ThreatLabZ Ransomware Review: The Advent of Double Extortion

zscaler™

Table of contents

Introduction

For businesses around the world, 2020 was a year of change and disruption for reasons that go beyond the pandemic: ransomware was on the rise in a big way and underwent more change and innovation in 2020 than it had in a decade. Double extortion, third-party attacks, and DDoS techniques emerged, pushing ransomware even further up the list of cybersecurity concerns for organizations across industries.

Ransomware is one of the most frequent topics of conversation that we have with our customers—and for good reason. Ransomware was the third-most common and second-most damaging[1] type of malware attack in 2020, accounting for 27 percent of attacks[2] for a total of $1.4B in ransom demands and an average of $1.45M to remediate an incident. With cybercrime up 69 percent compared to 2019[3], the threat of a ransomware incident weighs heavily on the minds of security leaders, as each incident has the potential to cost millions of dollars in ransom payments, data loss, business disruptions, and reputational damage.

The Zscaler™ ThreatLabZ threat research team analyzes more than 150 billion platform transactions and 100 million blocked attacks every day to understand emerging threats and how to stop them. In 2020, ThreatLabZ observed a notable escalation of ransomware in terms of frequency and the sophistication and severity of incidents, resulting in higher—and more guaranteed—payouts from victims.

In this document, we'll walk through key ransomware trends that have emerged in the last year and will provide a detailed overview of some of the most prolific ransomware examples to illustrate prevailing attack tactics—helping you to understand what your organization must defend against.

[1] Source: "Global Risks Report 2020", World Economic Forum

[2] Source: https://www.gartner.com/smarterwithgartner/6-ways-to-defend-against-a-ransomware-attack/

[3] Source: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

The anatomy of a ransomware attack

Ransomware is a type of malware actively used by cybercriminals 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 proportionate to the number of systems infected and the value of the data that threat actors are able to encrypt. Essentially, the higher the stakes, the higher the payment.

In late 2019, attackers evolved their ransomware tactics to include data exfiltration. In the event the victim didn’t want to pay the ransom to decrypt the data and instead tried to restore the data from a backup, the attackers would then threaten to leak the stolen data. In late 2020, some attackers also began to use DDoS attacks to bombard the victim’s website or network, creating even more business disruption, thus pressuring the victim to negotiate. We expect this trend to escalate in the coming years.

Double-extortion ransomware attack sequence

Attackers use a variety of intrusion vectors to gain access to systems, including phishing emails, exploits of vulnerabilities in remote or virtual private network (VPN) tools, and using brute-force or stolen credentials to access Remote Desktop Protocol (RDP) connections. Upon success, they proceed to gather victims' infrastructure information and move laterally across network systems, stealing sensitive data to use as a secondary extortion tactic so they can demand higher ransom payments. Next, they deploy and execute the ransomware, encrypting all the files in the network. Ransomware typically terminates processes related to security software and databases in order to maximize the number of files it is able to encrypt. Shadow copy backups are also usually deleted from the system to hinder file recovery.

Victims receive a file explaining that they’ve been hit by ransomware, with instructions for paying the ransom and decrypting their files. Victims have reduced leverage: even if they are able to recover the encrypted data from backups, they still must face the threat of the cybercriminals leaking the stolen data. If the victim does not negotiate, some hacking groups will wage a distributed denial of service (DDoS) on the victim’s network or website to gain additional leverage. The below chart displays the overall attack chain of a typical ransomware attack.

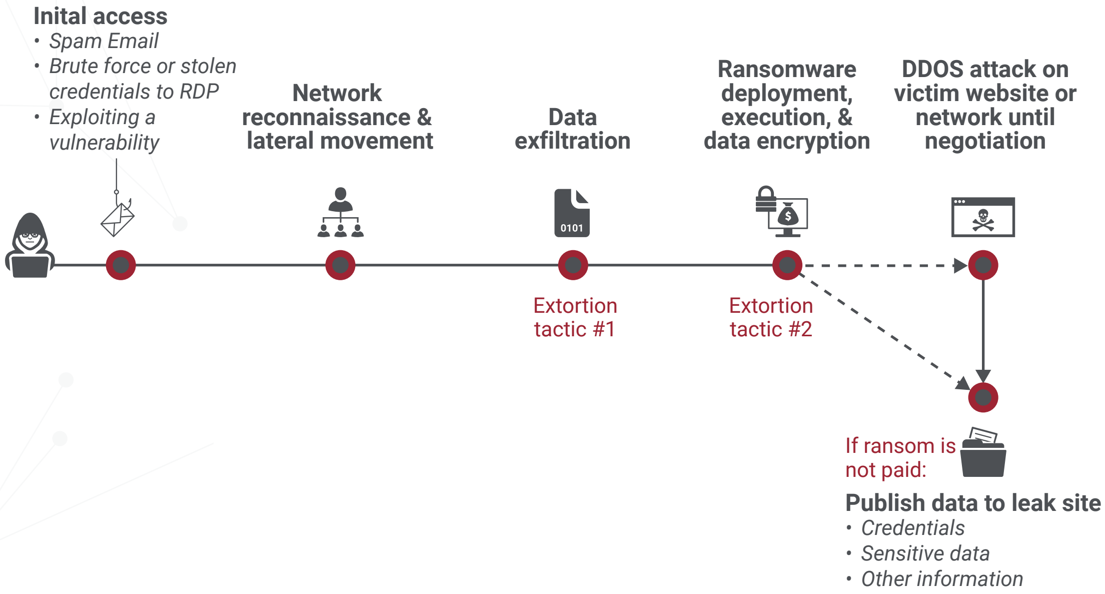

Inital access
• Spam Email
• Brute force or stolen credentials to RDP
• Exploiting a vulnerability
Network reconnaissance & lateral movement
Data exfiltration
0101
Ransomware deployment, execution, & data encryption
DDOS attack on victim website or network until negotiation
Extortion tactic #1
Extortion tactic #2
If ransom is not paid:
Publish data to leak site
• Credentials
• Sensitive data
• Other information

Fig. 1: Operation of a ransomware attack

The growth of double-extortion attacks

The high volume of transaction data on the Zscaler Zero Trust Exchange provides a unique lens into who is being targeted by cybercriminals. In the past two years, many different industries have been targeted by double-extortion ransomware attacks, with the top industry targets including manufacturing (12.7 percent of attacks), services (8.9 percent), transportation (8.8 percent), retail & wholesale (8.3 percent), and high-tech (8 percent). The below chart illustrates the percentage of ransomware involving double extortion waged on each industry vertical:

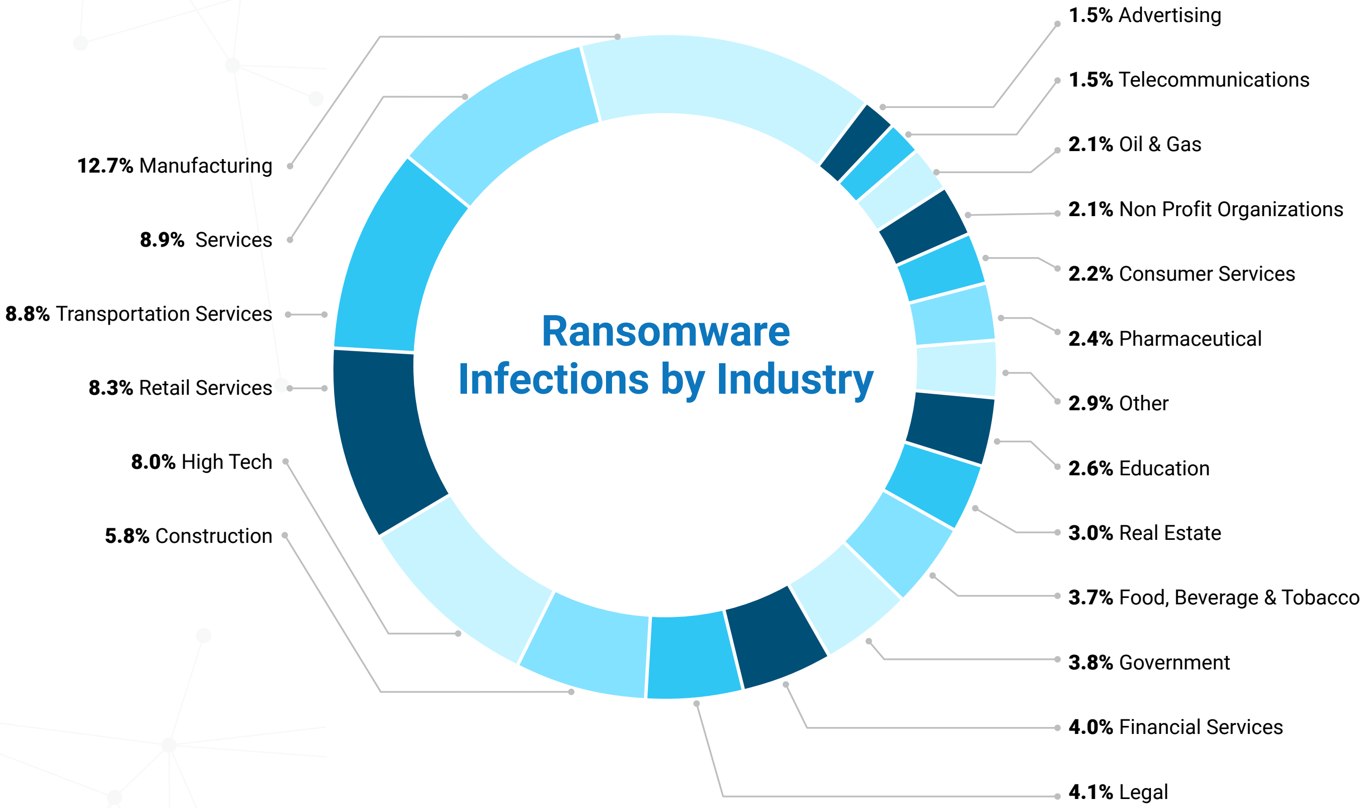


Fig. 2: Percentage of ransomware attacks involving double extortion observed between November 2019 and January 2021

There are many families of malware used in ransomware attacks, but some are more common than others. The specific ransomware family that affected the highest number of organizations between November 2019 and January 2021 was Maze (273 attacks), followed by Conti (190), Doppelpaymer (153), and Sodinokibi/REvil (125). The number of infected victims (derived from data leak websites) of 15 ransomware families is shown below.

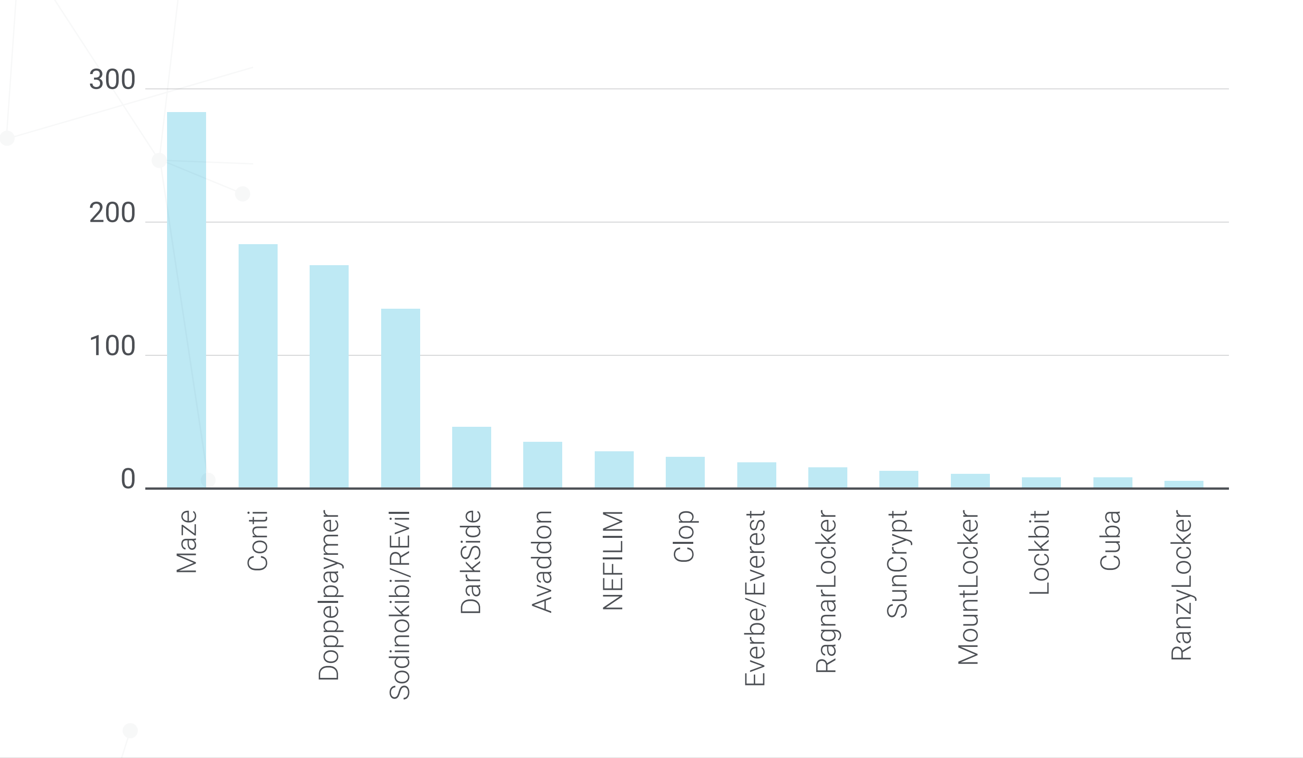


Fig. 3: Ransomware families that affected the highest number of organizations

The first ransomware to use double-extortion tactics was known as Robinhood[4]. This attacker published its victims' sensitive data on the attacker's Twitter account, which was later suspended. Double extortion was kickstarted as a trend after Maze ransomware threatened to publicly release data on hacking forums at the end of 2019. Other ransomware families quickly followed this trend by launching their own data leak sites and waging double-extortion attacks, as shown in the below chart.

[4] Source: https://www.darkreading.com/threat-intelligence/baltimore-ransomware-attacker-was-behind-now-suspended-twitter-account-/d/d-id/1334860

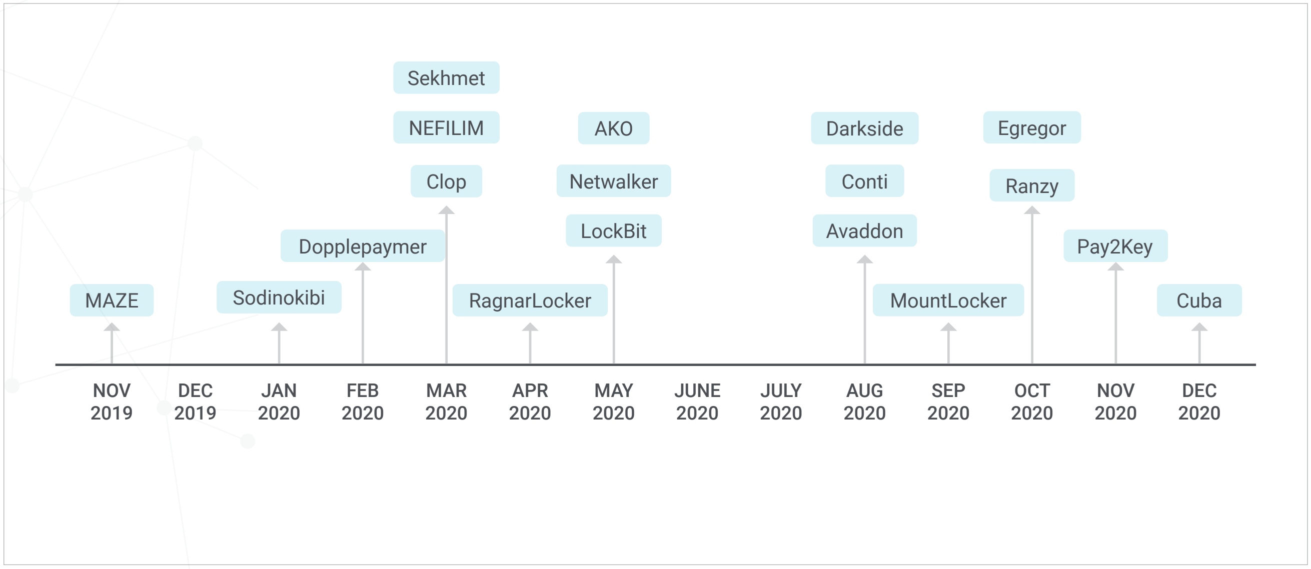


Fig. 4: Timeline of ransomware families publishing data on data leak sites or hacking forums

In October 2020, SunCrypt ransomware started the trend of waging DDoS attacks on its victims' websites or networks until the victim began negotiating ransom amounts. This trend has begun to increase, allowing attackers to get the instant attention of their victims and force them to negotiate. SunCrypt, Avaddon, and RagnarLocker ransomware actors have all been observed using these techniques[5].

Seven high-impact ransomware families

What follows is an overview of seven different ransomware families and their attack sequences. We've chosen these seven to focus on due to their prevalence and their use of double-extortion tactics. Collectively, these seven provide a good sense of what modern ransomware attacks consist of, and what your organization can expect if you should be impacted by a ransomware attack. Details on additional ransomware families can be found in the appendix of this document.

[5] Soure: https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/

Maze ransomware

Maze ransomware appeared prominently in May 2019 and was the most actively used ransomware in double-extortion attacks until the attackers ceased operations in November 2020. Attackers gained access to systems using spam email campaigns, exploit kits, such as Fallout and Spelevo, and through hacked RDP services, planting the ransomware into the network after initial compromise. Maze encrypts every file using a combination of ChaCha and RSA algorithms, appends the extension ".{random 4-7 alphanumeric characters}", and drops a ransom note "DECRYPT-FILES.txt".

Maze ransomware is one of the ransomware families that started the trend of double extortion. It threatened its first victim organization and published the victim's sensitive data on a hacking forum in November 2019. Shortly thereafter, Maze operators launched their own data leak site. Maze operators have since published many other companies' data and successfully collected huge ransoms—reportedly as high as $15M[6] —from other companies that wished to avoid the same fate.

Following in the footsteps of Maze, other ransomware groups began stealing data prior to encrypting it and utilizing double-extortion schemes to increase their ransoms. The below chart displays the industry verticals that have been most heavily impacted by Maze double extortion attacks. The IT and technology industry has been most impacted by Maze, which has used lateral movement to wage supply-chain attacks. Notably absent from this list is the healthcare industry, which the Maze group promised not to attack following the outbreak of COVID-19.

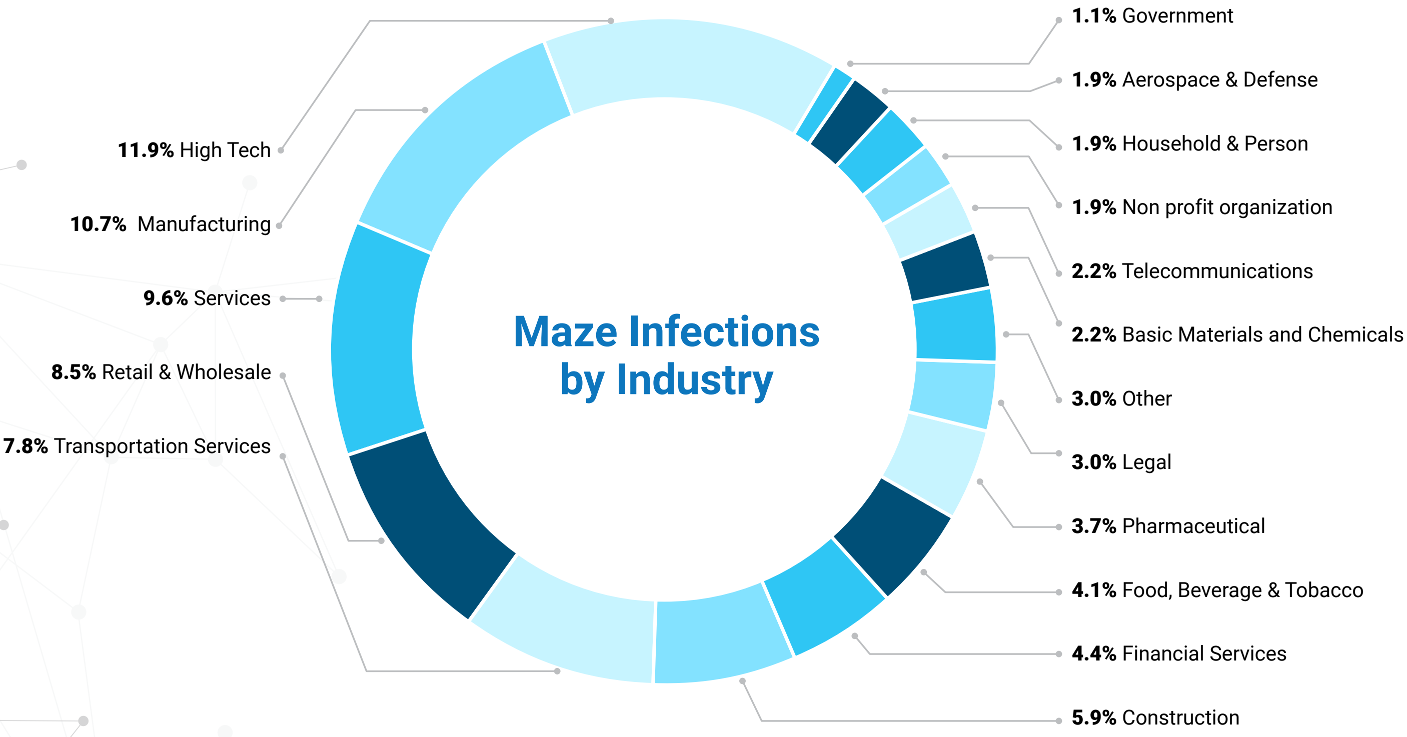
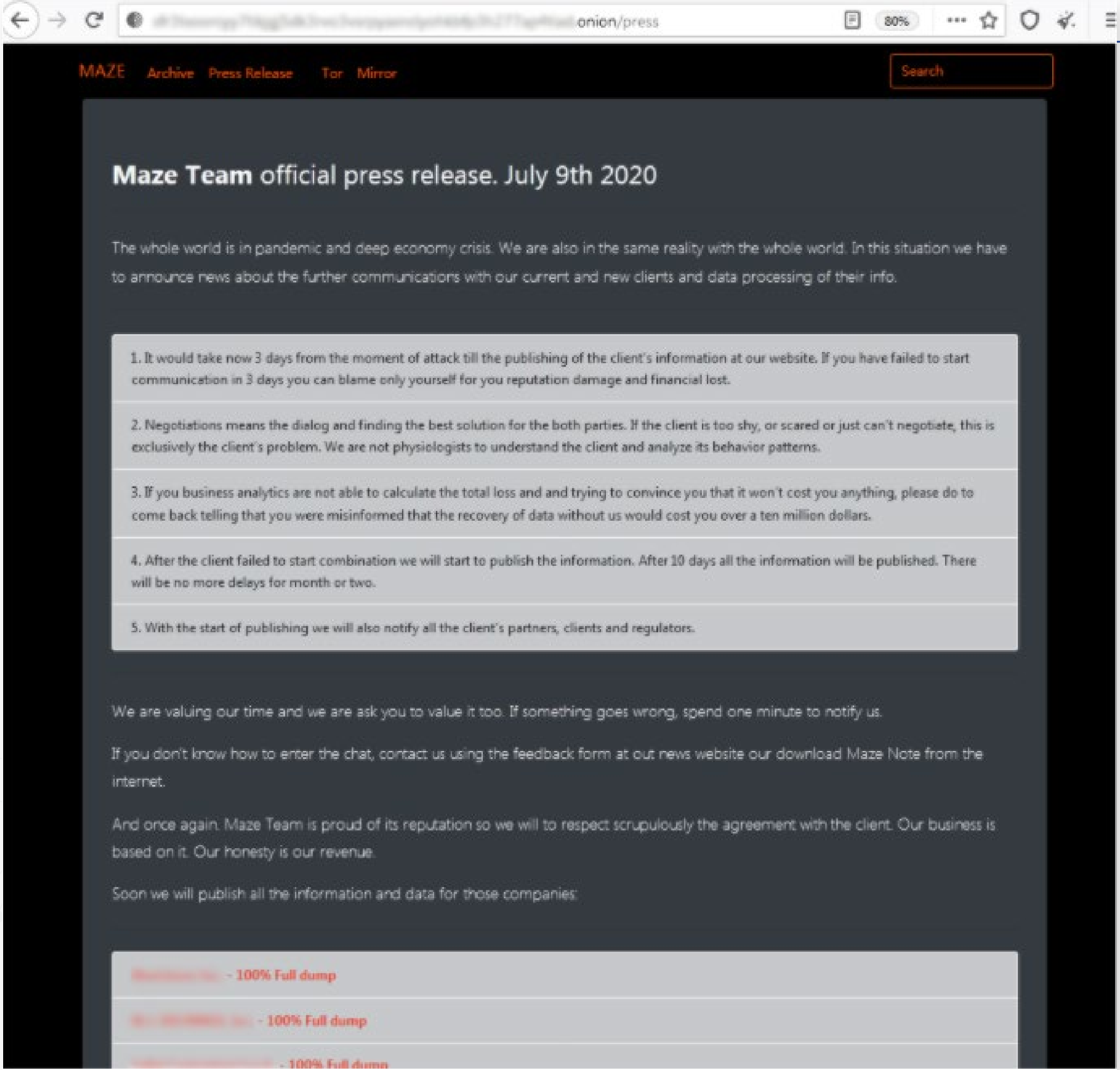


Fig. 5: Percentage of Maze ransomware attacks by vertical markets

[6] Source: https://news.sophos.com/en-us/2020/09/22/mtr-casebook-blocking-a-15-million-maze-ransomware-attack/

In a September 2020 campaign, Maze ransomware used virtual machines to deploy a payload inside the host machine. This technique had been previously used by RagnarLocker ransomware to evade detection[7]. Maze ransomware operators later formed a cartel with RagnarLocker and Lockbit ransomware gangs, colluding to maximize profits in ransomware attacks[8]. In this arrangement, Maze published data stolen by Lockbit and RagnarLocker on its own data leak site, shown below.



Maze Team official press release. July 9th 2020

The whole world is in pandemic and deep economy crisis. We are also in the same reality with the whole world. In this situation we have to announce news about the further communications with our current and new clients and data processing of their info.

1. It would take now 3 days from the moment of attack till the publishing of the client's information at our website. If you have failed to start communication in 3 days you can blame only yourself for you reputation damage and financial lost.

2. Negotiations means the dialog and finding the best solution for the both parties. If the client is too shy, or scared or just can't negotiate, this is exclusively the client's problem. We are not physiologists to understand the client and analyze its behavior patterns.

3. If you business analytics are not able to calculate the total loss and and trying to convince you that it won't cost you anything, please do to come back telling that you were misinformed that the recovery of data without us would cost you over a ten million dollars.

4. After the client failed to start combination we will start to publish the information. After 10 days all the information will be published. There will be no more delays for month or two.

5. With the start of publishing we will also notify all the client's partners, clients and regulators.

We are valuing our time and we are ask you to value it too. If something goes wrong, spend one minute to notify us.

If you don't know how to enter the chat, contact us using the feedback form at out news website our download Maze Note from the internet.

And once again. Maze Team is proud of its reputation so we will to respect scrupulously the agreement with the client. Our business is based on it. Our honesty is our revenue.

Soon we will publish all the information and data for those companies:

[redacted] - 100% Full dump

[redacted] - 100% Full dump

[redacted] - 100% Full dump

Fig. 6:

Maze ceased operations in 2020, but shortly thereafter, the same threat group introduced new ransomware known as Egregor. In February 2021, members of the group were arrested[9].

[7] Source: https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/

[8] Source: https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/)

[9] Source: https://www.computerweekly.com/news/252496480/Egregor-ransomware-arrests-confirmed

Maze – MITRE ATT&CK Tactics and Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Exfiltration	Impact
External Remote Services	Command-Line Interface	Boot or Logon Autostart Execution	Process Injection	Deobfuscate / Decode Files or Information	System Network Configuration Discovery	Automated Exfiltration	Data Encrypted for Impact
Spear phishing Attachment	Execution through Module Load		Valid Accounts	Obfuscated Files or Information	Remote System Discovery	Exfiltration Over Alternative Protocol	Inhibit System Recovery
Exploit Public-Facing Application	PowerShell			Process Hollowing	File and Directory Discovery		
	Service Execution			Disable or Modify Tools			
	Scheduled Task/Job						

Sodinokibi/REvil ransomware

Sodinokibi ransomware (aka REvil, Sodin) was first spotted in April 2019 and has been used increasingly since then. Similar to Maze ransomware, it is distributed through spam emails, exploit kits, and compromised RDP accounts; Sodinokibi also frequently exploits vulnerabilities in Oracle WebLogic. The authors of Sodinokibi have been connected to the retired ransomware GandCrab, which has been responsible for 40 percent of ransomware infections globally. Sodinokibi has been on the rise since the threat group behind GandCrab announced that it had shut down its operations[10]. Sodinokibi is targeted to specific geographies and most active in Asia—as part of its execution, it checks for keyboard languages to avoid infecting systems in CIS countries.

Sodinokibi introduced a new campaign that spreads through obfuscated PowerShell scripts and JavaScript. These scripts decode an executable (PE) file and provide it to a loader function, injecting the Sodinokibi payload directly into the system's memory[11]. Sodinokibi deletes a number of services before encryption, with user account control (UAC) bypass techniques to perform functions with elevated privileges.

Sodinokibi encrypts every file and appends the .{random alphanumeric characters} extension. It uses a combination of Salsa20 and ECDH-based key exchange algorithms in the encryption process. It drops the ransom note "{random alphanumeric characters}-readme.txt" and changes the wallpaper in the infected system.

[10] Source: https://www.cybereason.com/blog/the-sodinokibi-ransomware-attack

[11] Source: https://www.zscaler.com/blogs/security-research/fileless-malware-campaign-roundup

Sodinokibi started double extortion in January 2020, first publishing data on a hacking forum. In February 2020, Sodinokibi attackers launched their own data leak site dubbed "Happy Blog." They also experimented with auctioning stolen data on their leak site, but that proved to be unsuccessful so they ceased that activity. The below chart displays the industry verticals targeted by Sodinokibi in double-extortion attacks: transportation, manufacturing, and retail/wholesale have been most heavily impacted.

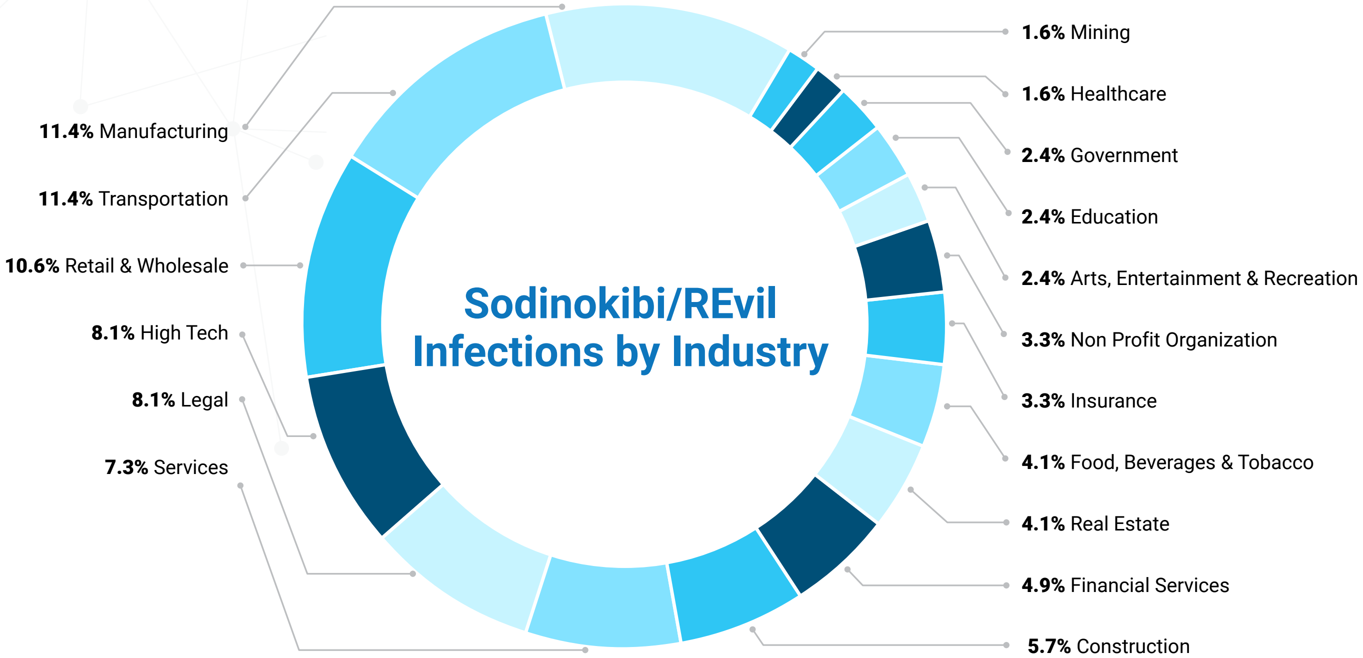
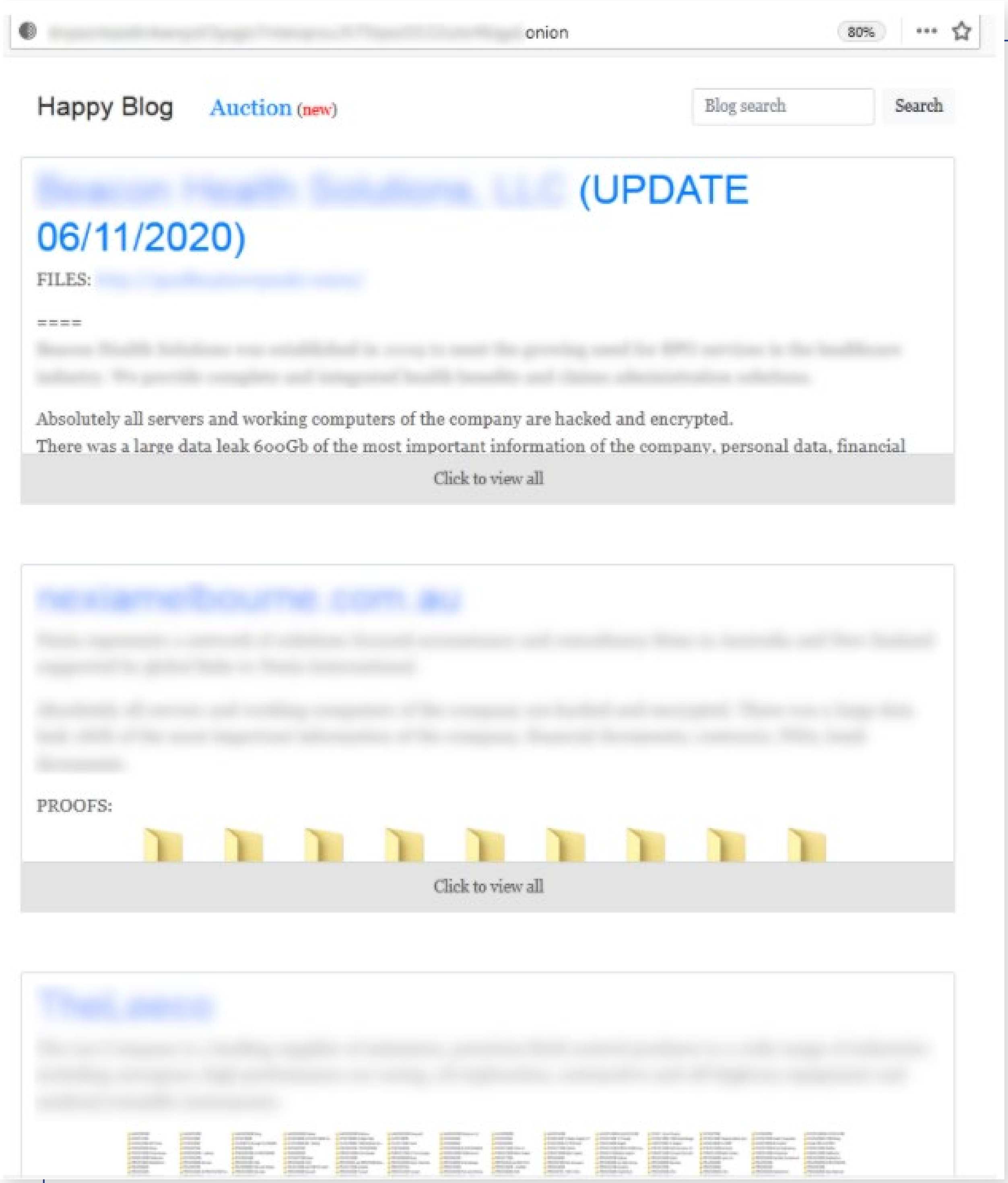


Fig. 7: Percentage of Sodinokibi ransomware attacks by vertical markets



[redacted]onion

Happy Blog Auction (new) Blog search Search

[redacted] (UPDATE 06/11/2020)

FILES: [redacted]

====

[redacted]

Absolutely all servers and working computers of the company are hacked and encrypted.
There was a large data leak 600Gb of the most important information of the company, personal data, financial

Click to view all

[redacted]

[redacted]

PROOFS:

Click to view all

[redacted]

Fig. 8: Auction on Sodinokibi data leak site "Happy Blog"

Sodinokibi/REvil – MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Exfiltration
Spear phishing Link	Command-Line Interface	Boot or Logon Autostart Execution	Access Token Manipulation	Deobfuscate/ Decode Files or Information	System Network Configuration Discovery	Automated Exfiltration
Spear phishing Attachment	Execution through Module Load	Registry Run Keys / Startup Folder	Bypass User Account Control	Disable or Modify Tools	Remote System Discovery	Exfiltration Over Alternative Protocol
Exploit Public-Facing Application	PowerShell		Exploitation for Privilege Escalation	Process Hollowing	File and Directory Discovery	
	User Execution					

Doppelpaymer ransomware

Doppelpaymer ransomware was first spotted around July 2019, disrupting a number of industries and often demanding six- and seven-figure payouts. Doppelpaymer is suspected to be based on the BitPaymer ransomware, with a few notable improvements.

Initial Infection starts with a spam email containing either a malicious link or malicious attachment that downloads Emotet malware. Emotet further downloads Dridex malware and executes it. Dridex is used either to download Doppelpaymer directly or download other tools such as CobaltStrike, PsExec, PowerShell Empire, and Mimikatz, each of which is used for other tactics such as lateral movement, executing commands, and so on[12].

Doppelpaymer ransomware encrypts files using a combination of RSA and AES algorithms, and appends the " .locked, .doppeled” extension. It drops the ransom note “.{original_filename}.readme2unlock.txt, .{original_filename}.how2decrypt.txt”. In February 2020, Doppelpaymer published its own data leak site.

[12] Source: https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html

The below chart displays the industry verticals targeted by Doppelpaymer in double extortion attacks. A December 2020 notice from the FBI noted that Doppelpaymer targets critical industries such as healthcare, emergency services, and education[13] —yet Doppelpaymer operators told BleepingComputer that they "avoid" groups that provide essential services[14]. While ThreatLabZ data does not show healthcare as a target for Doppelpaymer, there was a confirmed attack on a German hospital in 2020[15], and our cloud shows that government agencies were the third-most targeted vertical in Doppelpaymer's double extortion attacks:

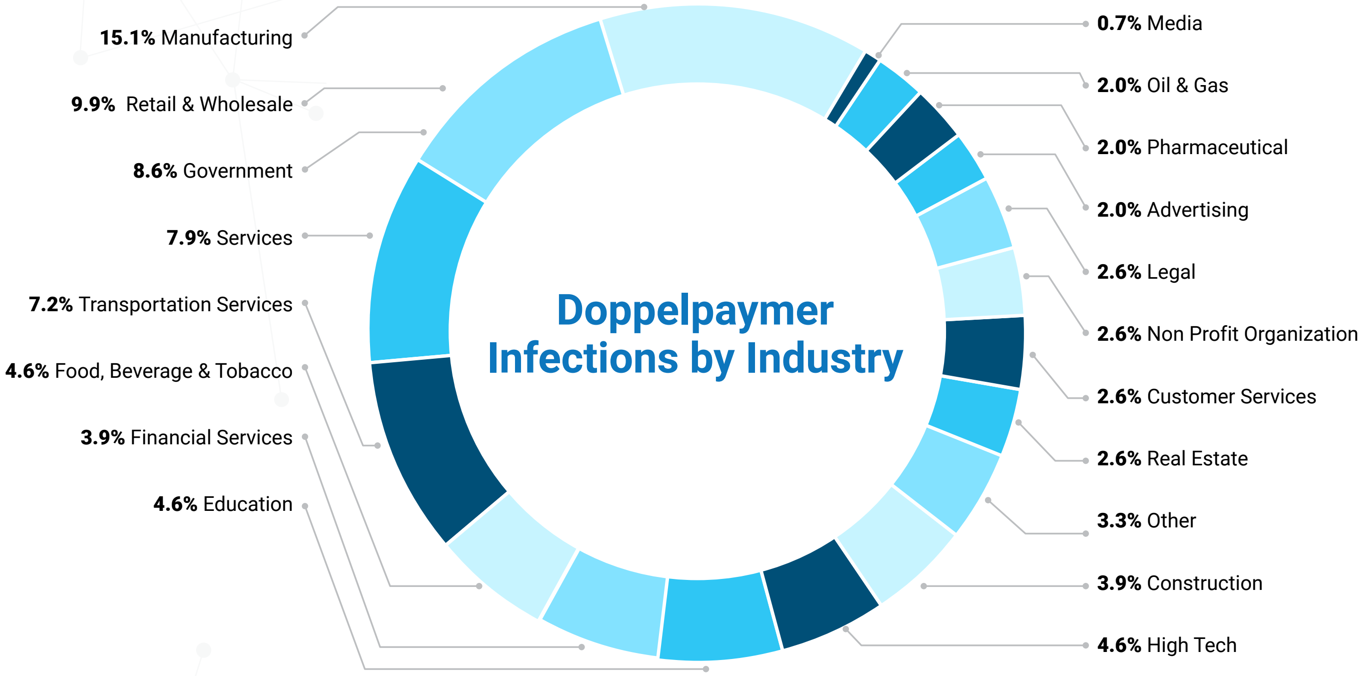
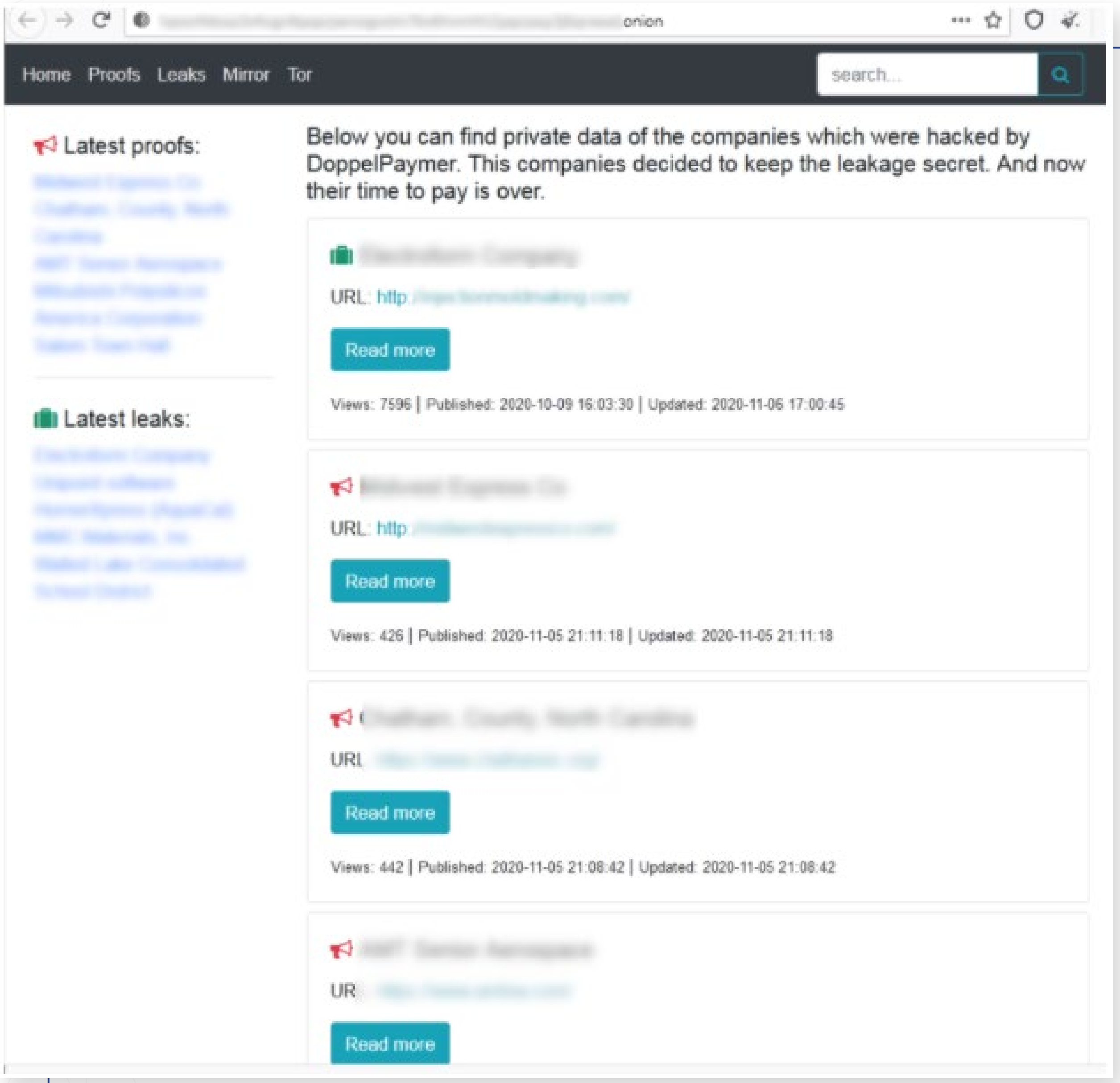


Fig. 9: Doppelpaymer attacks by industry vertical

[13] Source: https://www.ic3.gov/Media/News/2020/201215-1.pdf

[14] Source: https://www.bleepingcomputer.com/news/security/ransomware-gangs-to-stop-attacking-health-orgs-during-pandemic/

[15] Source: https://www.securityweek.com/fbi-warns-doppelpaymer-ransomware-targeting-critical-infrastructure



Latest proofs:

[redacted]

Latest leaks:

[redacted]

Below you can find private data of the companies which were hacked by DoppelPaymer. This companies decided to keep the leakage secret. And now their time to pay is over.

[redacted]

URL: http[redacted]

Read more

Views: 7596 | Published: 2020-10-09 16:03:30 | Updated: 2020-11-06 17:00:45

[redacted]

URL: http[redacted]

Read more

Views: 426 | Published: 2020-11-05 21:11:18 | Updated: 2020-11-05 21:11:18

[redacted]

URL [redacted]

Read more

Views: 442 | Published: 2020-11-05 21:08:42 | Updated: 2020-11-05 21:08:42

[redacted]

UR [redacted]

Read more

Fig. 10: Doppelpaymer data leak site

Doppelpaymer – MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Defense Evasion	Discovery	Exfiltration	Impact
Spear phishing Attachment	Command and Scripting Interpreter	Deobfuscate/ Decode Files or Information	System Network Configuration Discovery	Automated Exfiltration	Data Encrypted for Impact
Spear phishing Link	Windows Command Shell	Obfuscated Files or Information	Remote System Discovery		Inhibit System Recovery
	PowerShell	Disable or Modify Tools	File and Directory Discovery		
		Process Injection			

Ragnar Locker ransomware

Ragnar Locker was first seen in December 2019, and gained notoriety in April 2020, when it was used to solicit an $11M ransom from a large unnamed company. Ragnar Locker is notable for a combination of techniques that differentiates it from many other ransomware families. The FBI sent out a notification in November 2020 warning of its increased use across various industries[16]. The below chart displays the industry verticals targeted by double-extortion attacks using Ragnar Locker, with the highest prevalence of attacks in manufacturing and high-tech verticals.

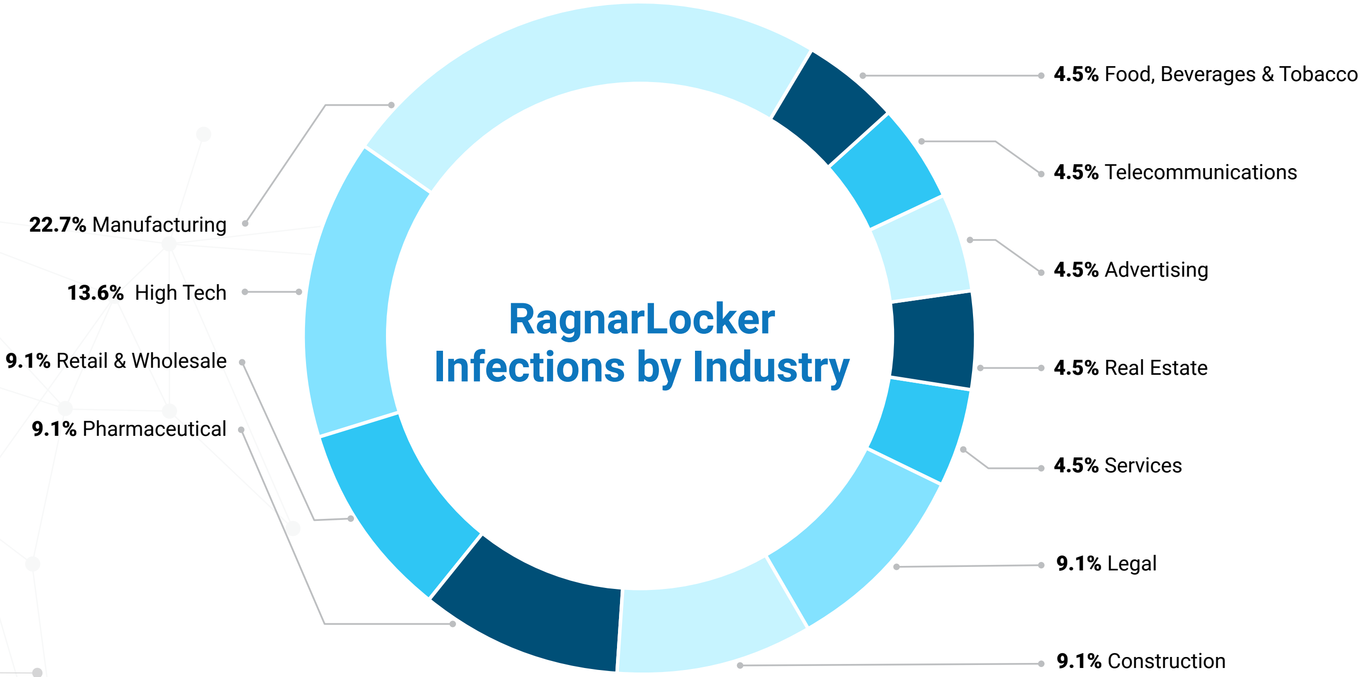


Fig. 11: Ragnar Locker attacks by industry vertical

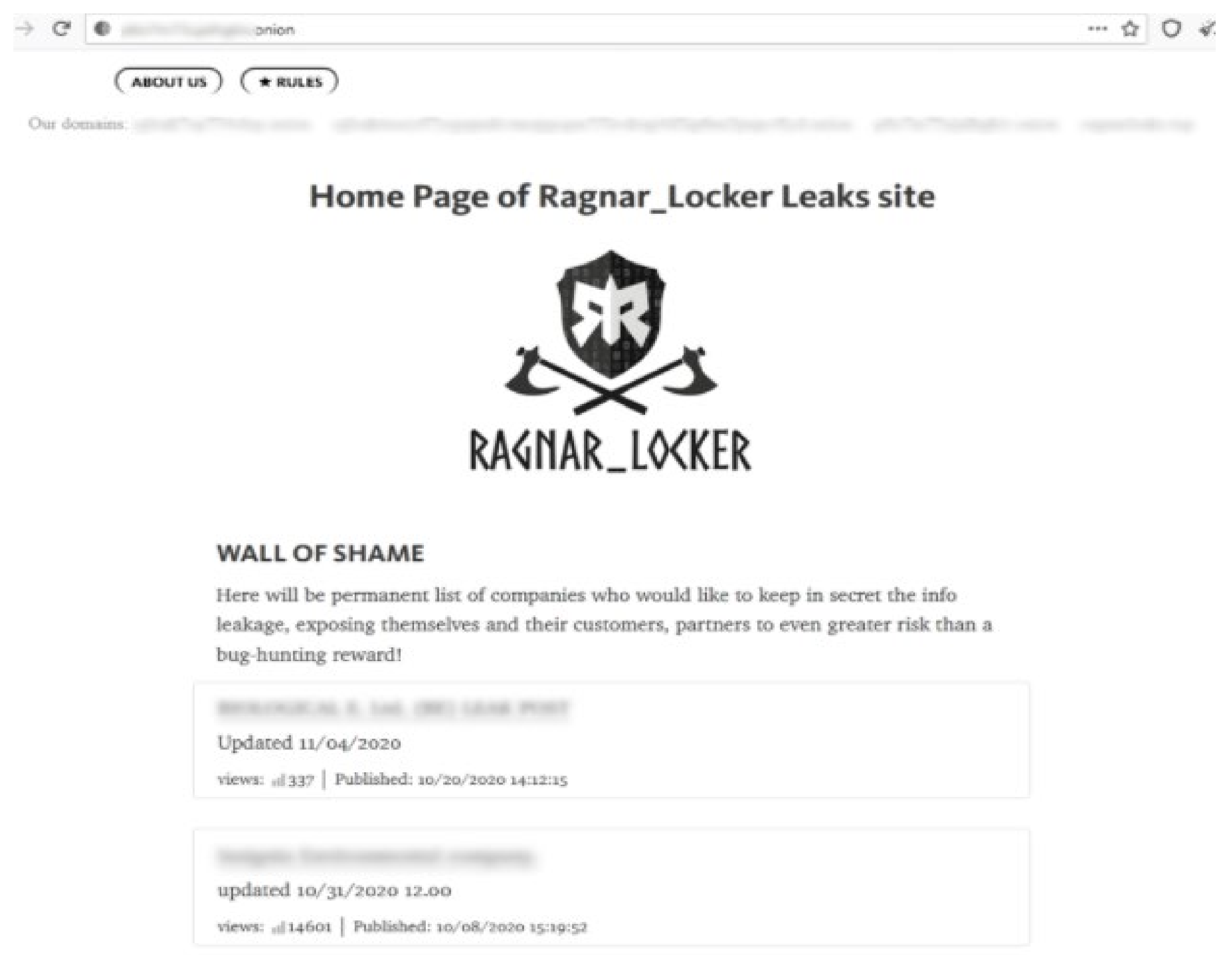
[16] Source: https://www.ic3.gov/Media/News/2020/201208-2.pdf

Ragnar Locker has been distributed mostly through brute-force attacks and/or using weak credentials of RDP. In May 2020, Ragnar Locker introduced a new technique to evade detection, deploying a payload inside of an Oracle VirtualBox Windows XP virtual machine. With this technique, the installer fully sets up the virtual machine in the host system and executes the ransomware inside the virtual machine. The script inside the package mounts the shared drives configured in micro.xml on the host machine within the guest VM. This means that the ransomware in the guest environment can now fully access the host's local disks, mapped networks, and removable drives[17].

Ragnar Locker encrypts every file using a combination of RSA and Salsa20 algorithms. Authors of the malware have changed the file extensions and ransom note files several times:

December 2019: ".ragnar_{ID}" extension; ransom note name RGNR_ {ID}.txt. I
July 2020: ".ragn@r_{ID}" extension; ransom note name "!$R4GN4R_{ID}$!.txt".
October 2020: ".__ r4gN4r__{ID}" extension; ransom note name " !!! _ READ_ME_XXXXXXXX _ !!!. Txt".

In April 2020, Ragnar Locker published its own data leak site called "Wall Of Shame," displayed below.



Our domains: [redacted]

Home Page of Ragnar_Locker Leaks site

WALL OF SHAME

Here will be permanent list of companies who would like to keep in secret the info leakage, exposing themselves and their customers, partners to even greater risk than a bug-hunting reward!

[redacted]

Updated 11/04/2020

views: 337 | Published: 10/20/2020 14:12:15

[redacted]

updated 10/31/2020 12.00

views: 14601 | Published: 10/08/2020 15:19:52

Fig. 12: Ragnar Locker data leak site "Wall of Shame"

[17] Source: https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/

Ragnar Locker – MITRE ATT&CK Tactics and Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Exfiltration	Impact
Drive-by Compromise	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Abuse Elevation Control Mechanism	Deobfuscate / Decode Files or Information	System Network Configuration Discovery	Automated Exfiltration	Data Encrypted for Impact
Spear phishing Attachment	Exploitation for Client Execution	Scheduled Task / Job	Process Injection	Abuse Elevation Control Mechanism	Remote System Discovery	Scheduled Transfer	Inhibit System Recovery
Exploit Public-Facing Application	User Execution		Exploitation for Privilege Escalation	Modify Registry	File and Directory Discovery		Service Stop
	Service Execution			Disable or Modify Tools			
				Disable or Modify Tools			

Avaddon ransomware

Avaddon ransomware was first spotted in June 2020 and has been widely distributed in spam campaigns, although it has also been spotted using brute-force attacks or hacking weak credentials of RDP services to gain access to networks. The spam emails commonly have photo-related subjects such as “Look at this photo!” with a single winky-face in the body of the mail to pique the interest of the recipient. When the victim clicks the attachment, it downloads a zip attachment with either a JavaScript or Excel file.

- The JavaScript attachment executes PowerShell and the BITSAdmin command-line tool to download and execute the Avaddon ransomware payload
- The Excel attachment executes a malicious macro to download the Avaddon ransomware

The Avaddon infection chain is shown in the below screenshot.

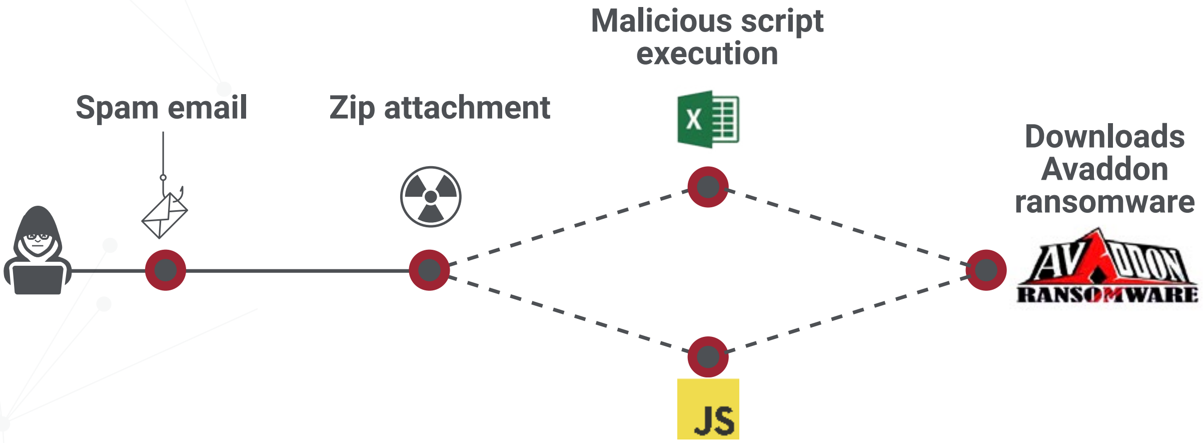


Fig. 13: Avaddon infection chain

Avaddon has been used to target a variety of industry verticals, but has waged a particularly high frequency of double-extortion attacks on government targets, followed by high-tech, manufacturing, and financial services. The below chart displays the frequency of double-extortion attacks by Avaddon in 2020:

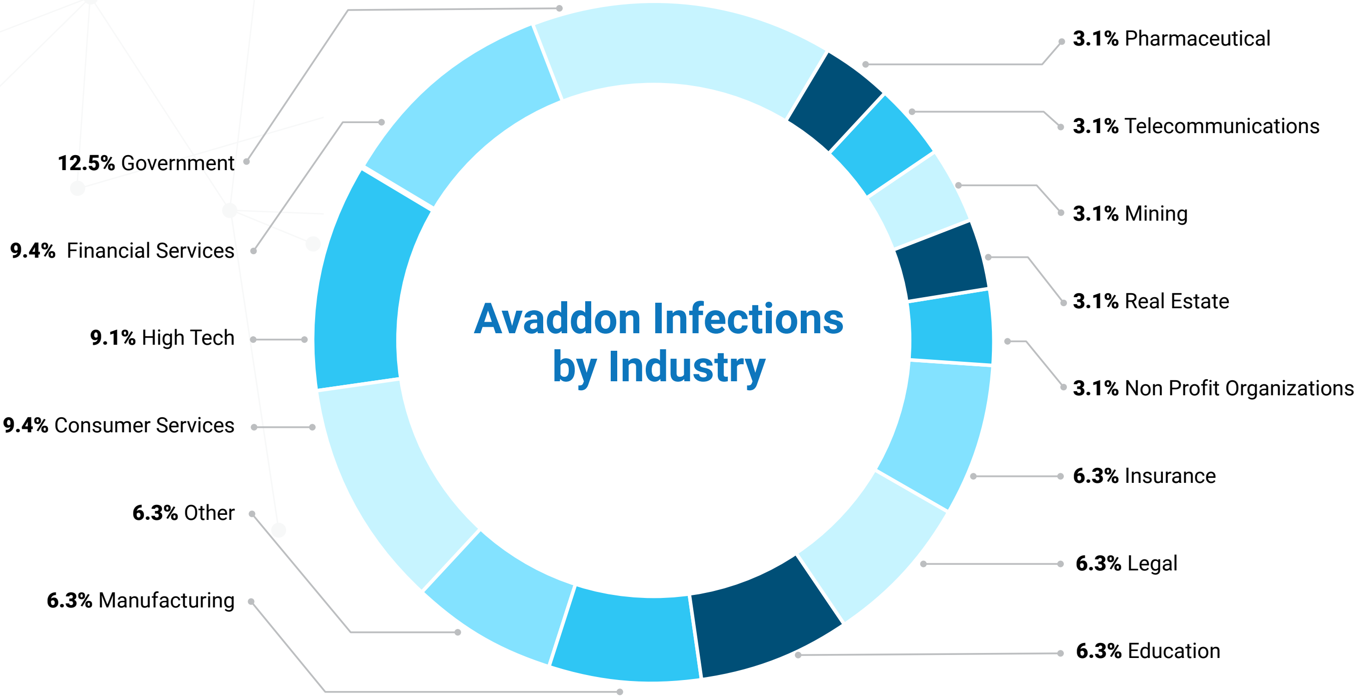
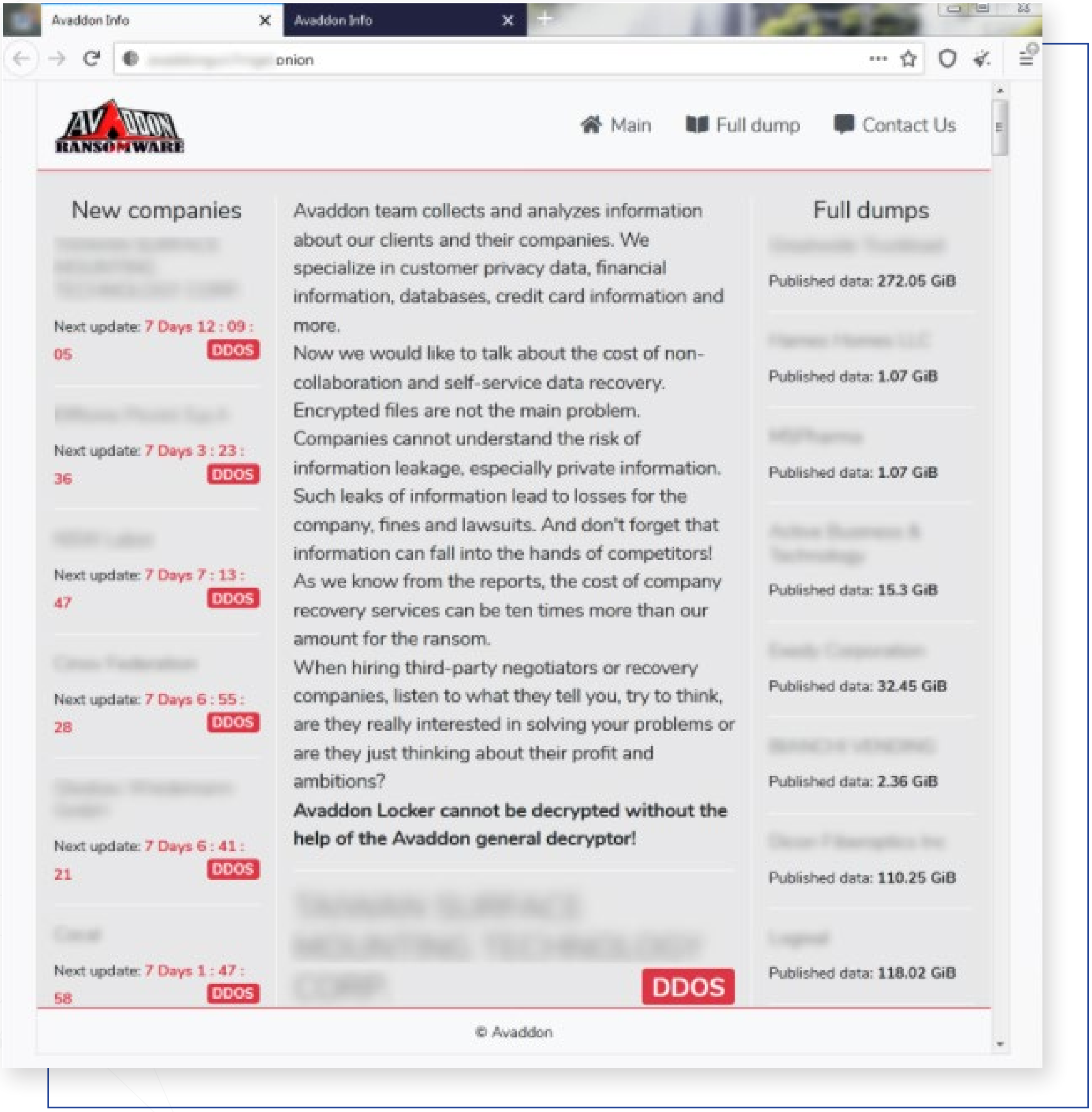


Fig. 14: Avaddon attacks by industry vertical

Avaddon uses a combination of RSA and AES algorithms to encrypt files. After encryption, Avaddon appends ".avdn, .{random alphanumeric},.{randomly selecting letter A to E}" and drops the ransom note "{ID}-readme. html". Avaddon uses UAC bypass techniques to perform functions with elevated privileges and—like many ransomware families—terminates various processes related to security products in order to maximize the number of files it can encrypt.

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 below.



New companies

[redacted]

Next update: 7 Days 12 : 09 : 05 DDOS

[redacted]

Next update: 7 Days 3 : 23 : 36 DDOS

[redacted]

Next update: 7 Days 7 : 13 : 47 DDOS

[redacted]

Next update: 7 Days 6 : 55 : 28 DDOS

[redacted]

Next update: 7 Days 6 : 41 : 21 DDOS

[redacted]

Next update: 7 Days 1 : 47 : 58 DDOS

Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.

Now we would like to talk about the cost of non-collaboration and self-service data recovery.

Encrypted files are not the main problem.

Companies cannot understand the risk of information leakage, especially private information. Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!

As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.

When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just thinking about their profit and ambitions?

Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

[redacted]

DDOS

Full dumps

[redacted]

Published data: 272.05 GiB

[redacted]

Published data: 1.07 GiB

[redacted]

Published data: 1.07 GiB

[redacted]

Published data: 15.3 GiB

[redacted]

Published data: 32.45 GiB

[redacted]

Published data: 2.36 GiB

[redacted]

Published data: 110.25 GiB

[redacted]

Published data: 118.02 GiB

© Avaddon

Fig. 15: Avaddon data leak site

In January 2021, Avaddon added DDoS tactics into its operation. Avaddon wages DDoS attacks on either the victim's website or network to encourage the victim to negotiate with its operators and to force higher ransom amounts.

Avaddon – MITRE ATT&CK Tactics and Techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Exfiltration	Impact
Spear phishing Attachment	Command and Scripting Interpreter	Boot or Logon Autostart Execution	Bypass User Account Control	Deobfuscate / Decode Files or Information	System Network Configuration Discovery	Automated Exfiltration	Data Encrypted for Impact
Exploit Public-Facing Application	Windows Management Instrumentation	Registry Run Keys / Startup Folder		Obfuscated Files or Information	Remote System Discovery		Inhibit System Recovery
	User Execution			Disable or Modify Tools	File and Directory Discovery		

Conti ransomware

Conti ransomware was first spotted in February 2020. Conti and Ryuk share similar code and both have been distributed through TrickBot. Therefore, Conti ransomware appears to be the successor of Ryuk ransomware. The first version of Conti appended the extension .CONTI after encryption, used RSA and AES algorithms in the encryption process, and dropped the ransom note “CONTI.txt.” In September, a new version was spotted that appends a random five character alphabetic extension after encryption. The file encryption algorithm has changed from AES to ChaCha20 in encryption, and the ransom note name changed to R3ADM3.txt.

Conti ransomware uses the Windows Restart Manager API before encrypting files, so the ransomware can encrypt more files. The Windows Restart Manager API helps to terminate processes and services to free up the accessed file, allowing the ransomware to encrypt them. The below chart displays the industry verticals targeted by double extortion attacks using Conti.

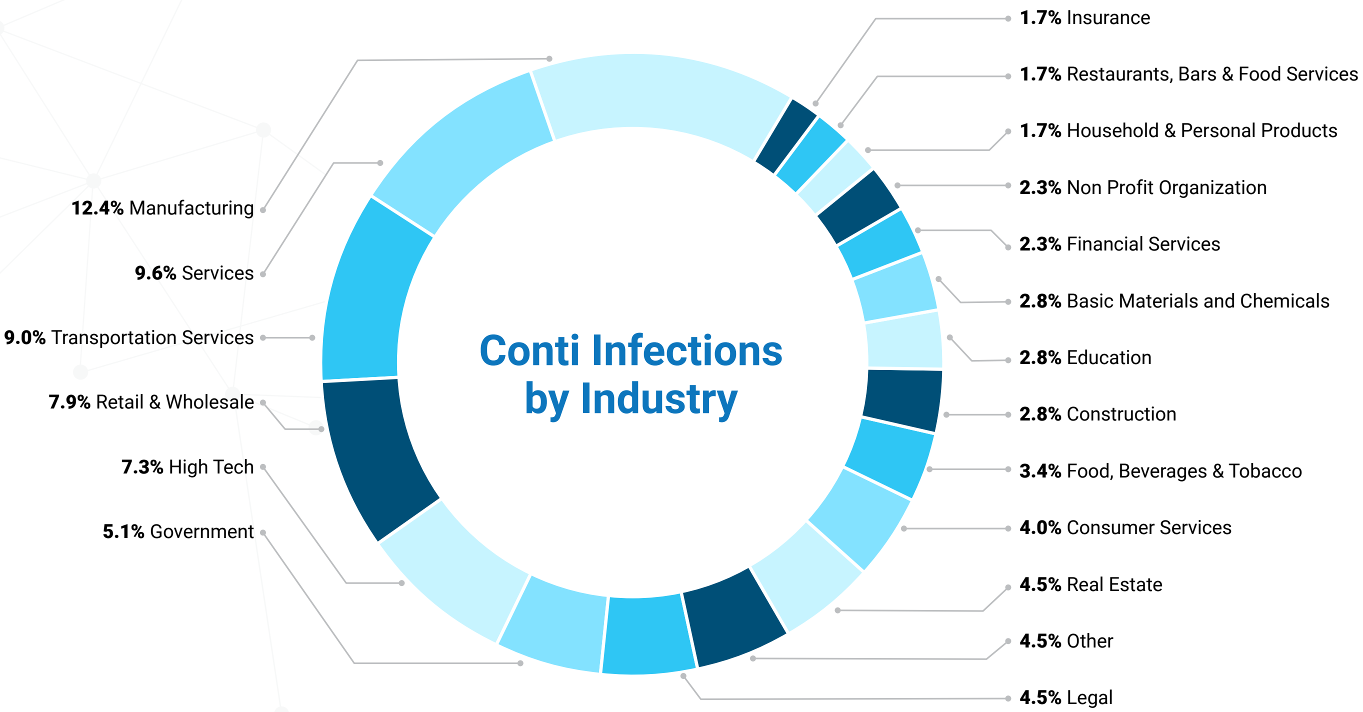
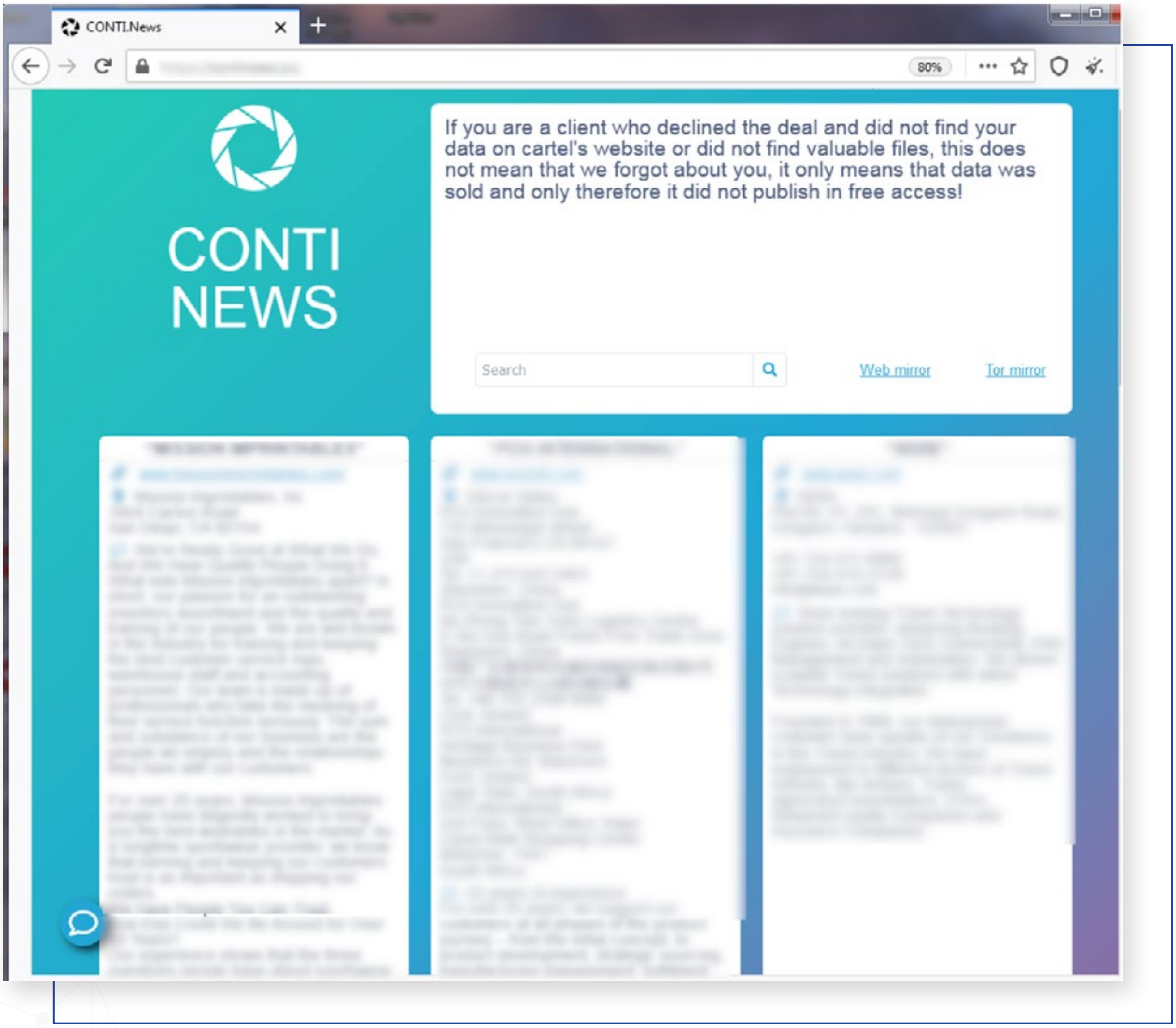


Fig. 16: Conti ransomware infections by vertical market

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



If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

Fig. 17: Conti data leak site

Conti – MITRE ATT&CK Tactics & Techniques

Initial Access	Execution	Defense Evasion	Exfiltration	Discovery	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Deobfuscate/ Decode Files or Information	Automated Exfiltration	System Network Configuration Discovery	Data Encrypted for Impact
	Windows Command Shell	Obfuscated Files or Information		Remote System Discovery	Inhibit System Recovery
	Windows Management Instrumentation	Disable or Modify Tools		Network Service Scanning	
		Process Injection		File and Directory Discovery	

DarkSide ransomware

DarkSide was first spotted in August 2020. DarkSide has made the news a number of times with innovative twists on its double-extortion schemes. In May 2021, DarkSide halted 2.5 million barrels per day of fuel distribution across the United States with its attack on the Colonial Pipeline. Attackers have also threatened to target companies on the NASDAQ stock exchange and to notify crooked market traders in advance to negatively influence stock prices[18].

DarkSide is distributed through weak or compromised credentials of Virtual Desktop Infrastructure (VDI) or RDP connections. It encrypts files and appends the extension ".{random 6 alphanumeric/numeric characters}." It uses a combination of RSA and SALSA20 algorithms to encrypt files. It drops the ransom note "README.{random 6 alphanumeric/numeric characters}.txt". The below chart displays the industry verticals targeted by DarkSide in double extortion attacks.

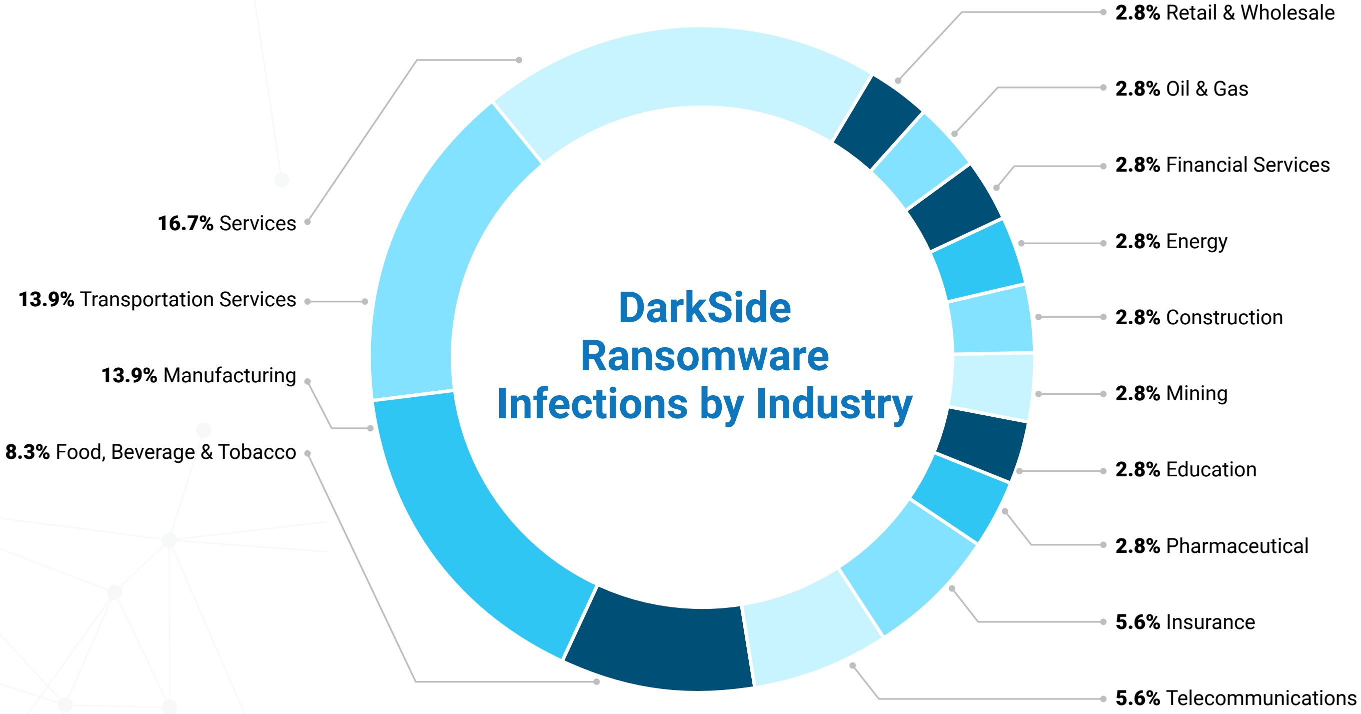
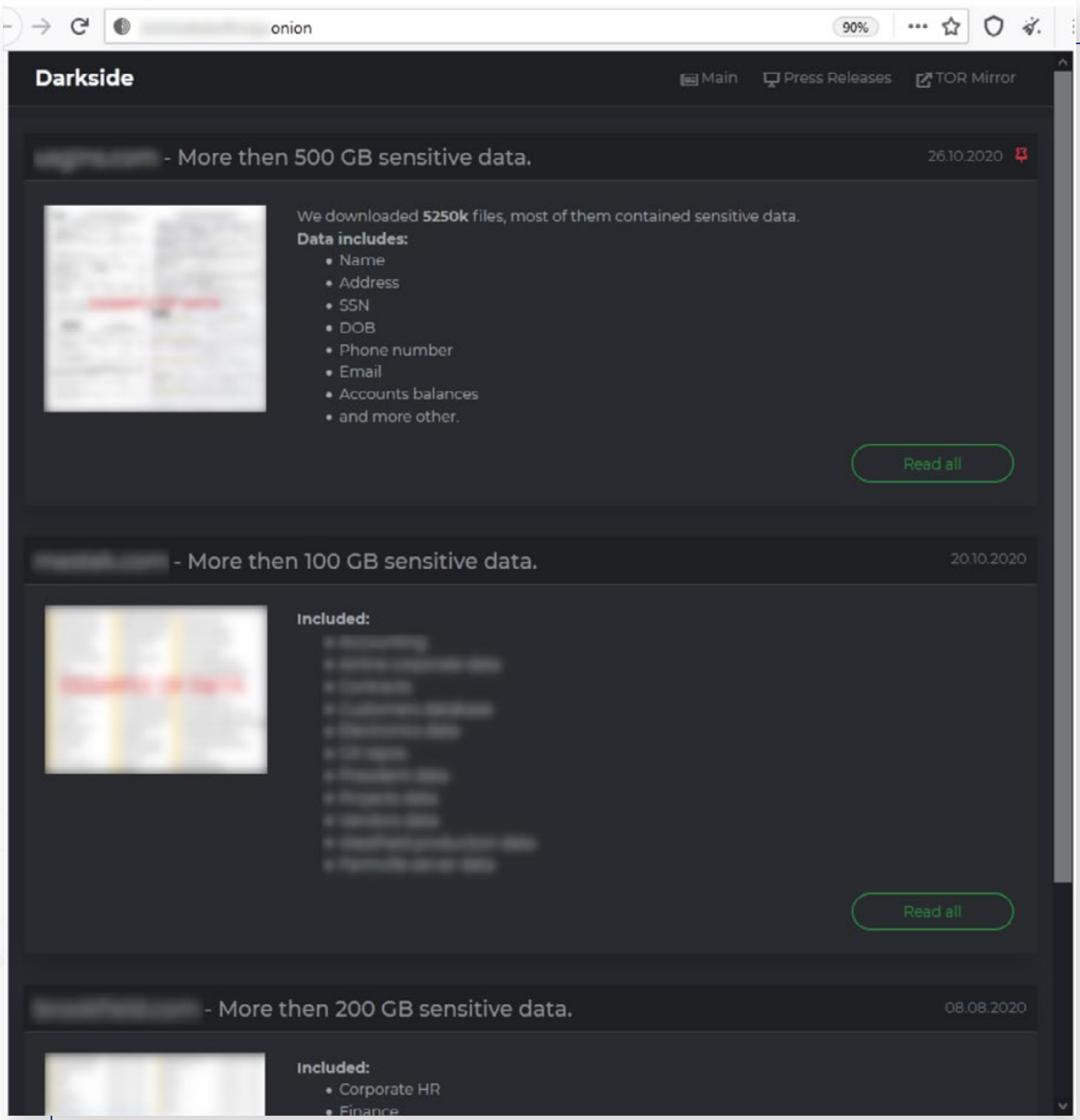


Fig. 18: Percentage of DarkSide ransomware attacks by vertical market

[18] Source: https://therecord.media/ransomware-gang-wants-to-short-the-stock-price-of-their-victims/

DarkSide ransomware also steals data from victims before encrypting files. Attackers launched their own data leak site in August 2020, as shown below.



[redacted] - More then 500 GB sensitive data. 26.10.2020

We downloaded **5250k** files, most of them contained sensitive data.
Data includes:

- Name
- Address
- SSN
- DOB
- Phone number
- Email
- Accounts balances
- and more other.

[redacted] - More then 100 GB sensitive data. 20.10.2020

Included:

[redacted]

[redacted] - More then 200 GB sensitive data. 08.08.2020

Included:

- Corporate HR
- Finance

Fig. 19: DarkSide data leak site

DarkSide – MITRE ATT&CK Tactics and Techniques

Initial Access	Execution	Privilege Escalation	Defense Evasion	Command and Control	Exfiltration	Discovery	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Access Token Manipulation	Deobfuscate / Decode Files or Information	Multi-hop Proxy	Automated Exfiltration	System Network Configuration Discovery	Data Encrypted for Impact
	Windows Command Shell		Obfuscated Files or Information			Remote System Discovery	Inhibit System Recovery
	PowerShell		Disable or Modify Tools			File and Directory Discovery	
			Process Injection				

Key steps to protecting your organization from ransomware

A growing number of ransomware families are incorporating double-extortion techniques into their operations by exfiltrating sensitive information from the victim environment. In many cases, ransomware attacks must be treated as data breach incidents by victim organizations, requiring proper response. Here are some best practices recommendations to safeguard your organization against ransomware:

1. **Enforce a consistent security policy to prevent initial compromise.** With a distributed workforce, it is important for organizations to implement a secure access service edge (SASE) architecture that can enforce consistent security policy no matter where the users are working (in-office or remotely).

2. **Implement zero trust network access (ZTNA) architecture.** Segment environments as granularly as possible and implement dynamic least-privileged access controls to eliminate lateral movement and reduce the external attack surface.

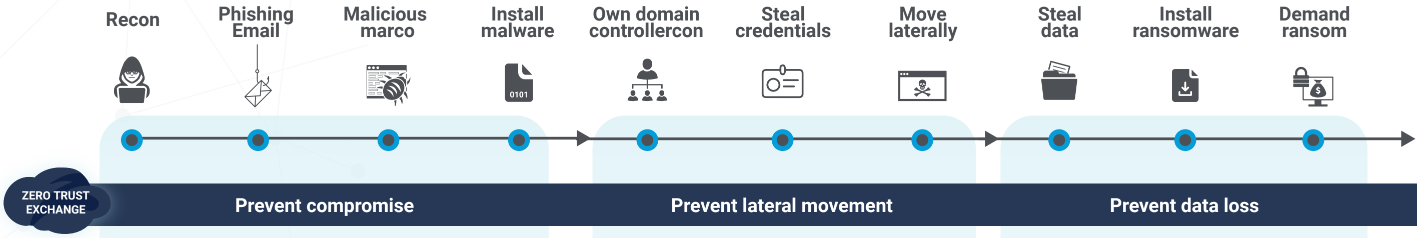
3. **Deploy in-line data loss prevention.** Prevent exfiltration of sensitive information with trust-based data loss prevention tools and policies to thwart double-extortion techniques.

4. **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.

5. **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.

How the Zscaler Zero Trust Exchange™ protects against ransomware

Zscaler's cloud-native, proxy-based architecture provides a unique advantage by safely connecting users directly to the apps, making internal apps invisible to the internet, and providing inline scanning of all traffic, including SSL-encrypted traffic. Here is how organizations can leverage the Zscaler Zero Trust Exchange to safeguard against targeted ransomware attacks:



Block threats before they reach you

Eliminate the attack surface
Private apps are visible to the internet, can't discovered and attacked

Inline content inspection (SSL)
Proprietary proxy architecture, sophisticated content inspection engine with AL-powered cloud-effect

Protect publie cloud data
Fix misconfigurations to prevent unauthorized access to cloud resources

Stop the spread of infection (LAN/WAN)

User to app segmentation
Connects and authenticated user and device to an authorized app without bringing the user on the network

Workload to workload segmentation
Uses software identity to allow or block workload communications in hybrid and multi-cloud environments

Prevent data loss to the internet

Inline content inspection (SSL)
Proprietary proxy architecture with Inline DLP policies for users, servers, workloads, IoT and OT Systems

Innovative data classification engine
With advanced exact data match, document fingerprinting capabilities

Secure SaaS data (CASB)
Prevent oversharing and discover sensitive data-at-rest

Conclusion

Over the last few years, the threat of ransomware has become more and more significant. Ransomware is become more sophisticated in every respect, from infecting an organization more efficiently, to leveraging double extortion to collect larger ransoms. The increase use of double extortion and DDoS attacks makes it very difficult for organizations to negotiate with an attacker, as the prospect of simply decrypting the data is no longer an option. After being infected with ransomware, a company's reputation can be severely damaged if attackers publish its stolen, sensitive data.

Organizations should understand the risk of ransomware and take proper precautions to avoid attacks. Remember: always patch vulnerabilities, educate employees to stay away from spam emails, back up files regularly, and use a zero trust architecture to minimize the attack surface.

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.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com