Avaddon RaaS | Breaks Public Decryptor, Continues On Rampage

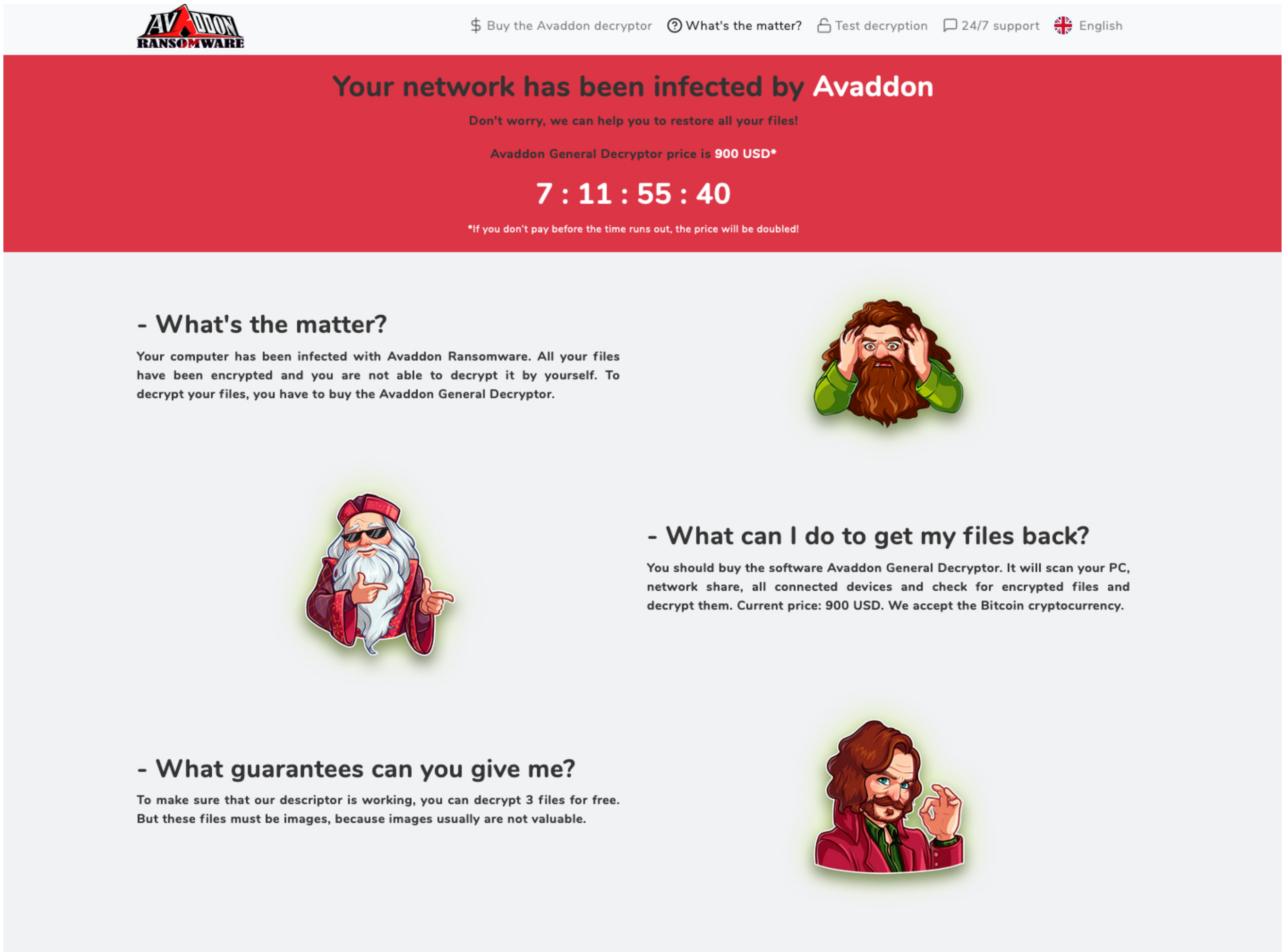
labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/

Jim Walter

SentinelLABS
Avaddon RaaS | Breaks Public Decryptor, Continues On Rampage
By Jim Walter
READ BLOG

The Avaddon ransomware family was first sighted in the wild in February 2020, but fully emerged as a robust Ransomware-as-a-Service (RaaS) model in June of that year. Over the last 9 months or so, the operator behind Avaddon has been successful in building a strong and reliable brand, moving quickly to support affiliates with an update after security researchers released a public decryptor in February 2021. Since then, we have observed a spike in Avaddon activity and note that the actor is actively engaged in developing “Version 2” of this aggressive RaaS offering.

In this post, we detail the rapid development of Avaddon, highlighting the malware author’s ability to adapt to circumstances and maximize payouts for Avaddon affiliates.



Your network has been infected by Avaddon

Don't worry, we can help you to restore all your files!

Avaddon General Decryptor price is 900 USD*

7 : 11 : 55 : 40

*If you don't pay before the time runs out, the price will be doubled!

- What's the matter?

Your computer has been infected with Avaddon Ransomware. All your files have been encrypted and you are not able to decrypt it by yourself. To decrypt your files, you have to buy the Avaddon General Decryptor.

- What can I do to get my files back?

You should buy the software Avaddon General Decryptor. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt them. Current price: 900 USD. We accept the Bitcoin cryptocurrency.

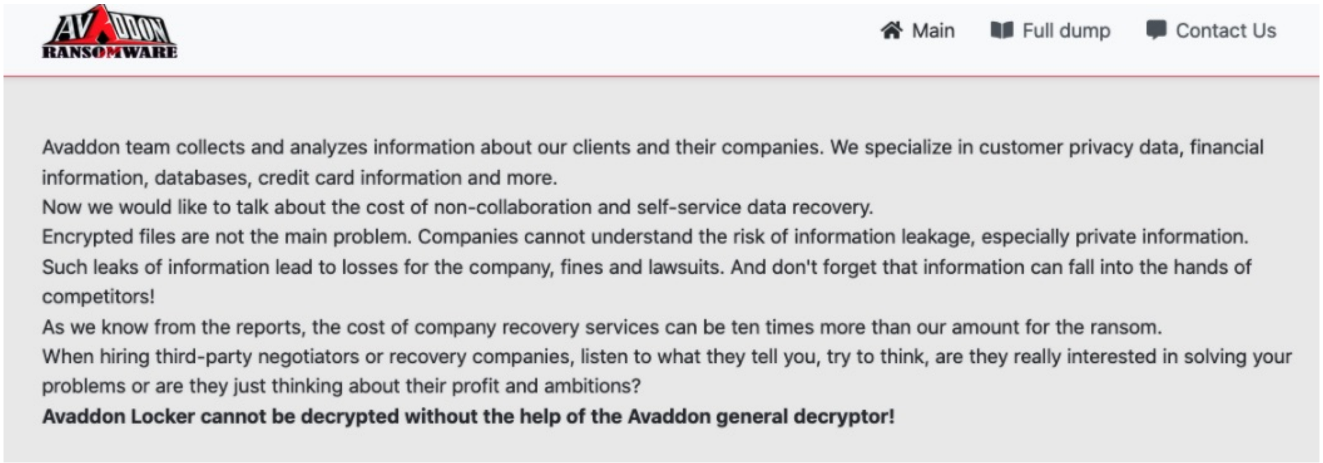
- What guarantees can you give me?

To make sure that our descriptor is working, you can decrypt 3 files for free. But these files must be images, because images usually are not valuable.

Avaddon RaaS Overview

After initial sightings in attacks from February 2020 onwards, Avaddon fully emerged as a RaaS in June of 2020. It was heavily promoted in underground markets as a fast, bespoke, highly-configurable, and well-supported ransomware service.

The Avaddon operator offered partners fairly standard terms with the RaaS taking an initial 25% cut but willing to drop that percentage for higher volume affiliates. Over the following months, Avaddon became one of the more aggressive ransomware groups targeting both individuals and businesses. Following the model of other RaaS families that came before it, Avaddon soon put up a blog site dedicated to leaking victim data should victims fail to pay the ransom demand.



Avaddon team collects and analyzes information about our clients and their companies. We specialize in customer privacy data, financial information, databases, credit card information and more.
Now we would like to talk about the cost of non-collaboration and self-service data recovery.
Encrypted files are not the main problem. Companies cannot understand the risk of information leakage, especially private information. Such leaks of information lead to losses for the company, fines and lawsuits. And don't forget that information can fall into the hands of competitors!
As we know from the reports, the cost of company recovery services can be ten times more than our amount for the ransom.
When hiring third-party negotiators or recovery companies, listen to what they tell you, try to think, are they really interested in solving your problems or are they just thinking about their profit and ambitions?
Avaddon Locker cannot be decrypted without the help of the Avaddon general decryptor!

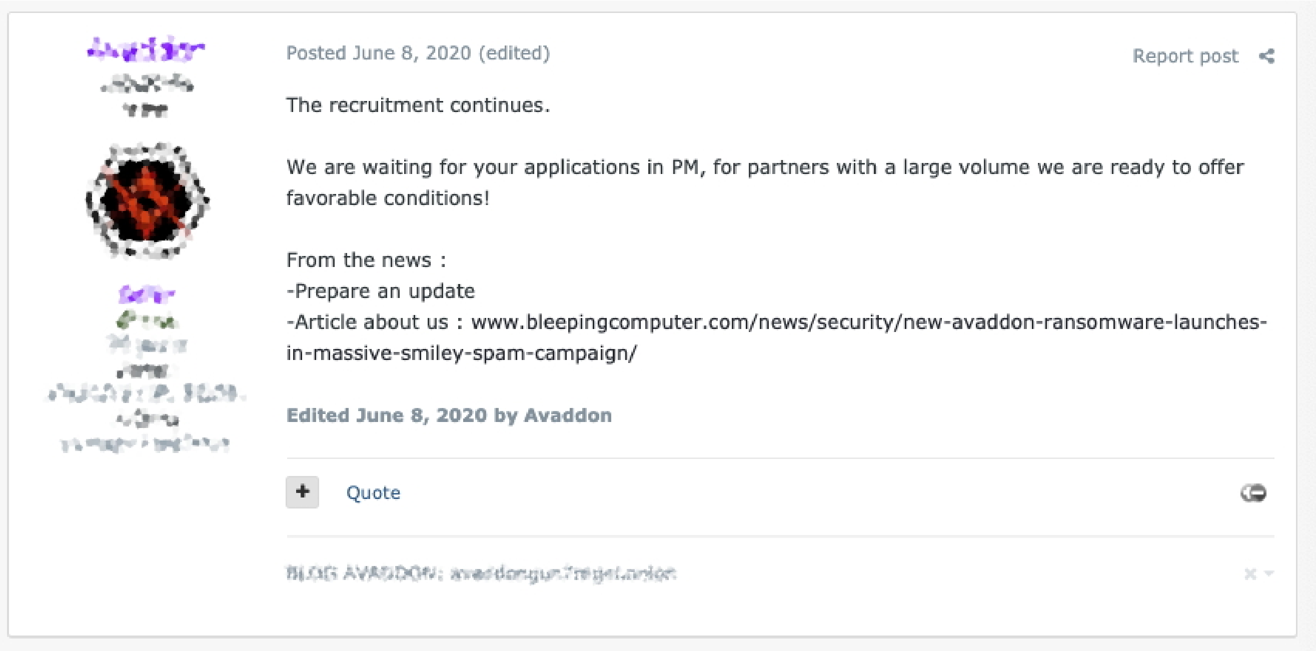
Since its inception, Avaddon refused to accept affiliates targeting CIS (Commonwealth of Independant States) countries. This is in addition to being critical of any dealings with non-Russian-native speaking individuals.

Right out of the gate, Avaddon touted their speed, configurability, and robust feature set. The first version of Avaddon was advertised with the following features:

- Unique payloads written in C++
- File encryption via AES256 + RSA2048, supporting full-file encryption & custom parameters
- Full offline support, initial contact to C2 not required
- “Impossible” 3rd party decryption
- Support for Windows 7 and higher
- Multi-threaded file encryption for max performance
- Encryption of all local and remote (and accessible) drives
- IOCP Support for parallel file encryption
- Persistently encrypts newly written files and newly connected media
- Ability to spread across network shares (SMB, DFS)
- Multiple delivery options (script, PowerShell, .EXE payload, .DLL)
- Payload executes as administrator
- Encrypts hidden files and volumes
- Removes trash, Volume Shadow Copies (VSS), and other restore points
- Termination of processes which inhibit encryption of files
- Configurable ransom note behavior

Initially, affiliates were able to build and manage their payload via an elegant administration panel hosted via TOR (.onion). The panel allowed for management of specific campaigns, payment types and behaviors, victim tracking and management. It also served as the portal to Avaddon’s technical support resources.

Over the following weeks, Avaddon picked up a great amount of momentum, continued to advertise for recruitments and boasted about their coverage in the press.



[redacted]

Posted June 8, 2020 (edited)

The recruitment continues.

We are waiting for your applications in PM, for partners with a large volume we are ready to offer favorable conditions!

From the news :
-Prepare an update
-Article about us : www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/

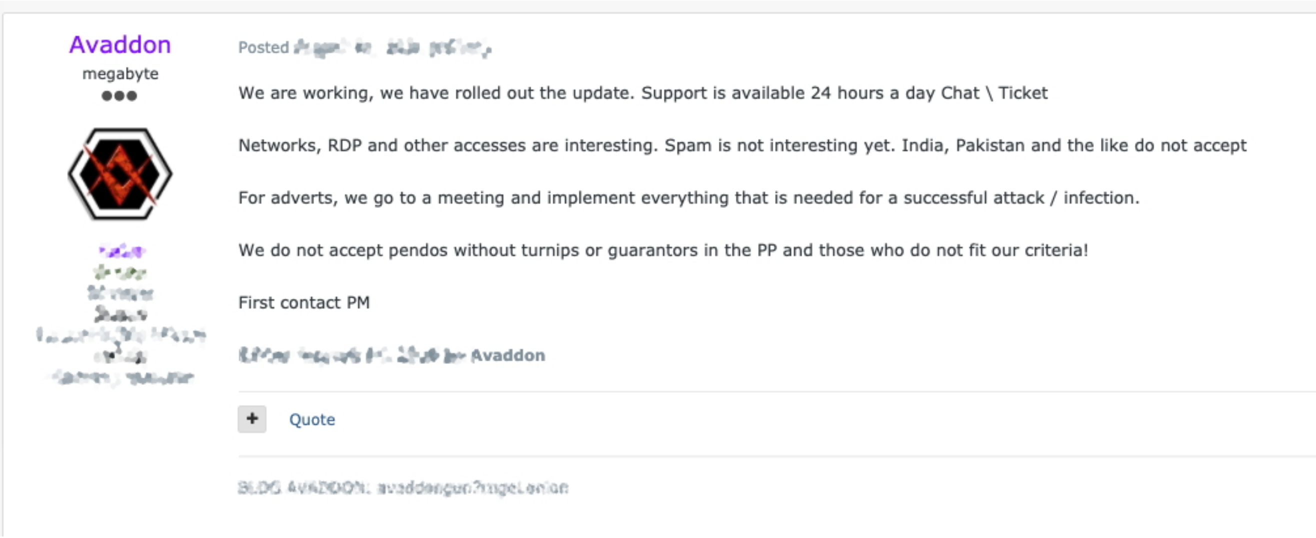
Edited June 8, 2020 by Avaddon

[redacted]

In the second half of 2020, Avaddon continued to build its infected base, while also continuing to upgrade the service and payloads.

As AV engines began adding detection rules for Avaddon, the operator responded with frequent updates to ensure the desired level of stealth. In late June 2020, the malware added the option to launch payloads via PowerShell.

In August 2020, some more significant upgrades to the service came in the form of 24/7 support. The actors indicated at the time that 24×7 support for affiliates was now available via chat and ticketing systems.



Avaddon
megabyte
●●●

[redacted]

Posted [redacted]

We are working, we have rolled out the update. Support is available 24 hours a day Chat \ Ticket

Networks, RDP and other accesses are interesting. Spam is not interesting yet. India, Pakistan and the like do not accept

For adverts, we go to a meeting and implement everything that is needed for a successful attack / infection.

We do not accept pendos without turnips or guarantors in the PP and those who do not fit our criteria!

First contact PM

[redacted] Avaddon

[redacted]

In addition, Avaddon was one of the early adopters of additional extortion methods to taunt and advertise the breach of non-compliant victims, including the use of targeted advertisements. The authors continued to improve the payloads themselves with better

Distributed File System (DFS) support, different encryption mechanisms, and DLL payload support.

New Year 2021 brought further changes to the Avaddon platform. In January, the actor added support for Windows XP and 2003 in the payloads, as well as tweaks to the encryption feature set. Notably, Avaddon was one of the first to add DDoS attacks as yet another intimidation mechanism to their arsenal: If clients failed to comply with the ransom demands, they stood to experience a damaging DDoS attack in addition to their data being leaked to the public, and any tarnishing of their reputation as a result of the breach.

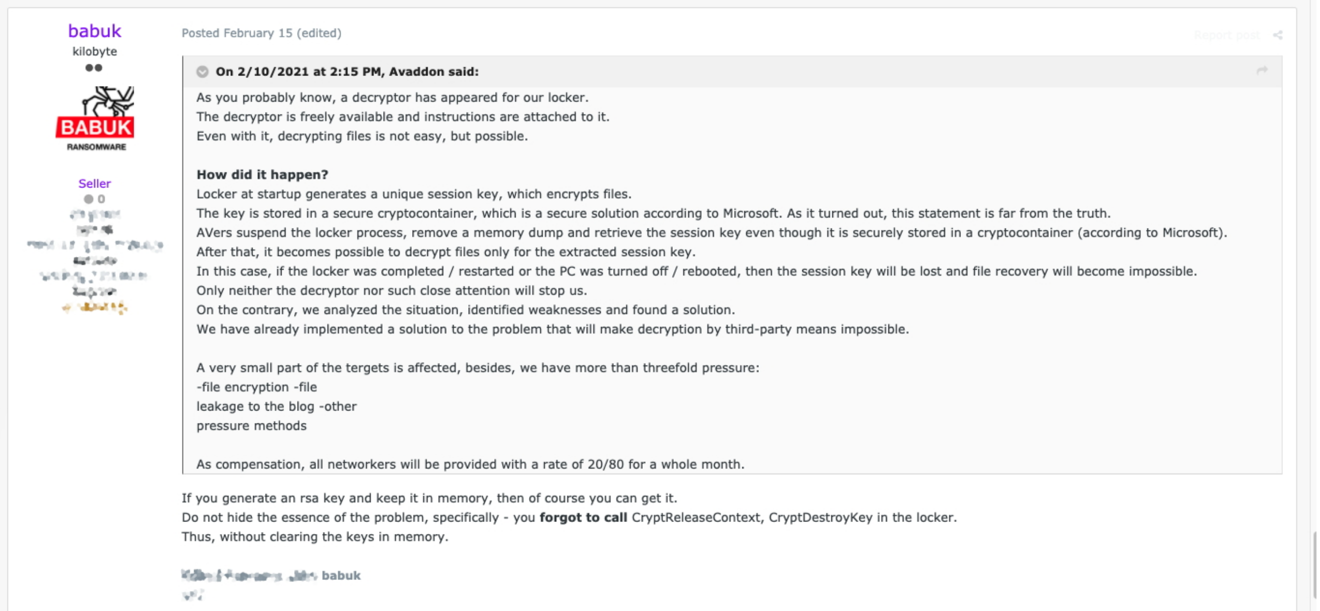
Everything seemed to be going well for the Avaddon RaaS, but then they hit a hurdle.

Avaddon Public Decrypter

In early 2021, a decryption tool for Avaddon was released by Bitdefender. Additionally, an open-source decryptor was also released by researcher Javier Yuste based on his extensive paper detailing the internals of Avaddon.

Under the hood, Avaddon payloads were storing the ‘secret’ session keys for encryption in memory. This allowed analysts and researchers to locate the data and extract the key for analysis and eventual development of the decryption tool. The tool was widely released, and posted to NoMoreRansom.org.

During this period, we even observed actors behind Babuk ransomware offering technical assistance to the Avaddon actors.



[redacted]

Posted February 15 (edited)

On 2/10/2021 at 2:15 PM, Avaddon said:

As you probably know, a decryptor has appeared for our locker.
The decryptor is freely available and instructions are attached to it.
Even with it, decrypting files is not easy, but possible.

How did it happen?
Locker at startup generates a unique session key, which encrypts files.
The key is stored in a secure cryptocontainer, which is a secure solution according to Microsoft. As it turned out, this statement is far from the truth.
AVers suspend the locker process, remove a memory dump and retrieve the session key even though it is securely stored in a cryptocontainer (according to Microsoft).
After that, it becomes possible to decrypt files only for the extracted session key.
In this case, if the locker was completed / restarted or the PC was turned off / rebooted, then the session key will be lost and file recovery will become impossible.
Only neither the decryptor nor such close attention will stop us.
On the contrary, we analyzed the situation, identified weaknesses and found a solution.
We have already implemented a solution to the problem that will make decryption by third-party means impossible.

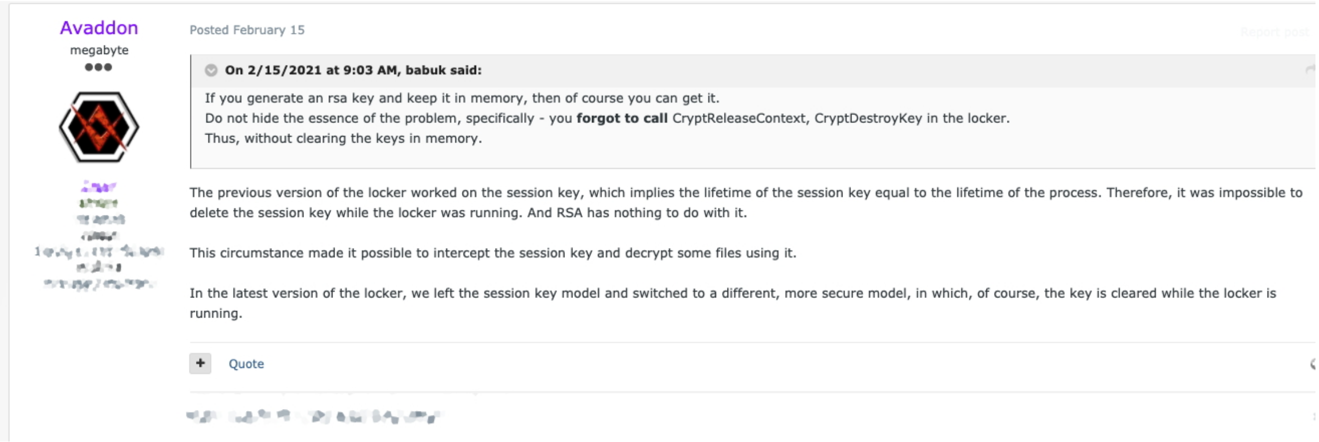
A very small part of the tergets is affected, besides, we have more than threefold pressure:
-file encryption -file
leakage to the blog -other
pressure methods

As compensation, all networkers will be provided with a rate of 20/80 for a whole month.

If you generate an rsa key and keep it in memory, then of course you can get it.
Do not hide the essence of the problem, specifically - you **forgot to call** CryptReleaseContext, CryptDestroyKey in the locker.
Thus, without clearing the keys in memory.

[redacted] babuk
[redacted]

Those behind Avaddon were quick to pivot and move to a different model altogether, nullifying the effect of the decryptor. They also offered affiliates an 80% cut for a full month as compensation.



Avaddon

megabyte

[redacted]

Posted February 15

Report post

> **On 2/15/2021 at 9:03 AM, babuk said:**
>
> If you generate an rsa key and keep it in memory, then of course you can get it.
> Do not hide the essence of the problem, specifically - you **forgot to call** CryptReleaseContext, CryptDestroyKey in the locker.
> Thus, without clearing the keys in memory.

The previous version of the locker worked on the session key, which implies the lifetime of the session key equal to the lifetime of the process. Therefore, it was impossible to delete the session key while the locker was running. And RSA has nothing to do with it.

This circumstance made it possible to intercept the session key and decrypt some files using it.

In the latest version of the locker, we left the session key model and switched to a different, more secure model, in which, of course, the key is cleared while the locker is running.

[redacted]

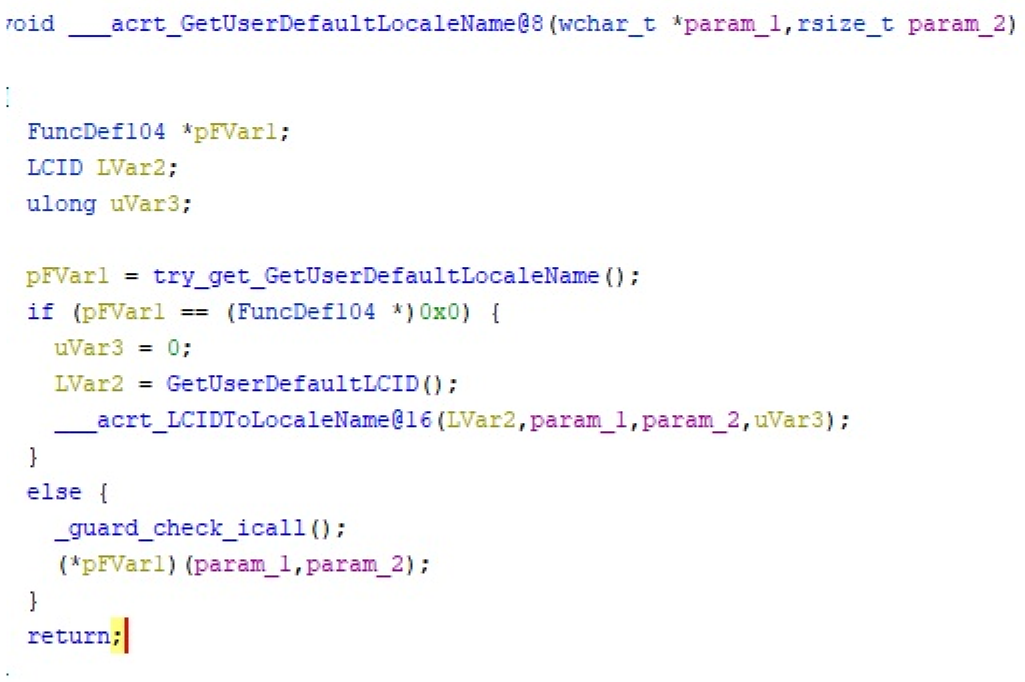
Following the requisite upgrades to address the encryption issues, Avaddon continued to update their services and toolset, in addition to becoming more aggressive with recruitment. February 2021 also saw the addition of Monero support.

Subsequently, we have observed a spike in Avaddon activity, including new victim entries on their blog. The actor’s most recent public statements indicate that the development of Avaddon V2 is well underway.

Avaddon RaaS Technical Breakdown

In the majority of cases, the initial delivery vector for Avaddon is via phishing email. However, affiliates have been known to use RDP along with exploitation of network-centric vulnerabilities. We have observed malicious emails with attached .js payloads, which in turn retrieve the Avaddon payloads from a remote location. In some cases, threat actors have simply attached the ransomware directly to the email messages.

Avaddon payloads perform checks to insure they are not executing on a victim device located in certain regions of CIS.



```
void ___acrt_GetUserDefaultLocaleName@8(wchar_t *param_1,rsize_t param_2)

{
  FuncDef104 *pFVar1;
  LCID LVar2;
  ulong uVar3;

  pFVar1 = try_get_GetUserDefaultLocaleName();
  if (pFVar1 == (FuncDef104 *)0x0) {
    uVar3 = 0;
    LVar2 = GetUserDefaultLCID();
    ___acrt_LCIDToLocaleName@16(LVar2,param_1,param_2,uVar3);
  }
  else {
    _guard_check_icall();
    (*pFVar1)(param_1,param_2);
  }
  return;
}
```

The `GetUserDefaultLCID()` function (and/or `GetKeyboardLayout()`) is used to determine the users' default locale. The following countries are most frequently excluded from execution:

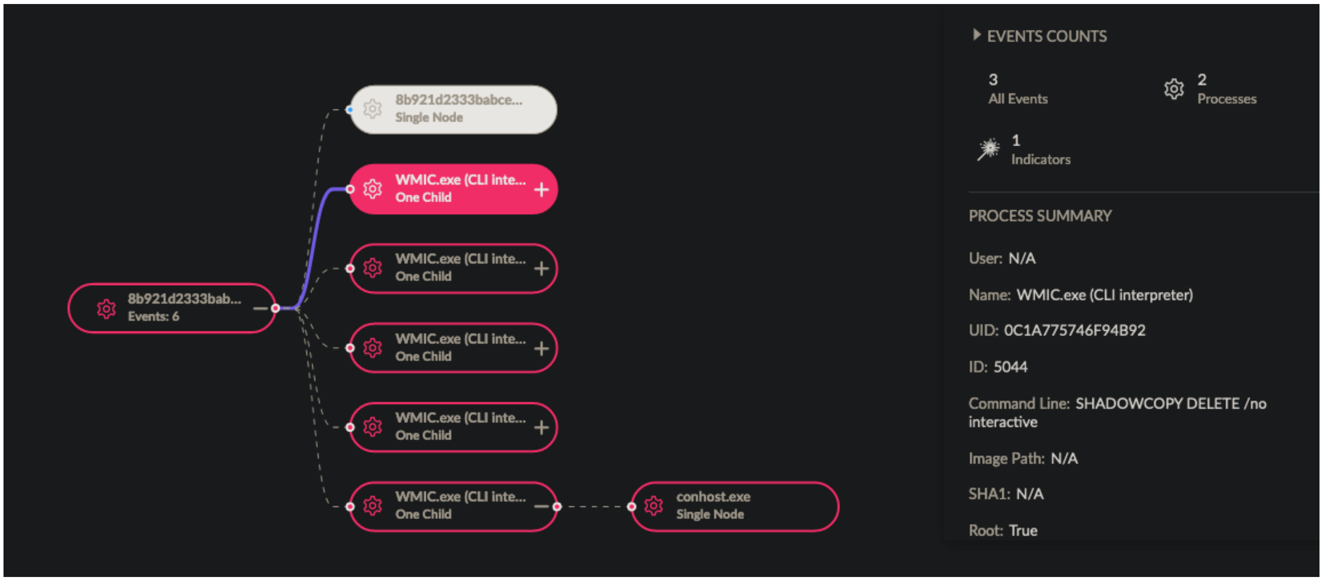
- Russia
- Cherokee Nation
- Ukraine
- Tatar
- Yakut
- Sakha

A commonly used UAC bypass technique is utilized to ensure that the threat is running with the required privileges. Specifically, this is a UAC bypass via CMSTPLUA COM interface.

Existing Windows tools and utilities are used to manipulate and disable system recovery options, backups, and Volume Shadow Copies. Some syntax can vary across variants. WMIC.EXE is typically used to remove VSS via SHADOWCOPY DELETE /nointeractive.

We have also observed the following commands issued by Avaddon payloads:

- bcdedit.exe /set {default} recoveryenabled No
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- vssadmin.exe Delete Shadows /All /Quiet
- wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest



PROCESS SUMMARY

User: N/A

Name: WMIC.exe (CLI interpreter)

UID: 0C1A775746F94B92

ID: 5044

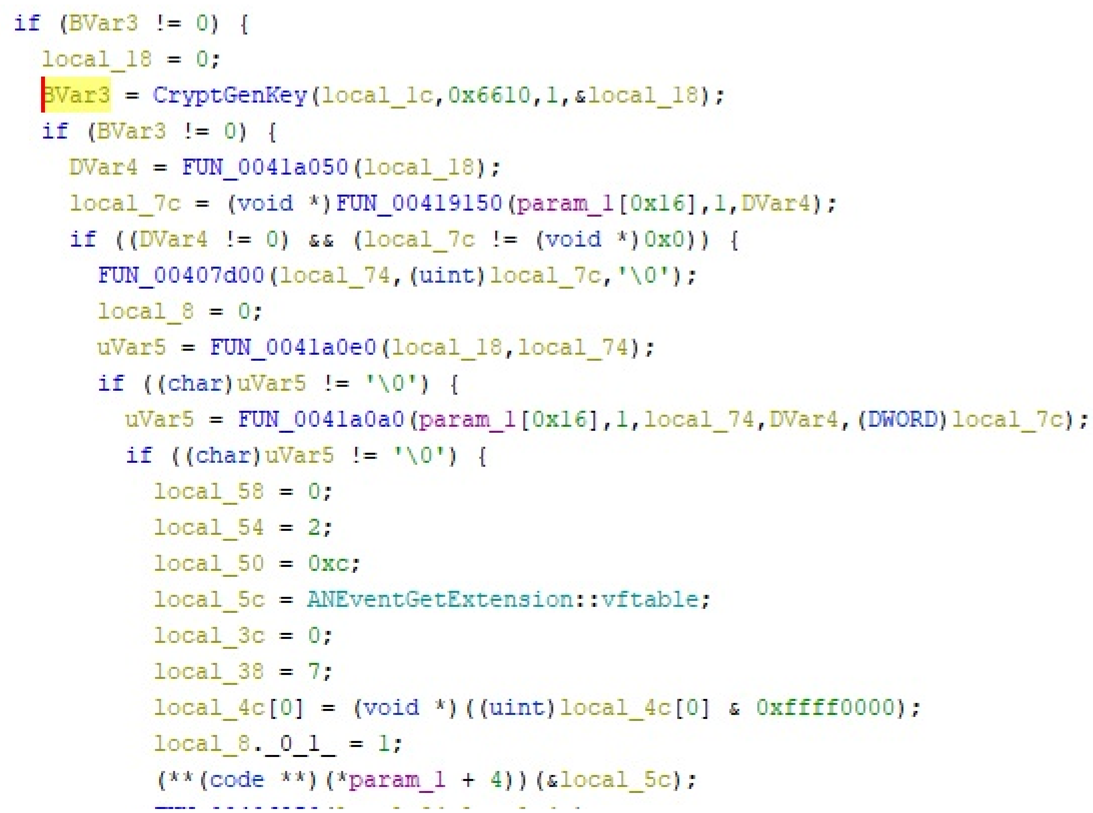
Command Line: SHADOWCOPY DELETE /no interactive

Image Path: N/A

SHA1: N/A

Root: True

While there have been changes to Avaddon's encryption routine to combat 3rd party decryption, the historic flow, simplified, would be:



```
if (BVar3 != 0) {
  local_18 = 0;
  BVar3 = CryptGenKey(local_1c,0x6610,1,&local_18);
  if (BVar3 != 0) {
    DVar4 = FUN_0041a050(local_18);
    local_7c = (void *)FUN_00419150(param_1[0x16],1,DVar4);
    if ((DVar4 != 0) && (local_7c != (void *)0x0)) {
      FUN_00407d00(local_74,(uint)local_7c,'\0');
      local_8 = 0;
      uVar5 = FUN_0041a0e0(local_18,local_74);
      if ((char)uVar5 != '\0') {
        uVar5 = FUN_0041a0a0(param_1[0x16],1,local_74,DVar4,(DWORD)local_7c);
        if ((char)uVar5 != '\0') {
          local_58 = 0;
          local_54 = 2;
          local_50 = 0xc;
          local_5c = ANEventGetExtension::vftable;
          local_3c = 0;
          local_38 = 7;
          local_4c[0] = (void *)((uint)local_4c[0] & 0xffff0000);
          local_8._0_1_ = 1;
          (**(code **)(*param_1 + 4))(&local_5c);
```

1. Generation of session Key (AES 256)
2. Update master key (AES 256)
3. Master key encrypts relevant user and environment data, along with the ransom note (typically Base64)
4. Files are encrypted via the session key
5. Append encrypted session key (RSA 2048) to the end of each encrypted file

Avaddon Evasion Techniques

Avaddon can be configured to terminate specific processes. This is frequently done to target security products or processes which might interfere with the encryption process. An example process list would be:

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

Avaddon has also been known to prioritize the encryption of Microsoft Exchange-related directories.

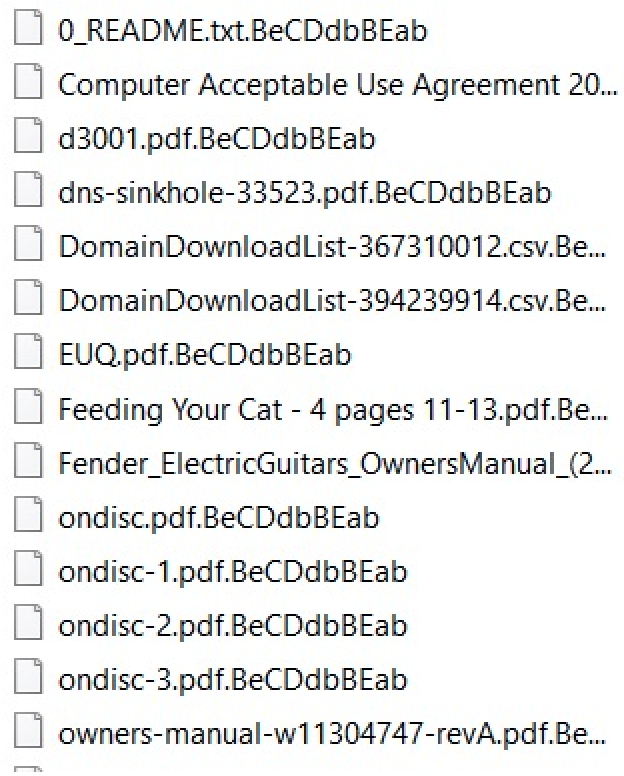
Most Avaddon payloads will exclude the following critical OS locations from encryption:

```
C:PERFLOGS
C:PROGRAM FILES (X86)
C:PROGRAMDATA
C:USERS<USER>APPDATA
C:USERS<USER>APPDATALOCALTEMP
C:USERSPUBLIC
C:WINDOWS
```

Persistence mechanisms can also vary, and we have observed variations of Avaddon that utilize the creation of a new Windows service, as well as the use of scheduled tasks for persistence.

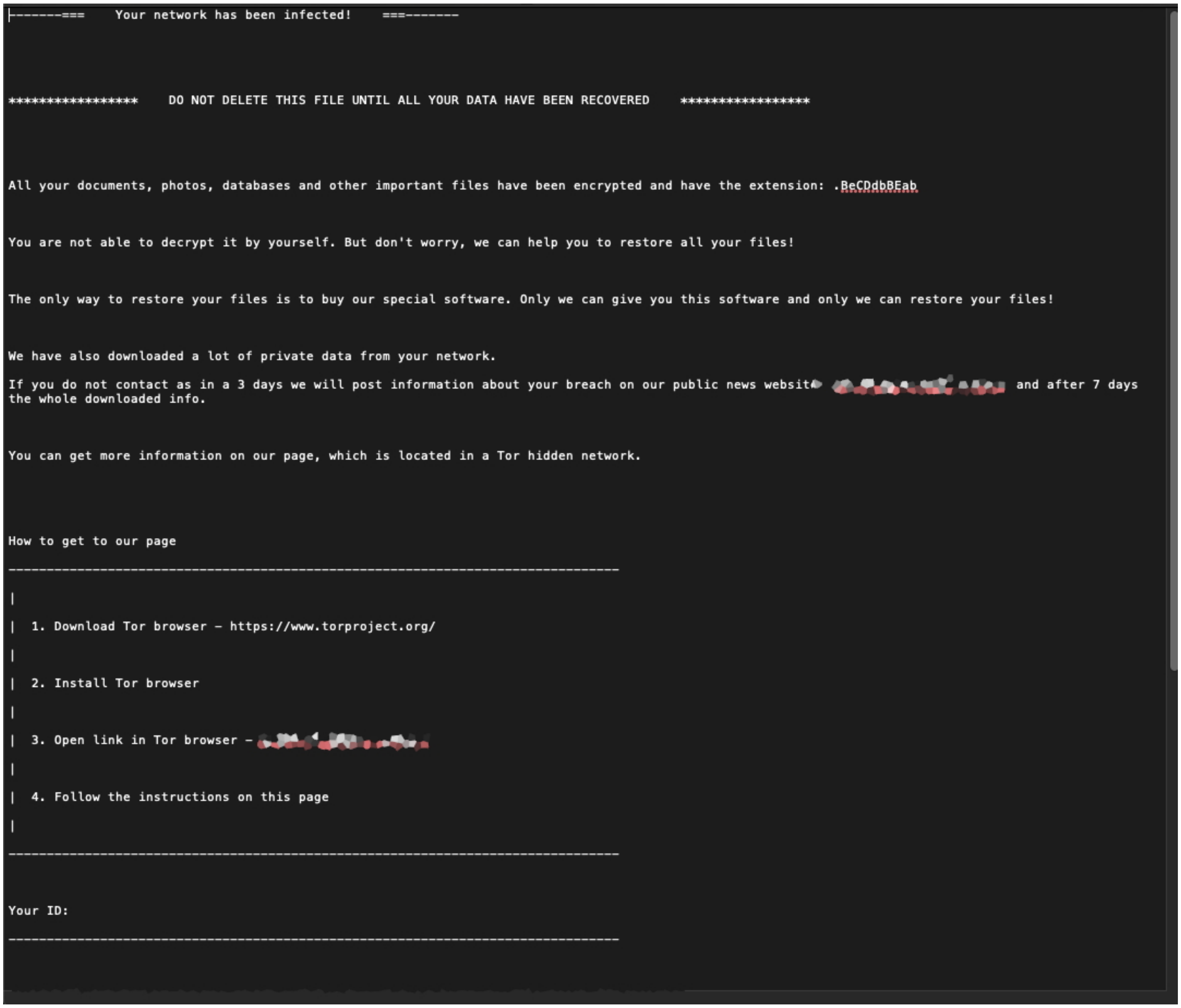
Avaddon Post-Infection Behavior

Infected files are renamed with an extension consisting of randomly generated letters. These extensions are unique for each victim.



0_README.txt.BeCDdbBEab
Computer Acceptable Use Agreement 20...
d3001.pdf.BeCDdbBEab
dns-sinkhole-33523.pdf.BeCDdbBEab
DomainDownloadList-367310012.csv.Be...
DomainDownloadList-394239914.csv.Be...
EUQ.pdf.BeCDdbBEab
Feeding Your Cat - 4 pages 11-13.pdf.Be...
Fender_ElectricGuitars_OwnersManual_(2...
ondisc.pdf.BeCDdbBEab
ondisc-1.pdf.BeCDdbBEab
ondisc-2.pdf.BeCDdbBEab
ondisc-3.pdf.BeCDdbBEab
owners-manual-w11304747-revA.pdf.Be...

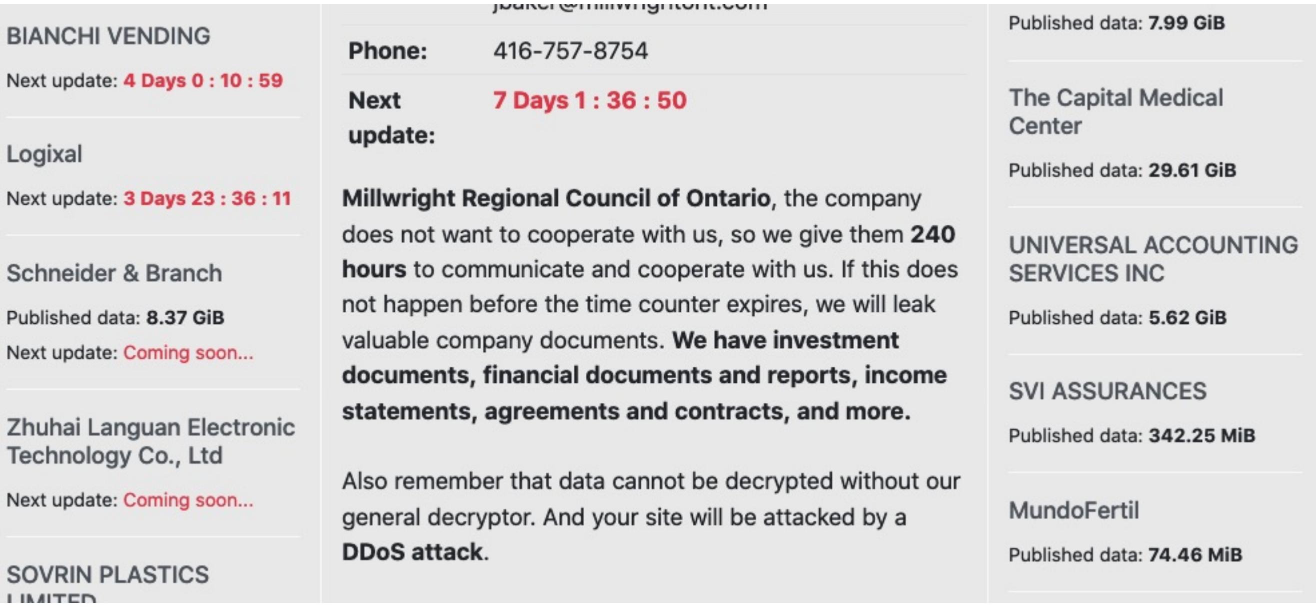
Earlier versions of Avaddon would also replace the infected hosts' wallpaper image. The current version presents victims with a ransom note as shown below. Victims are warned that aside from their data being encrypted, the actors "have also downloaded a lot of private data from your network".



```
-------===    Your network has been infected!    ===-------



*****************    DO NOT DELETE THIS FILE UNTIL ALL YOUR DATA HAVE BEEN RECOVERED    *****************



All your documents, photos, databases and other important files have been encrypted and have the extension: .BeCDdbBEab


You are not able to decrypt it by yourself. But don't worry, we can help you to restore all your files!


The only way to restore your files is to buy our special software. Only we can give you this software and only we can restore your files!


We have also downloaded a lot of private data from your network.
If you do not contact as in a 3 days we will post information about your breach on our public news websit[redacted] and after 7 days
the whole downloaded info.


You can get more information on our page, which is located in a Tor hidden network.



How to get to our page
--------------------------------------------------------------------------------

|

|  1. Download Tor browser - https://www.torproject.org/

|

|  2. Install Tor browser

|

|  3. Open link in Tor browser - [redacted]

|

|  4. Follow the instructions on this page

|

--------------------------------------------------------------------------------


Your ID:
--------------------------------------------------------------------------------
```

Victims are instructed to visit the Avaddon payment portal via the TOR browser, where they must enter their unique ID (found in the ransom note) to proceed.

The actors behind Avaddon do not wait for victims to become non-compliant before they are named and shamed on the blog. Company names appear with a timer, counting down to the posting time for any data stolen from the targeted environment.



BIANCHI VENDING

Next update: **4 Days 0 : 10 : 59**

Logixal

Next update: **3 Days 23 : 36 : 11**

Schneider & Branch

Published data: **8.37 GiB**

Next update: Coming soon...

Zhuhai Languan Electronic Technology Co., Ltd

Next update: Coming soon...

SOVRIN PLASTICS LIMITED

jbaker@millwrightont.com

Phone:	416-757-8754
Next update:	**7 Days 1 : 36 : 50**

Millwright Regional Council of Ontario, the company does not want to cooperate with us, so we give them **240 hours** to communicate and cooperate with us. If this does not happen before the time counter expires, we will leak valuable company documents. **We have investment documents, financial documents and reports, income statements, agreements and contracts, and more.**

Also remember that data cannot be decrypted without our general decryptor. And your site will be attacked by a **DDoS attack.**

Published data: **7.99 GiB**

The Capital Medical Center

Published data: **29.61 GiB**

UNIVERSAL ACCOUNTING SERVICES INC

Published data: **5.62 GiB**

SVI ASSURANCES

Published data: **342.25 MiB**

MundoFertil

Published data: **74.46 MiB**

It is important to note that victims appear on the leak site at the point when they are breached, and not just when the actor decides to release their data. This means that a company breach could easily become public knowledge regardless of any action taken by the victim, and potentially at a time where the target company would rather ‘control the release’ of that type of information.

At the time of writing, there are just over sixty companies listed, 19 of which include fully released dumps of sensitive information.

Avaddon does not appear to have any particular preference or scruples when it comes to targets. Whereas some ransomware groups have backed off certain types of targets during the ongoing pandemic, Avaddon victims to date include healthcare-related entities. That said, the most represented industries in their victimology are Information Technology & Services, Food Production, Legal Services, and Manufacturing.

Conclusion

Avaddon is another successful example of the current RaaS model. It has appeared on the scene and made an impact very quickly. The actors are disciplined with regard to whom they will accept as an affiliate, which ensures some degree of longevity and exclusivity. In addition, they very quickly adopted the more aggressive extortion techniques tied to modern ransomware families. This not only includes the public leaking of data but also the threat of DDoS attacks, personal threats, and advertisement-based taunting.

All of these, along with tight payment requirements for the victims, have put Avaddon in a potentially powerful position. They have yet to garner quite the same amount of media attention as predecessors such as Maze and Egregor, but there is no reason to believe that Avaddon is any less dangerous. At this time, those behind Avaddon are highly-engaged with their community and actively developing and iterating in response to security research and detection. With Avaddon version 2 on the horizon, we only expect to see increased activity from this actor as we move further into 2021.

Indicators of Compromise

SHA1:

c41d5b04b8219df57249ecdba8faa97c3d4a7fc2
c1f6f1e1a27e7be32a3f18440c05951fa7e52eb9
c0fc01350ae774f3817d71710d9a6e9adaba441f
4915feb5b5cccd9e75f0bd4af5e35211353a207e
fc12d7ad112ddabfcd8f82f290d84e637a4d62f8
f540a1f2fdc0670e1a7a3d55e335e70ebe3089f7
880e40932e56e0aa0b0ad8c413b50fca7d771bbe
7e835d1813f2eaf82c5e38eebf3bfd06ed6513e0
a1d6461e833813ccfb77a6929de43ab5383dbb98
a37a3b88a15d31a8951243cd6f3f08149244a67d
3b575420ceea4203152041be00dc80519d1532b5
dd2cce7e2f5dcf0a00e4ec9cdbc028476ceb3583
48385b39f2ad900377aba7442d93663506c2b9c5
60ab0dd2ef31cfb96d52fa0a429c3803417db5c2
5ddb793327e1e89ef8f406be11f97e5489f7a5c1
d680d790167a7f84f7e531b2d16db0a0e3359f73
cf5920569b7d802763463b2faf4bbd2cdc21cfad
f94fda611b71bd565c1d603864e21e9cfd3ca99e
40e0fff64ba685d97fe143880a7b01c0137b4ceb
9087d7b5f8b62a2afa4f229b7e254971d4d9b5c3
6a6956aff077aeda5b22873cfb891632fbce6bc7
35831310fa4f11909c44b5db64c44b1064ac1d35

SHA256:

28adb5fa487a7d726b8bad629736641aadbdacca5e4f417acc791d0e853924a7
0a052eff71641ff91897af5bdecb4a98ed3cb32bcb6ff86c4396b1e3ceee0184
0ff4058f709d278ed662719b9627618c48e7a656c59f6bfecda9081c7cbd742b
146e554f0d56db9a88224cd6921744fdfe1f8ee4a9e3ac79711f9ab15f9d3c7f
165c5c883fd4fd36758bcba6baf2faffb77d2f4872ffd5ee918a16f91de5a8a8
2946ef53c8fec94dcdf9d3a1afc077ee9a3869eacb0879cb082ee0ce3de6a2e7
29b5a12cda22a30533e22620ae89c4a36c9235714f4bad2e3944c38acb3c5eee
331177ca9c2bf0c6ac4acd5d2d40c77991bb5edb6e546913528b1665d8b501f3
46a8c1e768f632d69d06bfbd93932d102965c9e3f7c37d4a92e30aaeca905675
5252cc9dd3a35f392cc50b298de47838298128f4a1924f9eb0756039ce1e4fa2
61126de1b795b976f3ac878f48e88fa77a87d7308ba57c7642b9e1068403a496
64cfe726643c7783b0f13a2927ab330e35e94a9125122b0cc230eec2bea27dd1

6884d700284bc3158dbeb8745bcda3e3b17b69ad049528b125b36e2455bb6b27
6a4875ddaceaa91fb3369f0f6d962f77442daf1b1d97733457d12bcabdf79441
8d14c0c8faf6249b67a1d19b7bd1404eb416304d8f5c73b3bdc9c69367e829de
98388773dc5da7f73a32a08613404029c7cd23078d697700aec6b573b2fa8e09
a5e4cb2f47de005570110b7f3ef1f4b600894469d0561b7e5653671a484a913b
caf57646723fe7c34f89618d96af3c2b82816f5d995fd7b951f32571166d3768
dab7eb2503e0d61d02e6156a47361da97afc53c1dee17c420a0a05de891172c3
de48c7d7f4865099dba96b6e2c6dca54187fb64e07c319660f072b851ec8b3b3
f9b748cf35278dc4bfaa2127ca1d6016fafbeb768b1a09c7ab58560632dbd637
fa4bc4a1dd461ecaadd094a9a21668ecdbb60022fb1b088854a8d13c09155a5c

MITRE ATT&CK

T1027 Obfuscated Files or Information
T1497.001 Virtualization/Sandbox Evasion / System Checks
T1202 Indirect Command Execution
T1078 Valid Accounts
T1562.001 Impair Defenses: Disable or Modify Tools
T1070.004 Indicator Removal on Host / File Deletion
T1112 Modify Registry
T1012 Query Registry
T1082 System Information Discovery
T1120 Peripheral Device Discovery
T1490 Inhibit System Recovery
T1548.002 Abuse Elevation Control Mechanism / Bypass User Account Control
T1566 Phishing
T1498.001 Network Denial of Service / Direct Network Flood
T1486 Data Encrypted for Impact
T1543.003 Create or Modify System Process: Windows Service