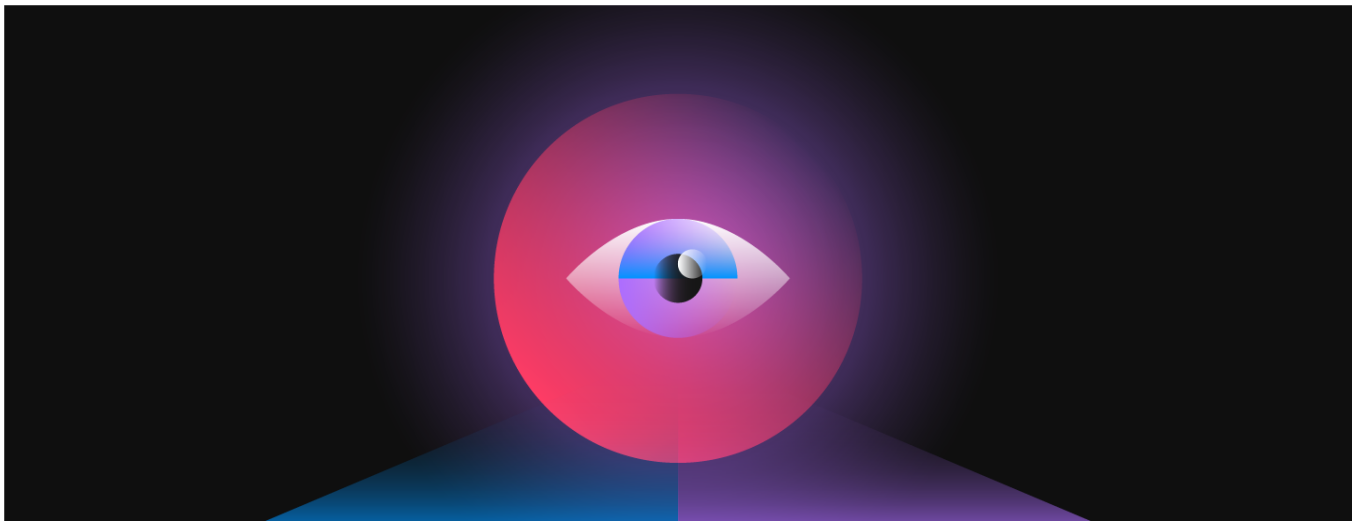
Avaddon Ransomware Analysis

atos.net/en/lp/securitydive/avaddon-ransomware-analysis



INTRODUCTION

Atos Digital Security regularly performs incident response and gather information on various attacker groups. Among them, Avaddon stands out for its modus operandi and its rise.

This article describes the results of investigations conducted about this group as well as the technical analysis of a sample found in the victims of this ransomware.

UPDATE – 11-06-21

Since this article was written, a new event occurred on June 11, 2021: the Avaddon group stopped its activities.

According to BleepingComputer[1] , its journalists received an anonymous message, claiming to be from the FBI that contained the keys to decrypt the files encrypted by Avaddon.

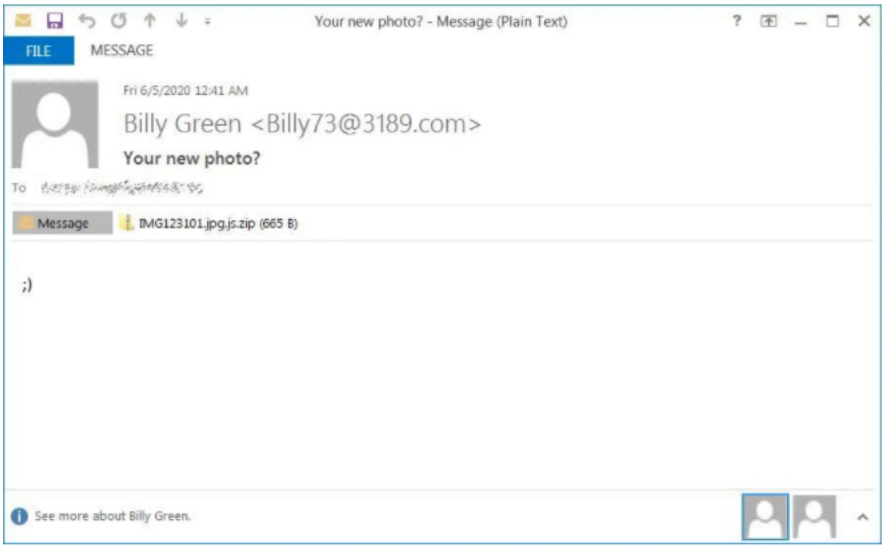
CERT-DS has indeed confirmed that the sample files collected during previous scans have been successfully decrypted.

The Avaddon website, hosted on a hidden service of the Tor network, is unavailable, which would confirm that the group's activity has been shut down.

The reasons behind this development are still unknown, but it could be related to the intensified fight against ransomware, recent events related to Colonial Pipeline[2] as well as political announcements from the United States.

DESCRIPTION OF AVADDON OPERATIONS

The Avaddon group was first observed in February 2020 and fully began to operate as a RaaS (Ransomware-as-a-Service) from June 2020 **[1]**. The ransomware acquired notoriety following a large-scale phishing campaign in which it was distributed by the Phorpiex/Trik. In this case, the fraudulent e-mails enticed victims to execute a compressed JavaScript file containing the ransomware payload. **[2] [3]**.



At the same time, the Avaddon group started to promote its ransomware on Russian-speaking hacker forums in order to seek new affiliates and increase its distribution. A month later, in August 2020, the group launched its data leak website **[4]**.

Since then, the group has quickly established itself as being able to deliver powerful, customisable and well-supported ransomware. Recent reports indicate a resurgence of its activity, confirmed by the recent publication of numerous repositories of data stolen from organisations in a wide range of sectors and countries **[5] [6]**.

THE AVADDON RAAS

Ransomware-as-a-Service (RaaS) is a business model in which ransomware developers provide attackers with the whole infrastructure necessary to encrypt a victim's data. This infrastructure includes the encryption software, the payment management, the data disclosure and the negotiation channel.Therefore, campaigns conducted by the Avaddon group under the RaaS model typically involve two threat actors. Initially, an attacker with access to an information system contacts the ransomware group. The Avaddon developers then examine the request as well as the credibility of the hacker's entry point. If the request is accepted, the attackers conclude an agreement with the group to allow it to use its infrastructure and the program that encrypts the data.

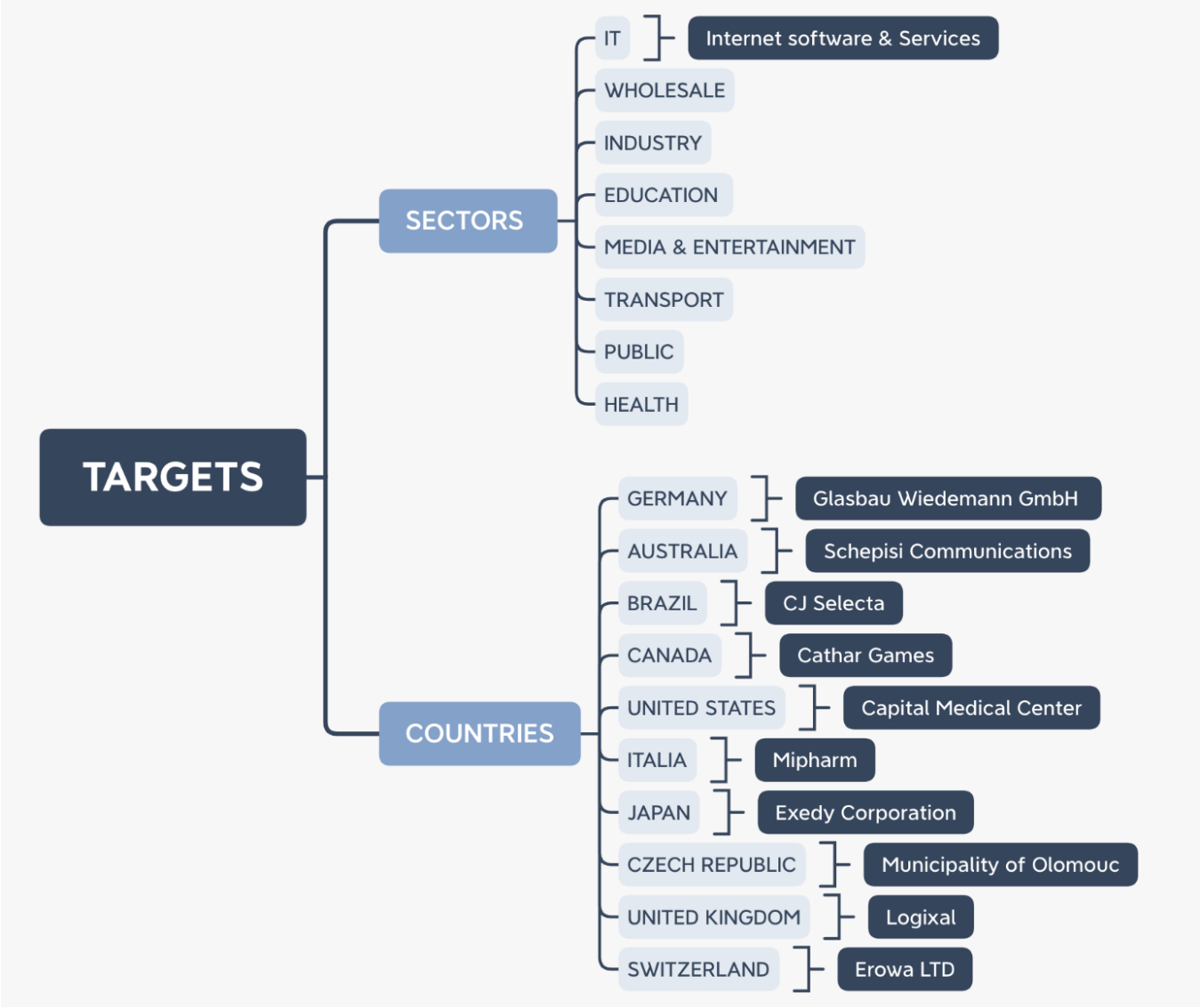
Affiliated attackers can then use the Avaddon ransomware and pay the developers with a share of the profits generated by the ransoms paid by their victims (between 15 and 35% of the profits on average). The Avaddon group's motives thus appear to be primarily lucrative, as is the case with most ransomware attacks, which are usually conducted with the opportunistic intent to obtain financial gain.

[1] Avaddon ransomware shuts down and releases decryption keys, BleepingComputer, https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

[2] Largest U.S. pipeline shuts down operations after ransomware attack, BleepingComputer, URL : https://www.bleepingcomputer.com/news/security/largest-us-pipeline-shuts-down-operations-after-ransomware-attack/

VICTIMOLOGY

The Avaddon ransomware targets international public and private organisations in a wide range of sectors including IT services, wholesale and health. Recent victims include the American company American Bank Systems (ABS) **[7]**, the Belgian consulting company Finalyse **[8]** and more recently a Maltese political party **[9]** and the insurer Group AXA **[10]**.



Major Avaddon intrusions

***Sources**: Ransomwatch – DataBreaches – DomainTools – HornetSecurity*

As a RaaS, Avaddon's targets are therefore not chosen by its developers but by their affiliated groups. However, the group prohibits buyers from targeting countries in the Commonwealth of Independent States (CIS). In addition, the ransomware runs a script to identify its targets' language during an intrusion. If it detects Russian or Ukrainian, it terminates its infection **[11]**.

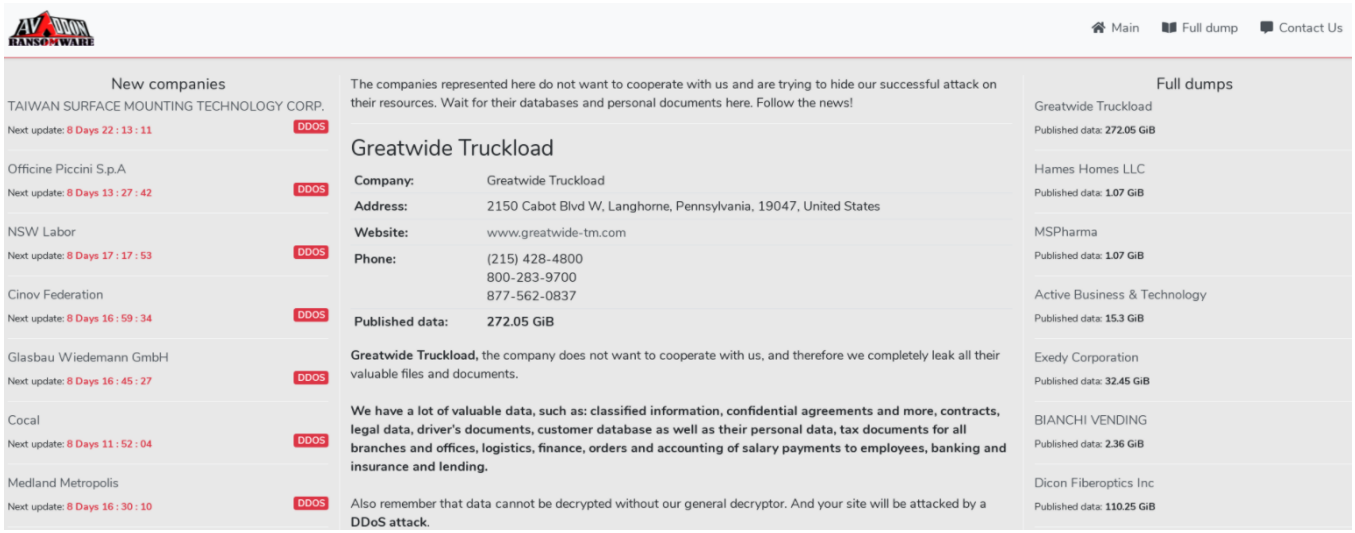
MODUS OPERANDI

Avaddon is usually distributed via phishing campaigns through e-mails containing obfuscated JPEG or ZIP attachments (which are actually JavaScript or Excel with macros). However, the ransomware exploits several other infection vectors, including being downloaded by other malware (Smoke Loader, Phorpiex/Trik, Rigek, etc.) or distributed directly once an information system has been compromised, notably via Remote Desktop Protocol (RDP) and Virtual Private Networks (VPN).

During one of our investigations, Avaddon was distributed primarily due to a lack of VPN updates and insecure passwords. The actor was then able to gain maximum privileges on the Active Directory domain, collect and exfiltrate sensitive data, and deploy his encryption software on numerous machines because of the process.

A portion of the stolen data is published on a data leak website accessible on the Deep Web to give credibility to their claims and to incite the victim to pay the ransom.

Avaddon's encryption mechanism avoids critical areas of the Windows system to allow the victim to use their computer and witness the damages. If the ransom is not paid within ten days (240 hours), the group publishes all the stolen data on its data leak website.



Avaddon Website in .onion
Source: Ransomwatch

Since January 2021, the group stated to be combining its ransomware attacks with Distributed Denial of Service (DDoS) attacks on its victims' Website to add additional pressure **[12]**.

MAJOR AVADDON UPDATES

The Avaddon ransomware has been modified and improved multiple times since the first version was released, especially regarding its encryption mechanism and its payload:

- As early as June 2020, the developers have integrated the ability to launch the payload via Powershell to address improved detection of Avaddon by antivirus software;
- In January 2021, Avaddon adds support for Windows XP and 2003;
- In February 2021, the developers fixed a vulnerability in the ransomware encryption mechanism.

This latest update follows the release of the AvaddonDecrytper decryption tool on February 9, 2021, developed by the researcher Javier Yuste. He managed to recover and analyse the ransomware encryption keys because they were stored in memory on the infected machines if they had not been rebooted **[13] [14]**.

However, this tool allowed the Avaddon developers to realise the vulnerability of their ransomware and to implement a patch a few days later **[15]**.

AVADDON MAIN FEATURES (V1)

According to SentinelOne, the first version of Avaddon includes the following features [5]:

- 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 behaviour ;

REFERENCES

[1]https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/

[2]https://appriver.com/resources/blog/june-2020/phorphiextrik-botnet-delivers-avaddon-ransomware

[3]https://www.checkpoint.com/press/2020/june-2020s-most-wanted-malware-notorious-phorpiex-botnet-rises-again-doubling-its-global-impact-on-organizations/

[4]https://www.bleepingcomputer.com/news/security/avaddon-ransomware-launches-data-leak-site-to-extort-victims/

[5] https://labs.sentinelone.com/avaddon-raas-breaks-public-decryptor-continues-on-rampage/

[6]https://www.ransomwatch.org/

[7]https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/

[8]https://www.databreaches.net/belgian-consultancy-finalyse-emerges-unscathed-from-ransomware-attack/

[9]https://timesofmalta.com/articles/view/cyber-attackers-hold-pn-to-ransom-with-major-data-leak-threat.865968

[10]https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/

[11]https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Ransom:Win32/Avaddon&ThreatID=2147768759

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

[13]https://arxiv.org/abs/2102.04796

[14]https://github.com/JavierYuste/AvaddonDecryptor

[15]https://www.zdnet.com/article/free-decrypter-released-for-avaddon-ransomware-victims-aaand-its-gone

TECHNICAL ANALYSIS

HOW AVADDON WAS ABLE TO BREACH ITS VICTIM?

Attack Description

The attacker group responsible for the attacks we investigated used the Avaddon ransomware. Knowing that Avaddon is a RaaS, different groups may use the ransomware. In general, attacker groups using this malware exploit the following entry points:

- Weak login credentials exposed on the internet (VPN SSL, RDP, etc…);
- Exploitation of a vulnerability allowing them to get a foothold in the network (Fortinet, Citrix…).

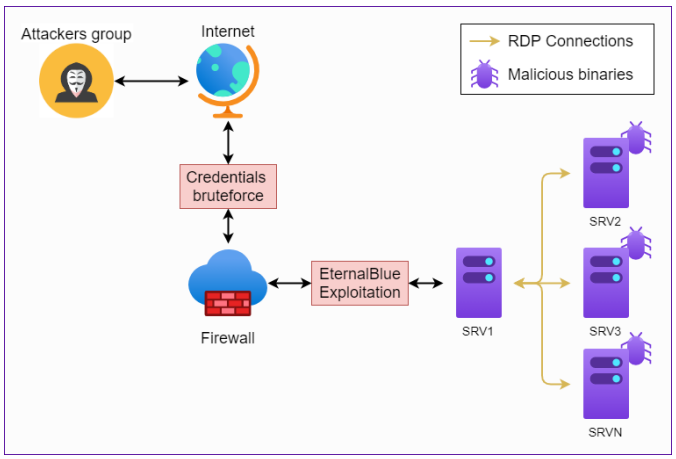


Figure 1 – Attack summary

As part of this attack, the group used weak credentials exposed via a firewall SSL VPN flaw. They then proceeded to guess other accounts based on what they obtained. One of the accounts they found was the domain administrator.

When the attackers were able to recover one or more firewall accesses, it was possible for them to move around the network. Exploiting the “EternalBlue” vulnerability, or MS17-010[3], allowed them to gain access to one of the servers. This security flaw allows an attacker to access the server without authentication, but above all it allows them to get a Super Administrator access (NT/SYSTEM).

Following this exploitation, the attacker’s group started their lateral movement in the network. The first action was to connect to other machines with the domain administrator account using remote desktop protocol (RDP).

Finally, the attacker group performed several actions on the network:

- Deployment of persistence using Cobalt Strike beacons;
- Deployment of a Mimikatz[4] executable used to retrieve credentials in memory;
- Internal network scan;
- Sensitive data exfiltration.

TTPs in use during the different attacks we investigated are referenced in a MITRE ATT&CK matrix at the end of the document.

Cobalt Strike Deployment

Cobalt Strike[5] is a Command and Control (C2) server, which allows attackers or red teamers to control infected machines. Beacons are malicious programs that allow an attacker to perform actions on the compromised machines.

Beacons analysed on the information system are deployed with a Powershell script.
This power shell script uses the “iex” cmdlet to execute scripts, binaries or binary streams. In this case, the different steps of the power shell decode base64 and execute it in memory.

```
IEX (New-Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,
[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

Figure 2 – First execution stage

This script executes a second power shell script. This one also uses the “iex” cmdlet to execute the real Cobalt Strike binary load in memory:

```
If ([IntPtr]::size -eq 8) {
    start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {
    IEX $DoIt
}
```

Figure 3 – Second execution stage

The final execution step is the Cobalt Strike beacon.

It was possible to extract the beacon configuration, allowing analysts to find the C2 address and other information. Finally, when all sensitive data was exfiltrated, attackers deleted the Firewall event logs and deployed the “Avaddon” ransomware.

[3] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
[4] https://github.com/gentilkiwi/mimikatz/wiki
[5] https://www.cobaltstrike.com/

AVADDON RANSOMWARE IN USE

The analysed sample is a 32-bit PE Windows executable file called “**exe_CLIENTNAME.en.exe**“. It is compiled with Microsoft Visual C++ with a compilation date/time group of March 09, 2021 18:35:19.

When the executable is launched, the ransomware checks if it has privileged user rights. If not, it does not run.

When files are encrypted, the ransomware drops the note “XXXXXX_readme.txt” in all folders with encrypted files. This note contains instructions for victims to pay the ransom.

At the end of this note, an identifier is indicated. The attacker group to identify the infected machines uses this identifier.

RCID – Machiner identifier

This identifier is represented by a base64 encoded block. Decoding this block shows two elements:

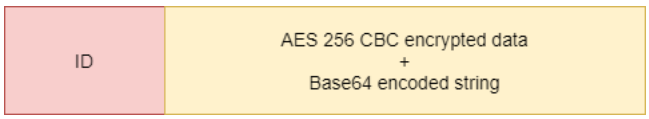


Figure 4 – RCID format

The red “ID” part is a numerical value: “**XXXX**“. It was possible to find this value in the malware code. It can be a campaign number or a malware version.

The key and the initialisation vector are hardcoded in the malware:

- AES key (b64) : **REDACTED**
- IV (b64) : **REDACTED**

This data contains the encrypted file extension, an “RCID”, the list of mounted disks, language of the machine and its host name.

The RCID represents the unique identifier of the compromised machine and is based on an asymmetric algorithm (RSA). Below, a summary diagram of the RCID generation:

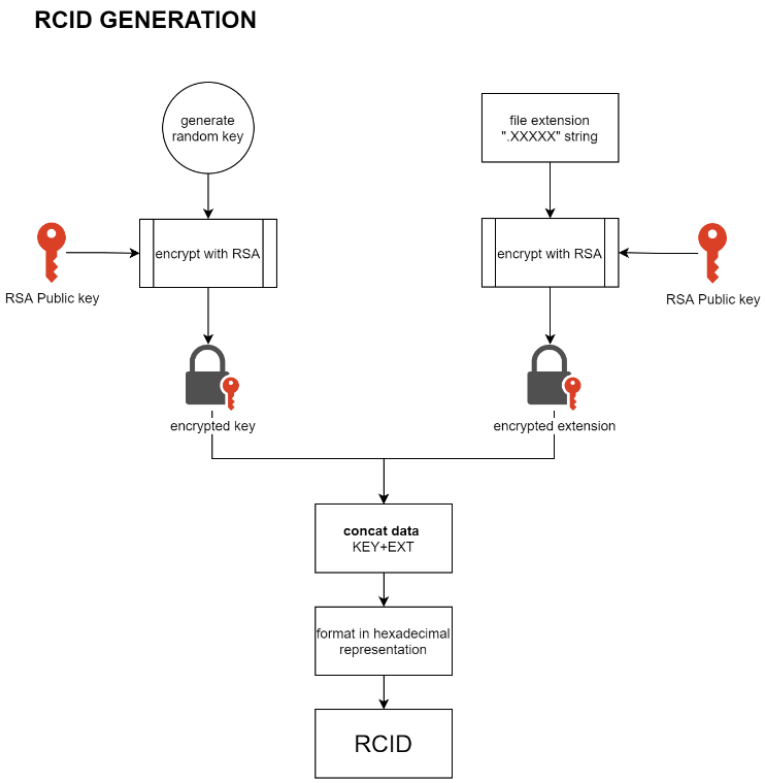


Figure 5 – RCID generation

Malware configuration

The configuration of this ransomware is encrypted using a XOR. This operation can be easily reversed when the key is known. Below are the main elements extracted from the configuration:

Extensions not to encrypt	.exe,.bin,.sys,.ini,.dll,.lnk,.dat,.drv,.rdp,.prf,.swp
RSA1 public key (b64)	**REDACTED**
Database extension	.mdf,.mds,.sql
Services to kill	DefWatch,ccEvtMgr,ccSetMgr,SavRoam,dbsrv12,sqlservr,sqlagent,Intuit.QuickBooks.FCS,dbeng8,sqladhlp,QBIDPService,Culserve
Processes to kill	sqlservr.exe,sqlmangr.exe,RAgui.exe,QBCFMonitorService.exe,supervise.exe,fdhost.exe,Culture.exe,RTVscan.exe,Defwatch.exe,w
Note ID	**REDACTED**
AES 256 key (b64)	**REDACTED**
IV (b64)	**REDACTED**

Deleting backups

Since Windows XP, Microsoft has developed a technology known as **Volume Snapshot Service** or **Shadow Copy**. Shadow Copy allows automatic file backups to be made transparently to the user. When the ransomware starts, this feature is disabled and then the backups are deleted by executing multiple wmic and wbadmin commands. Most of the commands are executed with the **CreateProcessW** API. These commands are console applications, so they display a **cmd.exe** window when executed.

```
result = CreateProcessW(0, vss_cmd, 0, 0, 1, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
if ( result )
{
  WaitForSingleObject(ProcessInformation.hThread, 0xFFFFFFFF);
  CloseHandle(ProcessInformation.hProcess);
  result = CloseHandle(ProcessInformation.hThread);
}
```

Figure 6 – Commands execution routine

Nevertheless, the first wmic command differs from the others. It is executed 3 times through the Microsoft Component Object Model (COM) technology with the WBEM Locator interface. This interface allows to execute a WMI command with **Win32_Process** class and **Create** method. This method is equivalent to the previous **CreateProcessW** API, but it is less detectable by attack response systems. At the same time, the recycle garbage is emptied of its contents with the **SHEmptyRecycleBinW** API.

Disabling the UAC

To avoid user interaction during the encryption process as much as possible, UAC (User Account Control) is disabled in the registry. Thus, no dialog box will appear when the system requires access to administrator rights. Below the code that edits registry key *EnableLUA*:

```
if ( !RegOpenKeyExW(HKEY_LOCAL_MACHINE, (LPCWSTR)enable_uac_key, 0, 0xF003Fu, &phkResult) )
{
  if ( v3->cap >= 8u )
    v3 = (wstring_obj_s *)v3->wstr;
  RegSetValueExW(phkResult, (LPCWSTR)v3, 0, 4u, Data, 4u);// remove UAC dialog box
  RegCloseKey(phkResult);
}
```

Figure 7 – Registry key modification in order to disabling the UAC

Searching for hidden volumes

Some volumes are mounted by different users on the same machine. Each user therefore has access to his or her own mounted volumes. In order to encrypt these volumes, Avaddon will disable this partitioning by modifying the registry. This modification allows all processes running as an administrator to access volumes mounted by users of the machine. Some volumes are also hidden. To find and encrypt them, the ransomware will browse all volumes on the disks with the **FindFirstVolume** API and then attempt to mount these volumes with **SetVolumeMountPointW** to access them:

```
do
{
  if ( !*(_DWORD *)(v4 + 40) && v2 != v3 )
  {
    v3 -= 6;
    strcpy(lpszVolumeMountPoint, v3);
    v5 = (unsigned int)v3[5];
    if ( v5 >= 8 )
      free_string(*v3, 2 * v5 + 2);
    v3[4] = 0;
    v3[5] = (void *)7;
    v6 = (const WCHAR *)v4;
    *(_WORD *)v3 = 0;
    v7 = *(_DWORD *)(v4 + 20) < 8u;
    HIDWORD(v13) = v3;
    if ( !v7 )
      v6 = *(const WCHAR **)v4;
    v8 = (const WCHAR *)lpszVolumeMountPoint;
    if ( v12 >= 8 )
      v8 = lpszVolumeMountPoint[0];
    SetVolumeMountPointW(v8, v6);
    v10 = 1;
    if ( v12 >= 8 )
      free_string((void *)lpszVolumeMountPoint[0], 2 * v12 + 2);
  }
  v4 += 72;
}
while ( v4 - 24 != vol[0] );
```

Figure 8 – Browsing all volumes

Services and processes kill list

Avaddon cannot access some files, because they are already open by another program. For example, the files in a Microsoft SQL server database. To overcome this problem, a routine allows stopping a selection of processes/services that are defined in the configuration. Examples of the code allowing deleting a service:

```
v3 = OpenSCManagerW(0, 0, 0xF003Fu);
v4 = v3;
if ( v3 )
{
  if ( *((_DWORD *)lpServiceName + 5) >= 8u )
    v1 = *(const WCHAR **)lpServiceName;
  v5 = OpenServiceW(v3, v1, 0x10020u);
  v6 = v5;
  if ( v5 )
  {
    v2 = DeleteService(v5);
    CloseServiceHandle(v6);
  }
  CloseServiceHandle(v4);
}
```

Figure 9 – Kill list of services and process according to the malware configuration

Persistence

To persist in the system, Avaddon copies itself into the **%APPDATA%\Microsoft\Windows** folder with the same file name. Then it installs itself in the Windows task scheduler using the **ITaskService** interface through the Microsoft COM technology. The task is set to run the ransomware copy every 10 minutes indefinitely:

```
if ( CoCreateInstance(&stru_488F5C, 0, 1u, &CLSID_ITaskService, (LPVOID *)&v90) < 0 )
  return;
```

Figure 10 – Interaction with task scheduler

To avoid multiple execution of the ransomware and thus encrypting files that have already been encrypted, a mutex is created under the name: **Global{REDACTED}.** The presence of this mutex is checked at each launch, if it is present then the program ends, because an instance of Avaddon is already running.

Asynchronous Multithreading

To encrypt as quickly as possible Avaddon will use a Windows kernel technology called **I/O CompletionPorts**. This technology allows to create a thread pool to handle asynchronous I/O requests efficiently on multi-core systems. Each of the threads has the task of encrypting one file at a time. The number of threads created is proportional to the number of processors/cores the machine has:

```
n_core = get_number_of_proc();
handle_ioc = CreateIoCompletionPort((HANDLE)0xFFFFFFFF, 0, 0, n_core);
if ( handle_ioc != (HANDLE)-1 && n_core )
{
  do
  {
    v9 = create_thread(0, 0, (LPCWSTR)get_queued_completion_status, this, 0, 0);
    if ( v9 )
```

Figure 10 – Asynchronous multithreading

The threads are then put on hold until they are presented with a file path to encrypt.

Encryption through network

As noted earlier the ransomware will encrypt all volumes it encounters, whether local or remote. However, Avaddon goes further by using the machine's ARP cache to discover new networks. Each new network is then fully scanned for a CIFS/SMB volume that can be mounted and encrypted:

```
if ( wcscmp_0(v9, ip_addr) && req_send_arp(ip_addr, (LPCWCH)v9) )// request ARP cache
{
  v39 = 0;
  *(_QWORD *)Src = 0i64;
  net_share_enum((int)Src, ip_addr);      // network enumeration
  LOBYTE(v40) = 4;
  v11 = *(_QWORD *)Src;
  if ( Src[0] != Src[1] )
  {
```

Figure 11 – Network enumeration using ARP cache

File encryption

Avaddon scans every file on the machine (or on remote volumes). Some file extensions are not encrypted according to the ransomware configuration, as they could affect the system stability and prevent the recovery of the ransom note and data.

To encrypt a file, Avaddon uses two modes. A first mode that allows you to specify how many bytes it should encrypt using the configuration, and a second mode that by default encrypts a maximum of 1048576 bytes. In our sample it is this second mode that is used. Thus beyond the first 1048576 (1000000h) bytes of a file, the data are no longer encrypted. Example of a text file :

```
000FFFB0  FA C0 E8 02 88 AA 3E 9D 92 F3 BF 36 27 97 22 AF  úÀè.ˆª>.'ó¿6'—"¯
000FFFC0  95 E3 95 B9 FD F8 E0 FD F6 67 D0 BD 35 1D D2 45  •ã•¹ýøàýögÐ½5.ÒE
000FFFD0  9C 8F C6 56 6B B8 32 [illegible]                 œ.ÆVk¸2/Tnyï-.#"
000FFFE0  1F 68 D7 3A 8C C6 8E [illegible]                 .h×:ŒÆŽ.´Æ`r&-ä·
000FFFF0  9B BE 47 B6 0A 19 EE 49 8D D5 E5 56 A3 A4 12 CA  ›¾G¶..îI.ÕåV£¤.Ê
00100000  2E 20 73 74 61 72 74 69 6E 67 20 22 73 63 72 69  . starting "scri
00100010  70 74 2E 70 79 22 20 69 6E 73 74 65 61 64 20 6F  pt.py" instead o
00100020  66 20 22 70 79 74 68 [illegible]                 f "python script
00100030  2E 70 79 22 29 2C 0D 0A 20 20 20 20 20 20 20 20  .py"),..
00100040  72 65 64 69 72 65 63 74 73 20 6D 61 79 20 6E 6F  redirects may no
00100050  74 20 77 6F 72 6B 20 75 6E 6C 65 73 73 20 79 6F  t work unless yo
```

Encrypted data

Clear text data

Figure 12 – Data examples

In order to encrypt a file, Avaddon generates a random 256 CBC crypto-quality AES key with the CryptGenKey API. Each file is encrypted with a unique key per block of 8192 bytes. This key is then encrypted with the RSA public key and concatenated to the encrypted string stands for malware extension (identical to the RCID). This data is then inserted at the end of the file (see next section) and the AES key is deleted. In order to retrieve the AES key and decrypt the file, you must have the private key that Avaddon has. Below is the summarised diagram:

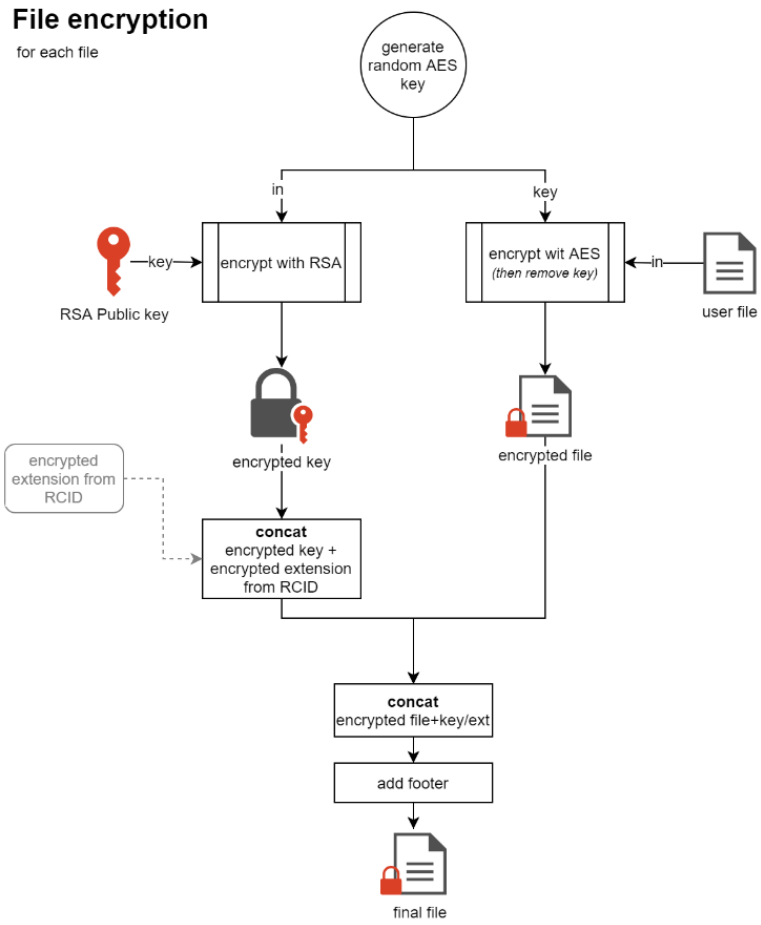


Figure 13 – File encryption process

1.1.1. File identifier

Each encrypted file embeds at its end, some data containing its own AES key to allow decryption. The end structure is composed as follows (data in little endian):

- Encrypted AES key using RSA;
- RSA encrypted extension ;
- In red on 8 bytes, the size of the original file;
- In blue on 4 bytes, the sum of the size of the blocks: AES key + the size of the extension block;
- In green on 4 bytes, the encryption mode which corresponds here to the maximum (see previous section);
- In yellow on 4 bytes, the Avaddon identifier (magic value);

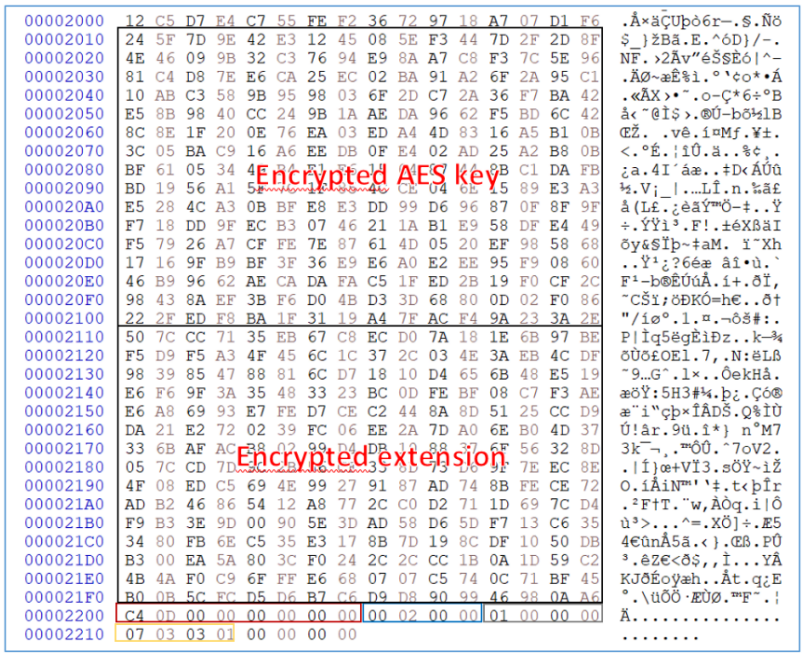


Figure 14 Encrypted data

1.2. MITRE Att&ck Framework

ID	TTP	Détection
T1021	Remote Services	Usage of RDP and SMB services
T1133	External Remote Services	Usage of external VPN
T1595	Active Scanning	Network scan – Firewall logs – Exposed IP address scans.
T1190	Exploit Public-Facing Application	Attackers have exploited CVE-2018-13379 for FortiGate VPNs to gain access to existing accounts
T1498	Denial of Service	In order to pressure his victims, Avaddon performs denials of service on his victims' external services.
T1035	Exécution	Avaddon creates Windows services such as wmic, wbadmin, vssadmin and bcdedit.
T1003	OS Credential Dumping	The Mimikatz tool was used by the attackers on different servers, thanks to the retrieval of the in-memory value of the lsass.exe process.
T1046	Network Scanning Service	Network scanning tools have been detected on several compromised machines.
T1098	Account Manipulation	Credentials have been maintained by obtaining full access.
T1485	Data Destruction	Destruction of files through the encryption of elements of the majority of servers and workstations.
T1486	Data Encrypted for Impact	File encryption of all affected machines.
T1112	Defence Evasion	Antivirus / EDR deletion.
T1083 T1016 T1120	Discovery	Avaddon searches for files by extension, requests machine and network information, detects if it is in a sandbox and requests device information from the affected machine
T1060	Persistence Scheduled Task / jobs	To persist in the system, Avaddon copies itself into the %APPDATA%\Microsoft\Windows\ folder. Then it installs itself in the Windows task scheduler using the ITaskService interface through Microsoft COM technology.
T1055.012	Process Injection: Process Hollowing	Process Injection with Cobalt Strike
T1043	Command and Control	Avaddon uses port 443 for communication.

T1059	Command and Scripting Interpreter: PowerShell	Powershell was used to leverage the download and launch of a fileless Cobalt Strike beacon
T1490	Inhibit System Recovery	Avaddon uses vssadmin, bcdedit and wbadmin to remove recovery capabilities from the Windows machine.

Posted on: **Jun 7th**

By **Loïc Castel**,
Head of Digital Forensics & Incident Response, CERT-DS, Atos

Follow or contact Loïc :

Share this article

Follow us on

twitter@Atos_Security
[#DataProtection] 🔐 Do you need to protect your sensitive data in #Microsoft365 ? Dual key encryption #DKE technology enables you to keep control of your #encryption keys & ensures that #sensitivedata remains inaccessible from any 3d party. ➡️ https://t.co/WTS3sBqDA
May 27, 2022

twitter@Atos_Security

🤔 Better connected, but less secure? #Cyberattacks can come from anywhere, and spread fast. More and more organizations need tighter #cybersecurity for their people, their data, and #IoT. Watch the full video 👉 https://t.co/RQqy6sdTYT#Zer

May 27, 2022

twitter@Atos_Security

[#EVENT] During #ICTSpring2022@Vasco_M_Gomes will be speaker on June 30th on the session: "The battle of AI to solve virtual-world digital identity challenges" To know more 👉 https://t.co/EmHGk9UPbV@ICTSpring#AI#DigitalIdent

May 26, 2022