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].

S 🖬 🔊	Of ↑ ↓ = Your new photo? - Message (Plain Text)	? 🛧 – 🗆 🗙
FILE M	IESSAGE	
	Fri 6/5/2020 12:41 AM	
	Billy Green <billy73@3189.com></billy73@3189.com>	
	Your new photo?	
o desperied	ngh an the second	
Message	100 IMG123101.jpg.js.zip (665 B)	
See more at	bout Billy Green.	29.

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.

DANSONWADE
RARSO MARE

New companies TAIWAN SURFACE MOUNTING TECHNOLOGY CORP. Next update: 8 Days 22 : 13 : 11	The companies repres their resources. Wait f	sented here do not want to cooperate with us and are trying to hide our successful attack on for their databases and personal documents here. Follow the news!	Full dumps Greatwide Truckload Published data: 272.05 Gi8	
Officine Piccini S.p.A	Company:	Greatwide Truckload	Hames Homes LLC	
Next update: 8 Days 13 : 27 : 42	Address:	2150 Cabot Blvd W, Langhorne, Pennsylvania, 19047, United States	Published data: 107 GiB	
NSW Labor	Website:	www.greatwide-tm.com	MSPharma	
Next update: 8 Days 17 : 17 : 53	Phone:	(215) 428-4800	Published data: 1.07 GiB	
Cinov Federation Next update: 8 Days 16: 59: 34 DDDDS	Published data:	800-283-9700 877-562-0837 272.05 GiB	Active Business & Technology Published data: 15.3 GiB	
Glasbau Wiedemann GmbH	Greatwide Truckload	, the company does not want to cooperate with us, and therefore we completely leak all their uments.	Exedy Corporation	
Next update: 8 Days 16 : 45 : 27	valuable files and doc		Published data: 32.45 GiB	
Cocal Next update: 8 Days 11 : 52 : 04 DDOS	We have a lot of valu legal data, driver's do branches and offices	able data, such as: classified information, confidential agreements and more, contracts, ocuments, customer database as well as their personal data, tax documents for all , logistics, finance, orders and accounting of salary payments to employees, banking and	BIANCHI VENDING Published data: 2.36 GiB	
Medland Metropolis	Also remember that da	g.	Dicon Fiberoptics Inc	
Next update: 8 Days 16 : 30 : 10 DDOS		ata cannot be decrypted without our general decryptor. And your site will be attacked by a	Published data: 110.25 GiB	

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-globalimpact-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.



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:



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:

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:

encrypt RSA1 REDACTED public key (b64) .mdf,.mds,.sql Database extension DefWatch,ccEvtMgr,ccSetMgr,SavRoam,dbsrv12,sqlservr,sqlagent,Intuit.QuickBooks.FCS,dbeng8,sqladhlp,QBIDPService,Culserve Services to kill Processes sqlservr.exe,sqlmangr.exe,RAgui.exe,QBCFMonitorService.exe,supervise.exe,fdhost.exe,Culture.exe,RTVscan.exe,Defwatch.exe,w to kill Note ID REDACTED AES 256 REDACTED key (b64) IV (b64) REDACTED

Extensions .exe,.bin,.sys,.ini,.dll,.lnk,.dat,.drv,.rdp,.prf,.swp not to

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.



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*:



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:





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:



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:



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:



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:



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 :

úÀè.^ª>.'ó;6'-" [—]	AF	22	97	27	36	BF	F3	92	9D	3E	AA	88	02	E8	C0	FA	000FFFB0
•㕹ýøàýögĐ½5.ÒE	45	D2	1D	35	BD	D0	67	F6	FD	E0	F8	\mathbf{FD}	В9	95	E3	95	000FFFC0
œ.ÆVk,2/Tnyï#"	93	23	ita	é	ha.	ot?	rŴł	nici	2	32	B8	6B	56	C6	8F	9C	000FFFD0
.h×:ŒZŽ.´ZÈ`r&-ä`	в7	E4	2D	26	-72	~60	-66	-B4	15	8E	C6	8C	3A	D7	68	1F	000FFFE0
>¾G¶îI.ÕåV£¤.Ê	CA	12	A4	A3	56	E5	D5	8D	49	EE	19	0A	B6	47	BE	9B	000FFFF0
 starting "scri 	69	72	63	73	22	20	67	6E	69	74	72	61	74	73	20	2E	00100000
pt.py" instead o	6F	20	64	61	65	74	73	6E	69	20	22	79	70	2E	74	70	00100010
f "python script	74	70	ta	ō2	хŧ	ťê	aîr	ē	6	68	74	79	70	22	20	66	00100020
.py"),	20	20	20	20	~20	20	~20	~20	0 A	0D	2C	29	22	79	70	2E	00100030
redirects may no	6F	6E	20	79	61	6D	20	73	74	63	65	72	69	64	65	72	00100040
t work unless yo	6F	79	20	73	73	65	6C	6E	75	20	6B	72	6F	77	20	74	00100050

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);

$\begin{array}{c} 00002010 \\ 00002020 \\ 4E 46 09 9B 32 C3 76 94 E9 8A A7 C8 F3 7C 5E 96 \\ 00002030 \\ 8I C4 D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D8 7E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D 87E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D 87E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D 87E EG CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ A2 a81 C 4D 87E EG CA 25 EC 02 BA 91 A2 6F 2A 92 5A 28 80 B \\ C0002070 \\ 3C 05 BA C9 16 A6 EE DB 0F E4 02 AD 25 A2 B8 0B \\ C 2 & v^{2} (1) A . & c^{2} (1) A . & c$	00002000	12	C5	D7	E4	C7	55	FE	F2	36	72	97	18	A7	07	D1	F6	.Å×äÇUþò6r—.§.Ñö
$\begin{array}{c} 00002020 \\ 00002020 \\ 81 C4 D8 7E E6 CA 25 EC 02 BA 91 A2 6F 2A 95 C1 \\ .Å@~aE$i^~o^co^*A \\ 00002040 \\ 10 AB C3 58 9B 95 98 03 6F 2D C7 2A 36 F7 BA 42 \\ .Å@~aE$i^~o^co^*A \\ 00002050 \\ E5 8B 98 40 CC 24 9B IA AE DA 96 62 F5 BD 6C 42 \\ .Å~aTs, o^cb^{+}A \\ 00002070 \\ 3C 05 BA C9 I6 A6 EE DB 0F E4 02 AD 25 A2 B8 0B \\ .~e^*E.i^{+}A. \\ .00002080 \\ BF 61 05 34 4E BCF VIEL AAE DA 96 62 F5 DB 61 DA FB \\ .outer AAE A \\ .outer$	00002010	24	5F	7D	9E	42	E3	12	45	08	5E	F3	44	7D	2F	2D	8F	\$_}žBã.E.^óD}/
$\begin{array}{c} 00002030 \\ 00002040 \\ 10 \ AB \ C3 \ 58 \ 9B \ 95 \ 96 \ 03 \ 6F \ 2D \ C7 \ 2A \ 36 \ F7 \ BA \ 42 \\ (aK_{X})^{-}, o-C^{+}6^{+}B \\ (aK_{X})^{-}, o-C^{+}B \\ (aK_{X})^{+}, o-C^{+}B \\ (aK_{X})^{-}, o-C^{+}B$	00002020	4E	46	09	9B	32	C3	76	94	E9	8A	Α7	C8	F3	7C	5E	96	NF.>2Ãv″銧Èó ^-
$\begin{array}{c} 00002040 & 10 \ \text{AB C3 58 9B 95 98 03 6F 2D C7 2A 36 F7 BD 64 22 \\ 00002050 & E5 8B 98 40 CC 24 9B 1A AE DA 96 62 F5 BD 6C 42 \\ a^{<}\text{eff},, 0-c^{<}6+^{\circ}\text{B}\\ a^{<}\text{eff},, 1.1, n., n^{<}\text{a}\\ a^{<}\text{eff},, 1.1, n., 1.1, n.$	00002030	81	C4	D8	7E	Eб	CA	25	EC	02	BA	91	A2	бF	2A	95	C1	.ÄØ∼æÊ%ì.°`¢o*•Á
$\begin{array}{c} 00002050 \\ 00002050 \\ 8C & 8E \\ 1F \\ 20 \\ 00002070 \\ 3C & 05 \\ BA \\ CP \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 1$	00002040	10	AB	C3	58	9B	95	98	03	6F	2D	C7	2A	36	F7	BA	42	.≪ÃX>•~.o−Ç*6÷°B
$\begin{array}{c} 00002060 \\ 00002070 \\ 3C 05 BA C9 16 A6 EE DB 0F E4 02 AD 25 A2 B8 0B \\ c. ^{e}C. ^{i}(10.3%c,) \\ 00002080 \\ BF 61 05 34 4E 11C FLOED C1 AFB \\ c. ^{e}C. ^{i}(10.3%c,) \\ c. ^{e}C. ^{i}(10.3%c,) \\ c. ^{e}C. ^{i}(10.3%c,) \\ 00002090 \\ BD 19 56 A1 55 C C C C C C C C C C C C C C C C C C$	00002050	E5	8B	98	40	CC	24	9B	1A	AE	DA	96	62	F5	BD	6C	42	å∢~@Ì\$>.®Ú−bõ½lB
$\begin{array}{c} 00002070 \\ 00002070 \\ BF 61 05 34 \\ 4E \\ ncrvptcl cl c$	00002060	8C	8E	1F	20	0E	76	EA	03	ED	A4	4D	83	16	Α5	В1	0B	ŒŽvê.í¤Mf.¥±.
00002080 BF 61 05 34 4E AFR of the construction of the constructin of the construction of the constructin of the construction of	00002070	3C	05	BA	C9	16	Aб	EE	DB	0F	E4	02	AD	25	A2	B8	0B	<.°É.¦1Û.ä%¢,.
00002090 BD 19 56 A1 55.15.14 figs.46 Ch 04 cF 15 89 E3 A3 4z.v[.]Li.n.tat 00002080 F7 18 DD 9F E2 83 4C A3 0B BF E8 E3 DD 99 D6 96 87 0F 8F 9F Å (Lf.:¿àáǐmö-tÝ 00002080 F7 18 DD 9F E2 80 746 21 1A B1 E9 58 DF E4 49 ÷.ÝÌi's.F'.téXbăi 00002080 F7 18 DD 9F E2 80 746 21 1A B1 E9 58 DF E4 49 ÷.ÝÌi's.F'.téXbăi 00002080 F7 18 DD 9F E7 78 26 A7 CF FE 7E 87 61 4D 05 20 EF 98 58 68 öysšIp-taM. 1'Xh 00002080 46 B9 96 62 AE CA DA FA C5 1F ED 28 19 F0 CF 2C F'-bsÉtôtâ.1+.ði. 00002100 22 2F ED F8 BA 1F 31 19 A4 7F AC F4 9A 23 3A 2E "/iø°.1.αðš#:. 00002110 50 7C CC 71 35 EB 67 C8 EC DO 7A 18 1E 68 97 BE Plig5egÈlbzk-44 00002120 98 39 85 47 88 81 6C D7 18 10 D4 65 6B 48 E5 19 "jő.ixôekHå. 00002140 E6 F8 93 A5 48 33 23 BC DF EB F08 C7 F3 AE a*0%5154*4.b;.ç.óc % övöc5021.7, N:eLB 00002150 B6 A8 69 93 E7 FE D7 CE C2 44 8A 8D 51 25 CC D9 a*i*cpxfAb5.Q*l0 00002160 DA 1E 272 02 39 FC 06 E2 A7 DA 06 EB 04 D3 70 ú!ar-gu.i*a) övö.70.70 00002160 DA 21 E2 72 02 39 FC 06 E2 A7 DA 06 EB 04 D3 70 ú!ar-gu.i*a) ö.0.70 00002160 DA 21 E2 72 02 39	00002080	BF	61	05	34	4 2	h ŕ	r vi	n f	h	Δ^4	8	120	βB	C1	DA	FB	;a.4I´áæ‡D∢ÁÚû
$\begin{array}{c} 000020A0 \\ 000020B0 \\ F5 & 28 & 4C & A3 & 0B & BF & E8 & E3 & DD & 99 & D6 & 96 & 87 & 0F & 8F & 9F \\ 000020B0 \\ F7 & 18 & DD & 9F & EC & B3 & 07 & 46 & 21 & 1A & B1 & E9 & 58 & 0F & E4 & 49 \\ 000020D0 & 17 & 16 & 9F & B9 & BF & 3F & 36 & E9 & E6 & A0 & E2 & EF & 98 & 58 & 68 \\ 000020D0 & 17 & 16 & 9F & B9 & BF & 3F & 36 & E9 & E6 & A0 & E2 & EF & 9F & 98 & 68 \\ 000020D0 & 17 & 16 & 9F & B9 & BF & 3F & 36 & E9 & E6 & A0 & E2 & EF & 9F & 98 & 68 \\ 000020D0 & 17 & 16 & 9F & B9 & BF & 3F & 36 & E9 & E6 & A0 & E2 & EF & 9F & 98 & 68 \\ 00002100 & 22 & 2F & ED & F8 & BA & 1F & 31 & 19 & A4 & 7F & AC & F4 & 9A & 23 & A2 & E \\ 00002110 & 50 & 7C & CC & 71 & 35 & EB & 67 & C8 & EC & D0 & 7A & 18 & 1E & 6B & 9F & BF & 116 \\ 00002120 & F5 & D9 & F5 & A3 & FF & 45 & 6C & 1C & 37 & 2C & 03 & 4E & 3A & EB & 4C & DF & 00002130 \\ 98 & 39 & 85 & 47 & 88 & 81 & 6C & D7 & 18 & 10 & D4 & 65 & 6B & 48 & E5 & 19 \\ 00002140 & E6 & F6 & 9F & 3A & 35 & 48 & 33 & 23 & BC & DF EB & F0 & C7 & F3 & AE & & & & & & & & & & & & & & & & & $	00002090	BD	19	56	A1	5	- filos	-1 de	haran	410	CE	04	6Ŀ	15	89	E3	A3	½.V;_ LÎ.n.‰ã£
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	000020 A 0	E5	28	4C	A3	0B	BF	E8	E3	DD	99	D6	96	87	0F	8F	9F	å(L£.;èãÝ™Ö-‡Ÿ
000020C0 F5 79 26 A7 CF FE 7E 87 61 4D 05 20 EF 98 58 68 öyssfb~+aM. 1*Xh 000020D0 17 16 9F B9 BF 3F 36 E9 E6 A0 E2 EE 95 F9 08 60 .°Y:266æ âî•ù.` 000020E0 46 B9 96 62 AE CA DA FA C5 1F ED 2B 19 F0 CF 2C F'-bo®D'UA.i+.8T 00002100 22 2F ED F8 BA 1F 31 19 A4 7F AC F4 9A 23 3A 2E "/io°.1öš#:. 00002110 50 7C CC 71 35 EB 67 C8 EC D0 7A 18 1E 6B 97 BE Pliq5egÈlbz.k-å 00002120 98 39 85 47 88 81 6C D7 32 C0 3 4E 3A EB 4C DF ÖÜOCOE1.7.N.*LB 00002120 F5 D9 F5 A3 4F 45 6C 1C 37 2C 03 4E 3A EB 4C DF ÖÜOCOE1.7.N.*LB 00002120 F6 9F 3A 35 48 33 23 BC DF EB F08 C7 F3 AE mö'S:513#4.jc.jc.¢c% 00002120 DA 21 E2 72 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 "i'ar.9u.i*] n°M7 00002100 DA 21 E2 72 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 "i'ar.9u.i*] n°M7 00002100 DS 7C CD 7D.5C C4 MD B 3A 25 7F 56 32 8D XF*ÔU.70'2 00002100 Ja B2 46 86 54 12 A8 77 2C C0 27 11 DF 69 7C D4 .'' 00002100 AD B2 46 86 54 12 A8 77 2C C0 12 71 1D 69 7C D4 .' 00002100 B3 08 FB 6C 53 5E 31 78 B7 D1 98 CD F10 50 D8 46tmÅ5a 000021100 B3 00 EA 5A A0 3C 70 24 2C 2C CC 1B A0 A1 59 7C D4	000020B0	F7	18	DD	9F	EC	B3	07	46	21	1A	В1	E9	58	\mathbf{DF}	E4	49	÷.ÝŸì³.F!.±éXßäI
00002000 17 16 9F B9 BF 3F 36 E9 E6 A0 E2 EE 95 F9 08 60	000020C0	F5	79	26	Α7	CF	FE	7E	87	61	4D	05	20	EF	98	58	68	õy&§Ïþ~‡aM. ï~Xh
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	000020D0	17	16	9F	В9	BF	3F	36	E9	E6	A0	E2	EE	95	F9	80	60	Y¹;?6éæ âî•ù.`
000020F0 98 43 8A EF 3B F6 D0 4B D3 3D 68 80 D0 02 F 86 "CS1; dBKO=h6dt 00002100 22 2F ED FB AA 1F AA FA AC F4 9A 23 3A 2E "/io°.1oš#:. 00002110 50 7C CC 71 35 EB 67 CE EC D7 18 1E 6B 97 BE Plig5egÈlbzk-% 00002140 E6 F6 97 A3 54 83 23 BC DF BF 88 51 25 "	000020E0	46	В9	96	62	AE	CA	DA	FA	C5	1F	ED	2B	19	F0	CF	2C	F ¹ -b®ÊÚúĂ.í+.ðÏ,
00002100 22 22 FE BA F 31 19 A4 7F AC F4 9A 23 A2 "/fa°.1."ôš#:. 00002100 50 7C CC 71 35 EB 67 C8 EC D0 7A 18 1E 6B 97 BE Pliq5ägåiDz.k.*% 00002120 F5 P5 A3 4F 45 CC 13 10 D4 65 6B 48 E5 19 "ôc*L.*% 00002140 E6 F6 9F 3A 54 33 23 BC DF BF 08 CT 7A A8 #5':S1B3#4.bz.c% #2:C CO #2':C CC D9 #2':C CD	000020F0	98	43	8A	EF	3B	Fб	D0	4B	D3	3D	68	80	0D	02	F0	86	~CŠï;öÐKÓ=h€ð†
00002110 50 7C CC 71 35 EB 67 C8 EC D0 7A 18 1E 6E 97 BE Pl1q5egEiDzk.→4 00002120 F5 D9 F5 A3 4F 45 6C 1C 37 2C 03 4E 3A EB 4C DF FÖD6DE1.7, N:&LA 00002130 98 39 85 47 88 81 6C D7 18 10 D4 65 6B 48 E5 19 ¬9.G^1.×ôekHå 00002140 E6 F6 9F 3A 35 48 33 23 BC 0D FE BF 08 C7 F3 AE ∞85'5H3#4.bjCó@ 00002160 DA 21 E2 72 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 ∞3'f6 56 32 8D 00002170 33 6B AF AC F8 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 %1*a.9mi.*1* n ^m T 00002180 D5 7C CD 7D 12 42 02 9C 10 0 0 E1 A 88 37 6F 56 32 8D %1*a.9mi.*1* n ^m T 00002180 G5 7C CD 7D 12 42 0 20 9C 10 0 35 50 77 18 EF 7E EC 72 %1#a.9mi.*1* n ^m T 00002180 G5 7C CD 7D 12 42 0 2C CO D2 71 1D 69 7C D4 %2*fT."w, Àòq.ilô 00002180 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 %3<*EX0}+.E5	00002100	22	2F	ED	F8	BA	1F	31	19	A4	7F	AC	F4	9A	23	3A	2E	"/íø°.l.¤.¬ôš#:.
00002120 F5 D9 F5 A3 4F 45 6C 1C 37 2C 03 4E 3A EB EC DF 5 D9 F5 A3 4F 45 6C 1C 37 2C 03 4E 3A EB CD T 8 10 D4 65 6B 48 E5 19 "	00002110	50	7C	CC	71	35	EB	67	C8	EC	D0	7A	18	1E	6B	97	BE	P İq5ëgÈìĐzk—¾
00002130 98 39 85 47 88 81 6C D7 18 10 D4 65 6B 48 51 15	00002120	F5	D9	F5	A3	4F	45	6C	1C	37	2C	03	4E	3A	EΒ	4C	DF	õÙõ£OEl.7,.N:ëLß
00002140 E6 F6 9F 3A 35 48 33 23 BC 0D FE BF 08 C7 F3 AE æở%:FB3#4.p2.çó@ 00002150 E6 A8 69 93 E7 FE D7 CE C2 44 8A 8D 51 25 CC D9 æ°%:°cp×fÅDS.Q%iD 00002160 DA 21 E2 72 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 w°b*iÅDS.Q%iD 00002170 33 6B AF AC E% 0.2 % D4 00 b1 A 88 37 6F 56 32 8D w°b*iÅDS.Q%iD 00002180 05 7C CD 7D ESCLAPTE 03 85 00 5F 7F 26 32 8D w°b*iÅDS.Q%iPiČ 00002180 05 7C CD 7D ESCLAPTE 03 85 00 5F 7F 26 32 8D w°b*iÅDS.Q%iPiČ 00002180 05 7C CD 7D ESCLAPTE 03 85 00 5F 7F 26 32 8D w°b*iÅDS.Q%iPiČ 00002100 4F 08 ED C5 69 4E 99 27 91 87 AD 74 8B FE CE 72 o`LÅIN"''.t.kpÅT 00002180 AD B2 46 86 54 12 A8 77 2C C0 D2 71 1D 69 7C D4 .°FT*w,ÅÒq.i[ô 00002180 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 ½°~EX0]+.ES 00002180 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 10 50 DB 4°CmÅ53~EX0]+.ES 00002180 B3 00 EA 5A 80 3C F0 24 2C 2C CC 1B 0A 1D 59 CZ 3.2€Ce35, 00002180 B4 0A F0 C9 6F FF E6 68 07 07 C5 74 0C 71 BF 45 %Jûô·Eû0.mFF! 00002180 B0 0B 5C FC D5 D6 B7 C6 D9 D8 90 99 46 98 0A A6 °Júô·Eû0.mFF! 000022100	00002130	98	39	85	47	88	81	6C	D7	18	10	D4	65	6B	48	E5	19	~9G^.l×ÔekHå.
00002150 E6 A8 69 93 E7 FE D7 CE C2 44 8A 8D 51 25 CC D9 #"i"cp×IAD5.0%I0 00002150 DA 21 E2 72 02 39 FC 06 EE 2A 7D A0 6E B0 4D 37 Ú!ar.9u.1*}n*M7 00002170 33 6B AF AC E8 C2 09 rd DD 36 88 37 6F 56 32 8D 3K - ,*00. ^70V2. 00002180 05 7C CD 7D.51 CE PARTE 23 3 FC 0 20 rd DD 37 8F 27 56 52 8D 3K - ,*00. ^70V2. *00. ^70V2. 00002180 05 7C CD 7D.51 CE PARTE 23 3 FC 0 20 71 7 EE CE 72 *1[ne+VI3.s0V-1Z 00002180 AD 82 46 86 54 12 A8 77 2C CD 27 11 D 69 7C D4 *FTT.*w, A0q.il 00002180 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 0*3*=.X0]+.E5 00002100 B3 00 FB 6E C5 35 E3 17 8B 7D 19 8C DF 10 50 DB 4%Dáta5a}.E8.P0 00002120 B4 0A F0 C9 6F FF E6 68 07 07 C5 74 0C 71 BF 45 KJdéoyahÅt.g;E 00002120 B0 0B 5C FC D5 D6 B7 76 D9 D8 90 99 46 98 0A A6 ° 00002120 C4 0D 00 00 00 00 00 00 00 00 00002120 C4 0D 00 00 00 00 00 00 00	00002140	E6	F6	9F	3A	35	48	33	23	BC	0D	FE	BF	08	C7	F3	AE	æöŸ:5H3#¼.þ¿.Çó®
00002160 DA 21 E2 72 O2 39 FC 06 EE 2A 7D A0 GE B0 4D 37 Ú!år.90.1*) n*M7 00002170 33 6B AF AC B8 72 001 40 DB 14 68 37 6F 56 32 8D 3k ⁻ ,%00.^rov2. 3k ⁻ ,%00.^rov2. 00002180 05 7C CD 7D CD AC CPUT 40 DB 14 69 37 6F 56 32 8D 3k ⁻ ,%00.^rov2. %00.^rov2. 00002190 4F 08 ED C5 69 4E 99 27 91 87 AD 74 8B FE CE 72 0.1ÅN ⁻ ".*t.t¢fr 00002180 AD B2 46 86 54 12 A8 77 2C CD D2 71 1D 69 7C D4 .²FTT.'w, Åòg.ilô 000021C0 34 80 FB 6E C5 35 E3 17 8B 7D 19 8C DF 10 50 DB 4¢cînÅ5s,%.XÔ]÷.E5 000021D0 B3 00 EA 5A 80 3C FO 24 2C 2C CC 1B 0A 1D 59 C2 ³.eze<δ;,YÅ	00002150	E6	A 8	69	93	E7	FE	D7	CE	C2	44	8A	8D	51	25	CC	D9	æ¨i"çþ×ÎÂDŠ.Q%ÌÙ
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	00002160	DA	21	E2	72	02	39	FC	06	EE	2A	7D	A0	6E	в0	4D	37	Ú!âr.9ü.î*} n°M7
00002180 05 7c CD 7D.53C 124 Matter 123 × 5% 13 70×917 7E EC 8E .[1]me+VI3.s0%-12 00002190 4F 08 ED C5 69 4E 99 27 91 87 AD 74 8B FE CE 72 0.iÅiN"'±.t¢fr 00002180 AD B2 46 86 54 12 A8 77 2C C0 D2 71 1D 69 7C D4 .FFT."w,Ådq.i 00002180 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 .*FT."w,Ådq.i 000021D0 B3 00 FB 6E C5 35 E3 17 8B 7D 19 8C DF 10 50 DB 40máša~EX0j+.E5 000021D0 B3 00 EA 5A 80 3C F0 24 2C 2C CC 1B 0A 1D 59 C2 .*Ezc63, f/Å 000021E0 B4 4A F0 C9 6F FF E6 68 07 07 C5 74 0C 71 BF 45 KJdéoyahÅt.g;E 00002120 C4 0D 00 00 00 00 00 00 00 00 00	00002170	33	6B	AF	AC	28	Chr.	199	- <u>D4</u>	DB	vf.	3 ⁸ n	3i7	6F	56	32	8D	3k_¬,.™ÔÛ.^7oV2.
00002190 4F 08 ED C5 69 4E 99 27 91 87 AD 74 8B FE CE 72 0.1ÅiN™''+tkpľr 000021A0 AD B2 46 86 54 12 A8 77 2C C0 D2 71 1D 69 7C D4 .²FtT.'w,Àòq.i ô 000021B0 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 ů³>²=KT.'w,Àòq.i ô 00002100 B3 00 EA 5A 80 3C F0 24 2C 2C C1 B 0A 1D 59 C2 ³.eZe<ð\$, îYÅ	00002180	05	7C	CD	7D	-36.	žB.	Lo.	- mil	35	% Ε	73	206	9F	7E	EC	8E	. ĺ}œ+VÏ3.sÖŸ~ìŽ
000021A0 AD B2 46 86 54 12 A8 77 2C C0 D2 71 1D 69 7C D4 . ² FfT."w,ÅQ;i Ô 000021B0 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 u³>	00002190	4F	08	ED	C5	69	4E	99	27	91	87	AD	74	8B	FE	CE	72	O.íÅiN™'`‡.t<þÎr
000021B0 F9 B3 3E 9D 00 90 5E 3D AD 58 D6 5D F7 13 C6 35 u³>=XÖ]+.Æ5 000021C0 34 80 FB 6E C5 35 E3 17 8B 7D 19 8C DF 10 50 DB 4€ûnÅ5ā.<].œB.PÛ	000021 A 0	AD	B2	46	86	54	12	A 8	77	2C	C0	D2	71	1D	69	7C	D4	.²F†T.¨w,ÀÒq.i Ô
000021C0 34 80 FB E3 17 88 7D 19 8C DF 10 50 DB 4€ûnÅ5 CES.PÜ 000021D0 B3 00 EA 5A 80 3C F0 24 2C 2C CC 1B 0A 1D 59 C2 3 2 3 3 3 3 1 3 2 3 3 3 3 3 3 3	000021B0	F9	В3	3E	9D	00	90	5E	3D	AD	58	D6	5D	F7	13	C6	35	ù³>^=.XÖ]÷.Æ5
000021D0 B3 00 EA 5A 80 3C F0 24 2C 2C CC 1B 0A 1D 59 C2 3.62€<δ\$, 1YÅ	000021C0	34	80	FB	6E	C5	35	E3	17	8B	7D	19	8C	DF	10	50	DB	4€ûnÅ5ã.<}.Œß.PŰ
000021E0 4B 4A F0 C9 6F FF E6 68 07 07 C5 74 0C 71 BF 45 KJðÉoyæh.Åt.qr 000021F0 B0 0B 5C FC D5 D6 B7 C6 D9 D8 90 99 46 98 0A A6 00002200 C4 0D 00 00 00 00 00 00 00 00 00 00 00 00	000021D0	B3	00	EA	5A	80	3C	F0	24	2C	2C	CC	1B	0A	1D	59	C2	³.êZ€<ð\$,,ÌYÂ
000021F0 B0 0B 5C FC D5 D6 B7 C6 D9 D8 90 99 46 98 0A A6 00002200 C4 0D 00 00 00 00 00 00 00 02 00 00 01 00 00 00 00 00002210 07 03 03 01 00 00 00 00 00 00 00 00 00 00 00 00	000021E0	4B	4A	F0	C9	бF	FF	Eб	68	07	07	C5	74	0C	71	BF	45	KJðÉoÿæhÅt.q;E
00002200 [C4 0D 00 00 00 00 00 00 02 00 00][01 00 00 00] Ä 00002210 07 03 03 01 00 00 00 00	000021F0	B0	0B	5C	FC	D5	D6	В7	C6	D9	D8	90	99	46	98	0A	A6	°.\üÕÖ ·ÆÙØ.™F~.¦
00002210 07 03 03 01 00 00 00 00	00002200	C4	0D	00	00	00	00	00	00	00	02	00	00	01	00	00	00	Ä
	00002210	07	03	03	01	00	00	00	00									

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 Isass.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	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
T1120		
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

Posted on: Jun 7th



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

machine.

Follow or contact Loïc :



@

Share this article



Follow us on



twitter@Atos_Security

[#DataProtection] 🔐 Do you need to protect your sensitive data in <u>#Microsoft365</u> ? Dual key encryption <u>#DKE</u> technology enables you to keep control of your <u>#encryption</u> keys & ensures that <u>#sensitivedata</u> remains inaccessible from any 3d party.
A https://t.co/WTS3sBqDA

▲ 17♥ May 27, 2022

twitter@Atos_Security

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

€t∓♥

May 27, 2022



twitter@Atos_Security

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

▲ t↓ ♥ May 26, 2022