Ransomware

Vice Society Ransomware Group Targets Manufacturing Companies

In this blog entry, we'd like to highlight our findings on Vice Society, which includes an end-to-end infection diagram that we were able to create using Trend Micro internal telemetry.

By: Ieriz Nicolle Gonzalez, Paul Pajares, Arianne Dela Cruz, Warren Sto.Tomas
January 24, 2023
Read time: 5 min (1393 words)

Updated on January 26, 2023 to remove references to Kape Tool and to remove Trend Micro Apex One from the list of programs that the ransomware disables.

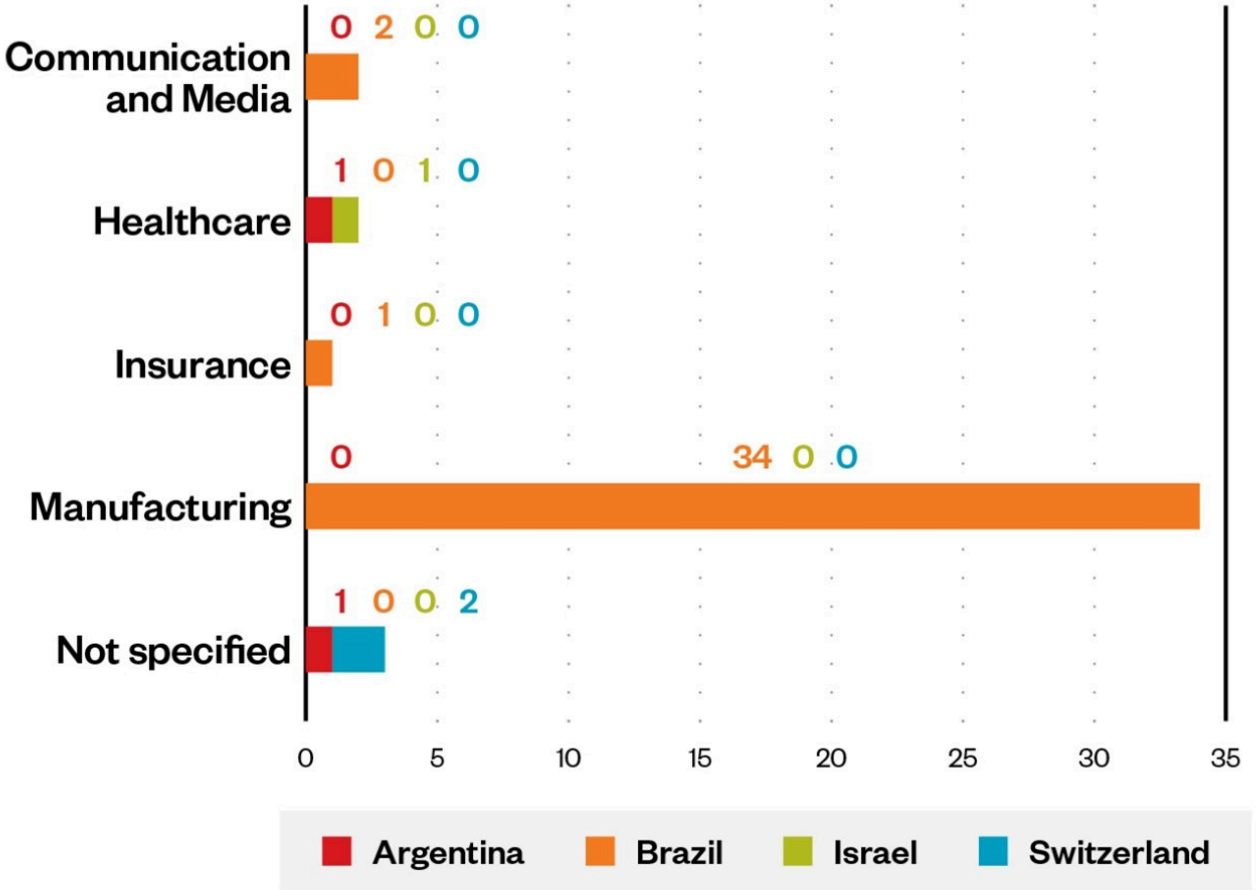
The Vice Society ransomware group made headlines in late 2022 and early 2023 during a spate of attacks against several targets, such as the one that affected the rapid transit

data, we have evidence that the group is also targeting the manufacturing sector, which means that they have capability and desire to penetrate different industries — most likely accomplished via the purchasing of compromised credentials from underground channels. We have detected the presence of Vice Society in Brazil (primarily affecting the country's manufacturing industry), Argentina, Switzerland, and Israel.

Vice Society, which was initially reported to be exploiting the PrintNightmare vulnerability in their routines, have previously deployed ransomware variants such as Hello Kitty/Five Hands and Zeppelin (the group's email has been in their ransom notes). More recently, Vice Society has been able to develop its own custom ransomware builder and adopt more robust encryption methods. This, and any further enhancements, could mean that the group is preparing for their own ransomware-as-a-service (RaaS) operation.

In this blog entry, we'd like to highlight our findings on Vice Society, which includes an end-to-end infection diagram that we were able to create using Trend Micro internal telemetry. Our detection name for this variant of Vice Society's ransomware is Ransom.Win64.VICESOCIETY.A .

Figure 1. Vice Society's evolution throughout 2021 to late 2022



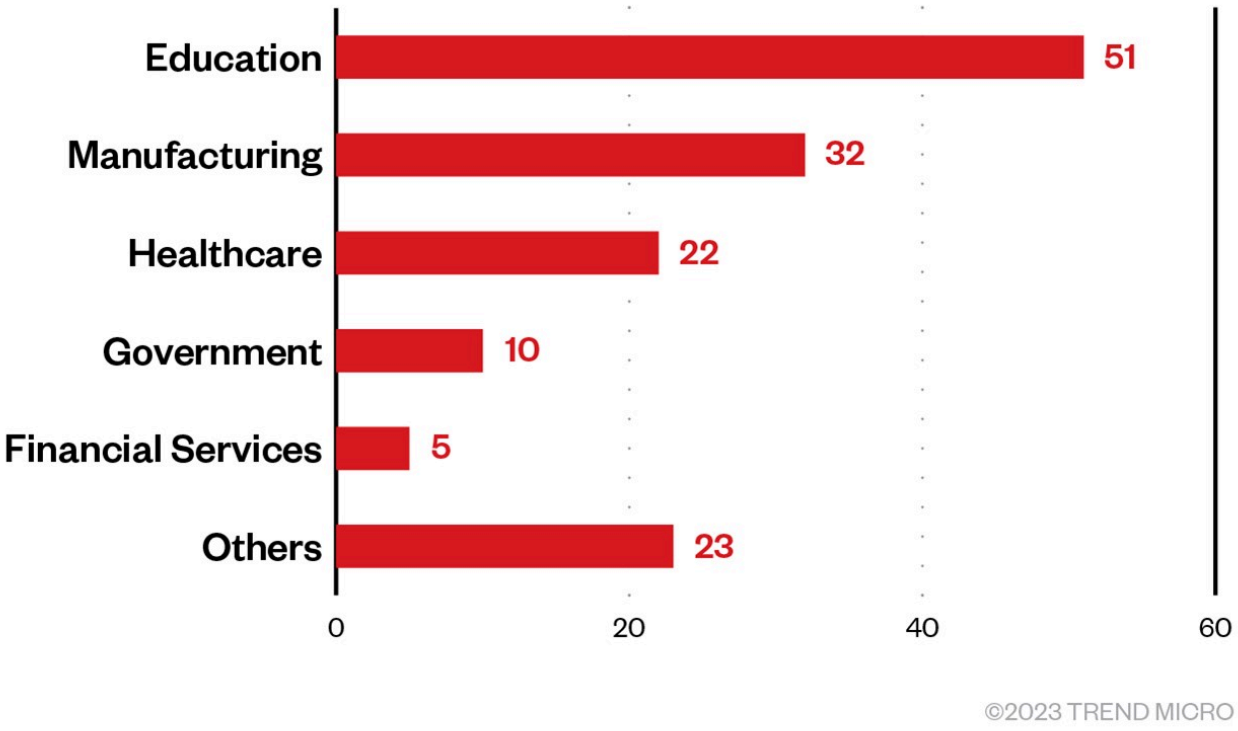


Figure 3. Distribution of affected industries based on the Vice Society leak site

Technical analysis and infection flow

Based on our internal telemetry, we were able to create infection diagram for a Vice Society ransomware attack (illustrated in Figure 4). The arrival vector likely involves the exploitation of a public-facing website or abuse of compromised remote desktop protocol (RDP) credentials.

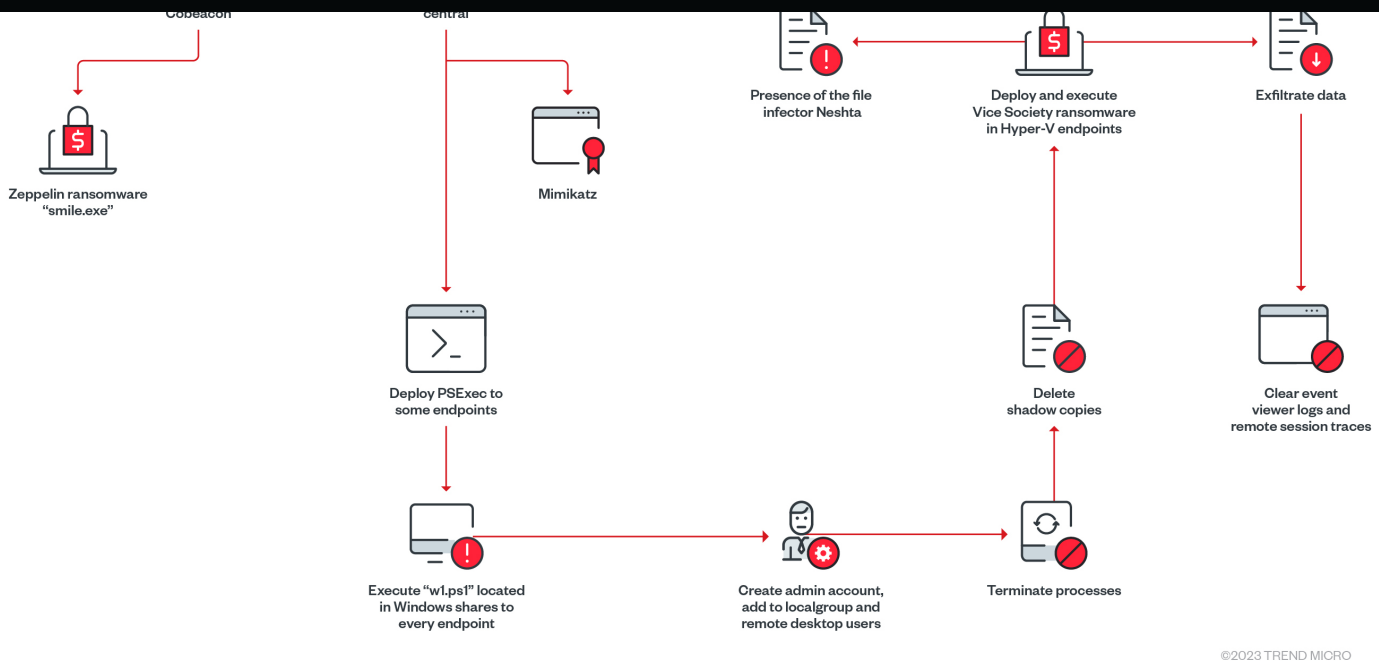


Figure 4. The infection chain of a Vice Society attack

The following table shows what we were able to observe from a Vice Society attack. Note that all endpoints indicated belong to one Pointer to the GUID.

Date	Description

	Cobalt Strike connects to 57thandnormal[.]com
November 12, 2022	Deployed Zeppelin ransomware Path: C:\mnt\smile.exe
November 12, 2022	Deployed Mimikatz Path: C:\ProgramData\toolkiit\{redacted}\output\C\$Recycle.Bin\{redacted}\$RY0DNVE.exe
November 12, 2022	Executed a PowerShell script (w1.ps1) Command: /c powershell.exe -ExecutionPolicy Bypass -file \\{ComputerName}\s$\w1.ps1 -ExecutionPolicy Bypass -file \\{ComputerName}\s$\w1.ps1
November 12, 2022	Disabled antivirus (AV) programs such as Windows Defender add "HKLM\Software\Policies\Microsoft\Windows Defender" /v DisableAntiVirus /t REG_DWORD /d 1 /f

	add "HKEM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v MpEnablePus /t REG_DWORD /d 0 /f
November 12, 2022	Deployed Vice Society ransomware Path: C:\ProgramData\test.exe
November 12, 2022	Created Administrator account on each endpoint, add to Administrators and Remote Desktop Users localgroup user Administrator {password} /add user Administrator {password} /add localgroup Administrators Administrator /ADD localgroup "Remote Desktop Users" Administrator /ADD add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\Userlist" /v Administrator /t REG_DWORD /d 0 /f
November 12, 2022	Terminated processes such as AV and security software. process where “name like ‘%Agent%’” delete process where “name like ‘%Malware%’” delete process where “name like ‘%Endpoint%’” delete

	process where "name like '%Core.Service%' delete
November 12, 2022	Exfiltrated important files
November 12, 2022	Multiple deployments of Vice Society ransomware was dropped in the %Temp% directory on different endpoints Path: C:\windows\temp\svchost.exe
November 12, 2022	Observed file infector Neshta
November 12, 2022	Performed ransomware routine via $mytemp$\svchost.exe "/c vssadmin.exe Delete Shadows /All /Quiet
November 12, 2022	Vice Society ransomware routine is performed (files are encrypted, ransom note with email contacts is dropped and files are appended with the extension .v1cesO0ciety)

	Contact email of ransom operators: 876505846904@onionmail[.]org 316186524106@onionmail[.]org v-society.official@onionmail[.]org
November 12, 2022	Event viewer logs and remote session traces such as RDP and terminal services were cleared reg delete ""HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default"" /va /f reg delete ""HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"" /f reg add ""HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"" cd %userprofile%\documents\ attrib Default.rdp -s -h del Default.rdp for /F ""tokens=*"" %1 in ('wevtutil.exe el') DO wevtutil.exe cl ""%1"""
November 12, 2022	Deleted itself from the system "%System%\cmd.exe" /c del {Malware File Path}\{Malware File Name} -> nul -> to delete itself

The weaponized tool used by Vice Society is Cobalt Strike, which allows the group to remotely access and control the infected endpoint. The threat actor also used the Rubeus C# toolset for raw Kerberos interaction and abuse (although this is not a new technique, since it has been previously used by Ryuk, Conti, and BlackCat).

To laterally move within the target network, Mimikatz was used to dump passwords. We also observed the presence of the Zeppelin ransomware from another endpoint. Vice Society was known to have deployed Zeppelin before, however, perhaps due to its weaker encryption, the threat actor decided to go with custom-built ransomware.

Vice Society will then execute a PowerShell script to create an administrator account that allows for the remote access of other endpoints and to terminate several processes such as running security software before dropping the custom-built ransomware. In most of the ViceSociety detections we also observed the presence of Neshta file infector (which can be cleaned by Trend Micro), although it is not clear how this occurred.

Virtual servers, such as Microsoft Hyper-V, are also affected in this attack. We also found the attacker removing traces of RDP sessions such as wevtutil.exe, a technique that was previously used by Clop ransomware and KillDisk.

```
We are the only who can give you tool to recover your files.

To prove that we have the key and it works you can send us 2 files and we will decrypt it for free (not more than 2 MB each).

Write to email:

Alternative email:

Public emai:l

Our tor website:

Our mirrors:

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to ours) or you can become a victim of a scam.
```

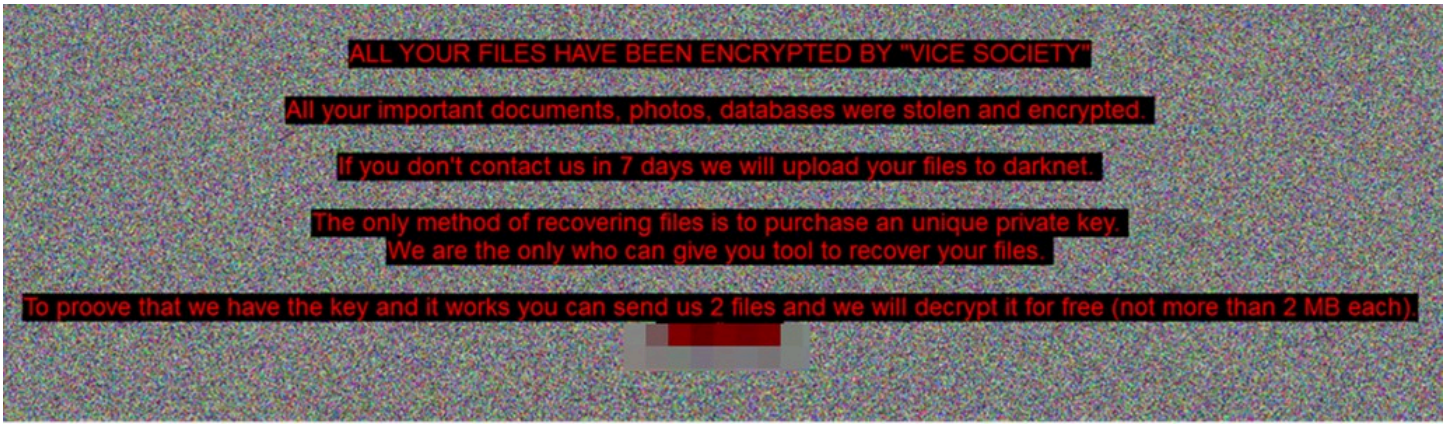


Figure 5. The ransomware note (top) and desktop ransom message (bottom) displayed on the victim's machine

Figure 6. The primary TOR website and mirror links

Figure 7. Vice Society's file storage site

Once the administrator account is added and established, Vice Society can terminate several processes, including security-related ones, to enable the successful deployment and execution of its ransomware on the affected endpoints.

- %sql%
- %Veeam%
- %Core.Service%
- %Mongo%
- %Backup%
- %QuickBooks%
- %QBDB%
- %QBData%
- %QBCF%
- %Kaspersky%
- %server%
- %sage%
- %http%
- %apache%
- %segurda%
- %center%
- %silverlight%
- %exchange%
- %manage%
- %acronis%
- %autodesk%
- %database%
- %firefox%
- %chrome%
- %barracuda%
- %arcserve%
- %sprout%
- %anydesk%
- %protect%
- %secure%
- %adobe%
- %java%

- %engine%
- %web%
- %vnc%
- %teamviewer%
- %OCSInventory%
- %monitor%
- %security%
- %def%
- %dev%
- %office%
- %Framework%
- %AlwaysOn%
- %Agent%
- %Malware%
- %Endpoint%
- %sql%
- %Veeam%
- %acronis%
- %autodesk%
- %database%
- %adobe%
- %java%
- %logmein%
- %microsoft%
- %solarwinds%
- %engine%
- %QBDB%
- %QBData%
- %QBCF%
- %Kaspersky%
- %server%
- %sage%

- %vnc%
- %AlwaysOn%
- %Framework%
- %sprout%
- %firefox%
- %chrome%
- %barracuda%
- %arcserve%
- %exchange%
- %manage%
- %Core.Service%
- %Mongo%
- %Backup%
- %QuickBooks%
- %teamviewer%
- %OCSInventory%
- %monitor%
- %security%
- %def%
- %dev%
- %office%
- %anydesk%
- %protect%
- %secure%
- %segurda%
- %center%
- %silverlight%

Conclusion and Trend Micro solutions

Strike and malware such as Zeppelin and Hello Kitty/Mehlands to enhance their routines. Given what we know of the group's technical knowledge and their willingness to target several different industries and regions, we can expect them to remain a significant player in the ransomware landscape and a threat that organizations must keep track of moving forward.

A multilayered approach can help organizations guard possible entry points into their system, such as endpoints, emails, web, and networks. The following security solutions can detect malicious components and suspicious behavior, which can help protect enterprises.

- **Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.**
- **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

The indicators of compromise for this blog entry can be found here.

Tags

Authors

Ieriz Nicolle Gonzalez
Threat Analyst

Paul Pajares
Threats Analyst

Arianne Dela Cruz
Threats Analyst

Warren Sto.Tomas
Sr. Threat Research Engineer

Related Articles

Understanding the Initial Stages of Web Shell and VPN Threats: An MXDR Analysis

Attacker Abuses Victim Resources to Reap Rewards from Titan Network

A Cybersecurity Risk Assessment Guide for Leaders

See all articles ›

Country Headquarters

Trend Micro - United States (US)

225 East John Carpenter Freeway
Suite 1500
Irving, Texas 75062

Phone: +1 (817) 569-8900

TREND MICRO | Business