

Ransomware – The Bad, The Bad & The Ugly

Cyberint Research

TABLE OF CONTENTS

Introduction	4
Tactics Techniques and Procedures	7
Victim Reconnaissance	7
Initial Infection	7
Post Intrusion	10
Encryption Phase	11
Ransomware Note	11
The Worst of The Worst.....	12
Conti.....	12
Lockbit	16
PYSA.....	22
Retired Groups.....	25
Sodinokibi/REvil.....	25
DarkSide/BlackMatter.....	25
Avaddon	26
New Players.....	27
Khonsari.....	27
Avoslocker.....	27
Predictions For 2022	29
Information Sharing.....	29
Adaptability.....	29
New Extortion Methods.....	29
Business vs Law Authorities Conflict.....	30
Is It All About The Money?	30

Recommendations.....31

Employee Awareness.....31

Prevent Credential Misuse31

Practice Least Privilege.....31

Monitoring31

Threat Intelligence.....32

Third Party Security32

Patch Mangament32

Secure Sensitive Data32

Applications Permissions List.....32

Network Segregation.....33

Email Security33

Recovery and Backup33

References34

Contact Us35

INTRODUCTION

Ransomware remains a growing and increasingly problematic threat to organizations across all industries. Posing a significant and increasing threat throughout 2021, 'Big game hunter' ransomware campaigns, orchestrated by highly sophisticated organized cybercriminal groups, continue to compromise and extort high-value ransoms from victim organizations across all industries. While statistics related to ransomware activity over the past year differ, all are consistent in identifying a week-on-week increase in attacks. The United States is one of the top targeted countries (Figure 1).

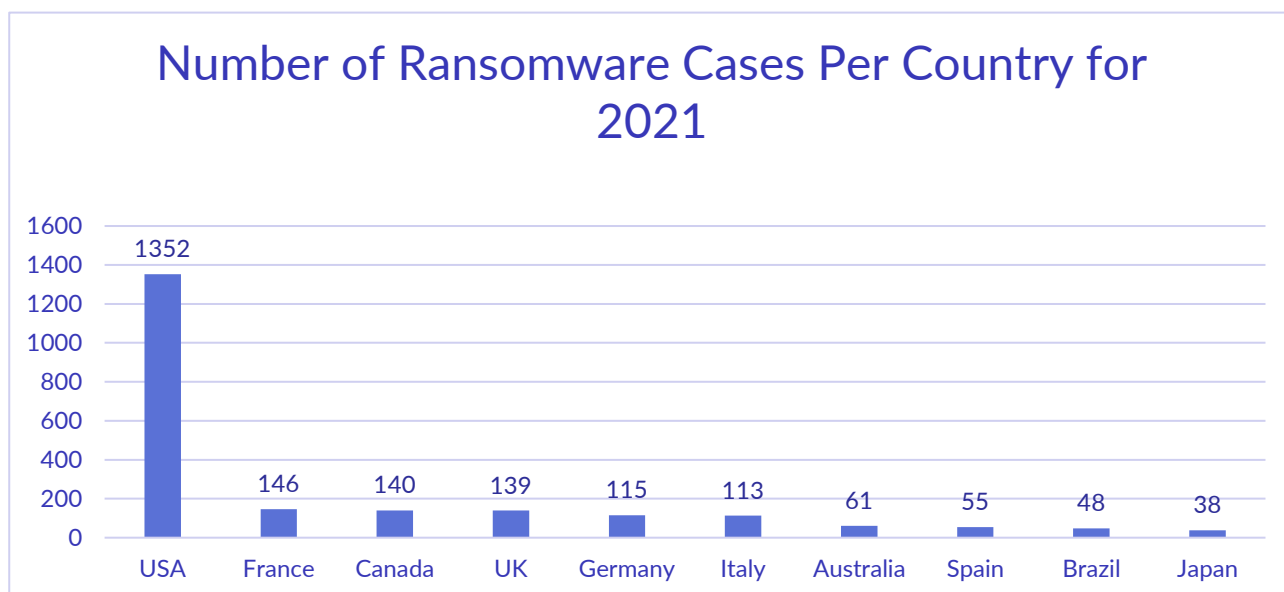


Figure 1: Top 10 countries hit by ransomware for 2021

We witnessed an overall number of 2845 ransomware cases this year, and found that the top three sectors hit by successful campaigns were the Industrial & Energy, Retail, and Finance sectors, respectively (Figure 2).

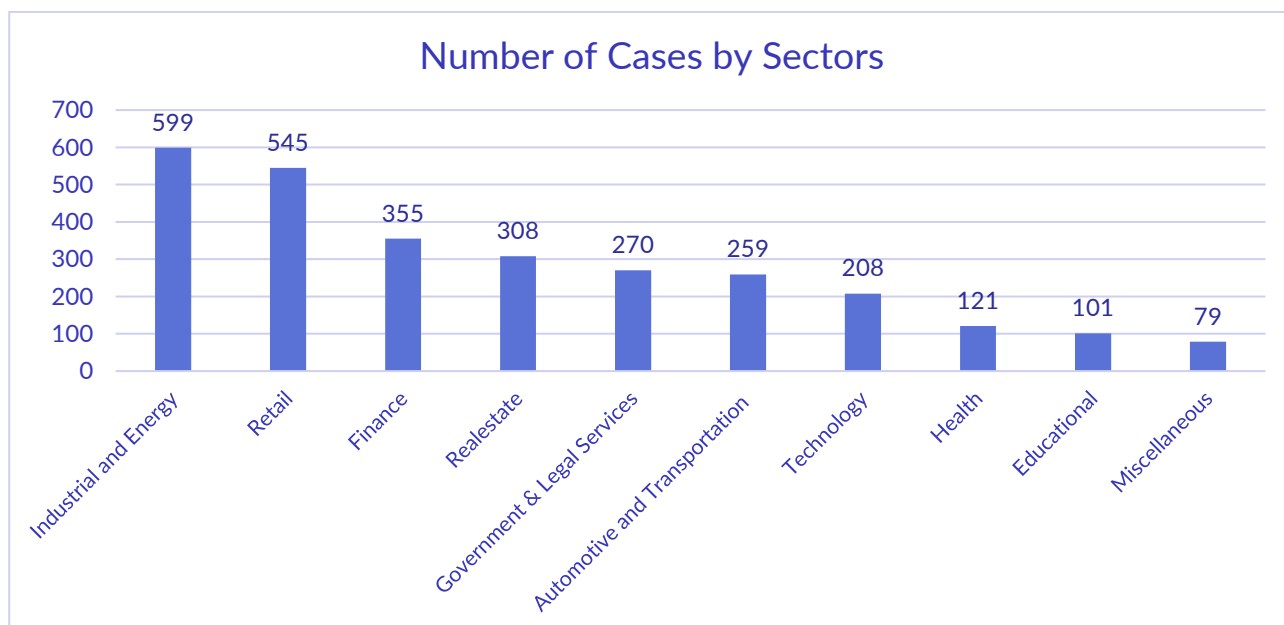


Figure 2: Number of ransomware cases by sector in 2021

Conti most effective, with 599 successful campaigns, showing dominance in this sector, while Lockbit was right behind with “only” 545 successful campaigns (Figure 3).

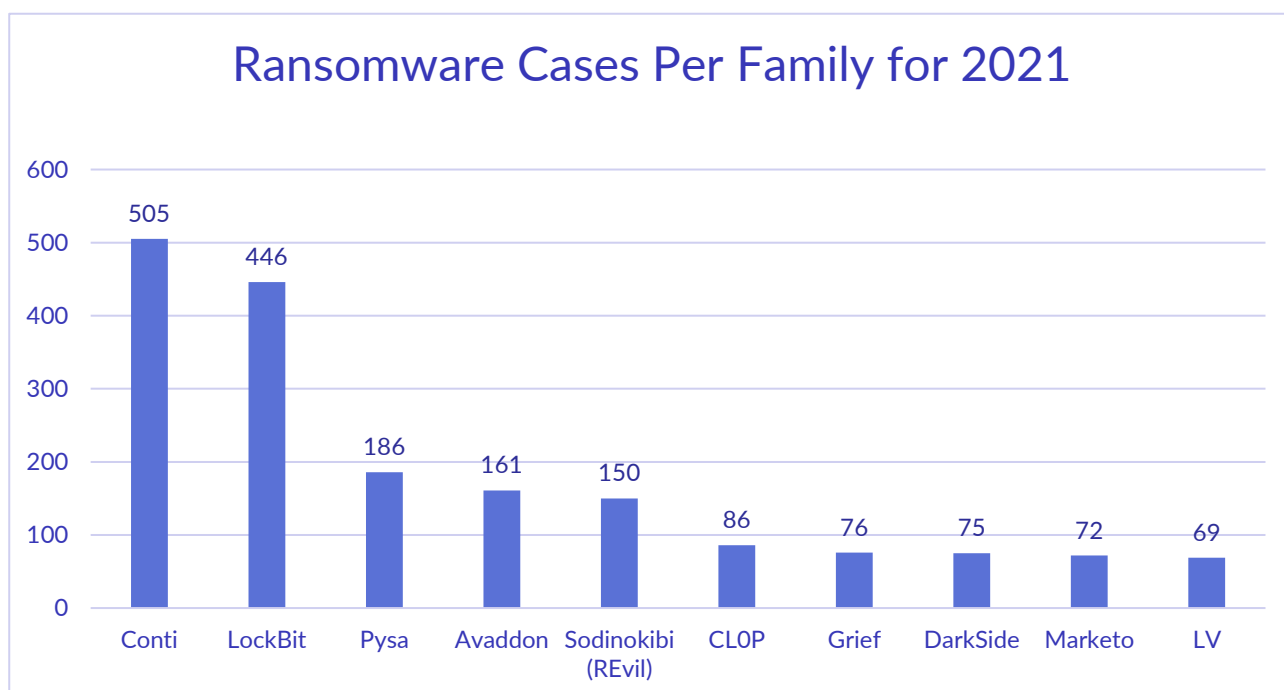


Figure 3: Ransomware cases per family for 2021

Typically, major ransomware groups utilize 'steal, encrypt and leak' tactics, pressuring their victims into paying high-value ransoms to avoid exposure. These groups continue to evolve their tactics,

techniques, and procedures (TTP), with new developments and recruitment, undoubtedly fueled by the enormous financial gains being made.

While the United States Department of the Treasury's Office of Foreign Assets Control (OFAC) introduced sanctions against several ransomware threat actors in late 2020, prohibiting US-interests from making ransom payments to individuals or entities on the 'Specially Designated Nationals and Blocked Persons List (SDN List)', in addition to countries with other embargoes, these ransomware groups continue to operate and reap financial rewards.

With many ransomware attacks resulting in the widespread encryption of data and systems across victim networks, often leading to significant periods of downtime, unprotected victims may feel inclined to promptly pay ransoms, especially if covered by a cyber-insurance policy, to regain access to their data.

TACTICS TECHNIQUES AND PROCEDURES

VICTIM RECONNAISSANCE

Based on the number and diversity of the currently active ransomware groups, almost any organization from any industry or region could fall victim to an indiscriminate malware campaign, impacting anything from a single machine to an advanced campaign attempting to encrypt all hosts across a victim network.

Given the ransomware business model employed by most groups, victims will typically be selected based on their ability to pay a significant ransom. In some cases, organizations may be given a reprieve if they are found in the threat actor's home nation, especially those operating out of countries within the Commonwealth of Independent States (CIS), or if they are part of specific sectors such as education or healthcare.

However, while some threat actors could be lauded for not targeting healthcare organizations, others have specifically selected these organizations as targets due to their criticality and, therefore, the increased chances of ransoms being paid promptly to restore service.

Furthermore, many groups operate Ransomware-as-a-Service (RaaS) which is a subscription-based model that enables affiliates to use already-developed ransomware tools to execute ransomware attacks; Therefore, target selection will often be based on an 'affiliate' threat actor gaining access to an organization's network. As such, many victims may be selected solely based on being vulnerable to a preferred or specific exploit, with external infrastructure and remote desktop protocol (RDP) vulnerabilities often being favored.

INITIAL INFECTION

Although corporations only happen occasionally, imitations of techniques, especially within the initial intrusion phase, are common between ransomware threat groups. Phishing campaigns, low-volume targeted attacks against multiple organizations, compromised credentials, and vulnerabilities in public-facing infrastructure are being exploited to gain a foothold within a victim network.

PHISHING AND MALSPAM

Many ransomware families are delivered via common attack vectors such as phishing and malspam campaigns. While both techniques are mainly applied using social engineering techniques, this delivery method is via email lures masquerading as legitimate business communications that encourage the recipient to open the attachment or input its credentials. Based on an analysis of recent campaigns, these communications include content related to urgent or pressing matters such as new orders, payment, purchase order and quotation, as well as the apparent reuse of prior legitimate email threads that include contact details for, and mimic, an unwitting third party.

Given the nature of the email lure, targeted recipients will likely include those working within Business Administration, Finance, and Sales teams. Furthermore, the compromise of one organization could lead to legitimate email accounts being abused to send effective lures to other organizations.

As such, customers, partners, or vendors of any victim organization could potentially be targeted with incredibly effective email lures, especially if the group were to infiltrate and send malicious email lures from the original victim's email server.

As mentioned, the main goal of phishing campaigns is to compromise credentials so the threat actor can gain an initial foothold within the victim's network. Although it is widespread, some threat actors "save the hustle" and purchase compromised credentials from reliable third-party sources such as other threat actors who run stealer campaigns and have relevant logs.

VULNERABILITY EXPLOITATION

Ransomware groups often look for more lethal and efficient methods to deploy their products within the victim's network while having a minimal dependency on human error and social engineering. The more skilled threat groups often seek to utilize vulnerabilities relevant to the victim's infrastructure, such as front-facing services, e.g., web servers, SQL servers, RDP and VPN clients, file transfer appliances, and more.

An excellent example of ransomware groups exploiting vulnerabilities within their campaigns is the CIOP group, which has utilized this tactic to target organizations using a vulnerable version of 'Accellion FTA', a file transfer appliance. As such, the following vulnerabilities have reportedly been exploited to gain access to victim data as well as potentially pivoting into victim networks:

- **CVE-2021-27101** - Critical SQL Injection via a crafted Host header in versions $\leq 9_12_370$;
- **CVE-2021-27102** - Command execution via a local web service call in versions $\leq 9_12_411$;
- **CVE-2021-27103** - Critical server-side request forgery (SSRF) in versions $\leq 9_12_411$;
- **CVE-2021-27104** - Critical command execution via a crafted POST in versions $\leq 9_12_370$.

Another useful example is the notorious Conti group, which has utilized infrastructure exploit tactics to target unprotected Remote Desktop Protocol (RDP) hosts to gain access to victim data and potentially pivot into the broader victim network.

Category: Vulnerabilities | Type: Exploitable Ports | Impact: Data Breach/Compromise, Unauthorized Access +1

Exploitable Port on Company Server Detected

Severity: **High** | Confidence: **100** | Tags: [Add Tags +](#)

Description

IP Address	Port
[REDACTED]	3389

Service Description
 Port 3389 is used for Windows Remote Desktop connections (RDP).
 When this port is open, a remote attacker can launch a brute force attack against the server and thus pass authentication when successful. This process can also cause the server to have slow performance.

Another security issue can arise when there is no proper encryption for the end-to-end connection, meaning it is prone to man-in-the-middle attacks.

Service	Source Category
Remote Desktop Connections (RDP)	Attack Surface Monitoring

Argos™ detected a potentially exploitable open port on an IP address belonging to [REDACTED].
 The IP [REDACTED] is part of a netblock that was registered by a company email address ([REDACTED]).

Figure 4: exposed RDP port susceptible to compromise. From Argos Edge™

In addition, network intrusion and ransomware deployment phases are reportedly conducted around the weekend to minimize the chance of detection and potentially increase the success of the encryption phase, given that a lot of corporate data would be under-utilized therefore not 'locked' open. On some occasions, the infiltration methods and the exact vulnerability used is not clear.

LOG4SHELL VULNERABILITY

A new game changer vulnerability was discovered on Dec 9, 2021, which causes a remote code execution (RCE) vulnerability [2] in Apache log4j 2, affecting massive amounts of servers worldwide. As it gained high traction worldwide and much was said about this issue, threat actors, from amateurs to veterans, rapidly started utilizing this vulnerability within their products, and the ransomware families didn't fall behind. New families such as Khonsari and more famous ones such as Conti and TellYouThePass, which has returned from leave, have already weaponized their campaigns with this vulnerability's exploits. Given that, at the time of writing, there are still many cases and methods for

exploiting this vulnerability, and no permanent solution is available, threat actors will seek to use it as much as possible.

THIRD-PARTY SERVICES

Third-party infiltration services are often used by ransomware families, especially for Ransomware-as-a-Service (RaaS). Many threat actors looking to take part in a ransomware campaign will often use or rent infrastructures that will service distribution.

One of the most creative and active groups known today, Conti has often used the Emotet infrastructure for deployment of their ransomware over several networks, reasonably quickly after its return [1], which also implies the adaptability and opportunism by threat actors when it comes adding new abilities and improving their products.

Another example is the Defray777 ransomware delivered in tandem with other tools such as the Vatet loader, PyXie RAT, and Cobalt Strike through low-volume, targeted attacks against multiple organizations.

POST INTRUSION

Although the initial infection vector may differ from one victim to another, any ransomware group's objectives upon network intrusion remain consistent: the exfiltration of sensitive and valuable data prior to encryption to exert maximum pressure on victims, and encouraging prompt payment of ransom demands. Likely commencing with a thorough reconnaissance phase, data that was stolen by the group typically includes customer, employee, and financial records, likely of value to fraudsters, as well as sensitive emails, documents, and intellectual property that could be damaging in the hands of competitors or when shared publicly.

DEFENSE BYPASS

One of the ransomware deployment tasks is setting up a packed action process. The first phase of most ransomware products is the defenses bypass. The main goal is to bypass AV vendors' tools, Windows Defender, adjust Shadowcopy and backup configurations (Figure 5), ensuring a clean slate to work on without any interference and without leaving the victim any way to restore the lost files.

```
cmd.exe /c %SYSTEM%\wbem\WMIC.exe shadowcopy where "ID='{2D3E78C1-16F5-45C2-8C51-8B602BF398FB}'" delete
```

Figure 5: Conti example running shadowcopy delete commands

PERSISTENCE

Persistence is vital when it comes to the first stages of any ransomware campaign; the ability to gain a solid foothold within the victim's systems is essential for operating in the most efficient way possible. Most ransomware families add their payload to Windows Scheduled Tasks or set up their payload in the Startup Folder or Registry Keys.

ENCRYPTION PHASE

Having exfiltrated any potentially valuable data, a victim-specific ransomware threat is deployed and commences a preparatory phase in which services related to various applications, such as backup software and database servers, are stopped.

The encryption algorithms and implementations may vary, such as AES, RSA, and more. While the algorithms pretty much remained the same, the extension of the encrypted files changes depending on the ransomware family, e.g., Babuk is used to set up the extension of the encrypted file with the '.babyk' file extension. While challenges have been raised with AV mechanisms that identify the encryption phase by file extensions, ransomware families have adapted relatively quickly to the situation, and soon enough, most ransomware families will have added different extension mechanisms to add random bytes as the extensions of the encrypted files.

RANSOMWARE NOTE

Created on a per victim basis and encrypted within the victim-specific ransomware sample, ransomware groups create a text file with an eye-catching name such as "Restore-My-Files.txt" (Figure 6) on the target system desktop, typically explaining the situation and ways to contact the threat group in its various channels for purchasing decryptor software.

```

----- Welcome. Again. -----

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on you computer has expar
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwis

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do
To check the ability of returning files, You should go to our website. There you can decrypt one file for
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkxbxr6wketf56nf6aq2nmyoyd.onion/{UID}

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/{UID}

Warning: secondary website can be blocked, thats why first variant much better and more available.

```

Figure 6: Revil example ransom note

THE WORST OF THE WORST

As ransomware remains one of the most profitable fields in the cybercrime sector, it is no surprise that groups of different kinds vying to be as high as possible on the “leaderboards” of the most talented and successful ransomware group. Following are the top 3 ransomware groups currently appear to be the most successful:

CONTI

Conti is a well-known ransomware group that has been operating Ransomware-as-a-Service (RaaS) campaigns since 2020. In many cases, Conti has been linked to Wizard Spider, a cybercrime group based in Russia and Ukraine, which suggests that Conti is probably operating and based in that same region. Conti developers likely pay the deployers of the ransomware a wage rather than a percentage of the proceeds used by affiliate cyber actors, and receives a share of the profits from a successful attack. Conti is known for its efficiency, adaptability, and opportunism to exploit any vulnerable organization that can pay significant ransom payments. There is much speculation surrounding the amounts of funds sent to Conti in 2021, while most sources suggest that Conti made around 50 million USD from successful campaigns in 2021 alone.

Given that Conti is that popular and admired by other threat actors we found many evidence and discussion by threat actors regarding their ways of actions and tools used in their campaigns to learn from (Figure 7).

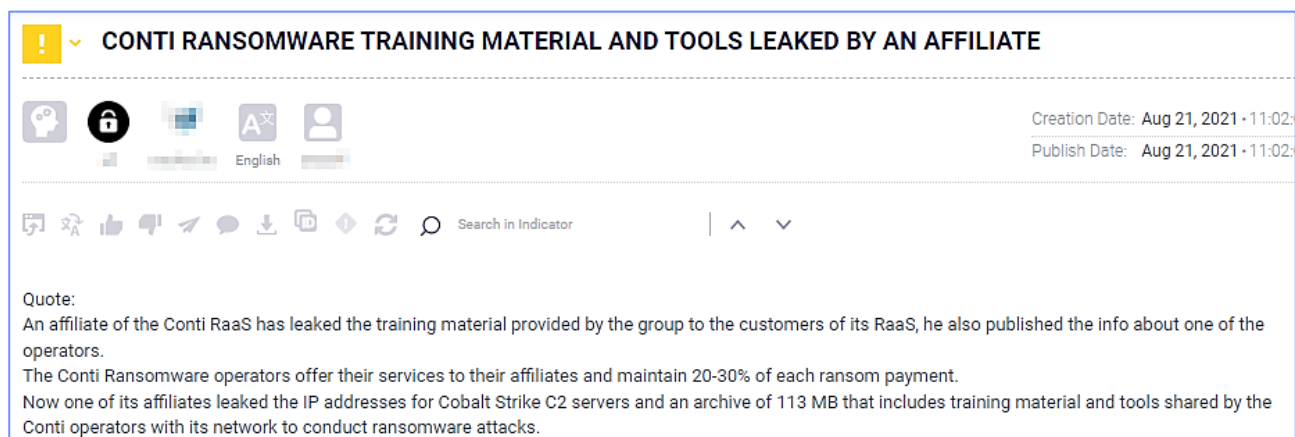


Figure 7: Conti materials shared and discussed among other threat actors.

INITIAL INFECTION

Like many other RaaS operations, the initial intrusion vector may vary in each campaign. It is documented that in most cases, Conti has focused their efforts on the following:

Valid Accounts

Conti operators and affiliates are known for looking for vulnerable hosts and accounts that can come in handy in their campaigns, such as stolen Remote Desktop Protocol (RDP) credentials they can purchase (Figure 8) and more.

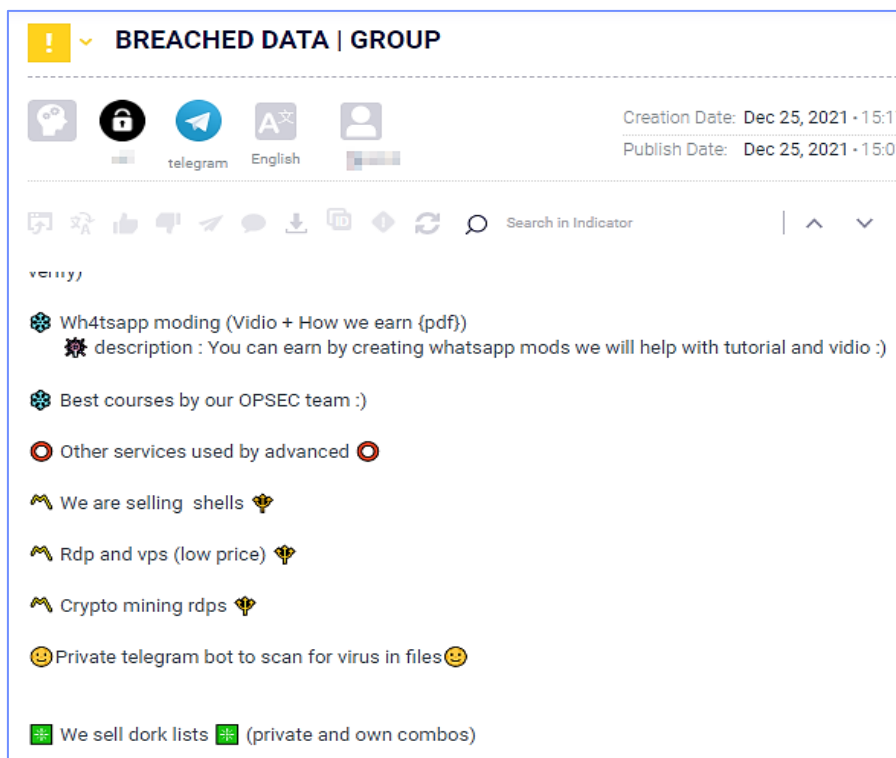


Figure 8: Telegram channel the sells compromised RDP credentials found in Argos Edge™

Phishing

Whether it's in spear-phishing attachments or links, Conti will look for creative ways to deliver Their payload using this method, such as malicious attachments and links that will lead to a TrickBot infection, eventually loading Conti into the victim's network.

Vulnerability Exploitation

Conti will look to weaponize their delivery methods, exploiting any vulnerability that will help their cause. In the past, we have witnessed campaigns utilizing PrintNightmare (CVE-2021-34527) [4] and Zerologon (CVE-2020-1472), leading to Conti's delivery. As mentioned, the devastatingly high severity Log4Shell vulnerability (CVE-2021-44228) discovered in December 2021, as suspected, was also added to their arsenal only a few days after the vulnerability was published, which, yet again, suggests the adaptability that is one of their main characteristics, and, with good reason, places them at the top of the pyramid.

POST INTRUSION

The first steps in every campaign might be crucial and directly affect whether the campaign is successful or not. These are Conti's initial steps in the victim's network:

Persistence

Conti usually applies persistence within the victim's network by leveraging external-facing remote services to initially access the network. Many external-facing remote services such as virtual private networks (VPNs), Citrix, Remote Desktop Protocol (RDP), and more were used in Conti's campaigns.

Defense Evasion

Applying defense evasion techniques often depends on the threat group's abilities. Conti is considered skilled in this area. They use encryption of the DLL files they use in their campaigns, and they obfuscate the Windows API calls, making it challenging for many static analysis defense mechanisms to identify their actions. Documentation of previous campaigns suggests that Conti can stop up to 146 Windows services related to backup, security, database, and email solutions, while deleting shadow copies.

Lateral Movement

Conti often spreads to other machines via SMB and network shared drives within the victim's network.

ENCRYPTION PHASE

The encryption phase of Conti contains a heavy use of `CreateIoCompletionPort()`, `PostQueuedCompletionStatus()` and `GetQueuedCompletionPort()` as it encrypts files relatively quickly. It does exclude .exe and .dll files and uses a different AES-256 encryption key per file with a bundled RAS-4096 unique public encryption key for each victim.

RANSOM NOTE

Conti usually leaves a detailed note with typical private and secured communication channels for negotiations (Figure 9).

All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :

(you should download and install TOR browser first <https://torproject.org>)

<http://contirec7nchr45nx6ympez5rjldibnqzh7lsa56lvjaeywhvoj3wad.onion/01QQWQhQ09Z1FH2CsVy45PwBL1JKWRKEYmnWtNtPtVQIU6K2MPtQgYuYKcurNC>

YOU SHOULD BE AWARE!

Just in case, if you try to ignore us. We've downloaded a pack of your internal data and are ready to publish it on our news website if you do not respond. So it will be better for both sides

---BEGIN ID---

01QQWQhQ09Z1FH2CsVy45PwBL1JKWRKEYmnWtNtPtVQIU6K2MPtQgYuYKcurNC

---END ID---

Figure 9: Conti ransom note example

MITRE ATT&CK

Defense-evasion

- Deobfuscate/Decode Files of Information – T1140
- Process Injection – T1055
- Obfuscate Files or Information – T1027

Discovery

- File and Directory Discovery – T1083
- Network Share Discovery - T1135
- Process Discovery - T1057
- Remote System Discovery - T1018
- System Network Configuration Discovery - T1016
- System Network Connections Discovery - T1049

Lateral-Movement

- Remote Services - T1021
- Taint Shared Content - T1080

Execution

- Command and Scripting Interpreter - T1059
- Native API - T1106

Impact

- Data Encrypted for Impact - T1486
- Inhibit System Recovery - T1490
- Service Stop - T1489

LOCKBIT

Launched in September 2019 and formerly known as ‘ABCD’, LockBit is a ransomware-as-a-service (RaaS) threat updated in June 2021, and improves on the group’s earlier claims of having the fastest encryption process on the ransomware scene (Figure 10).

Encryption speed comparative table for some ransomware - 02.08.2021 (added BlackMatter)							
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec, 2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963

Figure 10: LockBit encryption speed comparison

Like other RaaS offerings, LockBit operates an affiliate profit sharing program in which up to eighty percent of a ransom payment can be earned while the operators claim the remainder.

Reportedly only requiring the affiliate to gain access to a ‘core’ server, such as a Windows Domain Controller (DC), the advertised feature set (Figure 11) suggests that the LockBit ransomware will distribute itself across the network in addition to automating steps that aid in detection evasion, complicating post-incident analysis and preventing data restoration.

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

- administrator panel in Tor system;
- communication with the company via Tor, chat room with **PUSH** notifications;
- automatic test decryption;
- automatic decryptor detection;
- port scanner in local subnetworks, can detect all **DFS, SMB, WebDav** shares;
- automatic distribution in the domain network at run-time without the necessity of scripts;
- termination of interfering services and processes;
- blocking of process launching that can destroy the encryption process;
- setting of file rights and removal of blocking attributes;
- removal of shadow copies;
- creation of hidden partitions, drag and drop files and folders;
- clearing of logs and self-clearing;
- windowed or hidden operating mode;
- launch of computers switched off via **Wake-on-Lan**;
- print-out of requirements on network printers;
- available for all versions of **Windows OS**;

Figure 11 – LockBit 2.0 features

As is common with many 'big game hunter' ransomware threats, LockBit and their affiliates (Figure 12) utilize the double extortion tactic, stealing data and threatening its release to encourage ransom payments. The incident involving Accenture, a multinational consulting and professional services firm, is an example of campaign in which LockBit shared details of their victims on a Tor-hosted leak site (Figure 13), along with a timer the counted down to the date and time at which stolen data would be published unless a ransom payment of 50 million USD was received.


WAF HER YERDE AYNI MI?



Creation Date: Dec 05, 2021 • 15:18:09

Publish Date: Dec 05, 2021 • 15:12:16



Search in Indicator

^ v

' Alıntı:

Port nasıl bişi valla hiç bilmiyorum araştırmam lazım. Mesela port sayesinde sitenin veri tabanı çekilirmi? Genişletmek için tıkla ...

Dostum kusra bakma konu yazıyordum cevap veremedim evt sızarsın ama veri tabanları pek bilmiyom gelirmi ama 21. ve .22 portan sisteme bir zararlı yada solucan virusu sokarsan daha etkili olur ve bütün cihazları etkiemek istiyorsa Lockbit'i öneririm bütün sisteme sızıyor oradan yönetici sistem üzerinden diğer cihazlar lockbit gönderiyor yani araştırmam uzun sürmüştü

Aşk haram bize kaptan rotayı çevir hedefe hacking\:/

Figure 12: Threat actor recommends on LockBit affiliates program



accenture.com

Dudos every day. These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you're interested in buying some databases reach us

ALL AVAILABLE DATA WILL BE PUBLISHED !

Figure 13 – LockBit 'Accenture' leak

INITIAL INFECTION

While each affiliate will likely have their own preferred tactics, techniques and procedures (TTP) to distribute LockBit, most big game hunter ransomware groups operate in a similar manner when it comes to the initial intrusion vector.

Phishing

Targeted phishing campaigns remain a useful and most popular method of gaining access to user credentials or delivering a payload to an endpoint.

Vulnerability Exploitation

Many ransomware threat actors continue to target exposed Windows Remote Desktop instances with brute force attacks as well as exploiting known vulnerabilities in exposed network devices such as VPN gateways – Lockbit is not different. In one specific use case, Lockbit observed exploiting a three-year-old vulnerability in Fortinet FortiOS and FortiProxy products, CVE-2018-13379, which allows an unauthenticated threat actor to download system files via specially crafted HTTP requests and, presumably in these incidents, gain access to credentials and subsequently the target network.

Inside Threat Recruitment

Concerningly, in some incidents, reports suggest that LockBit has sought to recruit employees of target networks, which, depending on the insider threat's access, could save the ransomware group a considerable amount of time and effort. While it is hoped that most employees would ignore and/or report any nefarious recruitment attempt, cash-rich ransomware groups will be more than able to offer lucrative incentives that some may find hard to resist, especially if they already have some grievance against their employer.

POST INTRUSION

The objective upon gaining access to the victim network remains consistent: the exfiltration of sensitive and valuable data, prior to encryption, to exert maximum pressure on the victim and encourage prompt payment of any ransom demand.

Persistence

Like many others, Lockbit's persistence includes external-facing remote services to initially access the network such as virtual private networks (VPNs) and Remote Desktop Protocol (RDP) and more.

Defense Evasion

In order to prevent interference with the encryption process, it is typical for ransomware threats to terminate processes or services, such as applications or backup utilities that may 'lock' files open, as well as endpoint security solutions that may detect the threat. LockBit directly calls functions within the Windows API to achieve the same outcome, likely attempting to further evade detection where endpoint monitoring is in place. Subsequently, point-in-time backup copies of data created using the Windows Volume Shadow Copy Service (VSS) are deleted. Aside from utilizing the VSS administrative tool, vssadmin.exe, and the Windows Management Instrumentation utility, wmic.exe, to delete

existing volume shadow copies, the Boot Configuration Data (BCD) editor, bcdedit.exe, is used to ensure that subsequent system boot failures are ignored, and the recovery boot option disabled.

Lateral Movement

LockBit often spreads to other machines within the victim's network via SMB and network shared drives.

ENCRYPTION PHASE

Having prepared for the encryption process, LockBit version 2.0 utilizes an AES encryption algorithm that is performed on files 'in-place' to prevent recovery from disk.

RANSOM NOTE

LockBit usually leaves a precise note with typical private and secured communication channels for negotiations (Figure 14).

All your files have been encrypted by Loki locker!
 All your files have been encrypted due to a security problem with your PC.
 If you want to restore them, please send an email Unlockpls.dr01@protonmail.com
 You have to pay for decryption in Bitcoin. The price depends on how fast you contact us.
 After payment we will send you the decryption tool.
 You have to 48 hours(2 Days) To contact or paying us After that, you have to Pay Double .
 In case of no answer in 24 hours (1 Day) write to this email Unlockpls.dr01@yahoo.com
 Your unique ID is : E587FC94
 You only have LIMITED time to get back your files!
 If timer runs out and you dont pay us , all of files will be DELETED and you hard disk will be seriously DAMAGED.
 You will lose some of your data on day 2 in the timer.
 You can buy more time for pay. Just email us.
 THIS IS NOT A JOKE! you can wait for the timer to run out ,and watch deletion of your files :)
 What is our decryption guarantee?
 Before paying you can send us up to for free decryption. The total size of files must be less than 2Mb (non archived), and files should not contain valuable information.
 Attention!
 DO NOT pay any money before decrypting the test files.
 DO NOT trust any intermediary. they wont help you and you may be victim of scam. just email us , we help you in any steps.
 DO NOT reply to other emails. ONLY this two emails can help you.
 Do not rename encrypted files.
 Do not try to decrypt your data using third party software, it may cause permanent data loss.
 Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 14: LockBit ransom note example

MITRE ATT&CK

Defense-evasion

- Process Injection – T1055
- Impair Defenses – T1562
- Obfuscate Files or Information – T1027

Discovery

- File and Directory Discovery – T1083
- Network Share Discovery - T1135
- Process Discovery - T1057
- Remote System Discovery - T1018
- System Network Configuration Discovery - T1016
- System Network Connections Discovery - T1049

Lateral-Movement

- Remote Services - T1021
- Taint Shared Content - T1080

Execution

- Command and Scripting Interpreter - T1059
- Windows Management Instruments – T1047

Impact

- Data Encrypted for Impact - T1486
- Inhibit System Recovery - T1490
- Service Stop - T1489

PYSA

PYSA, which stands for “Protect Your System Amigo”, has been active since October 2019 and as the new variant of Mespinoza ransomware, PYSA is a RaaS given to anyone who is willing to pay the price while targeting mainly large private organizations and those in the healthcare industry. They have also hit government groups. Over the past couple of months, we have also seen PYSA targeting education groups. The victims suffers the known double extortion technique.

INITIAL INFECTION

PYSA is human-operated ransomware. This means that it has no self-propagation capabilities. The operators of the ransomware deploy the product manually., PYSA is not different to most ransomware and is mainly delivered via common ransomware attack vectors such as phishing campaigns and low-volume, targeted attacks against multiple organizations.

Phishing

Like many other ransomware groups and threat actors in general, phishing and malspam campaigns remain a popular way to infiltrate a victim’s network.

Vulnerability Exploitation

PYSA always looking to improve its method and techniques that do not depend on social engineering. One of these attack vectors is brute force attacks against management consoles, Active Directory (AD) accounts and, of course, Remote Desktop Protocol (RDP) vulnerable hosts.

POST INTRUSION

Persistence, defense evasion and lateral movement are the typical steps taken by PYSA in their campaign in the post intrusion phase. Data the group steals includes customer, employee and financial records, as well as sensitive emails, documents and intellectual property that could be damaging in the hands of competitors or when shared publicly in their underground blog “Leak List” used to publish their victim’s list and shame them if they don’t comply with their demands. Most of the tools used by the group in this phase are very common free, open-source tools.

Persistence

As mentioned, PYSA’s persistence includes full control over compromised hosts via Remote Desktop Protocol (RDP) and obtaining control on Active Directory (AD) and other management consoles. Another very common technique, to gain persistence, is by modifying a victim’s machine registry key to inject the PYSA software into the startup settings.

Defense Evasion

To prevent interference with the encryption process, it is typical for ransomware threats to terminate processes or services, such as applications or backup utilities that may ‘lock’ files open, as well as endpoint security solutions that may detect the threat. Before deployment, PYSA usually uses

PowerShell scripts to close any defense services that might interrupt their work such as Windows Defender, and also deletes shadow copies to prevent restoration of the lost or encrypted data.

Lateral Movement

As mentioned, PYSA use the following free opensource tools in their campaigns:

- **PowerShell Empire** - post-exploitation agent built on cryptologically-secure communications and a flexible architecture [5]
- **Mimikatz** – an open-source application that allows users to view and save authentication credentials like Kerberos tickets [6]
- **PsExec** – PsExec is a light-weight telnet-replacement that lets you execute processes on other systems [7]
- **Koadic** – Windows post-exploitation toolkit [8]
- **WinSCP** - WinSCP is a popular SFTP client and FTP client for Microsoft Windows [9]

These are only part of the toolkit PYSA uses in their campaigns for data exfiltration and lateral movement.

ENCRYPTION PHASE

The PYSA ransomware uses the CryptoPP, an open-source C++ library, for the encryption phase. The ransomware encrypts data by applying hybrid encryption that combines Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) and Rivest, Shamir, Adleman (RSA) encryption algorithms. This maximizes both encryption performance and security.

RANSOM NOTE

PYSA usually leaves a precise note with typical private and secured communication channels for negotiations (Figure 15).

```

Hi Company,

Every byte on any types of your devices was encrypted.
Don't try to use backups because it were encrypted too.

To get all your data back contact us:
kardalkareefhaddad@onionmail.org

Also, be aware that we downloaded files from your servers and in case of non-payment we will be forced to upload them on our website, and if necessary, we will sell them on the darknet.
Check out our website, we just posted there new updates for our partners: http://pysa2bitc5ldeyfak4seeruqymqs4sj5wt5qkcq7aoyg4h2acqieywad.onion/
To go to our site you have to use TOR Browser. Download link: https://www.torproject.org/download/
-----

FAQ:

1.
Q: How can I make sure you don't fooling me?
A: You can send us 2 files(max 2mb).

2.
Q: What to do to get all data back?
A: Don't restart the computer, don't move files and write us.

3.
Q: What if I have no response?
A: Wait and we will answer you in 24 hours.

4.
Q: What to tell my boss?
A: Protect Your System Amigo.

```

Figure 15: PYSA ransomware note example.

MITRE ATT&CK

Defense Evasion

- Impair Defenses - T1562
- Indicator Removal on Host - T1070
- Masquerading - T1036
- Modify Registry - T1112

Credential-Access

- Brute Force - T1110
- OS Credential Dumping - T1003
- Unsecured Credentials - T1552

Discovery

- Network Service Scanning - T1046
- System Network Configuration Discovery - T1016

Lateral-Movement

- Remote Services - T1021

Execution

- Command and Scripting Interpreter - T1059
- System Services - T1569

Impact

- Data Encryption for Impact - T1486
- Inhibit System Recovery - T1490
- Service Stop - T1489

RETIRED GROUPS

SODINOKIBI/REvil

As one of the ransomware groups responsible for one of the most talked-about incidents of 2021, REvil's, aka sodinokibi, big moment was the Kaseya incident [3] where news emerged throughout the day on July 3, 2021, of a seemingly large ransomware attack affecting hundreds of organizations following a software supply chain compromise at the supplier of software to managed service providers (MSPs). The incident was initially compared to the scale of the SolarWinds incident, but, ultimately, was relatively less severe.

REvil was a Russia-based ransomware group that operated ransomware-as-a-service (RaaS) operations from 2019 and was responsible for several major hacks against enterprises such as Apple. After the Kaseya incident, operations by U.S. Cyber Command and a foreign government hacked the gang's servers and blocked its website, according to the Washington Post. Furthermore, two of its main affiliates were arrested, which is also one of the reasons for the group's disappearance.

DARKSIDE/BLACKMATTER

Darkside first emerged in August 2020. Like REvil, Darkside operated an RaaS operation, and its most famous campaign was the Colonial Pipeline in early May. While the US government made significant efforts to find any leads for the ransomware group, Darkside decided to go silent for a while and published a notice claiming that they are retiring. A few months later, a new group emerged named BlackMatter that operates very similarly to the "retired" DarkSide. After further analysis of its infrastructure and samples of different campaigns, a strong link was discovered between Darkside and BlackMatter, suggesting that the latter might be the original DarkSide operators, or at least, other threat actors with direct access to the original code.

Although BlackMatter campaigns were successful, after some time being active, on November 1, they published a notice claiming that they are retiring (Figure 16). It seems that the proven link to DarkSide and a successful counter-campaign against BlackMatter that led to recovering victims' data, drew more attention than desired and led the group to decide to go silent.

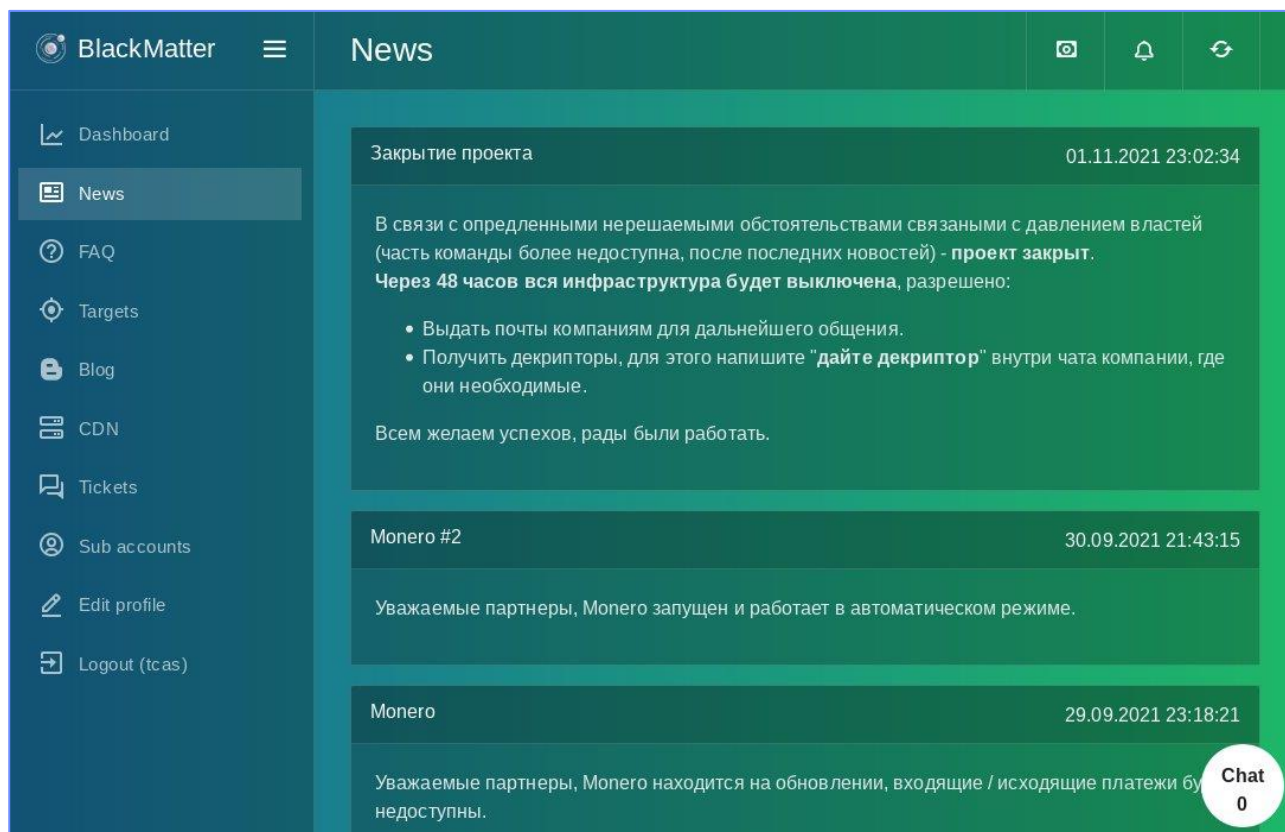


Figure 16: BlackMatter retirement announcement

AVADDON

Avaddon was a ransomware group that also operated an RaaS operation from March 2020. They used to have a dark web presence, where they leaked data stolen from victims' successful campaigns. Avaddon was linked to several sectors in their campaign including energy, finance, tech and more, while one of their most popular cases was the European insurance giant AXA.

When it comes to Avaddon's disappearance, it seems that fear led them to reveal a file containing 2934 victims' decryption keys, and go silent around June. Prior to the revelation, ransom negotiators noticed extreme flexibility and a sense of urgency from Avaddon negotiators, who basically accepted any counteroffer from the victims. It seems that during its operation, Avaddon made around 26 million USD.

NEW PLAYERS

As the market cap of ransomware grew massively over the past years, It is pretty obvious that many threat actors, will look to get into this industry and assemble their own franchise.

KHONSARI

A new family have emerged on December 11th named Khonsari, right after the first publications of the Log4Shell vulnerability (CVE-2021-44228). Khonsari have made a grand entrance with the one of the first ransomware groups to use this vulnerability on their distribution and delivery methods.


Few cases were documented of Khonsari being launched from compromised Minecraft clients.

Khonsari doesn't seem to follow other notorious ransomware groups such as Lockbit and Conti and does not operate a Ransom-as-a-Service (RaaS) enterprise, but rather operating on their own.

Exploiting the Log4Shell vulnerability in their campaigns often leads to downloading Orcus RAT that loads the Khonsari payload. While Khonsari payload is fairly simple to understand, it seems that the files that are being encrypted are added with the ".khonsari" extension. They currently stick to a more "classic" approach of ransomware campaigns and do not operate a leak site or any other "double extortion" techniques for that matter.

AVOSLOCKER

AvosLocker is a relatively new ransomware group that have made a name for itself quick. With 51 cases within the six months, ever since the group was stablished, AvosLocker becoming a growing threat. AvosLocker operates a Ransomware-as-a-Service (RaaS) (Figure 17) operations that was first announced on underground forums, but also on more conventional forums such as Reddit. As the group's first steps within the industry was requiting individuals, one of the assumptions suggest that AvosLocker is not a returning group, but rather threat actors that might have some experience as cybercriminals but not necessarily as a ransomware group.

Partnership Program


AvosLocker Partnership Program

Avos2, AvosLocker's latest Windows variant, is one of the fastest in the market, with highly scalable threading and selective ciphers.

AvosLocker provides the following services & qualities for its affiliates:

- Supports Windows, Linux & ESXi.
- Affiliate panel
- Negotiation panel with push & sound notifications
- Assistance in negotiations
- Consultations on operations
- Automatic builds
- Automatic decryption tests
- Encryption of network resources
- Killing of processes and services with open handles to files
- Highly configurable builds
- Removal of shadow copies
- Data storage
- DDoS attacks
- Calling services
- Diverse network of penetration testers, access brokers and other contacts

We don't allow attacks to post-Soviet Union countries.


Terms and conditions are determined individually.


Contact Information

- XMPP: avos@thesecure.biz | avos@strong.pm
- Tox: 9A751AC90A5F020521EE40D58208C272BD18D2E0C934AB6DA9B918627578095CD9847E24CE59


Figure 17: AvosLocker affiliate program

AvosLocker doesn't try to come with anything new but rather utilize the best techniques other groups have succeeded with such as using Safe Mode to bypass endpoint security – a technique that was very popular with BlackMatter and REvil. Given that AvosLocker is a new group that have relatively succeeded in the ransomware business, we have witnessed great number of discussions regarding the group and its actions by allegedly new threat actors that are looking to start their way in cybercrime as well (Figure 18), while AvosLocker seems like something more appealing to the new threat actors rather than the bigger groups such as Conti or Lockbit.


ВЫМОГАТЕЛЬ-НОВИЧОК AVOSLOCKER ЗАПУСКАЕТ ANYDESK В БЕЗОПАСНОИ



Creation Date: Dec 24, 2021 • 14:49:51
Publish Date: Dec 24, 2021 • 14:48:56


Search in Indicator

ЕМНИП, ТимВьюер пароли в реестре хранит.
Помню, ещё во времени ВинХП была в моде следующая тема: патчить ТимВьюер, чтобы чуть-чуть изменить алг сохранения пароля. Все стилаки, очевидно, становятся бесполезными

Figure 18: Discussion found on Argos Edge™ regarding AvosLocker by relatively new threat actor

PREDICTIONS FOR 2022

Given the enormous financial gains that these ransomware groups are making, there is ample funding for innovation and the evolution of their threat, be that the development of new and improved ransomware encryption capabilities or the recruitment of individuals with intrusion skills to target new victims.

INFORMATION SHARING

While many groups may be 'competitors', effective tactics, techniques and procedures (TTP) are seemingly adopted by others, for example, the widely used 'steal, encrypt and leak' tactic was first credited to 'Maze Team' in November 2019 and is now employed by most big game hunter groups. Another great example is the Log4Shell vulnerability exploitations in Conti and the new Khonsari team campaigns. This successful exploitation is noticeable to other ransomware group and is obvious that efforts are made to weaponize their campaigns with this valuable method.

ADAPTABILITY

Due to the better awareness and solutions for ransomware, It is very likely for threat actors in the coming year to look for more creative ways to utilize their attacks. as such, we might see campaigns in a different model as extortion for data leakage without the encryption phase.

Many of the victims in the past year had recovery and backup services. Still, they paid the requested ransom to prevent the data from being published, which acts like another good reason for big game hunters to migrate to this nature of extortion. We have seen these roots of extortion method back in 2020 in which 'REvil', also known as 'Sodinokibi', introduced an auction feature on their leak site to bid directly on stolen data. Aside from putting additional pressure on victims, this tactic may even encourage a victim to bid on their data to secure it and, in the event of a ransom not being paid, may provide the threat actor with some financial compensation for their 'efforts'.

Subsequently, we have witnessed cases in which major threat groups shared details of their ransomware victims on their leak site. This 'cartel' increases the number of potential victims and leaks that, in turn, applies more pressure on new victims leading to an increased chance of success for all cartel members.

NEW EXTORTION METHODS

A use-case we witnessed on a much smaller scale are scenarios in which threat groups have notified potential victims they are about to be attacked while presenting terms and payment to evade this situation - modern 'Protection' payments. Although, these types of threats typically are of DDoS attacks, it is not far fetch that ransomware groups will look to at least try some campaigns in the coming year applying this method.

BUSINESS VS LAW AUTHORITIES CONFLICT

As ransomware has become more popular, spreading over regions and sectors, a new challenge arose as a result of conflict between law enforcement authorities and organizations that were attacked successfully by ransomware, while the former urge the victims to refuse corporate or negotiate with the ransomware groups and the latter interests is to mitigate and restore the stolen data and the organization's actions on track as soon as possible.

While we have observed cases in which threat actors restored only around 60% of the stolen data once the ransom was paid in 2020, ironically, they have improved their "reliability" while restoring much higher percentage, around 90%, to the victims. This situation draws a picture for organizations that in a case of ransomware the more reliable way for them to get their data back is by paying the ransom rather than address the authorities, encouraging more threat actors to get into this business and veteran threat actors to continue their line of work.

IS IT ALL ABOUT THE MONEY?

The fact that ransomware incidents and new groups will arrive this year is obvious. Although it seems like financial gain is the main reason for threat actors to get into this business, winds of change in the way some communities address to ransomware threat actors might lead to more reasons. With underground interviews with major threat actors, even if it's in a context of "know what we are dealing with", those figures get the spot of "underground rockstars" and much attention with growing fan base, leading to a new aspect to get into the ransomware business – fame and ego.

RECOMMENDATIONS

These days, any organization, find itself needing to protect both their corporate IT infrastructure or cloud service network, as well as the account security of their customers. Based on previous incidents, threat actors typically gain access using common attack tactics, techniques, and procedures (TTP) before attempting to move laterally and/or act on their objectives.

EMPLOYEE AWARENESS

Given the current global situation with potentially increased remote working, now, more so than ever, security awareness training is an important step in ensuring that those on the front line are able to spot and stop attacks in their tracks. As many employees work from home or adapt to increased online habits, they should be reminded to be suspicious of any unsolicited or unusual communication, especially those containing attachments of links, as well as being mindful of any websites they visit using corporate assets. Furthermore, a repetitive reminder of the importance of the matter, and the consistently use of VPNs for work purposes might help keep employees alerted and aware of the threats of working from home.

PREVENT CREDENTIAL MISUSE

Given that many attacks continue to rely on the abuse of legitimate credentials, the implementation of multi-factor authentication (MFA) prevents threat actors from abusing stolen credentials without access to the 'token', be that physical hardware or software-based solution.

In addition to protecting credentials from brute-force and stuffing attacks, MFA can limit the effectiveness of social-engineering where a threat actor may attempt to gain access to high privilege user accounts. Employees should also be reminded to practice good credential hygiene, such as not reusing credentials, as well as due consideration being given to the security of any stored credential, such as within applications that may not use, or properly implement, encryption. Organizations making use of corporate social media accounts, and similar shared services, should also ensure that, where possible, MFA is enabled and consider the use of credential management tools that can provide an audit trail of credentials use.

PRACTICE LEAST PRIVILEGE

To limit the impact of any credential compromise, the enforcement of least privilege policies can prevent day-to-day accounts being compromised and used to gain elevated access to other systems. As such, organizations should ensure that devices, services and users only have the privileges required to perform their function, effectively segregating and limiting access.

MONITORING

Through the continuous monitoring of endpoint security events, organizations can maintain visibility of their environments and identify suspicious activity before it becomes a problem. Activity such as unexpected connections to external SMB servers, or other suspicious network traffic, can be

indicative of malicious intent as well as observed behaviors such as mass file operations, be they creation, modification or deletions, or event logs being cleared.

THREAT INTELLIGENCE

Maintaining awareness of current events, threat actor tactics, techniques, and procedures (TTP), and new threats can be achieved through the consumption of tactical and strategic threat intelligence. In turn, this can help organizations and cybersecurity teams to focus their efforts in the appropriate areas and mitigate cyber risks.

THIRD PARTY SECURITY

As mentioned, the rise of cloud services and third party services demands an organization to be alerted and to monitor the security and data leakage defense measures these services apply to secure their networks, processes and APIs.

PATCH MANGAMENT

Tried and tested techniques continue to be employed by threat actors including the exploitation of common vulnerabilities in exposed systems and end-point applications. As such, organizations should first secure the 'low-hanging fruit', ensuring that office and productivity applications are regularly updated and patched whilst end-of-life versions are phased out. Additionally, when considering update and patch management processes, attention should be given to internet-facing infrastructure due to the ever-increasing threat of targeted ransomware groups, that are conducting successful 'steal, encrypt and leak' operations against organizations of all sizes worldwide. When applying updates or patches, these should only be obtained from verified legitimate sources, such as the original vendor, and not third-party sources. Additionally, where possible, the validity of any patch should be checked against published checksums or digital signatures prior to execution or application.

SECURE SENSITIVE DATA

Aside from meeting any legal or regulatory requirements for data storage, such as to comply with PCI DSS, data leaked from numerous targeted ransomware victims has included infrastructure documentation and credentials within files that can subsequently be abused and used to compromise further systems. Sensitive data should be always be adequately encrypted and stored securely to prevent unauthorized access, which, even in the event of data theft, will render the data inaccessible to the threat actor.

APPLICATIONS PERMISSIONS LIST

The use of application permit and deny lists can detect and prevent the execution of unauthorized or unknown executables, effectively hardening an operating system against attack. When used in environments that have limited change, such as on web servers or appliances such as ATMs, a baseline can be generated and any subsequent attempt to launch an executable file, be that from another location, or a modified file, can be denied. Furthermore, denying the execution of administrative tools

by standard user accounts can prevent their misuse by threat actors. Commonly abused tools include command and script interpreters, used to execute payloads, as well as utilities used to disable security settings or remove backup files, as seen in ransomware attacks, such as the 'Volume Shadow Service Admin Tool' (vssadmin.exe) and 'Windows Backup' (wbadmin.exe).

NETWORK SEGREGATION

The use of appropriate network segregation, often by creating separate logical segments for assets that share a similar risk profile and limiting communications, especially between endpoints, allows attacks to be contained and provides damage limitation, preventing threats from propagating further across an organization.

EMAIL SECURITY

Aside from robust email security controls to limit the delivery of potentially malicious attachments to end-users, organizations should ensure that they take advantage of email security protocols and methods to validate email senders such as Domain-based Message Authentication, Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and the Sender Policy Framework (SPF).

RECOVERY AND BACKUP

As well as the threat of ransomware, destructive malware could be deployed in a disruptive nation-state sponsored attack. As such, it is imperative that organizations have procedures in place to regularly backup and verify the integrity of their data, as well as performing periodic exercises to ensure that disaster recovery plans work in practice. Additionally, given that many attacks move laterally across networks, backups should not be solely stored on an 'online' system; both offline and offsite storage, if regularly updated, can facilitate the restoration of services in the event of a large-scale catastrophic incident, potentially even allowing restoration to a 'stand-by' site that can provide business continuity.

REFERENCES

- [1] <https://cyberint.com/blog/research/emotet-returns/>
- [2] <https://cyberint.com/blog/research/cve-2021-44228-log4j2-rce/>
- [3] <https://cyberint.com/blog/research/msps-targeted-in-ransomware-attack/>
- [4] <https://cyberint.com/blog/research/cve-2021-34527-printnightmare-vulnerability/>
- [5] <https://www.powershellempire.com/>
- [6] <https://github.com/ParrotSec/mimikatz>
- [7] <https://docs.microsoft.com/en-us/sysinternals/downloads/psexec>
- [8] <https://0x1.gitlab.io/exploitation-tools/Koadic/>
- [9] <https://winscp.net/eng/>

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City