Ransomware Spotlight: AvosLocker

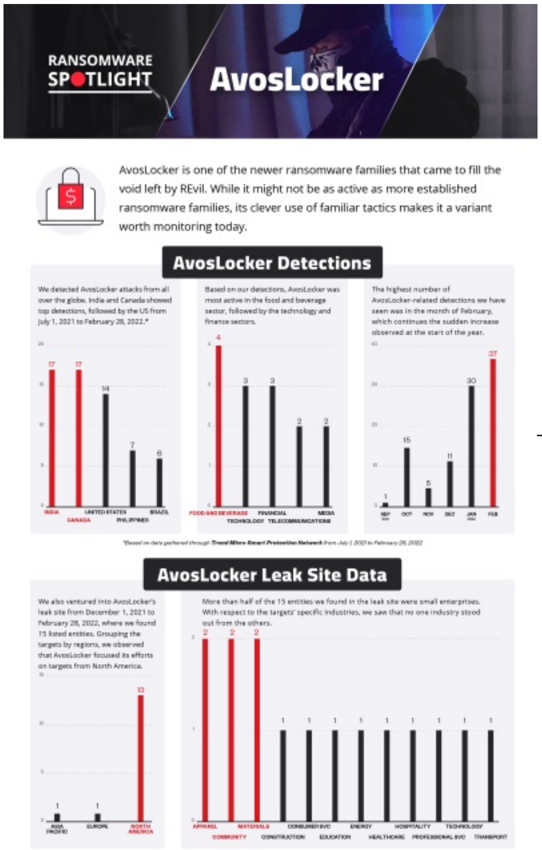
trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-avoslocker

X

AvosLocker

By Trend Micro Research

AvosLocker is a relatively new ransomware variant that sports the staples of modern ransomware, namely a layered extortion scheme that begins with stolen data. We shed light on this emerging ransomware family and its key techniques.



RANSOMWARE SPOTLIGHT

AvosLocker

AvosLocker is one of the newer ransomware families that came to fill the void left by REvil. While it might not be as active as more established ransomware families, its clever use of familiar tactics makes it a variant worth monitoring today.

AvosLocker Detections

We detected AvosLocker attacks from all over the globe. India and Canada showed top detections, followed by the US from July 1, 2021 to February 28, 2022.*

Based on our detections, AvosLocker was most active in the food and beverage sector, followed by the technology and finance sectors.

The highest number of AvosLocker-related detections we have seen was in the month of February, which continues the sudden increase observed at the start of the year.

*Based on data gathered through **Trend Micro Smart Protection Network** from July 1 2021 to February 28, 2022

AvosLocker Leak Site Data

We also ventured into AvosLocker's leak site from December 1, 2021 to February 28, 2022, where we found 15 listed entities. Grouping the targets by regions, we observed that AvosLocker focused its efforts on targets from North America.

More than half of the 15 entities we found in the leak site were small enterprises. With respect to the targets' specific industries, we saw that no one industry stood out from the others.

View infographic of "Ransomware Spotlight: AvosLocker"

AvosLocker is one of the newer ransomware families that came to fill the void left by REvil. While not as prominent or active as LockBit or Conti, it is slowly making a name for itself, with the US Federal Bureau of Investigation (FBI) releasing an advisory on this threat. According to the report, AvosLocker has been targeting critical infrastructure in different sectors of the US, with attacks also observed in other countries like Canada, UK, and Spain. Although detections are low, its clever use of familiar tactics makes it a ransomware variant worth monitoring today.

What do organizations need to know about AvosLocker?

AvosLocker is another variant that runs on a ransomware-as-a-service (RaaS) model. It was first spotted in July 2021 and has since come up with several variants released over time. The following are the key characteristics of AvosLocker:

- **It uses the remote administration tool AnyDesk.** One of the notable characteristics of AvosLocker campaigns is its use of AnyDesk, a remote administration tool (RAT) to connect to victim machines. Using this tool, the operator can manually operate and infect the machine.
- **It runs on safe mode.** Another key element of AvosLocker is running itself on safe mode as part of its evasion tactics. The attacker restarts the machine, disables certain drivers, and runs on safe mode, thus avoiding certain security measures that are unable to run in this mode. Operators also set up certain drivers to make sure that AnyDesk would run even in safe mode. It is important to note that this was a tactic previously employed by the now defunct REvil.
- **Operators auction stolen data.** AvosLocker again takes a leaf from REvil's page by auctioning stolen data on its site, on top of its double extortion scheme. This could be the group's way of further monetizing a single successful attack or salvaging a failed one.

As mentioned, AvosLocker operators have also released multiple versions of this ransomware. The tactic of running itself on safe mode was seen in the second version of AvosLocker. Following the trend of targeting Linux machines, AvosLocker also released a Linux variant as advertised by the group on October 2021. This variant is capable of attacking ESXi virtual machines (VMs), which makes it a variant to watch out for.

Operating as an RaaS, the actors behind AvosLocker conduct reconnaissance before each campaign. Actors choose their targets based on their ability to pay the demanded ransom and tailor their attacks accordingly.

In the next sections, we look at which regions and industries the group has targeted most often, based on our detections and information from their leak site.

Top affected industries and countries

Our telemetry shows data on AvosLocker activity or attack attempts. While we observed AvosLocker activity from all over the world, India and Canada showed top detections from July 1, 2021 to February 28, 2022.

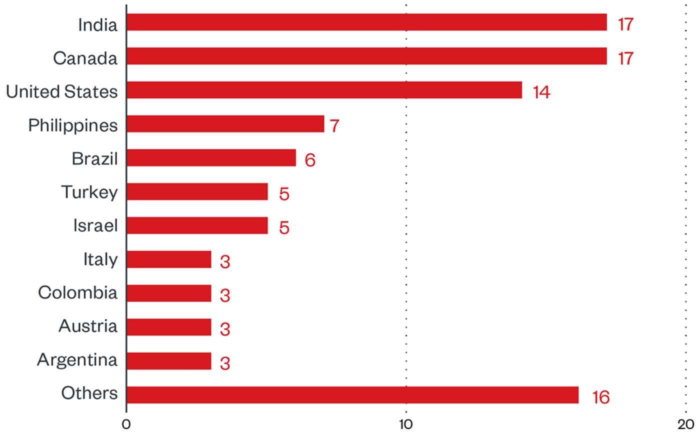


Figure 1. Countries with the highest number of attack attempts per machine for AvosLocker ransomware (July 1, 2021 to February 28, 2022)
Source: Trend Micro™ Smart Protection Network™

Based on our detections, AvosLocker was the most active in the food and beverage sector, followed by the technology and finance sectors. However, there is only by a slim margin given the small sample size.

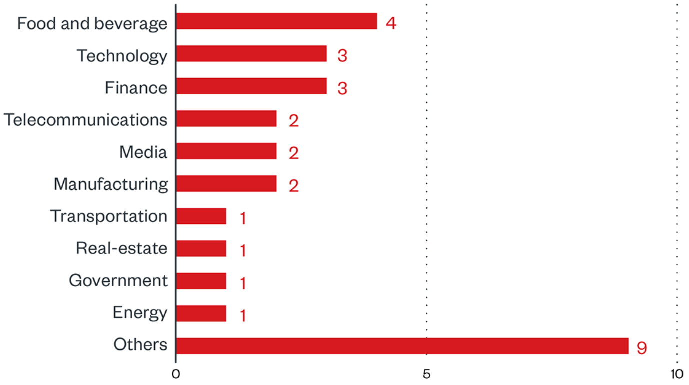


Figure 2. Based on our detections, AvosLocker was the most active in the food and beverage sector, followed by the technology and finance sectors. However, there is only a slim margin given the small sample size.
Source: Trend Micro Smart Protection Network

As of this writing, the highest number of AvosLocker-related detections we have seen was in the month of February, which continues the sudden increase observed at the start of the year.

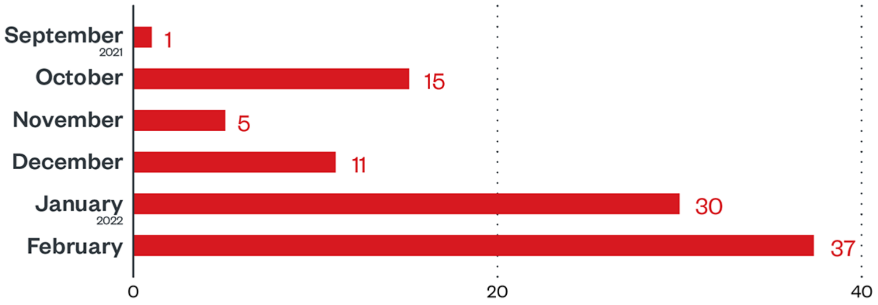


Figure 3. AvosLocker monthly detections per machine (July 1, 2021 to February 28, 2022)
Source: Trend Micro Smart Protection Network

Targeted regions and sectors according to AvosLocker leak site

We also ventured into AvosLocker's leak site, which offered a different perspective on its targets. From December 1, 2021 to February 28, 2022 we found 15 listed entities. The organizations listed in the site were successfully attacked and have not, in that period, paid the demanded ransom.

By grouping the list according to regions, we found that AvosLocker focused its efforts on targets from North America.

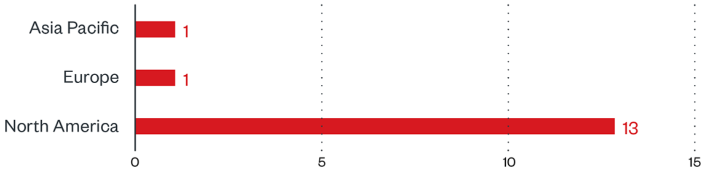


Figure 4. Regional distribution of AvosLocker victims according to the group's leak site (December 1, 2021 to February 28, 2022)

More than half of the 15 entities we found in the leak site were small enterprises. With respect to the targets' specific industries, we saw no trend emerging, as no one industry stood out from the others. This can be seen in Figure 6, where no single industry stood out from the rest.

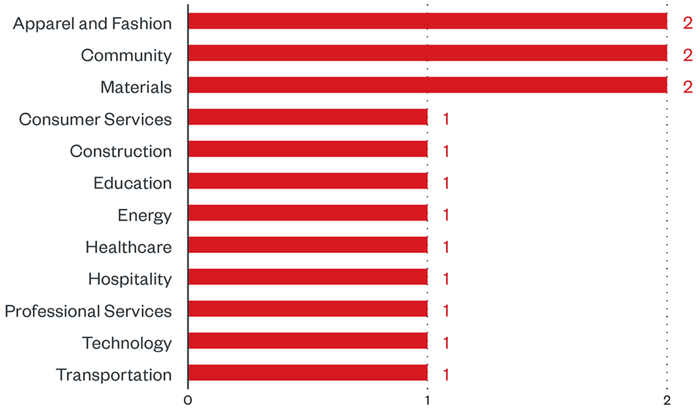


Figure 5. Sector distribution of AvosLocker victims according to the group's leak site (December 1, 2021 to February 28, 2022)

We do note, however, that AvosLocker has showed relatively less activity compared to other more prominent ransomware families in terms of our detections and observations from its leak site. Because of the limited sample size, further monitoring might be necessary to identify trends.

Infection chain and techniques

The AvosLocker infection chain, which operates on the RaaS model, can vary depending on the target. The following infection chain shows a variety of tactics and tools employed by this RaaS.

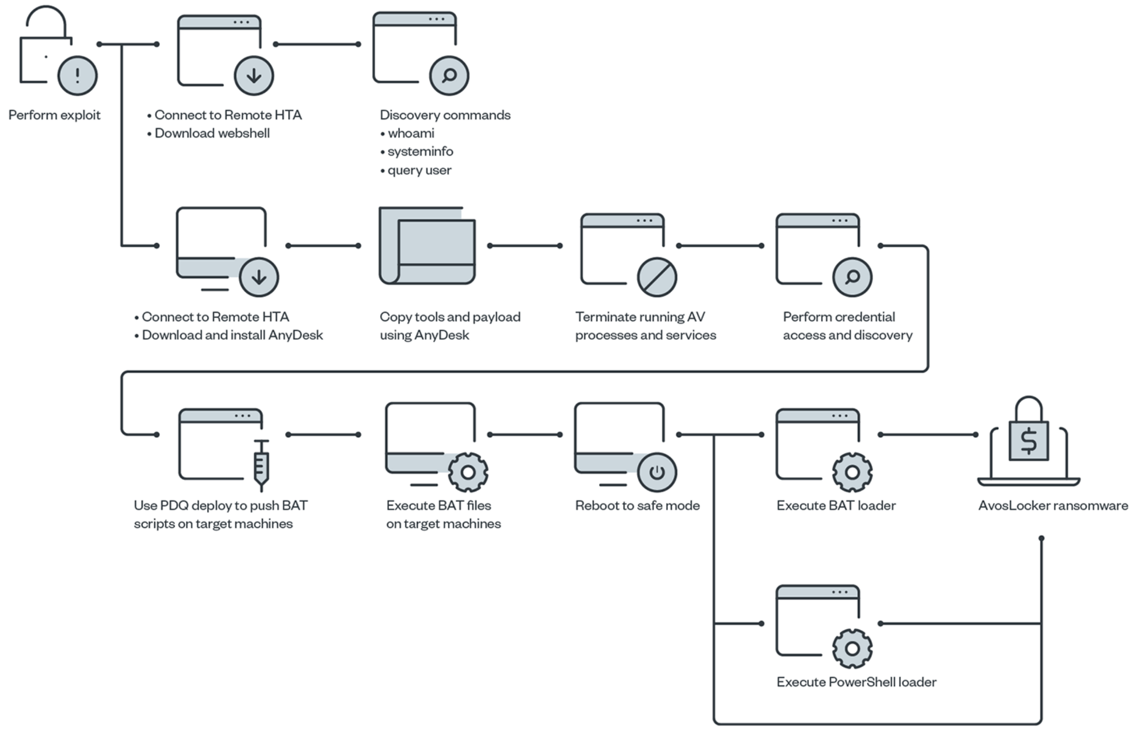

Perform exploit
• Connect to Remote HTA
• Download webshell
Discovery commands
• whoami
• systeminfo
• query user
• Connect to Remote HTA
• Download and install AnyDesk
Copy tools and payload using AnyDesk
Terminate running AV processes and services
Perform credential access and discovery
Use PDQ deploy to push BAT scripts on target machines
Execute BAT files on target machines
Reboot to safe mode
Execute BAT loader
AvosLocker ransomware
Execute PowerShell loader

Figure 6. AvosLocker infection chain

Initial Access

- AvosLocker uses Zoho ManageEngine ServiceDesk Plus and its exploit for initial access and to download of web shell and AnyDesk.
- It has been reported to make use of compromised accounts to access its victims via RDP or virtual private network (VPN).

Defense Evasion, Discovery, and Credential Access

- It uses Avast Anti-Rootkit Driver and a PowerShell script to disable certain antivirus processes.
- It uses a BAT script to disable antivirus services that can run on Windows Safe Mode.
- It uses Mimikatz and XenArmor Password Recovery Pro Tool to get credentials.
- It also uses Nmap, NetScan, and native Windows commands (such as ipconfig, nslookup, and others) to perform discovery on the target network.
- It avoids writing the ransomware payload in target systems.

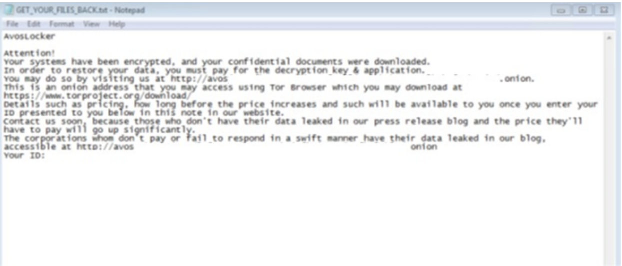
Lateral Movement and Command and Control

- AvosLocker installs AnyDesk to gain control of the targeted systems.
- It uses PDQ Deploy to push out and execute the Windows batch script on the targeted systems.

Impact

- It then executes the ransomware payload (AvosLocker) to perform its encryption routine once all other routines are done.
- It now has both Windows and Linux version of this ransomware payload. The Linux version is also known to terminate ESXi virtual machines.
- In its latest attacks, the Windows version was executed after restarting in safe mode to inhibit security software from detecting the ransomware variant.

- In order to execute on safe mode, it adds a RunOnce registry entry under autostart. Further investigation revealed multiple ways AvosLocker can be executed via the RunOnce registry, which are the following:
  1. Direct execution of the ransomware payload
  2. Execute a PowerShell script that will download and execute the ransomware payload
  3. Execute a PowerShell script that will decode and execute the ransomware payload from a disguised .jpg file.
- It drops a ransom note similar to the one in Figure 7.



```
AvosLocker

Attention!
Your systems have been encrypted, and your confidential documents were downloaded.
In order to restore your data, you must pay for the decryption key & application.
You may do so by visiting us at http://avos                                    .onion.
This is an onion address that you may access using Tor Browser which you may download at
https://www.torproject.org/download/
Details such as pricing, how long before the price increases and such will be available to you once you enter your
ID presented to you below in this note in our website.
Contact us soon, because those who don't have their data leaked in our press release blog and the price they'll
have to pay will go up significantly.
The corporations whom don't pay or fail to respond in a swift manner have their data leaked in our blog,
accessible at http://avos                                                     onion
Your ID:
```

Figure 7. Sample ransom note used by AvosLocker

Other technical details

- It avoids the following directories:
  - All Users
  - AppData
  - boot
  - bootmgr
  - Games
  - Intel
  - Microsoft. (Directory name starts with “Microsoft.)
  - Program Files
  - ProgramData
  - Public
  - Sophos
  - System Volume Information
  - Windows
  - Windows.old
  - WinNT
- It avoids encrypting the following files with strings in their file name:
  - autorun.inf
  - boot.ini
  - bootfont.bin
  - bootsect.bak
  - config.msi
  - desktop.ini
  - iconcache.db
  - ntldr
  - ntuser.dat
  - ntuser.dat.log
  - ntuser.ini
  - thumbs.db
  - Thumbs.db

- It avoids encrypting files with the following extensions:
  - .386
  - .adv
  - .ani
  - .avos
  - .avos2
  - .avos2j
  - .avoslinux
  - .bat
  - .bin
  - .cab
  - .cmd
  - .com
  - .cpl
  - .cur
  - .deskthemepack
  - .diagcab
  - .diagcfg
  - .diagpkg
  - .dll
  - .drv
  - .exe
  - .hlp
  - .hta
  - .icl
  - .icns
  - .ico
  - .ics
  - .idx
  - .key
  - .ldf
  - .lnk
  - .lock
  - .mod
  - .mpa
  - .msc
  - .msi
  - .msp
  - .msstyles
  - .msu
  - .nls
  - .nomedia
  - .ocx
  - .pdb
  - .prf
  - .ps1
  - .rom
  - .rtp
  - .scr
  - .shs
  - .spl
  - .sys
  - .theme
  - .themepack
  - .wpx

- It terminates the following processes:
    - encsvc
    - thebat
    - mydesktopq os
    - xfssvccon
    - firefox
    - infopath
    - winword
    - steam
    - synctime
    - notepad
    - ocomm
    - onenote
    - mspub
    - thunderbird
    - agntsvc
    - sql
    - excel
    - powerpnt
    - outlook
    - wordpad
    - dbeng50
    - isqlplussvc

MITRE tactics and techniques

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Imp

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	Imp
T1190 - Exploit public-facing application *Arrives by exploiting Zoho ManageEngine ServiceDesk Plus Exploit to download web shell and AnyDesk* *As it operates as a RaaS, depending on the affiliate, the following exploits might be used for initial access:• CVE-2021-31206• CVE-2021-31207• CVE-2021-34473• CVE-2021-34523• CVE-2021-26855* **T1078** - Valid accounts *Have been reported to make used of compromised accounts to access victims via RDP or VPN*	**T1059** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell and Windows Command shell* **T1072** - Software deployment tools *Used PDQ Deploy to distribute the batch file and payload on target computers*	**T1136** - Create account *Creates a new user to ensure automatic login when machine is restarted in safe mode* **T1547** - Boot or logon autostart execution *Creates an autostart entry to ensure execution of ransomware when restarted in safe mode*	**T1112** - Modify registry *Modifies registry entry to allow AnyDesk on safe mode and to enable automatic login when restarted in safe mode* **T1562** - Impair defenses *Abuses Avast Anti-Rootkit Driver and a PowerShell script to disable certain processes related to security tools and also restarts the machine in safe mode to inhibit security tools from executing* **T1140** - Deobfuscate/Decode files or information *Some ransomware samples are decoded using CertUtil and strings to be used by the ransomware are encrypted using XOR.* **T1070** - Indicator removal on host *It deletes created registry entries, scripts, and ransomware binary after encryption.*	**T1003** - OS credential dumping *Might utilize Mimikatz to dump credentials* **T1552** - Unsecured credentials *Might utilize Mimikatz or XenArmor Password Recovery Pro tool to gather credentials* **T1555** - Credentials from password stores *Might utilize XenArmor Password Recovery Pro tool to gain credentials*	**T1083** - File and directory discovery *Searches for specific files and directory related to its ransomware encryption* **T1135** - Network share discovery *Makes use of tools to enumerate network share* **T1057** - Process discovery *Discovers certain processes for process termination* **T1018** - Remote system discovery *Makes use of tools for network scans*	**T1021** - Remote services *Might use AnyDesk to remotely connect and transfer files* **T1072** - Software deployment tools *Used PDQ Deploy to distribute the batch file and payload on target computers*	**T1219** - Remote access software *Makes use of tools for network scans*	**T14** enc imp *Mig Any rem con tran It us sals stre to e vict Old vers use adv enc star (AE 256 RS enc and resp* **T14** - Se stop *Cor list ser be tern ens enc* **T14** - Inl syst rec *Del sha cop* **T14** - De *Rep des wal with ran*

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in AvosLocker attacks:

Initial Access	Execution	Credential Access	Discovery	Lateral Movement	Defense Evasion	Command and Control
Exploit for Zoho ManageEngine ServiceDesk Plus	• **PowerShell** • **Windows command shell**	• **Mimikatz** • **XenArmor Password Recovery Tool Pro**	• **NetScan** • **Nmap**	**PDQ Deploy**	• **BAT file** • **Avast Anti-Rootkit Scanner** • **PowerShell script**	**AnyDesk**

Recommendations

While AvosLocker is not yet as prominent as other ransomware families like LockBit, Conti, and Clop, it seems to follow in the footsteps of these more established players. It also reuses tactics that worked for infamous ransomware families, namely REvil. This should be enough reason for organizations to keep an eye on this ransomware family as well as to stay abreast with the latest trends and tactics employed by threat actors today.

To help defend systems against similar threats, organizations can establish security frameworks that can allocate resources systematically for establishing solid defenses against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee’s role.
- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allowlist that only executes legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.

Protect and recover

- Implement data protection, back up, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard possible entry points into the system (endpoint, email, web, and network). Security solutions that can detect malicious components and suspicious behavior can also help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools before the ransomware can do any damage.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

The IOCs for this article can be found here. Actual indicators might vary per attack.

HIDE