MANDIANT

One Source to Rule Them All: Chasing AVADDON Ransomware

ADRIAN SANCHEZ HERNANDEZ, PAUL TARTER, ERVIN JAMES OCAMPO

JAN 19, 2022

MANAGED DEFENSE

The ransomware-as-a-service (RaaS) model is lowering the barrier of entry into the cybercrime world, causing the number of ransomware attacks we're seeing to spike higher than ever before.

In the last few years, ransomware has become one of the principal sources of income in the cybercrime ecosystem, with increased use of extortion by shaming victims, threatening to release exfiltrated data, and in some cases hitting them with distributed denial-of-service (DDoS) attacks.

This blog post explores activity, similarities and overlaps between multiple ransomware families related to AVADDON ransomware, serving as a case study to understand how ransomware operators think and continue to turn a profit in a constantly evolving cybercrime ecosystem.

Various RaaS services have prevailed in compromising critical targets, leading to major impacts on victim networks and to sizable ransom demands. AVADDON is one of these ransomware services.

The threat actor behind the AVADDON ransomware service started activity in June 2020 and continued operations until June 2021. The service was apparently shut down rapidly—and private encryption keys released—as governments prioritized the fight against ransomware operations with new legislation and increased law enforcement operations.

Mandiant has observed notable overlaps between AVADDON and other ransomware families, indicating the possibility of rebranding in order to reintroduce itself into the RaaS business. Based on the profitability of these operations, it is almost certain that numerous threat actors will continue to conduct ransomware operations.

Victimology

Destructive attacks leveraging AVADDON ransomware have affected a wide variety of industries. Based on publicly named victims on AVADDON's own blog post and Mandiant's incident response investigations, we have observed AVADDON impacting industry verticals primarily based in North America, including education, technology, healthcare, financial and government.

Based on open-source data, AVADDON released nearly **3,000 private encryption keys**, indicating that targeting is almost certainly broader than directly observed.

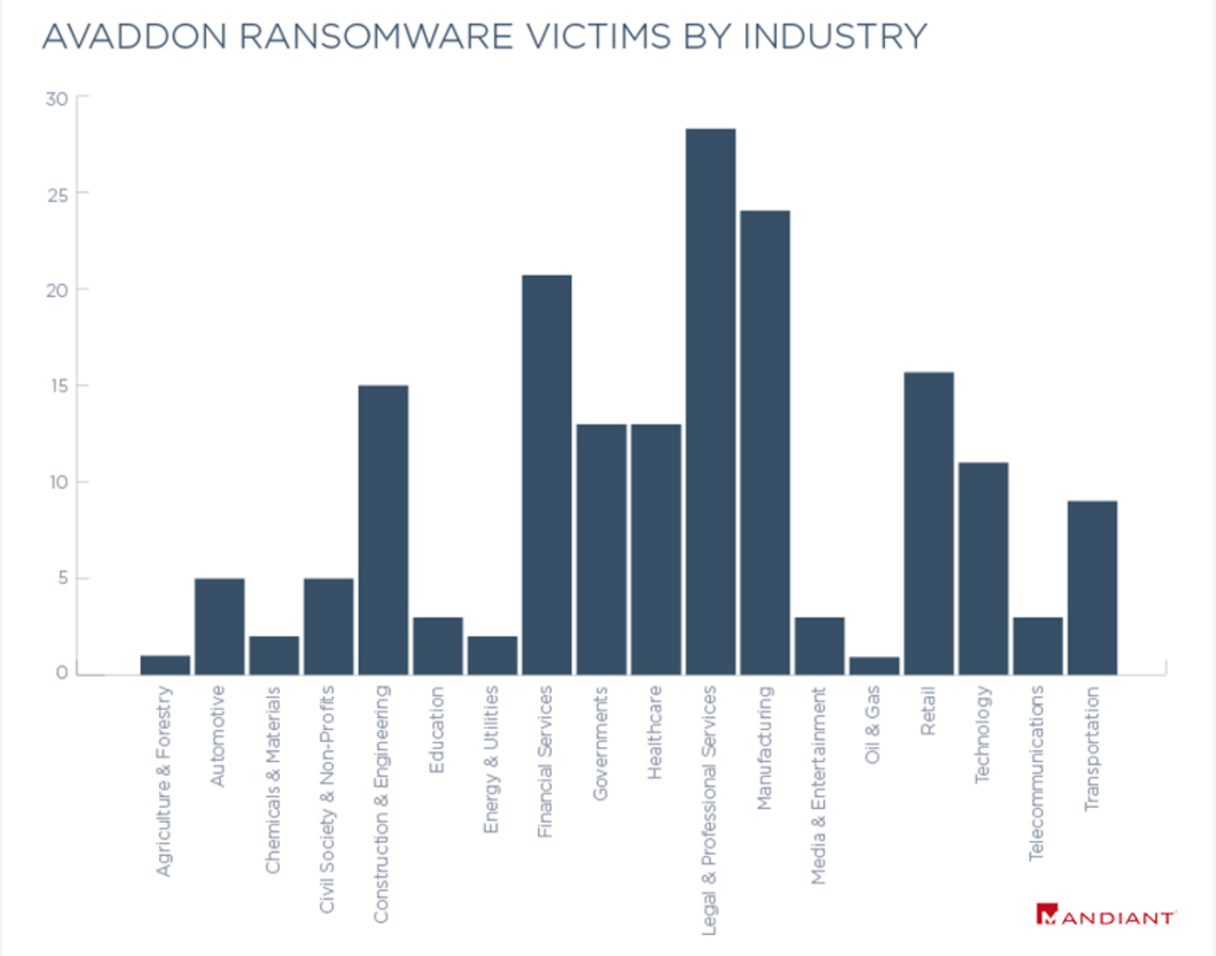
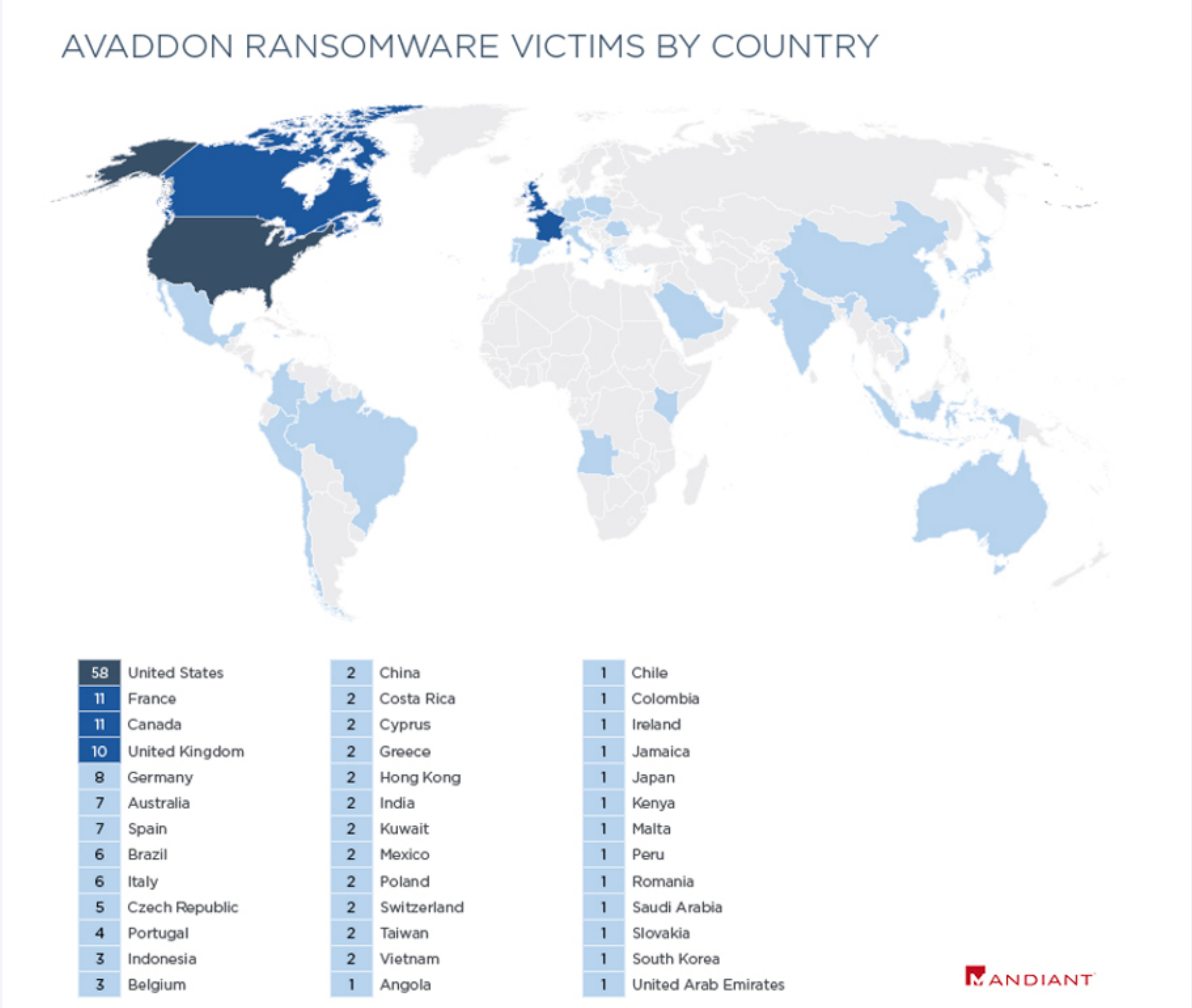


Figure 1: Industries impacted by AVADDON ransomware based on publicly named victims

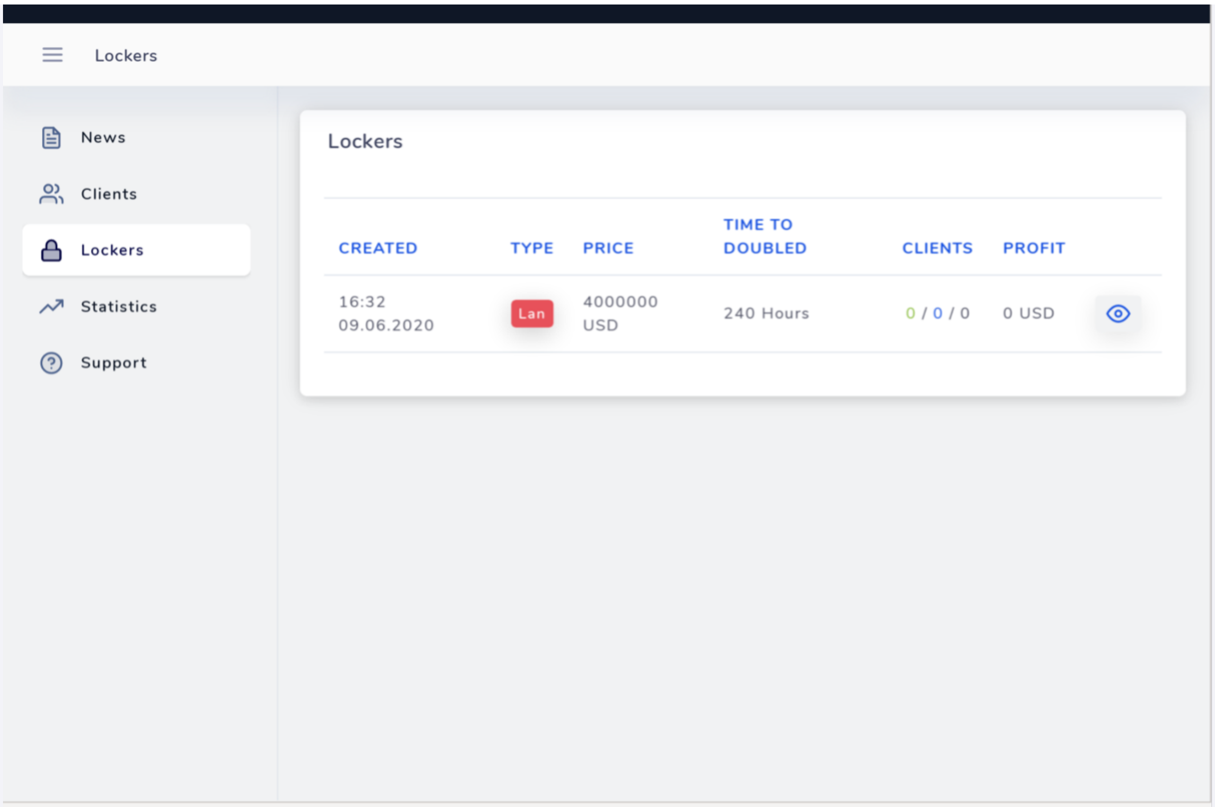


58	United States	2	China	1	Chile
11	France	2	Costa Rica	1	Colombia
11	Canada	2	Cyprus	1	Ireland
10	United Kingdom	2	Greece	1	Jamaica
8	Germany	2	Hong Kong	1	Japan
7	Australia	2	India	1	Kenya
7	Spain	2	Kuwait	1	Malta
6	Brazil	2	Mexico	1	Peru
6	Italy	2	Poland	1	Romania
5	Czech Republic	2	Switzerland	1	Saudi Arabia
4	Portugal	2	Taiwan	1	Slovakia
3	Indonesia	2	Vietnam	1	South Korea
3	Belgium	1	Angola	1	United Arab Emirates

Figure 2: Heatmap of publicly named AVADDON victims by country

AVADDON Ransomware Service

In June 2020, Mandiant reported the Russian-speaking threat actor **"Avaddon" advertising the AVADDON ransomware** affiliate program (RaaS) on the Russian-speaking forums exploit[.]in and xss[.]is. In March 2021, the threat actor Avaddon posted an update for the AVADDON RaaS to announce the development of AVADDON V2 and later that same year incorporated a DDoS feature designed to pressure victims into paying the ransom.



Lockers

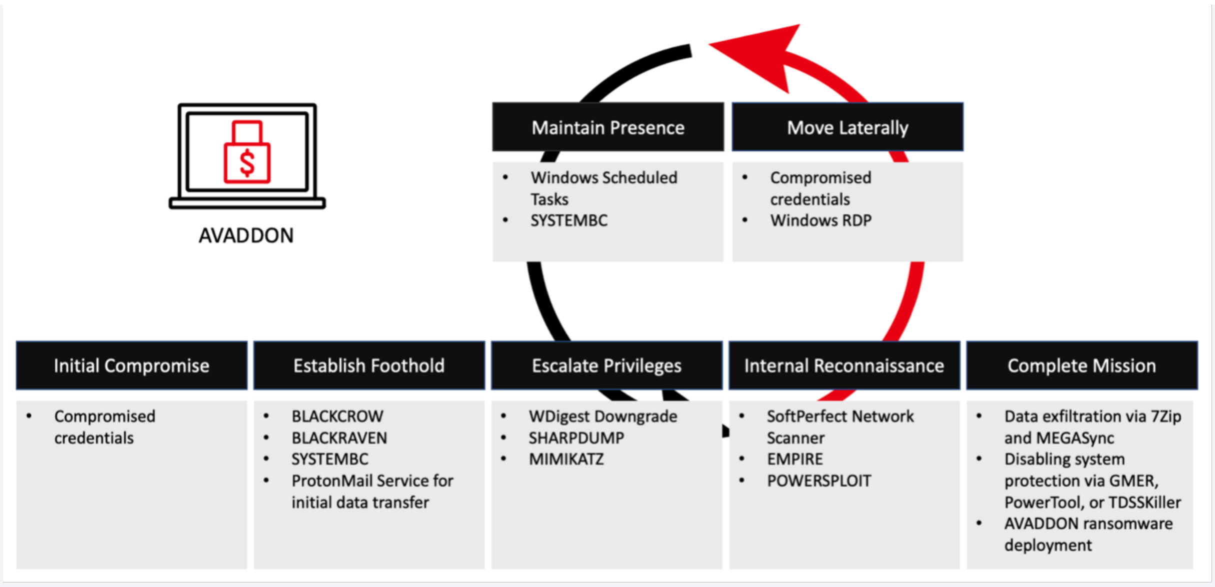
CREATED	TYPE	PRICE	TIME TO DOUBLED	CLIENTS	PROFIT
16:32 09.06.2020	Lan	4000000 USD	240 Hours	0 / 0 / 0	0 USD

Figure 3: AVADDON affiliate panel

The AVADDON panel seen in Figure 3, was hosted on a TOR hidden service (.onion domain) and was provided to AVADDON affiliates in order to monitor victims and their payments, track builds, provide a support ticketing system, and view statistics and related news publications. As typical with RaaS operations, AVADDON profits are divided according to their Terms of Service specified by the AVADDON operators, initially structured with 65% profit earned for the affiliate and 35% for the operators of the ransomware service (this is subject of change by the RaaS service). However, this could vary depending on the number of victims per affiliate, meaning that the profit percentage for the affiliate could be higher if the number of intrusions increased considerably.

AVADDON Affiliates

Mandiant identified multiple AVADDON affiliates involved in targeted destructive attacks leveraging AVADDON ransomware.



AVADDON

Maintain Presence
- Windows Scheduled Tasks
- SYSTEMBC

Move Laterally
- Compromised credentials
- Windows RDP

Initial Compromise
- Compromised credentials

Establish Foothold
- BLACKCROW
- BLACKRAVEN
- SYSTEMBC
- ProtonMail Service for initial data transfer

Escalate Privileges
- WDigest Downgrade
- SHARPDUMP
- MIMIKATZ

Internal Reconnaissance
- SoftPerfect Network Scanner
- EMPIRE
- POWERSPLOIT

Complete Mission
- Data exfiltration via 7Zip and MEGASync
- Disabling system protection via GMER, PowerTool, or TDSSKiller
- AVADDON ransomware deployment

Figure 4: TTPs seen through AVADDON ransomware incidents

These attacks employed various tactics, techniques, and procedures (TTPs), including:

- Compromised credentials from prior intrusions. In one instance, Mandiant observed evidence of an AVADDON affiliate working with an initial access broker to gain initial foothold in a victim's environment.
- Custom malware such as BLACKCROW and DARKRAVEN web shells to maintain access and interact with a compromised server.
- Publicly available remote administration tool SYSTEMBC for interacting with compromised hosts.
- Windows Remote Desktop Protocol (RDP) for lateral movement.
- WDigest downgrade attack in conjunction with SHARPDUMP or MIMIKATZ to dump clear-text credentials from memory.
- Open-source frameworks and scripts such as EMPIRE and POWERSPLOIT for post-exploitation activity.
- Windows Scheduled Task for persistence.
- Publicly available scanning tools such as SoftPerfect Network Scanner for internal reconnaissance.
- Publicly available rootkit removal tools such as GMER, PowerTool, and TDSSKiller to disable system protection software.
- ProtonMail service to send and receive data initially at the early stages of the intrusion.
- Publicly available archiving tool 7Zip and cloud storage synchronization tool MEGAsync for data staging and exfiltration.

From the TTPs, Mandiant has observed heavy reliance on open-source and publicly available tooling for different purposes across various stages of the intrusion.

Connecting the Dots

Mandiant continues to observe sophisticated TTPs and increased collaboration between different and specialized threat actors, each playing a particular role within the intrusion operation and has observed previous cases of rebranding where a new ransomware service aligns with another, suggesting collaboration between ransomware operators.

Mandiant has reported on multiple cases of potential rebranding and links between RaaS such as **BLACKMATTER** and **SABBATH** ransomware families and reported on the possibility of rebranding on **AVADDON** as the RaaS shut down.

Threat actors behind a RaaS may choose rebranding for a variety of reasons including fixing operational security flaws and the perception of reducing the risk of law enforcement disrupting their operations.

Mandiant has tracked AVADDON and analyzed its multiple versions along with potential ransomware families with which it shares similarities. In April 2021, Mandiant identified numerous ransomware services advertising in Russian-speaking underground forums, using assorted brands, yet having certain degrees of relations with AVADDON as far back as 2019, as seen in Figure 5.

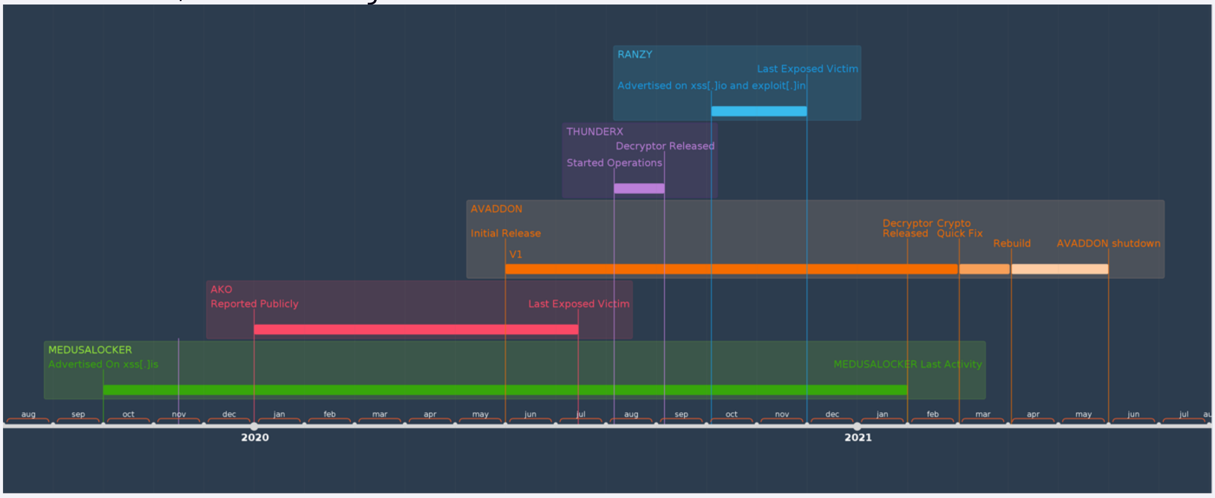


Figure 5: RaaS activity timeline based on forum activity, reported victims and PE timestamps

Mandiant has observed previous RaaS services operating since 2019 to 2021 connected to AVADDON source code. The variations among these ransomware families show an increase in maturity as the final product is improved in terms of performance and cryptographic functionality.

The timeline of these services and the similarities in the code may be part of the rebuilding process, suggesting collaboration between threat actors or access to a shared source code by multiple threat actors.

MEDUSALOCKER is ransomware that was advertised on the Russian-speaking forum xss[.]is by the threat actor 'Scourge' and reported by **Mandiant** in October 2019. During 2020, the service continued to be active and was updated with new versions of the ransomware. The last activity from the threat actor in the forum was in February 2021.

Ako, also known as MedusaReborn, is ransomware that was initially observed around **January 2020**. Ako operations **continued to be active during 2020** and their last publicly exposed victim was added to their shaming blog in July 2020. Mandiant determined that Ako ransomware shares numerous similarities with MEDUSALOCKER and considers Ako to be a variant of MEDUSALOCKER.

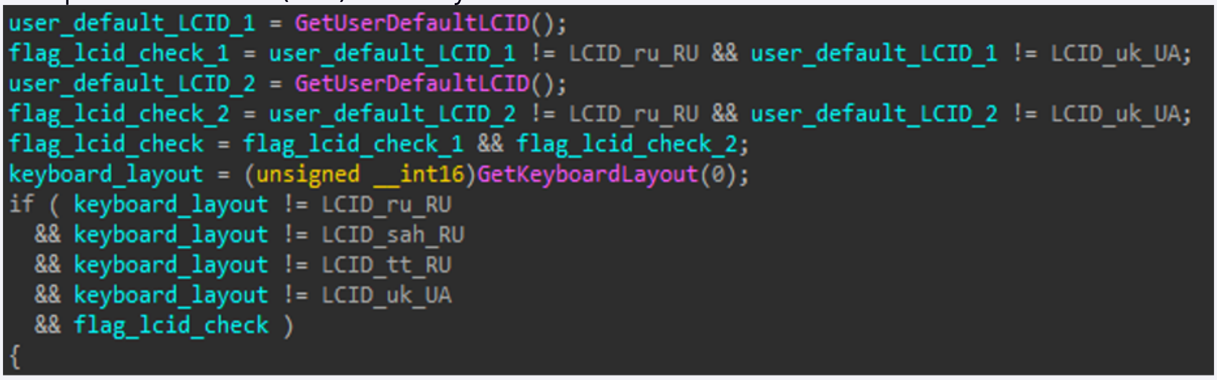
ThunderX is a ransomware that started operating in August 2020 according to PE timestamps and **public reports**. However, in September 2020, Tesorion **released** a free decryptor that appears to have interrupted ThunderX operations. Mandiant determined ThunderX and RANZY to be a single malware family due to numerous similarities and code overlap.

RANZY, also known as "Ranzy Locker", is a ransomware that was advertised on the Russian-speaking forums xss[.]is and exploit[.]in by the threat actor "Ranzycorp" in October 2020. RANZY has impacted multiple victims since late 2020, however, Mandiant did not observe publicly named victims on its shaming blog or activity in these forums in 2021.

AVADDON Ransomware Analysis

AVADDON encrypts files stored locally and on mapped network shares. It stops targeted processes and services prior to encrypting files. Mandiant has observed three major release versions that can be seen in Figure 5, for further detail on differences in encryption methodology, see the section AVADDON Encryption Evolution.

The ransomware contains host reconnaissance capabilities to retrieve the system's Language Code Identifier (LCID) and keyboard layout (Figure 6) and exits if the following languages are found: Russian, Ukrainian, Tatar (Russian) or Sakha (Russian). This is consistent with one of the mandatory policies to which AVADDON affiliates must adhere: the total prohibition of ransomware operations within the Commonwealth of Independent States (CIS) territory.



```
user_default_LCID_1 = GetUserDefaultLCID();
flag_lcid_check_1 = user_default_LCID_1 != LCID_ru_RU && user_default_LCID_1 != LCID_uk_UA;
user_default_LCID_2 = GetUserDefaultLCID();
flag_lcid_check_2 = user_default_LCID_2 != LCID_ru_RU && user_default_LCID_2 != LCID_uk_UA;
flag_lcid_check = flag_lcid_check_1 && flag_lcid_check_2;
keyboard_layout = (unsigned __int16)GetKeyboardLayout(0);
if ( keyboard_layout != LCID_ru_RU
  && keyboard_layout != LCID_sah_RU
  && keyboard_layout != LCID_tt_RU
  && keyboard_layout != LCID_uk_UA
  && flag_lcid_check )
{
```

Figure 6: Checks against language and keyboard layout passlist; AVADDON will exit if any of the languages are detected

AVADDON operates similarly to other ransomware samples and contains an embedded configuration. AVADDON's configuration is stored in the form of global stdstring variables that are initialized prior to main as a C++ global initializer. The strings are decoded as they are needed during execution. All configuration encoding is performed using Base64 and multiple iterations of arithmetic operations utilizing a hardcoded single-byte key that varies per binary. Figure 7 is an example python script used for decoding configuration data found in sample hash (MD5:ae663fa3b803d8c23e98373fa3f66d21).

Figure 7: AVADDON string decoding function

```
from base64 import b64decode
```

```
def decode_string(b64_string):
    return ''.join([chr(((x-5)^0xb3)&0xff) for x in b64decode(b64_string)])
```

AVADDON’s execution flow begins by stopping and deleting services and processes that might interrupt its operation (Figure 8). Next, the configuration runs multiple commands that prevent a user from restoring from backup (Table 1**)**. Finally, the ransomware begins its encryption operation by recursively iterating local drives and network shares while avoiding directories (Figure 9) and files with specific extensions (Figure 10).

AVADDON searches the following strings related to virtual machines, backups and antivirus services to stop and delete them:

Figure 8: Services to stop and delete

```
ccEvtMgr
ccSetMgr
Culserver
dbeng8
dbsrv12
DefWatch
Intuit.QuickBooks.FCS
msmdsrv
QBCFMonitorService
QBIDPService
RTVscan
SavRoam
sqladhlp
SQLADHLP
sqlagent
sqlbrowser
sqlservr
sqlwriter
tomcat6
VMAuthdService
VMnetDHCP
VMUSBArbService
vmware-usbarbitator64
vmware-usbarbitator64
VMwareHostd
```

The following processes are stopped. The ransomware stores a short-hand form of the full process name, but it does not appear to be used during process identification or termination.

Table 1: Processes to terminate

Process Name	Short Form

360doctor.exe	0doct
360se.exe	0se.e
axlbridge.exe	lbrid
Culture.exe	lture
Defwatch.exe	fwatc
fdhost.exe	host.
fdlauncher.exe	launc
GDscan.exe	scan.
httpd.exe	tpd.e
MsDtSrvr.exe	DtSrv
QBCFMonitorService	CFMon
QBDBMgr.exe	DBMgr
QBIDPService.exe	IDPSe
qbupdate.exe	updat
QBW32.exe	W32.e
RAgui.exe	gui.e
RTVscan.exe	Vscan
sqlbrowser.exe	lbrow
sqlmangr.exe	lmang
sqlservr.exe	lserv
supervise.exe	pervi
winword.exe	nword
wxServer.exe	Serve

wxServerView.exe	Serve
tomcat6.exe	mcat6
java.exe	va.ex
wdswfsafe.exe	swfsa

AVADDON deletes the Windows shadow volumes and empties the recycle bin to avoid file recovery. Next, it executes the anti-recovery commands in Figure 9. Finally, to prevent the system from restarting, AVADDON leverages the Windows Restart Manager by adding files actively being encrypted to the Restart Manager registry.

Figure 9: Anti-recovery commands

```
wmic.exe SHADOWCOPY /nointeractive
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -d
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
vssadmin.exe Delete Shadows /All /Quiet
```

The following directories are excluded from the encryption process and are consistent across different versions of AVADDON.

Figure 10: Directories excluded from encryption

```
C:\Windows
C:\Program Files
C:\Users\All Users
C:\Users\Public
C:\Users\user\AppData\Local\Temp
C:\Program Files (x86)
C:\Users\user\AppData
C:\ProgramData
C:\Program Files\Microsoft\Exchange Server
C:\Program Files (x86)\Microsoft\Exchange Server
C:\Program Files\Microsoft SQL Server
C:\Program Files (x86)\Microsoft SQL Server
```

Additionally, directories containing the following keywords are excluded.

Figure 11: Directories containing these keywords are also skipped

```
SYSTEMDRIVE
USERPROFILE
PROGRAMFILES(x86)
ProgramData
Program Files
ALLUSERSPROFILE
```

```
AppData
PUBLIC
TMP
Tor Browser
MSOCache
EFI
```

When encrypting the filesystem, the following extensions are excluded to ensure the system can be recovered after paying the ransom with the provided decryptor.

Figure 12: File extensions excluded

```
.bin
.sys
.ini
.dll
.lnk
.dat
.exe
.drv
.rdp
.prf
.swp
.mdf
.mds
.sql
```

Host Survey

The ransomware includes a host survey as part of the ransom note. The host survey is comprised of two parts that are separated by a hyphen character and then Base64 encoded. The first part is a plaintext victim id, the second part is an RSA encrypted JSON structure of data containing the fields in Figure 13.

Structure	Description
ext	Encrypted file extension
rcid	AES key and file extension encrypted with RSA key and stored in hex format
hdd	Detected and connected drives to the host
hdd.name	Drive letter A-Z
hdd.size	Drive size in GB
hdd.type	Drive type local/network

lang	Default locale language
name	Hostname

The following is an example JSON string containing the information gathered from the compromised system. This JSON string is not written to disk and is only stored in memory.

Figure 14: JSON blob containing host, user and encryption details

```
{
"ext": ".eDDDbCADB",
"rcid":
"796249FF39A076F96C3261D0913FEEF832759C1D2CA83DA9AF38D582B8C3E638E71F73
206D405BC60C0DFBC18DF9E0E8C404F8FE396D60BF7C478F0B74ACF678A163BC021AC5
3
82F683088E871687EF1F5D70E137152B90C4F5FB025CFF70DBC679259B2DAEE3A76D2AB
C5B6FD8CB1B7105DAD21D816A736239500BEB95BFA2538A5732A660B31571D36E22C5
5
E7C1B86B94B31D1208C1D6D077A2D52F65FD12F8A1E18FD63557DA0FEAF2781694DEC
D
7BA0080464401EBBED45E2213B15D868DF2384D0369D50BA075EDB852AFB8406D735B
0
0EBD56A73FEB304F18B9A92C63C333A1CB90E2AFBFFDD1F4B1666BF37F8B75A7DD3014
A3A00F8C4FC09589B186F498C9ACC510EA05B7BA3C5BA44723DEE00CC905230AB6E4C9
0C6DA3F703CD3AAE1003479DBF4707E2060BCC2E1316E4C05BFBAEB508C6A99107042D
37C92B50E468D805C67690788AC6B6A1A1BDEE3C2F87236F74A2868AA76E48E010F8C4
CDB998DEE1C47C946BAF596D315C1AB40D14A3E248072F5677D0CE5B1C3621F753E466
AD438ABA7726CC46C85F697890BEC2F414D18B752180721D4E05B496790FFE45C505D9
756ABE6368CFE6D89EE36013A6BB20D7B27613D275E7D7AD2B7EA1FED7D729526F5D7
D5E58AF3A90F01A2F0C257842D8B9909EA32FC82ED8D2A6B8361E058CBA08BA43C633F
1F9B37E96671DFBBB3F0B8F80A7CB0271FA66990F30",
"hdd": [{
"name": "C",
"size": 118,
"type": "local"
    },
    {
"name": "D",
"size": 0,
"type": "local"
    }
  ],
"lang": "English",
"name": "DESKTOP-AA1OUBT"
}
```

Earlier builds of AVADDON ransomware had a **User Access Control (UAC) bypass module to abuse CMSTPLUA COM interface**. This UAC bypass is common and has been used by multiple ransomwares such as **DARKSIDE** due to its easy implementation and the availability of public Proof of Concept (PoC) code. AVADDON added modifications over time and removed the UAC bypass.

AVADDON Encryption Evolution

Initially, AVADDON generated a single AES-256 key residing in memory during the encryption process, this key would stay resident until the process exited and was used to encrypt every file. This allowed researchers to develop a decryptor tool released in February 2021 on **GitHub,** abusing this flaw and dumping the cryptographic materials from the suspended process. Developers of the ransomware fixed this issue by generating a single AES key per file being encrypted.

AVADDON, when initially released, used a single AES key for encrypting all files. There are three ways to recover a file's AES session key:

- The ransom note, as part of the victim ID, requires attackers' private RSA key.
- Each file has a footer appended that contains the session key used to encrypt the file. The key can be extracted with the private RSA key.
- Find the session key resident in memory.

AVADDON later moved to using a "one key per file" method which resolved the third item of finding a key resident in memory. The other two methods require a private key and are therefore protected. One interesting note: the AES key generated and stored in the ransom note for later versions is never used, only the session keys stored in the file are correct, this is remnant of moving to a "one key per file" methodology vs a single key that could be stored once.

Analysis across AVADDON samples containing the file encryption fix showed the replacement of the used C++ structures for global variables indicating a quick fix was made by the threat actors developing AVADDON.

Samples observed later in 2021 with PE timestamps of April 2021 include improvements such as the addition of IOCompletionPort multithreading and the replacement of these global variables again for structures just like the original release.

This indicates that the threat actor implemented a quick fix after the release of the PoC decryptor to continue with the operations while improved and more consistent versions of the software were under development.

Additionally, latest versions of AVADDON had a function to force the restart of the victim host in safemode prior to encrypting the filesystem by providing the command line parameter "-safe" to the encryptor executable; mimicking other RaaS services that implemented similar features in attempt to bypass Antivirus and EDR software.

Ransomware Similarities and Technical Comparison

Mandiant analyzed multiple samples of MEDUSALOCKER, Ako, ThunderX, AVADDON and RANZY, finding multiple similarities between these ransomwares including the programming language, code similarities and functionalities, many of these can be observed in Figure 15.

Additionally, there's a significant overlap in their infrastructure as Ako and RANZY used the same Tor onion address 7rckgo66iydpvgpwve7b2el5q2zhjw4tv4lmyewufnpx4lhkekxkoqd[.]onion.

This Tor site was used for the purposes of shaming victims and coercing them to pay ransom demands, showing another degree of relationship between them.
Similar PDB strings have been seen across multiple samples of MEDUSALOCKER, ThunderX (MD5: fedadfa6ce199900ca0a6a1f588f8beb), RANZY (MD5: d3774470f4a1b2451fb314d6c37a7763) and in a sample of AVADDON decryptor (MD5: 01422fd3eec0d1a0ce238df01edf8a50) contributing to show potential links between them.
Note that both ThunderX and RANZY share the same PDB string.
Example PDB paths:

- C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject\MedusaLocker\Release\MedusaLocker.pdb
- C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject\MedusaLocker\Debug\MedusaLockerXP.pdb
- C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject\MedusaLocker\Release\MedusaLockerXP.pdb
- C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject\MedusaLocker\Debug\MedusaLocker.pdb
- C:\Users\Gh0St\Desktop\MedusaLockerInfo\MedusaLockerProject_v2\MedusaLocker\Debug\MedusaLocker.pdb
- C:\Users\Gh0St\Desktop\AvaddonProjectInfo\AvaddonProject\AvaddonLockerLite\Release\AvaddonUnlockerGlobalLiteXPStub.pdb
- C:\Users\Gh0St\Desktop\ThunderX\Release\LockerStub.pdb

Feature	MEDUSALOCKER	Ako*	AVADDON	ThunderX*	RANZY
Programming Language	C++	C++	C++	C++	C++
Symmetric Encryption	AES-256 CBC	AES-256 CBC	AES-256 CBC	Salsa20	Salsa20
Asymmetric Encryption	RSA	RSA	RSA	RSA	RSA
Key Generation	Same key per execution	Same key per execution	Depends on version	Unique key per file	Unique key per file

Language check	No	No	Yes	No	No
UAC bypass	CMSTPLUA COM interface	No	CMSTPLUA COM interface, depends on version	No	No
Network discovery technique	ICMP	ICMP	ARP, depends on version	ICMP	ICMP
Process and service termination similarity	Yes	No	Yes	Yes	Yes

Figure 15: Table showing similarities between ransomware
*Ako (MEDUSALOCKER variant)
*ThunderX (RANZY variant)

Encryption Operations

Code reuse appeared very similar throughout initializing a cryptographic context for all of them. After analyzing each ransomware extensively, many functions had the same architecture and similar structure for storage and were found to always be evident and easy to pick out once reversing a sample.

Between the five ransomware, there are four modes of file encryption supported describing how much of the file to encrypt and in one case wiping the contents of the file instead of encrypting. These modes are the same across each ransomware.

File Signature

MEDUSALOCKER initially did not use file signature to append to the encrypted files, however Ako appends the hex value 0xBEEFCACE.

AVADDON appends the hex value 0x1030307 to the end of the file within a 24-byte structure.

RANZY and ThunderX use the signature hex value 0xB0E0E0F0.

These signatures are part of a 24-byte structure that is very similar across all of them, prior to this footer is the file's session key encrypted with the attacker's public key.

Identifier Format

Ako, ThunderX and RANZY construct highly similar JSON blobs that are encoded and written to the ransom notes. These contain multiple keywords that overlap between them.

Ako and AVADDON written identifiers contain similarities and overlap some keywords, however, AVADDON constructs a larger JSON (seen in Figure 14) and uses additional keywords not present in Ako.

Obfuscation

MEDUSALOCKER and Ako contain plain text strings and only the RSA key blob is base64 encoded. AVADDON, ThunderX and RANZY have different implementations to obfuscate both the RSA key and the strings.

UAC Bypass

MEDUSALOCKER and AVADDON use a similar UAC bypass functionality abusing the CMSTPLUA COM interface while ThunderX and RANZY don’t include a bypass.

Backup Deletion

The ransomware families delete backups by executing very similar command arguments to delete the Windows Shadow Copies invoking wbadmin, bcedit.exe and vssadmin.exe and to empty the recycle bin.

Service and Process Enumeration

These pieces of ransomware use a remarkably similar list of process and services to scan and stop if found and following a similar order. However, AVADDON contains more processes and services related to VMWare, Antivirus, SQLServer and Tomcat services and processes.

ThunderX and RANZY have different process and services lists and only some overlap. Additionally, the list of services to stop is considerably shorter than the rest of the ransomware, while the list of processes is larger.

File and Directory Exclusions

MEDUSALOCKER and AVADDON contain nearly identical file and directory exclusions, however, AVADDON contains additional directories that are skipped including TOR browser directories and a shorter list of file extensions skipped from the encryption process.

Network Scanning

MEDUSALOCKER, Ako, ThunderX and RANZY contain similar code to scan the victim’s network by using IcmpSendEcho function.

First builds identified for AVADDON rely on SendARP function, however, some of the AVADDON samples with PE timestamps from February 2021 show a replacement in the network reconnaissance module to use the IcmpCreateFile and IcmpSendEcho functions.

Other Differences

- Different versions of AVADDON have added exclusion folders and it can receive a CLI argument.

- ThunderX and RANZY can receive the CLI argument –nolan.

Conclusion

The similarities between these ransomware families and the timespan of activity suggest that the MEDUSALOCKER code base was likely reused by different threat actors that started operating RaaS in 2020. The binary similarities and techniques used show a certain degree of relationship between them. However, the technical skills of each threat actor involved in the development of these RaaS and the implementations vary per ransomware.

AVADDON constitutes a considerable evolution compared to MEDUSALOCKER, however, it is unclear whether AVADDON was the successor of MEDUSALOCKER due to technical differences and overlap in their activity. The AVADDON service was operational for about a year and gained considerable popularity among threat actors to extort victims across multiple regions and industries until events forced a fast exit followed by the shutdown of its operations and the release of the victim's private keys. Given the similarities suggesting code overlap between these ransomware families, the different skillsets of the involved operators and the overlap in time, it is unclear whether the Law Enforcement disruption of ransomware operations at this time will be definitive for the threat actors responsible for AVADDON.

Rebranding, code sharing, or the purchase of source code by different threat actors are practical possibilities to get back into extortion operations as seen in previous cases such as SODINOKIBI's **connections with GANDCRAB** ransomware, or the rebuild and rebrand of a new ransomware using another's code base such as **BLACKMATTER**.

Appendix: ATT&CK Mapping

ATT&CK Tactic Category	Techniques
Resource Development	Acquire Infrastructure (T1583) · Virtual Private Server (T1583.003)
Initial Access	External Remote Services(T1133) · Valid Accounts(T1078)
Execution	User Execution (T1204) · Malicious File (T1204.002) Scheduled Task/Job (T1053) · Scheduled Task (T1053.005)
Persistence	Valid Accounts (T1078) Boot or Logon Autostart Execution (T1547) · Registry Run Keys / Startup Folder (T1547.001)
Privilege Escalation	Valid Accounts (T1078)
Defense Evasion	Impair Defenses (T1562) · Disable or Modify Tools (T1562.001) Obfuscated Files or Information (T1027) · Software Packing (T1027.002) Process Injection (T1055) Indicator Removal on Host (T1070) · File Deletion (T1070.004) Modify Registry (T1112) Deobfuscate/Decode Files or Information (T1140) Virtualization/Sandbox Evasion (T1497) · System Checks (T1497.001)
Credential Access	OS Credential Dumping (T1003)
Discovery	Account Discovery (T1078) Domain Trust Discovery (T1482)

	Permissions Groups Discovery (T1069)
Lateral Movement	Remote Services (T1021) · Remote Desktop Protocol (T1012.001)
Collection	Archive Collected Data (T1560) · Archive via Utility (T1560.001)
Command and Control	Application Layer Protocol (T1071) · Web Protocols (T1071.001) Encrypted Channel (T1573) Ingress Tool Transfer (T1105)
Exfiltration	Exfiltration Over Web Service (T1567) · Exfiltration to Cloud Storage (T1567.002)

Mandiant Security Validation Action

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name
A151-063	Command and Control - AVADDON, DNS Query, Live Host Check
A151-064	Host CLI - AVADDON, bcdedit Commands
A151-067	Malicious File Transfer - AVADDON, Download, Variant #1
A151-069	Protected Theater - AVADDON, Execution
A151-085	Protected Theater - AVADDON, Execution, Windows 10 Variant
A151-086	Protected Theater - AVADDON, Execution, Windows 7 Variant
A104-775	Protected Theater - WMIC Shadowcopy Delete, Variant #1

Appendix: Malware definitions

AVADDON

AVADDON is ransomware written in C++ that encrypts files stored locally and on mapped network shares. AVADDON terminates targeted processes and services prior to encrypting files. AVADDON uses the AES-256 encryption algorithm to encrypt files. AVADDON is a Windows ransomware written in C++. It is run as an affiliate program, RaaS. System files are encrypted using a single AES-256 key. The AES-256 key is generated at run-time and encrypted using an embedded RSA public key. The malware also has anti-analysis techniques and check that it is not running in a system with Russian language.

MEDUSALOCKER

MEDUSALOCKER is ransomware written in C++ that encrypts files stored locally and on network shares with a randomly generated AES-256 key. MEDUSALOCKER can bypass User Account Control (UAC) and terminates targeted processes and services prior to encrypting files. Persistence is established using a scheduled task. MEDUSALOCKER empties the Recycle Bin and delete volume shadow copies.

RANZY

RANZY is a ransomware written in C++ that encrypts files stored locally and on mapped network shares appending the extension "[.]ranzy" to them. RANZY uses Salsa20 stream cipher to encrypt files.

DARKRAVEN

DARKRAVEN is an ASPX webshell written in C# that functions as a backdoor. The backdoor supports shell command execution and file transfer. Supplied data is decrypted and decoded using 3DES and a custom Base64 decoding routine.

BLACKCROW

BLACKCROW is an ASPX webshell written in VB[.]NET that functions as backdoor. BLACKCROW expects an attacker to upload a [.]NET DLL payload alongside additional arguments. These arguments are used to invoke a series of methods within the DLL. The results of the final invocation are displayed to the attacker.

SYSTEMBC

SYSTEMBC is a tunneler written in C that retrieves proxy-related commands from a C2 server using a custom binary protocol over TCP. A C2 server directs SYSTEMBC to act as a proxy between the C2 server and a remote system. SYSTEMBC is also capable of retrieving additional payloads via HTTP. Some variants may utilize the Tor network for this purpose. Downloaded payloads may be written to disk or mapped directly into memory prior to execution. SYSTEMBC is often utilized to hide network traffic associated with other malware families. Observed families include DANABOT, SMOKELOADER, and URSNIF.

Acknowledgements

Advanced Practices team, FLARE team, Threat Pursuit team and Yash Gupta