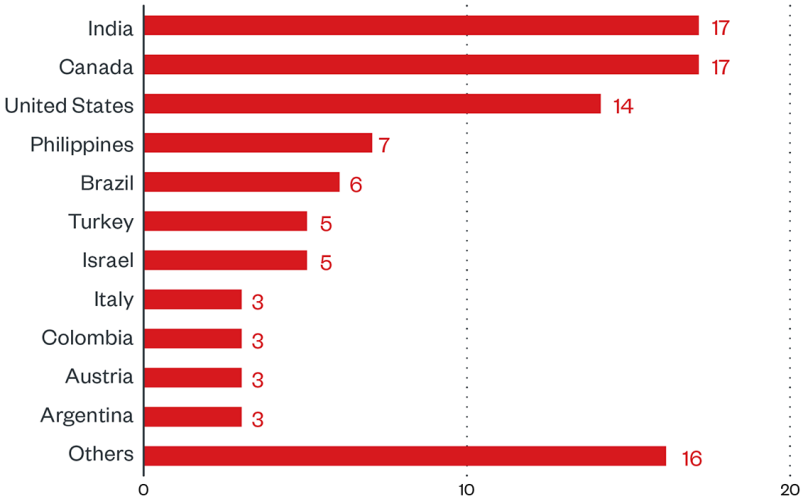
Ransomware Spotlight: AvosLocker

Archived: 2026-04-02 11:42:01 UTC

Top affected industries and countries

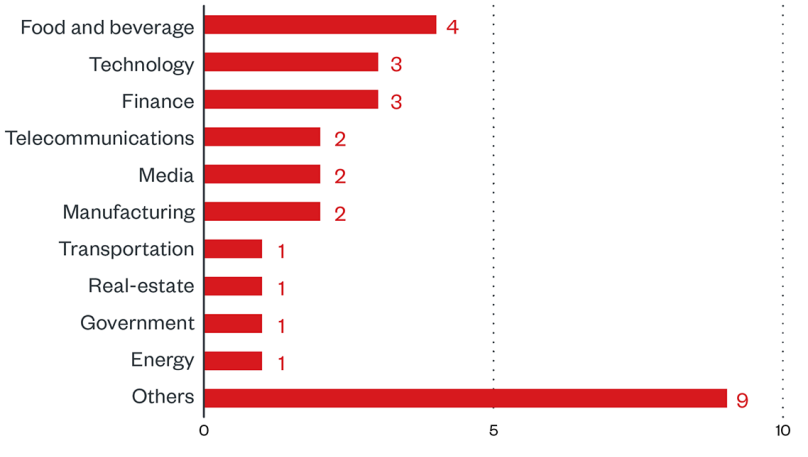
Our telemetry shows data on AvosLocker activity or attack attempts. While we observed AvosLocker activity from all over the world, India and Canada showed top detections from July 1, 2021 to February 28, 2022.



open on a new tab

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™

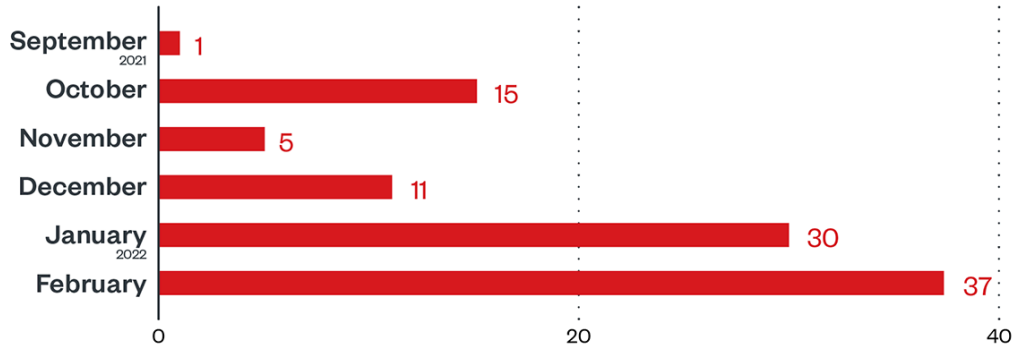
Based on our detections, AvosLocker was the most active in the food and beverage sector, followed by the technology and finance sectors. However, there is only by a slim margin given the small sample size.



open on a new tab

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.



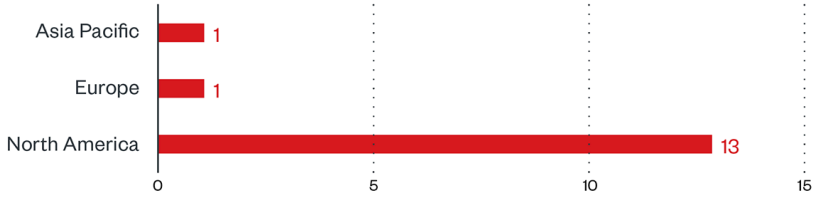
open on a new tab

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.

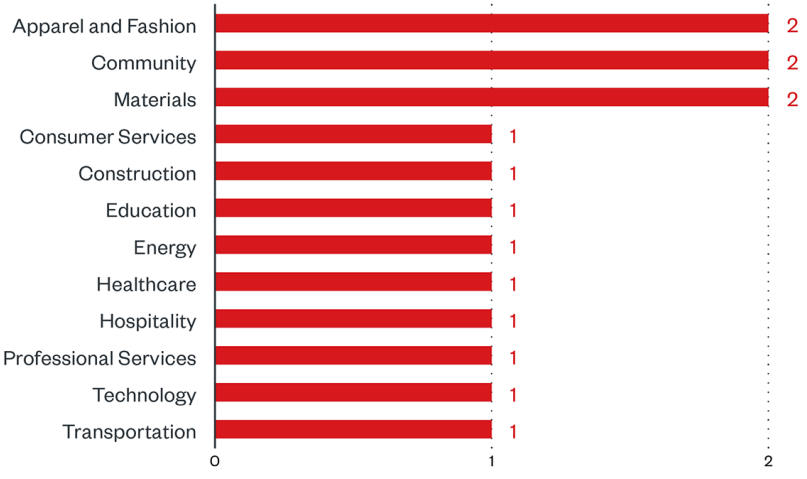
By grouping the list according to regions, we found that AvosLocker focused its efforts on targets from North America.



open on a new tab

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.



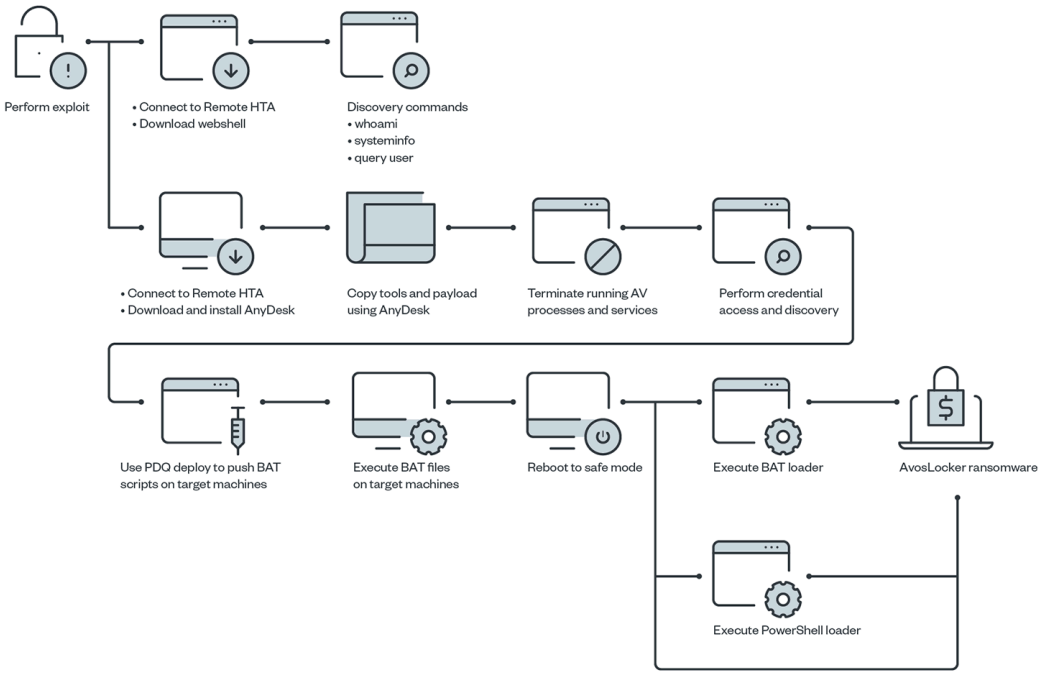
open on a new tab

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.



open on a new tab

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.

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	I
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:*	**T1059** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell and Windows Command shell* **T1072** - Software deployment tools *Used PDQ Deploy to*	**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*	**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*	**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*	**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*	**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*	**T1219** - Remote access software *Makes use of tools for network scans*	**T** D e f *M A r c t f I s s c e v C v u a e s

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Command and Control	In
• *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*	*distribute the batch file and payload on target computers*	*ransomware when restarted in safe mode*	*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.*	**T1555** - Credentials from password stores *Might utilize XenArmor Password Recovery Pro tool to gain credentials*	**T1057** - Process discovery *Discovers certain processes for process termination* **T1018** - Remote system discovery *Makes use of tools for network scans*	*target computers*		*(A* *2* *a* *e* *a* *re* **T** S st *C* *li* *se* *b* *te* *to* *e* **T** I sy re *D* *sh* *c* **T** I *R* *d* *w* *w* *r*

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	Comm Contr
• **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**	•

Recommendations

While AvosLocker is not yet as prominent as other ransomware families like LockBitnews article, Continews article, and Clopnews article, 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™products 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 Securityproducts 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 Inspectorproducts 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™products 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)

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- AI Security Starts Here: The Essentials for Every Organizationnews article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---