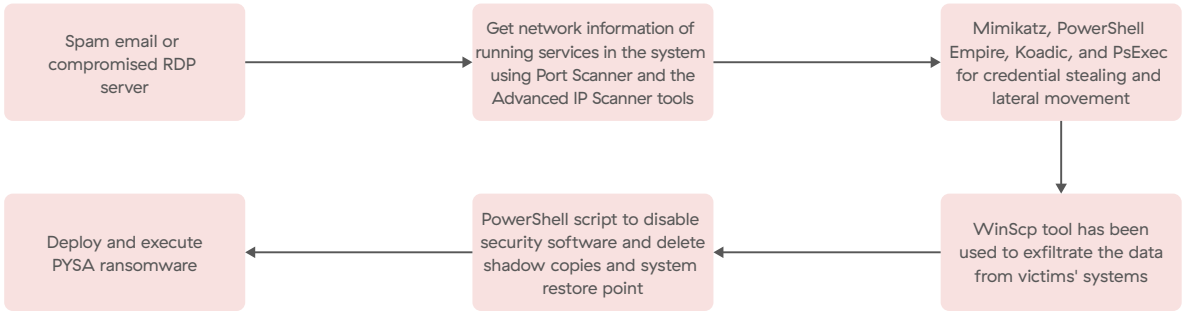


Figure 13: Anatomy of a PYSA ransomware attack

18% of PYSA attacks targeted educational institutions.

PYSA uses a combination of RSA and AES-CBC algorithms to encrypt files.

Figure 14 displays the industry verticals targeted by double extortion attacks using PYSA/Mespinoza.

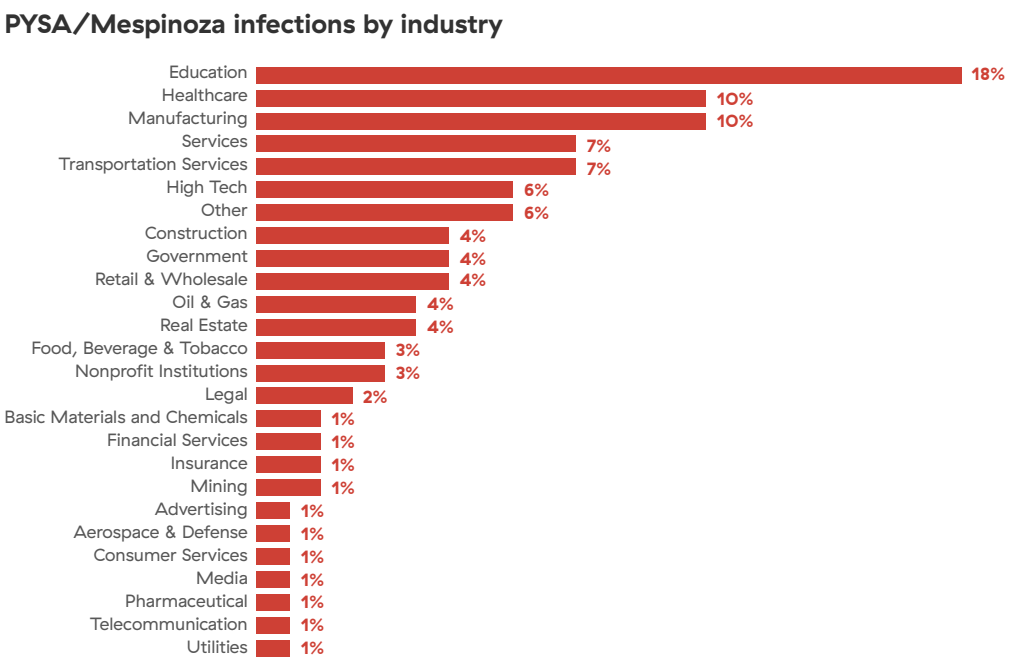


Figure 14: PYSA/Mespinoza attacks by industry

PYSA will publish stolen data on their leak site (shown in figure 15) if a victim does not pay a ransom.

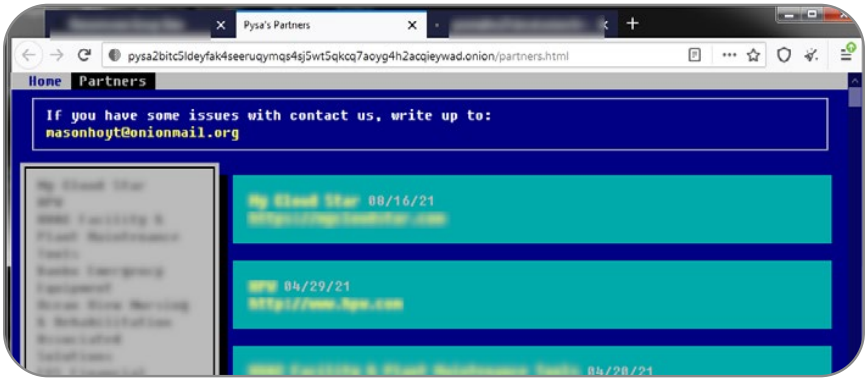


Figure 15: PYSA/Mespinoza data leak site

PYSA/Mespinoza: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Spear phishing link	Command–line interface	Boot or logon autostart execution	Access token manipulation	Deobfuscate/ Decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Exfiltration over alternative protocol	Data encrypted for impact
Spear phishing attachment	Execution through module load	Scheduled task/job		Impair defenses	Remote system discovery		Data from local system	Exfiltration over web service	Inhibit system recovery
Valid accounts	User execution			Domain policy modification: group policy modification	File and directory discovery				
					Security software discovery				
					Query registry				

REvil/Sodinokibi

REvil ransomware (a.k.a. Sodinokibi) was first spotted in April 2019 and has been one of the most active threat groups over the last several years. REvil also uses a RaaS ecosystem. REvil started double extortion in January 2020, first publishing data on a hacking forum. In February 2020, Sodinokibi attackers launched their own data leak site as shown in Figure 16.

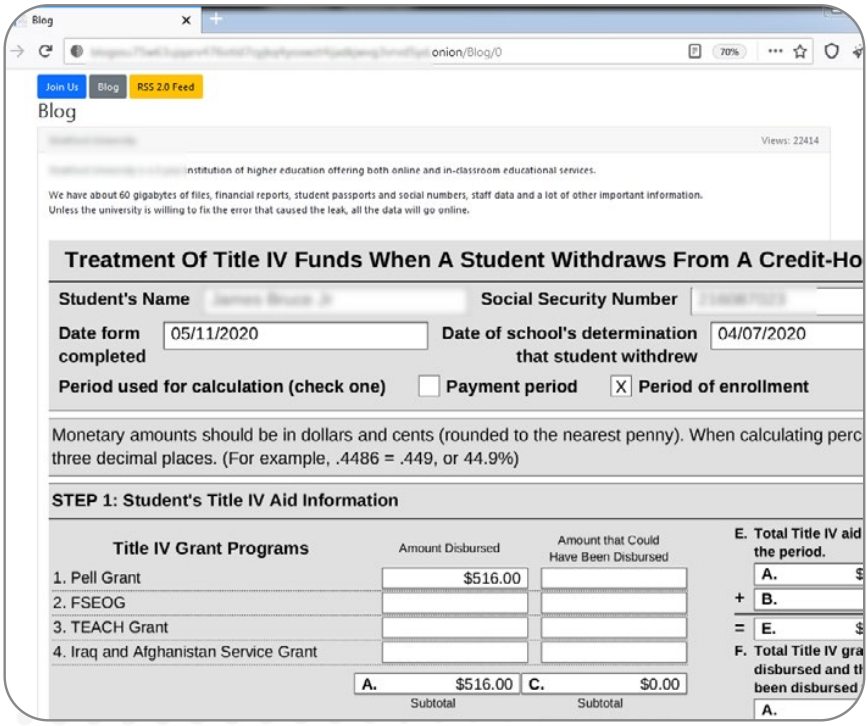


Figure 16: REvil/Sodinokibi data leak site

They also experimented with auctioning stolen data on their leak site until that proved unsuccessful.

The REvil threat group famously exploited a zero day vulnerability in the Kaseya VSA server in July 2021. The compromised Kaseya VSA server was used to send a malicious script to all clients that were managed by that VSA server.

As noted previously, members of REvil were apparently arrested by Russian law enforcement in January 2022. However, the ransomware was updated and the infrastructure came back online in April 2022, at which point REvil attacks resumed.

Infection chain

REvil affiliates have used a variety of initial access mechanisms, including spam emails, exploit kits, compromised RDP accounts, and vulnerability exploits. An example campaign starts with a spam email with a malicious attachment. Once opened, the malicious attachment downloads a trojan such as IcedID, which serves as a pivot point for lateral movement. As shown in figure 17, REvil affiliates use a variety of different tools like Cobalt Strike, SharpSploit, Mimikatz, and other post-exploitation tools to steal credentials. Further, affiliates collect network information using Netscan, BloodHound, AdFind, and other network discovery tools. The attackers move laterally using PsExec or RDP access. Data exfiltration has been performed using FileZilla, Rclone, MEGAsync, or FreeFileSync. Before deploying ransomware, REvil affiliates are known to use PC Hunter, Process Hacker, KillAV, and/or other scripts to terminate processes and services related to security software. Finally, the threat actor deploys the REvil ransomware and encrypts data.

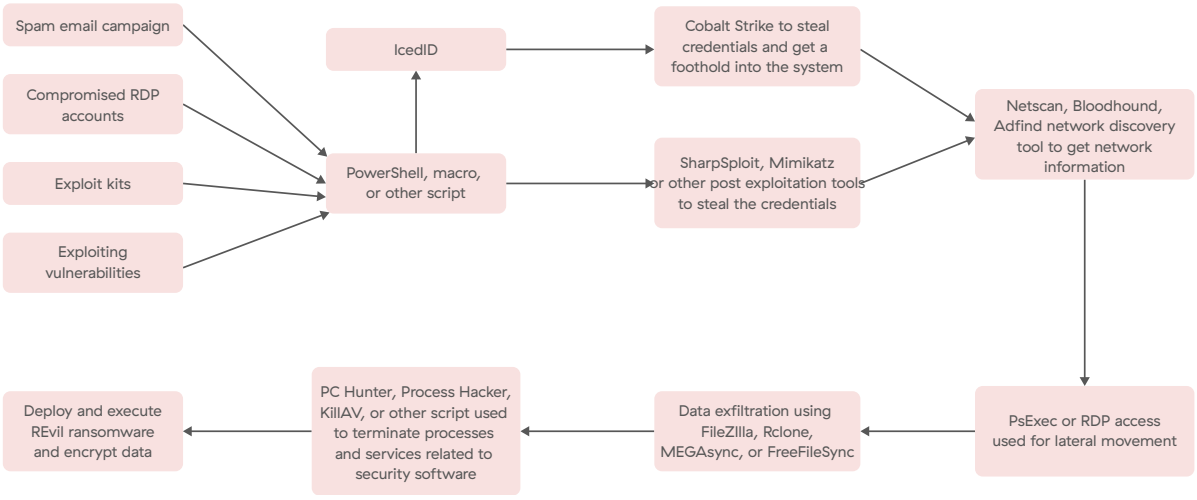


Figure 17: REvil/Sodinokibi attack chain

REvil uses asymmetric elliptic-curve cryptography, using Curve25519 in combination with Salsa20, to encrypt files.

Figure 18 displays the industry verticals targeted by double extortion attacks using REvil.

REvil/Sodinokibi infections by industry

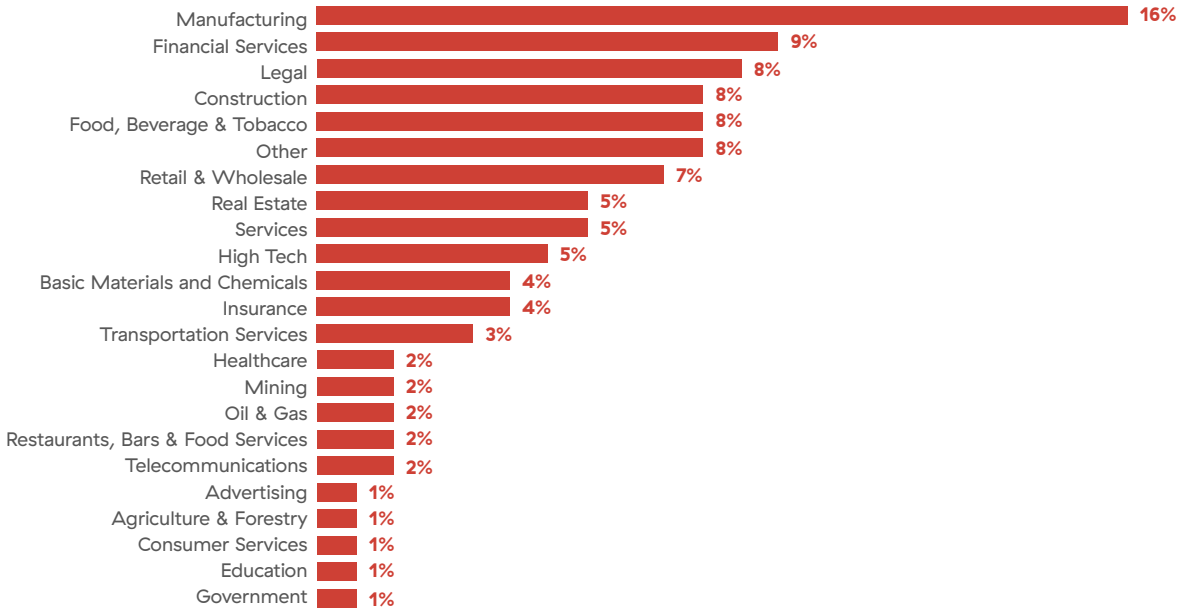


Figure 18: REvil/Sodinokibi infections by industry

REvil/Sodinokibi: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Spear phishing link	Command-line interface	Boot or logon autostart execution	Access token manipulation	Deobfuscate/ Decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Automated exfiltration	Data encrypted for impact
Spear phishing attachment	Execution through module load	Hijack execution flow	Hijack execution flow	Impair defenses	Remote system discovery	Remote services	Data from local system	Exfiltration over web service	Inhibit system recovery
Exploit public-facing application	Shared modules		Exploitation for privilege escalation		File and directory discovery				System shutdown/ reboot
Drive-by compromise	User execution				Security software discovery				Defacement
Valid accounts					Query registry				
Supply chain compromise									

Avaddon

Avaddon ransomware was first spotted in June 2020, and was very active at that time. Avaddon was yet another ransomware family that used the RaaS ecosystem. In January 2021, Avaddon added DDoS into its operation as a triple extortion tactic. Avaddon waged DDoS attacks on either the victim's website or network to encourage the victim to negotiate with its operators, forcing higher ransom amounts.

Infection chain

Avaddon gained access through different affiliates who utilized a range of vectors for the initial compromise. Avaddon was most widely distributed in spam campaigns and exploit kits, but some affiliates used brute force attacks or compromised RDP and VPN credentials to gain access to networks.

In an example attack chain, Avaddon gained access to an initial broker that was initially infected through compromised credentials and used custom malware, such as BlackCrow and DarkRaven web shells, to gain a foothold on the targeted system. Avaddon used SystemBC to get access to compromised hosts, then Mimikatz and SharpDump to steal credentials. The threat actor performed network scanning post-exploitation using SoftPerfect Network Scanner, PowerSploit, and Empire. For lateral movement, Avaddon affiliates used RDP, and Windows Scheduled Tasks for persistence. Before dropping the main ransomware payload, the threat actors exfiltrated data using MEGAsync and terminated processes and services related to security software. Finally, the threat actor dropped and executed the Avaddon payload and encrypted the targeted systems.

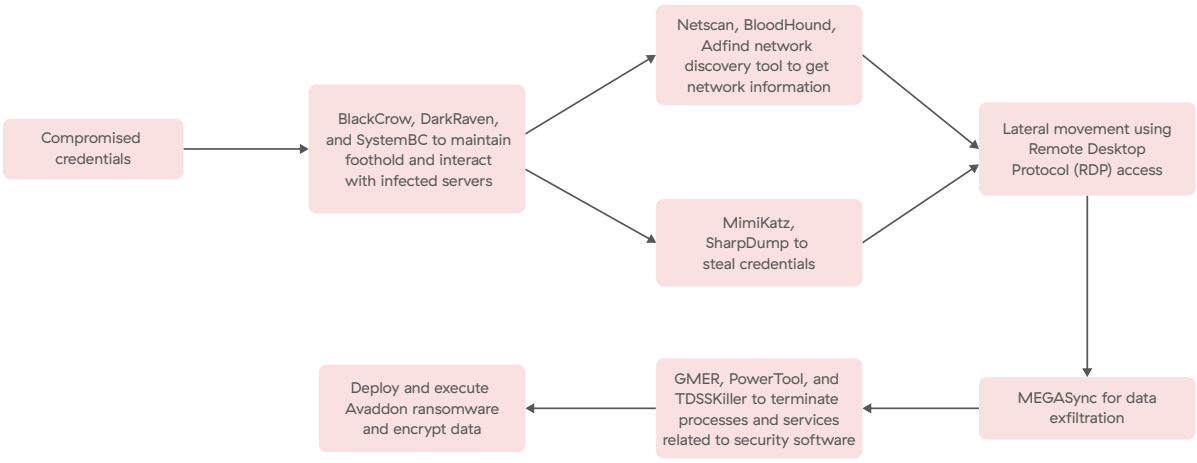


Figure 19. Anatomy of an Avaddon ransomware attack

Avaddon used a combination of RSA and AES algorithms to encrypt files. In February, a researcher released a free decrypter after discovering a flaw, which Avaddon then fixed. In June 2021, Avaddon shut down their operations and released victim's decryption keys, allowing Emsisoft to build a decrypter for Avaddon ransomware.

Similar to the other ransomware families discussed earlier, Avaddon followed the trend of creating data leak websites, launching its own in August 2020, as shown in figure 20.

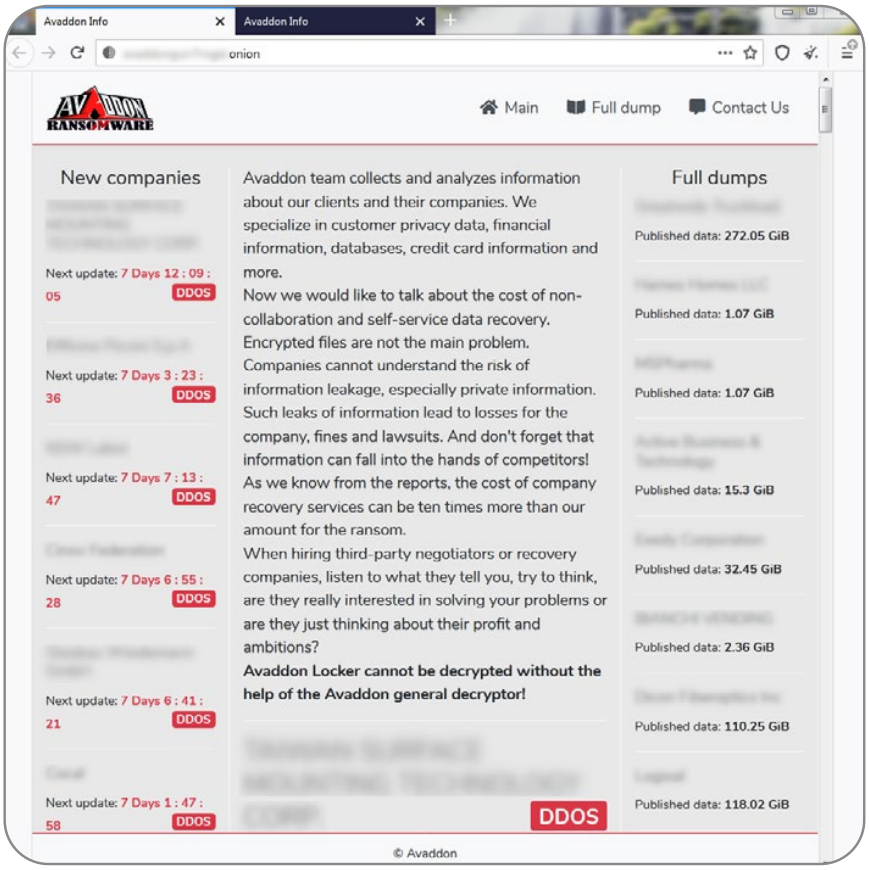


Figure 20: Avaddon data leak site

After Avaddon shut down in June 2021, the threat group relaunched attacks using the Thanos ransomware builder. The threat group rebranded Avaddon as Haron and, in October 2021, rebranded the ransomware again under the name Midas.

Figure 21 displays the industry verticals targeted by double extortion attacks using Avaddon.

Avaddon infections by industry

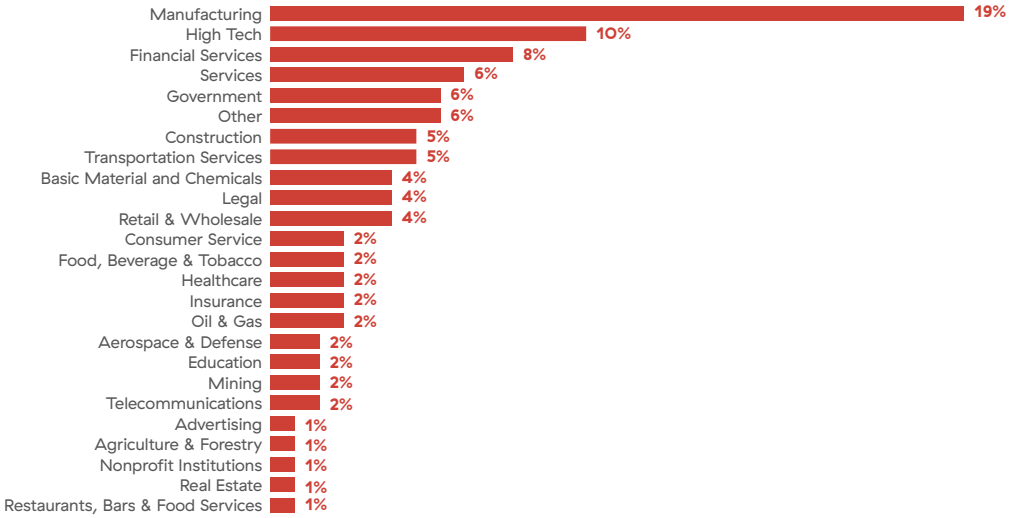


Figure 21: Avaddon infections by industry

Avaddon: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Collection	Exfiltration	Impact
Spear phishing link	Command-line interface	Boot or logon autostart execution	Valid accounts	Deobfuscate/ Decode files or information	System network configuration discovery	Lateral tool transfer	Archive collected data	Exfiltration over alternative protocol	Data encrypted for impact
Spear phishing attachment	Scheduled task/job	Valid accounts		Impair defenses	Remote system discovery	Remote services: remote desktop protocol	Data from local system		Inhibit system recovery
Exploit public-facing application	User execution			Process injection	File and directory discovery				
Drive-by compromise				Indicator removal on host	Security software discovery				
Valid accounts				Indicator removal on host	Security software discovery				

Clop

Clop ransomware was first spotted in February 2019. In March 2020, Clop started using double extortion, leaking stolen data of compromised organizations that did not pay ransoms to their data leak sites, as shown in figure 22.

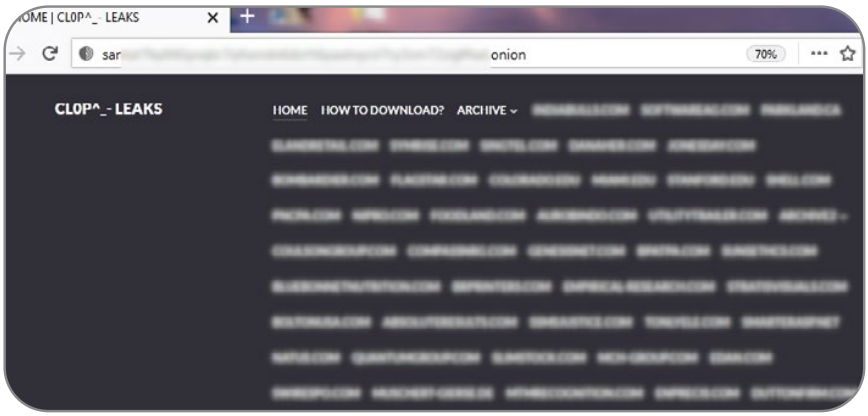


Figure 22: Clop data leak site

The Clop group focuses effort mostly on large organizations. ThreatLabz has observed the Clop ransomware group demand eight-figure ransom demands and even turn down multimillion-dollar ransom payment offers.

Clop ransomware was initially deployed by the TA505 and FIN11 threat groups. Clop has been widely distributed in spam campaigns carried out by threat actor TA505. ThreatLabz has observed several Clop attacks exploiting the SolarWinds Serv-U CVE-2021-35211 vulnerability, which enables remote code execution with elevated privileges, for initial access. The FIN11 threat group has exploited multiple vulnerabilities in the Accellion File Transfer Appliance (FTA) tracked as CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104. FIN11 then drops the DEWMODE web shell, which exfiltrates data before dropping and executing Clop ransomware.

Clop wages high-profile attacks, causing an estimated $500M in damage as of November 2021.

Infection chain

An example attack by TA505 achieved compromise through a spam email containing an HTML attachment. The attachment redirected to an XLS document file that further dropped the Get2 loader. The loader downloaded further payloads like SdBot, FlawedAmmy, FlawedGrace, and Cobalt Strike. After getting a foothold in the network and stealing and exfiltrating data, the threat group deployed and executed Clop ransomware, as illustrated in figure 23.

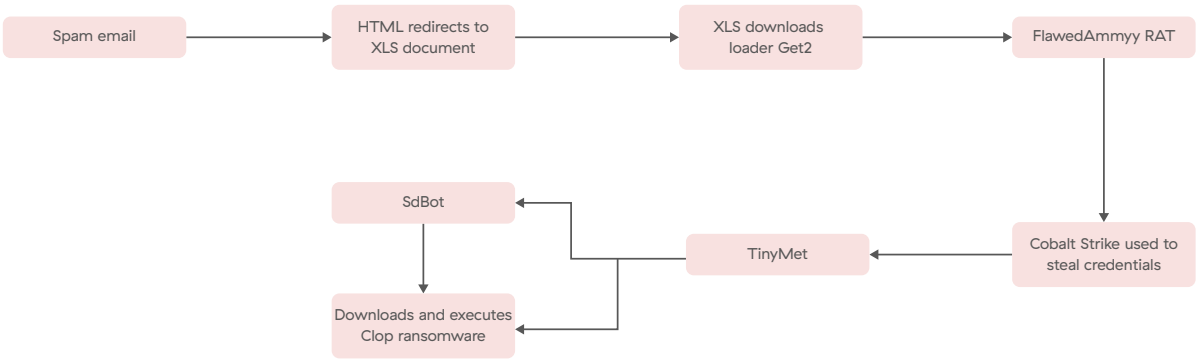


Figure 23: Anatomy of a Clop ransomware attack

Clop uses a combination of RSA and AES algorithms to encrypt files.

Figure 24 displays the industry verticals targeted by double extortion attacks using Clop.

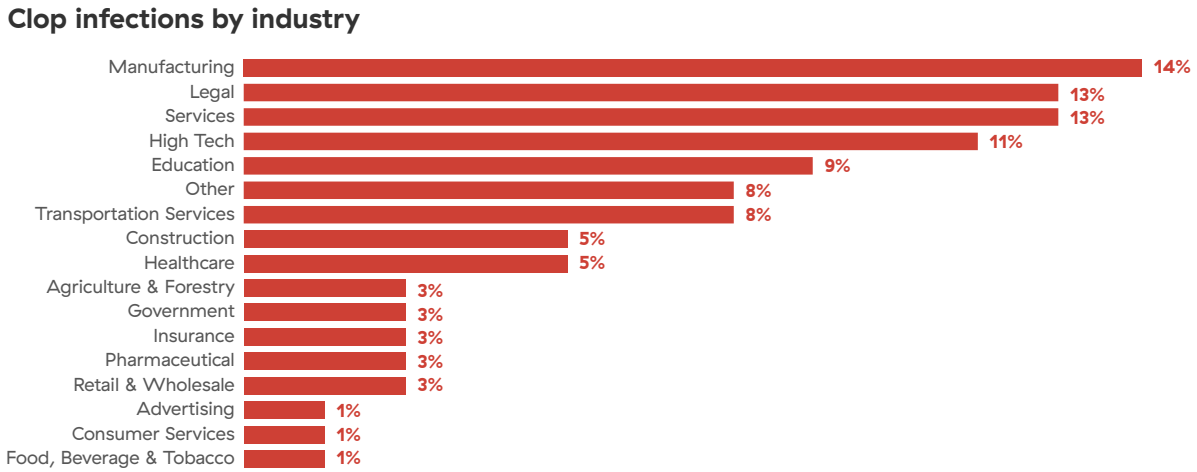


Figure 24: Clop infections by industry

Clop: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
Valid accounts	Command-line interface	Boot or logon autostart execution	Access token manipulation	Masquerading: invalid code signature	System network configuration discovery	Lateral tool transfer	Automated exfiltration	Data encrypted for impact
Spear phishing attachment	User execution	Create or modify system process: Windows service	Bypass user account control	Impair defenses: disable or modify tools	Remote system discovery	Remote services	Exfiltration over web service	Inhibit system recovery
Exploit public-facing application	Native API		Exploitation for privilege escalation	Deobfuscate/ Decode files or information	File and directory discovery			
Supply chain compromise				Process injection: DLL injection	Query registry			
				Indirect command execution	Security software discovery			

Grief

Grief ransomware is a rebranding of DoppelPaymer, whose activity dropped significantly in May 2021 following the Colonial Pipeline attack. Grief ransomware has lots of similarities with DoppelPaymer, including shared ransomware code and data leak websites. An example screenshot of the Grief leak site is shown in figure 25.

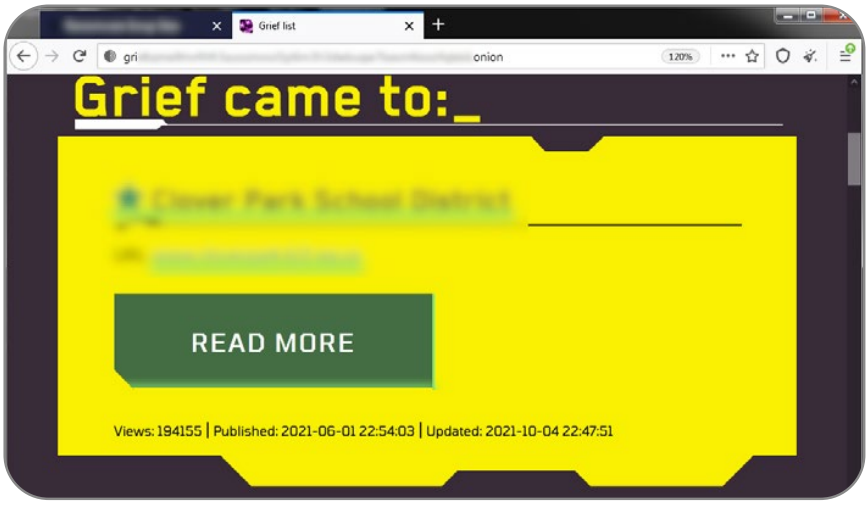


Figure 25: Grief data leak site

The Grief ransom portal has some differences from the DoppelPaymer portal. In particular, the ransom demand payment method is made in Monero instead of bitcoin. This switch in cryptocurrencies may be in response to the FBI recovering part of the Colonial Pipeline ransom payment, which was made in bitcoin.

Infection chain

Grief ransomware has been deployed on systems that were previously infected with Dridex, which the attacker uses before using Cobalt Strike and deploying and executing the Grief ransomware payload. Grief uses a combination of 2048-bit RSA and 256-bit AES algorithms to encrypt files.

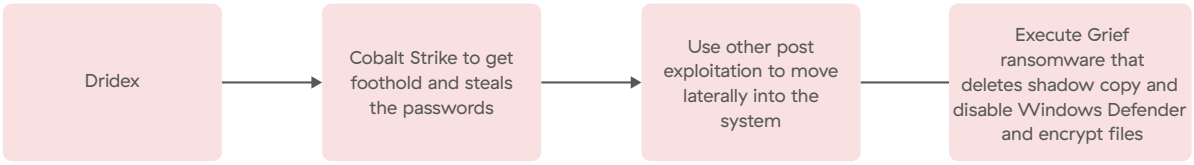


Figure 26: Anatomy of a Grief ransomware attack

Figure 27 displays the industry verticals targeted by double extortion attacks using Grief.

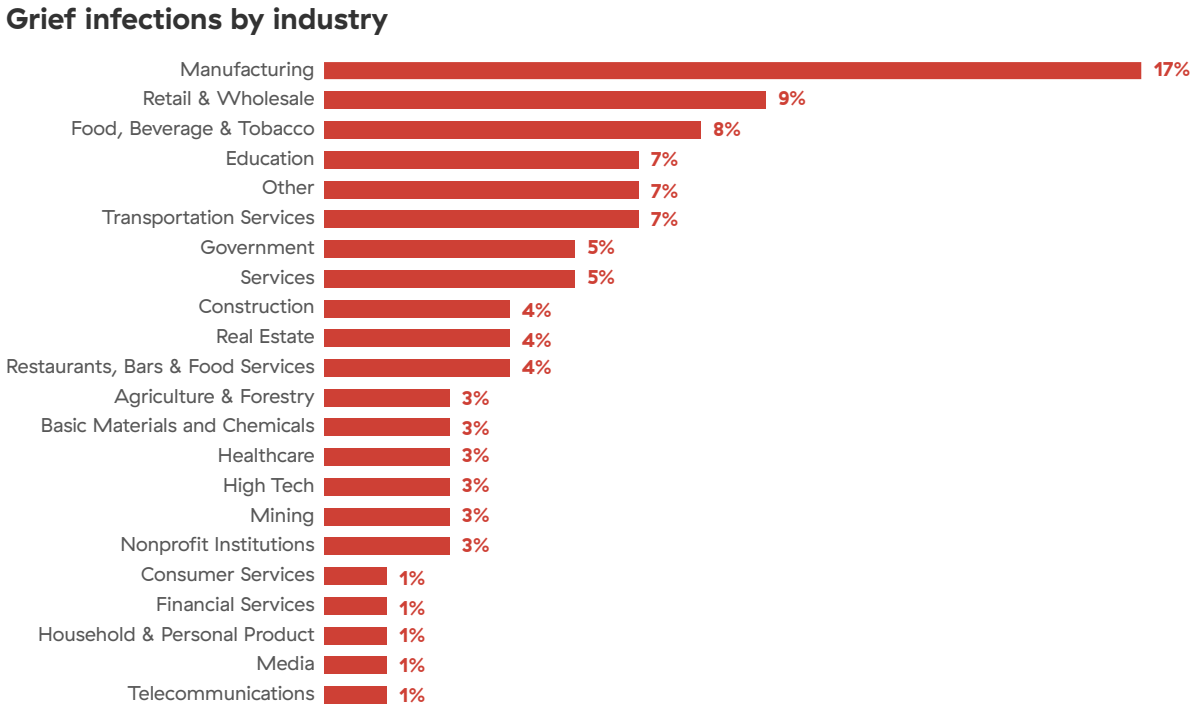


Figure 27: Grief infections by industry

Grief: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
Valid accounts	Command-line interface	Boot or logon autostart execution: registry run keys / startup folder	Process injection	Hijack execution flow: DLL search order hijacking	System network configuration discovery	Lateral tool transfer	Scheduled transfer	Data encrypted for impact
Spear phishing attachment	User execution	Scheduled task/job		Deobfuscate/Decode files or information	Remote system discovery			Inhibit system recovery
	Shared modules			Impair defenses: disable or modify tools	File and directory discovery			System shutdown/reboot
				Masquerading: match legitimate name or location	Security software discovery			

Hive

Hive ransomware was first spotted in June 2021, using a RaaS model. It uses multiple mechanisms to achieve initial access, including malicious spam emails, leaked VPN credentials, and vulnerability exploits in external-facing assets. The initial infection starts with exploiting the ProxyShell vulnerabilities present in Microsoft Exchange Server. ProxyShell exchange vulnerabilities are a combination of CVE-2021-34473 (Microsoft Exchange Server remote code execution vulnerability), CVE-2021-34523 (Microsoft Exchange Server elevation of privilege vulnerability), and CVE-2021-31207 (Microsoft Exchange Server security feature bypass vulnerability) vulnerabilities.

Infection chain

The attacker creates a draft email item within a mailbox, with an attachment that contains the encoded web shell. Then, the attacker exports the entire mailbox (malicious draft email included) to PST file format with an ASPX extension. This allows attackers to drop web shells on vulnerable servers. The web shell downloads the PowerShell script that contains the encoded Cobalt Strike payload. It further downloads additional stagers and establishes a foothold in the victim's system. It then uses Mimikatz to steal NTLM hashes and leverages a pass-the-hash tactic to access the domain control account. Hive performs further lateral movement over RDP using stolen credentials. It scans the network and gets additional information using the SoftPerfect Network scanner. At the end, it deploys and executes the Hive ransomware and encrypts the data.

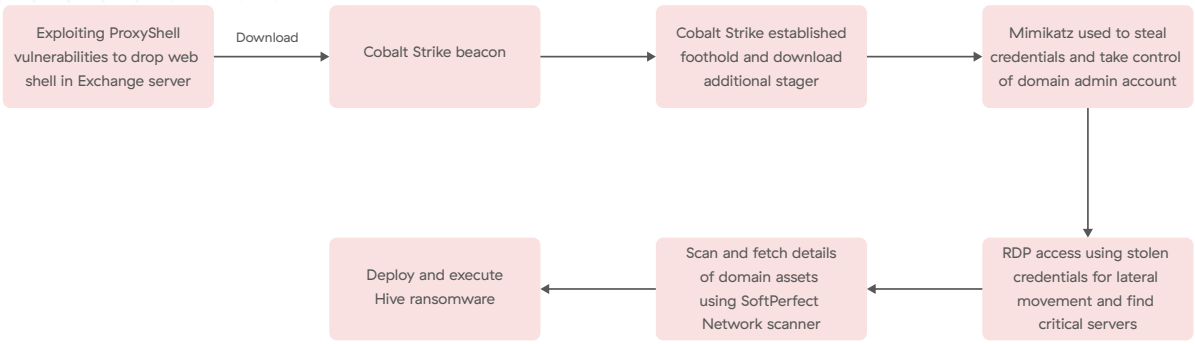


Figure 28: Hive attack chain

Earlier versions of Hive ransomware payload were written in the Go programming language and used a combination of RSA and AES algorithms to encrypt files. More recent versions of Hive are written in the Rust programming language and use Curve25519 and ChaCha20 for file encryption.

Hive affiliates also exfiltrate data from victims prior to file encryption. A screenshot of the Hive data leak site is shown in figure 29.

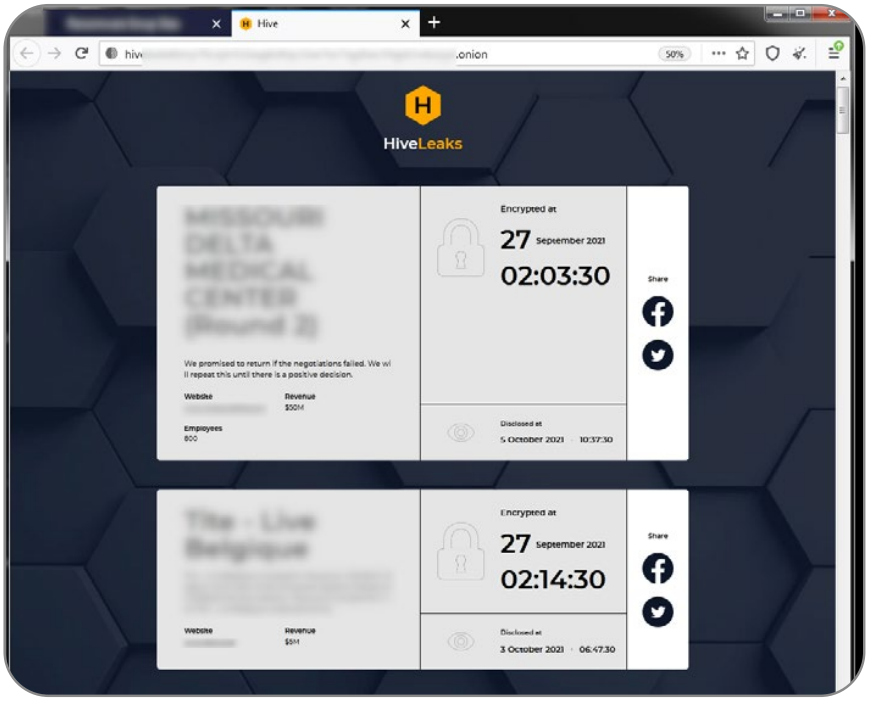


Figure 29: Hive data leak site

Figure 30 displays the industry verticals targeted by double extortion attacks using Hive.

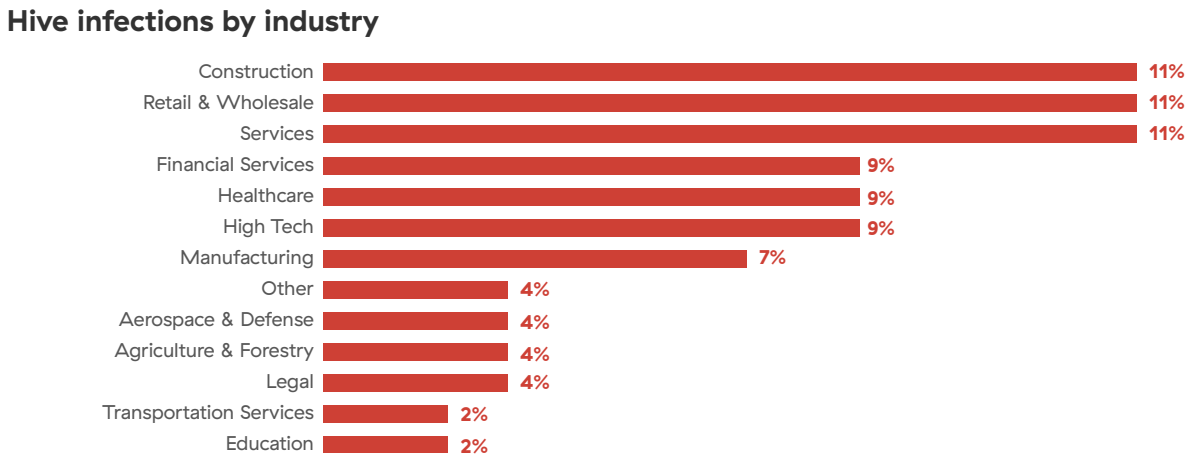


Figure 30: Hive infections by industry

Hive: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
External Remote services	Command-line interface	Valid accounts: Domain accounts	Valid accounts	Clear windows event logs	System network configuration discovery	Remote desktop protocol	Scheduled transfer	Data encrypted for impact
Spear phishing attachment	User execution	Create account: domain account	Domain accounts	Impair defenses: disable or modify tools	Remote system discovery	Remote services		Inhibit system recovery
Exploit public-facing application			Exploitation for privilege escalation	Deobfuscate/ Decode files or information	File and directory discovery			
					Query registry			
					Security software discovery			

BlackByte

BlackByte is another RaaS group that appeared prominently in July 2021. It was originally written in C# and later redeveloped in the Go programming language around September 2021. The Go-based version shares many similarities with the C# version, including the commands executed to perform lateral propagation, privilege escalation, and file encryption.

BlackByte campaigns start with exploiting the ProxyShell vulnerabilities present in Microsoft Exchange Server.

Infection chain

The attacker creates a draft email item within a mailbox. The email has an attachment that contains the encoded web shell. Then, the attacker exports the entire mailbox (malicious draft email included) to PST file format with an ASPX extension. This allows attackers to drop web shells on vulnerable servers.

Next, the web shell is used to drop a Cobalt Strike beacon on the targeted Exchange server. Cobalt Strike and other post-exploitation tools are used to steal credentials and gain access to service accounts to get a foothold into the system. Furthermore, BlackByte installs the AnyDesk RDP tool. AnyDesk is used for lateral movement and to drop Cobalt Strike in the infected domain controller. Finally, Cobalt Strike deploys and executes the BlackByte ransomware.

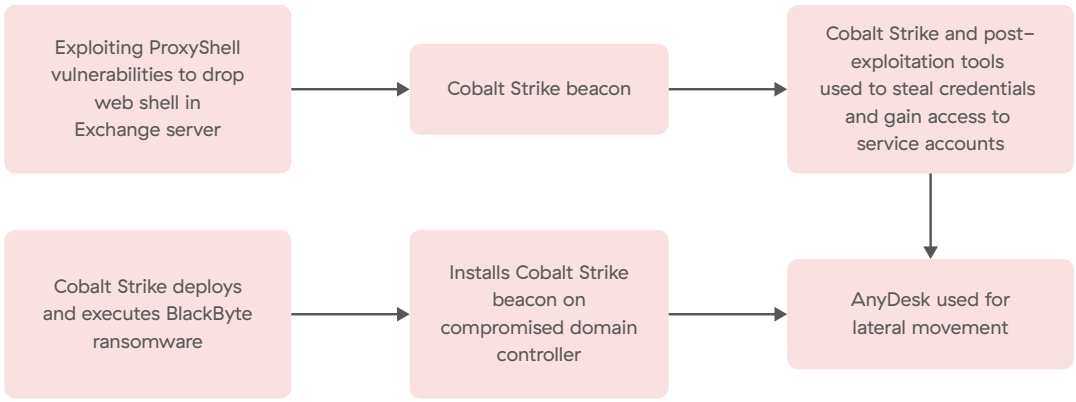


Figure 31: Anatomy of a BlackByte ransomware attack

Initial access by exploiting ProxyShell vulnerabilities to drop a web shell on the Exchange server. The web shell downloads the Cobalt Strike beacon. Cobalt Strike then steals credentials and installs the AnyDesk RDP tool. AnyDesk is used for lateral movement and drops Cobalt Strike in the infected domain controller. Cobalt Strike is then used to deploy and execute the BlackByte ransomware.

BlackByte uses a combination of RSA and AES algorithms to encrypt files. The most recent BlackByte versions use Curve25519 ECC for asymmetric encryption and ChaCha20 for symmetric file encryption.

The BlackByte threat actors also exfiltrate data from victims prior to file encryption. A screenshot of the BlackByte data leak site is shown in figure 32.

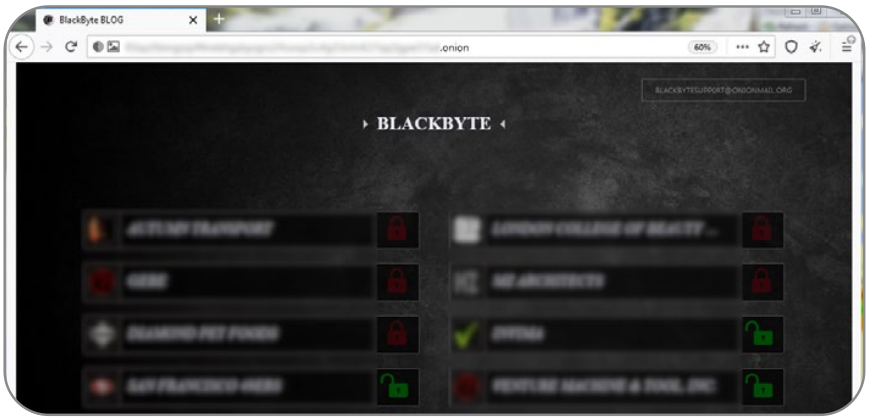


Figure 32: BlackByte data leak site

Figure 33 displays the industry verticals targeted by double extortion attacks using BlackByte.

BlackByte infections by industry

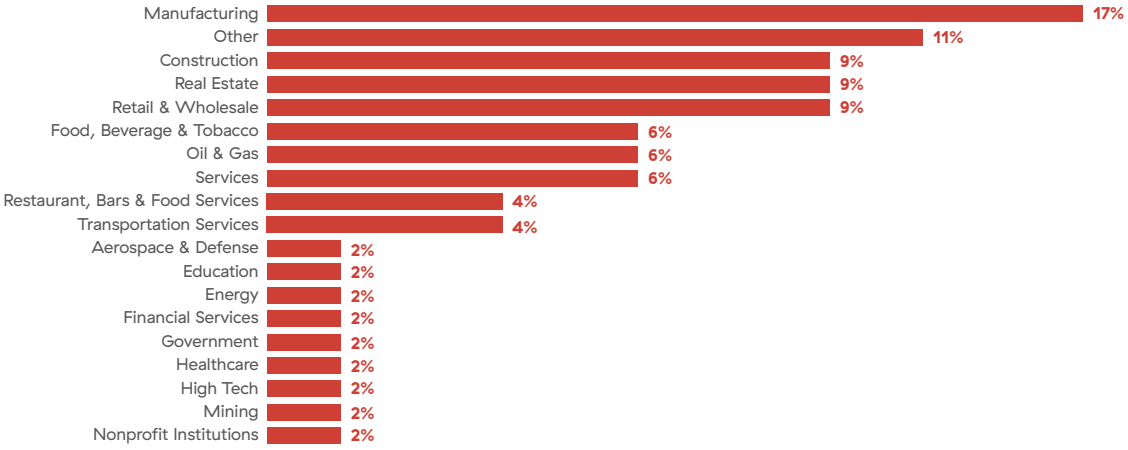


Figure 33: BlackBye infections by industry

BlackByte: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
Spear phishing attachment	Command and scripting interpreter	Create or modify system process: windows service	Domain accounts	Impair defenses: disable or modify tools	System network configuration discovery	Lateral tool transfer	Scheduled transfer	Data encrypted for impact
Exploit public-facing application	Native API		Exploitation for privilege escalation	Deobfuscate/ Decode files or information	Remote system discovery			Inhibit system recovery
	User execution			Modify registry	File and directory discovery			
					Query registry			
					Security software discovery			

AvosLocker

AvosLocker ransomware is a RaaS group that appeared prominently in July 2021. Like Hive and BlackByte, the initial infection starts with exploiting ProxyShell vulnerabilities CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207 present in the Microsoft Exchange server.

Infection chain

The attacker creates a draft email item within a mailbox. The email has an attachment that contains the encoded web shell. Then, the attacker exports the entire mailbox (malicious draft email included) to PST file format with an ASPX extension. This allows attackers to drop web shells on vulnerable servers.

Next, the web shells are used to drop Cobalt Strike on the infected exchange server. Cobalt Strike and Rclone are used to steal credentials and exfiltrate data to remote servers.

The attack installs AnyDesk RDP to access multiple systems, moving laterally. It drops several batch scripts to modify and delete registry keys related to security software. It also disables Windows Update and Windows Defender.

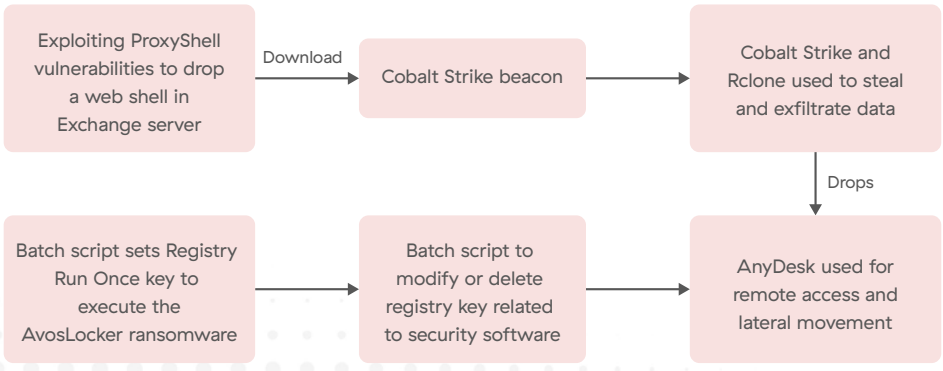


Figure 34: Anatomy of an AvosLocker ransomware attack

At the end, AvosLocker reboots the system in Windows Safe Mode, and then the ransomware starts file encryption. By booting in Safe Mode, AvosLocker can maximize the number of files that are encrypted, because business applications such as databases are likely not running. Therefore, those applications will not have open file handles that could prevent file encryption. In addition, many security software applications (e.g., antivirus programs) will not be loaded by default when the system is running in Safe Mode. The ability to encrypt files in Windows Safe Mode is a feature that has been observed in other ransomware families including Conti, REvil, and BlackMatter.

AvosLocker uses a combination of RSA and AES algorithms to encrypt files. AvosLocker created a Linux version of their ransomware that targets VMware ESXi.

After the attack, the attacker threatens to publish the victim's data to a data leak site and, in some cases, threatens and executes a DDoS attack on the victim network during negotiation. A screenshot of the AvosLocker data leak site is shown in figure 35.

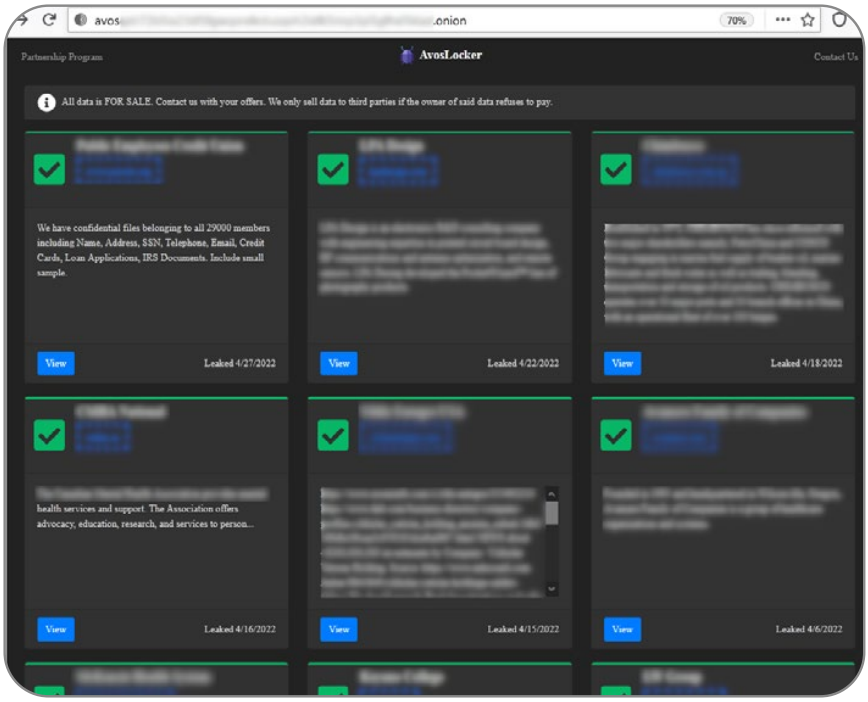


Figure 35: AvosLocker data leak site

Figure 36 displays the industry verticals targeted by double extortion attacks using AvosLocker.

AvosLocker infections by industry

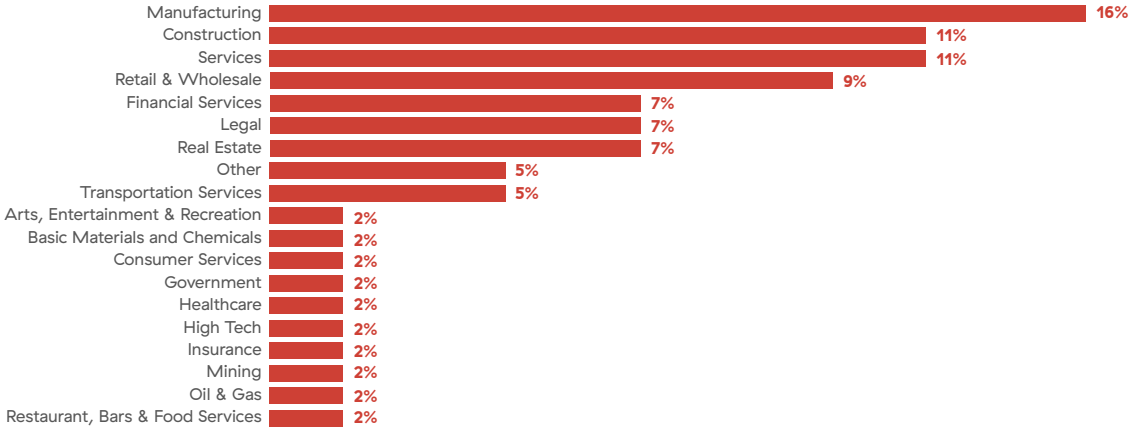


Figure 36: AvosLocker infections by industry

AvosLocker: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
Spear phishing attachment	Command-line interface	Boot or logon autostart execution: registry run keys / startup folder	Domain accounts	Impair defenses: disable or modify tools	System network configuration discovery	Lateral tool transfer	Scheduled transfer	Data encrypted for impact
Exploit public-facing application	User execution	Scheduled task/job	Exploitation for privilege escalation	Deobfuscate/Decode files or information	Remote system discovery			Inhibit system recovery
					File and directory discovery			System shut-down/reboot
					Security software discovery			

BlackCat/ALPHV

BlackCat, a.k.a. ALPHV, is a RaaS operation that was first spotted around November 2021. BlackCat has used the RUST programming language, which helps to improve performance and reliable concurrent processing.

Infection chain

Initial infection starts with the use of compromised credentials to gain access to victims' network systems. Initially it uses Cobalt Strike, PowerShell scripts, and batch script to get a foothold into the victim's network. Once it gets access, it compromises admin accounts in Active Directory. Further, it uses malicious Group Policy Objects (GPOs) to deliver and execute ransomware. It also uses Microsoft Sysinternals and other administrative tools in the attack.

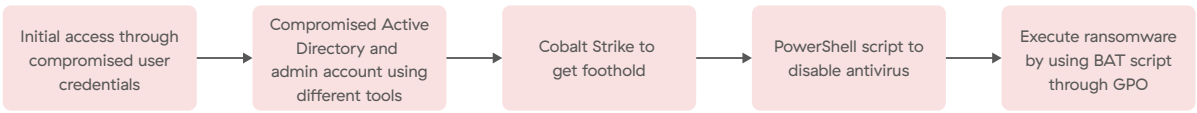


Figure 37: Anatomy of a BlackCat/ALPHV ransomware attack

BlackCat added DDoS tactics into its operation. BlackCat wages DDoS attacks on either the victim's website or network to encourage the victim to negotiate with its operators and force higher ransom amounts. An example screenshot of the BlackCat data leak site is shown in figure 38.

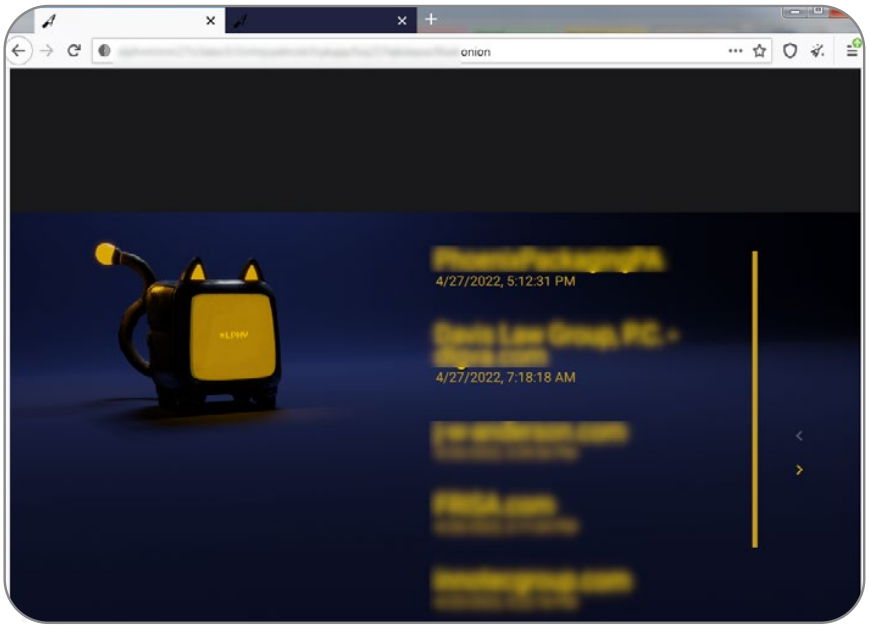


Figure 38: BlackCat/ALPHV data leak site

Figure 39 displays the industry verticals targeted by double extortion attacks using BlackCat/ALPHV.

BlackCat/ALPHV infections by industry

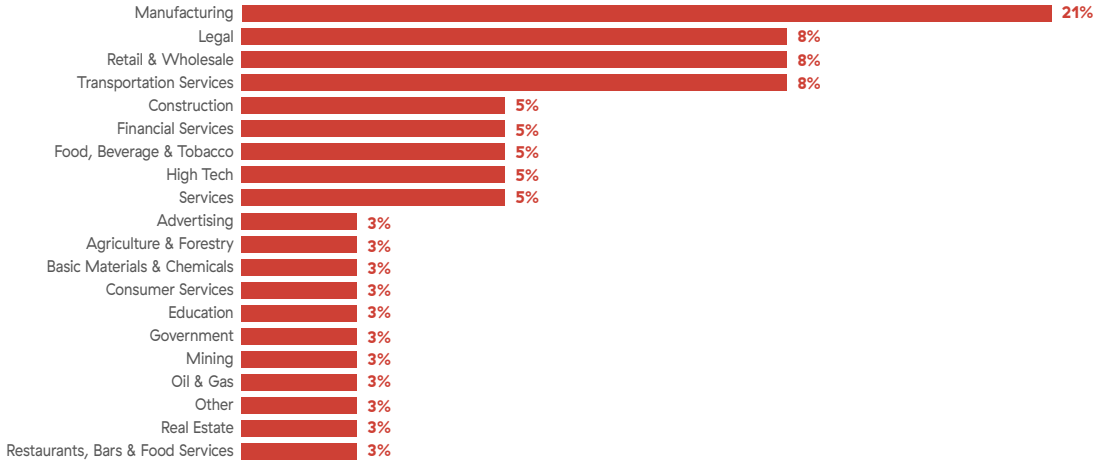


Figure 39: BlackCat/ALPHV infections by industry

BlackCat: MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltration	Impact
Valid accounts	Command and scripting interpreter	Boot or logon autostart execution: registry run keys / startup folder	Domain accounts	Impair defenses: disable or modify tools	System network configuration discovery	Lateral tool transfer	Scheduled transfer	Data encrypted for impact
	User execution	Scheduled task/ job	Exploitation for privilege escalation	Deobfuscate/ Decode files or information	Remote system discovery			Inhibit system recovery
				Domain policy modification: group policy modification	File and directory discovery			
					Security software discovery			

About ThreatLabz

ThreatLabz is the security research arm of Zscaler. This world-class team is responsible for hunting new threats and ensuring that the thousands of organizations using the global Zscaler platform are always protected. In addition to malware research and behavioral analysis, team members are involved in the research and development of new prototype modules for advanced threat protection on the Zscaler platform, and regularly conduct internal security audits to ensure that Zscaler products and infrastructure meet security compliance standards. ThreatLabz regularly publishes in-depth analyses of new and emerging threats on its portal, research.zscaler.com.

Stay updated on ThreatLabz research by subscribing to our Trust Issues newsletter today.

The Zscaler Zero Trust Exchange has been named by Gartner as a leading security service edge (SSE) platform, delivering ransomware protection across every stage of the attack chain to dramatically reduce your chance of being attacked and mitigate potential damages.

Zscaler natively integrates industry-leading capabilities to:

To learn more, visit our Zscaler Ransomware Protection page.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE–based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com