INTRINSEC
Innovative by design

Vice Society

CYBER THREAT INTELLIGENCE

Vice Society spreads its own ransomware

TLP: CLEAR

February 2023

Website
www.intrinsec.com

Blog
www.intrinsec.com/blog

Twitter
@Intrinsec

INTRUSION SET ANALYSIS

Vice Society spreads its own ransomware

TLP: CLEAR

Table of contents

Executive summary

Vice Society is a financially motivated organization encompassing operators and opportunistic intrusion sets known for intrusion, exfiltration and extorsion against a large sample of victims since June 2021. The operator(s) of these alleged intrusion sets offer(s) an active infrastructure as new victims are constantly added to the anonymized dedicated leak site where data of the victims is exposed.

The actors affiliated with Vice Society leverage not only custom Vice Society branded variants but also several ransomware-as-a-service payloads (BlackCat) as well as purchased malware (Zeppelin) for conducting attack campaigns. Sometimes, affiliates do not or cannot encrypt data, thus resorting only to the exposure of exfiltrated data for getting the ransom paid. The overall TTPs are close to those usually encountered by Russian-speaking extorsion groups making headlines in recent years.

INTRUSION SET ANALYSIS

Vice Society spreads its own ransomware

TLP: CLEAR

We hereby provide threat intel on a variant of a Vice Society locker specimen, dubbed PolyVice by SentinelOne. Slight overall changes were recently observed in terms of file extension and email contact which substantiates that Vice Society affiliates use customizable builders.

As a reminder, this type of threat is sometimes (though increasingly) endowed with Linux ESXi encryption capabilities to target critical systems being managed in virtualized environments.

Intrinsec CTI services

Organizations are facing a rise in the sophistication of threat actors and intrusion sets used by malicious actors.

To address these evolving threats, it is now necessary (but not sufficient) to take a proactive approach to the detection and analysis of any element deemed malicious, in order to allow companies to anticipate, or at least react as quickly as possible, to the attempted compromises they face.

For this report, shared with our clients in December 2022, Intrinsec relied on its Cyber Threat Intelligence service, which provides its customers with high value-added, contextualized and actionable content to understand and contain cyber threats.

To go further, Intrinsec offers you, through its “Risk Anticipation” module, dedicated and actionable intelligence to feed your security tools. For more information, go to www.intrinsec.com/veille-cybersecurite/.

Aliases (Operator)

- Vice Society
- V-society
- DEV-0832 (Microsoft)
- Vice Spider (CrowdStrike)

Victimology

Vice Society has been particularly active in 2022, with a peak from April – June. The following chart shows the groups’ activity per month. Their victims are mostly from the US (34) and the UK (18). As far as France is concerned, we identified 8 victims since the beginning of this year.

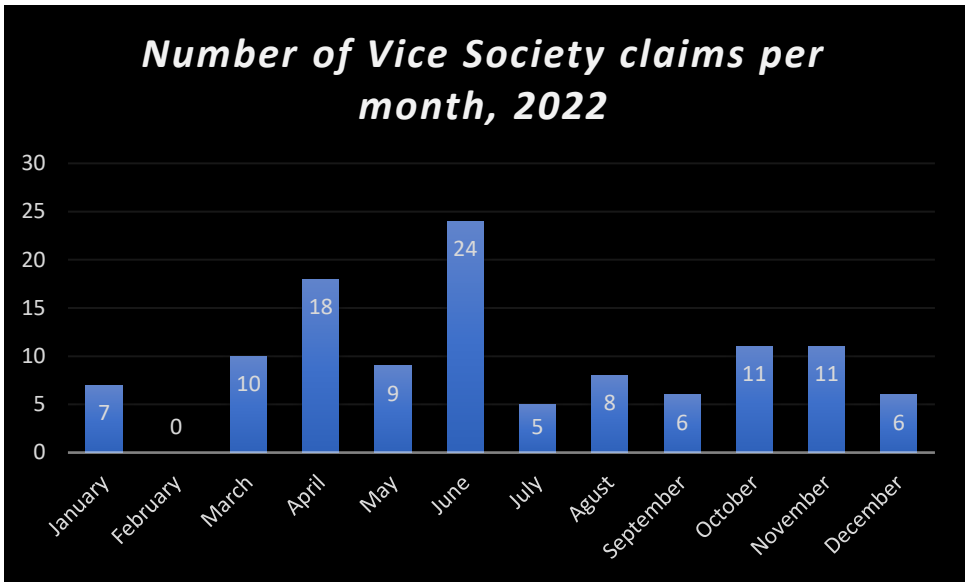

Figure 1: Vice Society's activity per month, 2022.

Vice Society is known for a high number of victims from the education sector, counting 38 claims in 2022, with the healthcare sector coming in second with 19 claims. Those organizations may be identified by advanced extorsion groups as Vice Society as entities with lower defences while having a greater likelihood of paying ransoms.

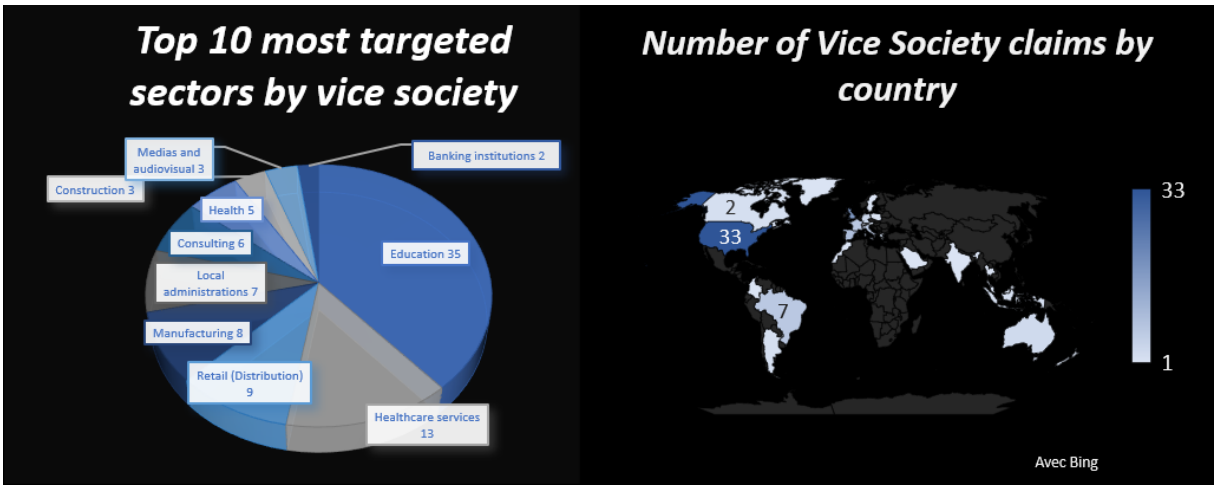

Figure 2: Left: Top 10 sectors claimed by Vice Society ransomware. Right: Number of Vice Society claims by country. This ranking is based on exposed victim's database from their DLS.

As demonstrated in the chart below, this threat exhibits the highest rate of claims in the education sector as compared with other extortion groups (we monitored 115 claims in 2022 and at the time of writing).

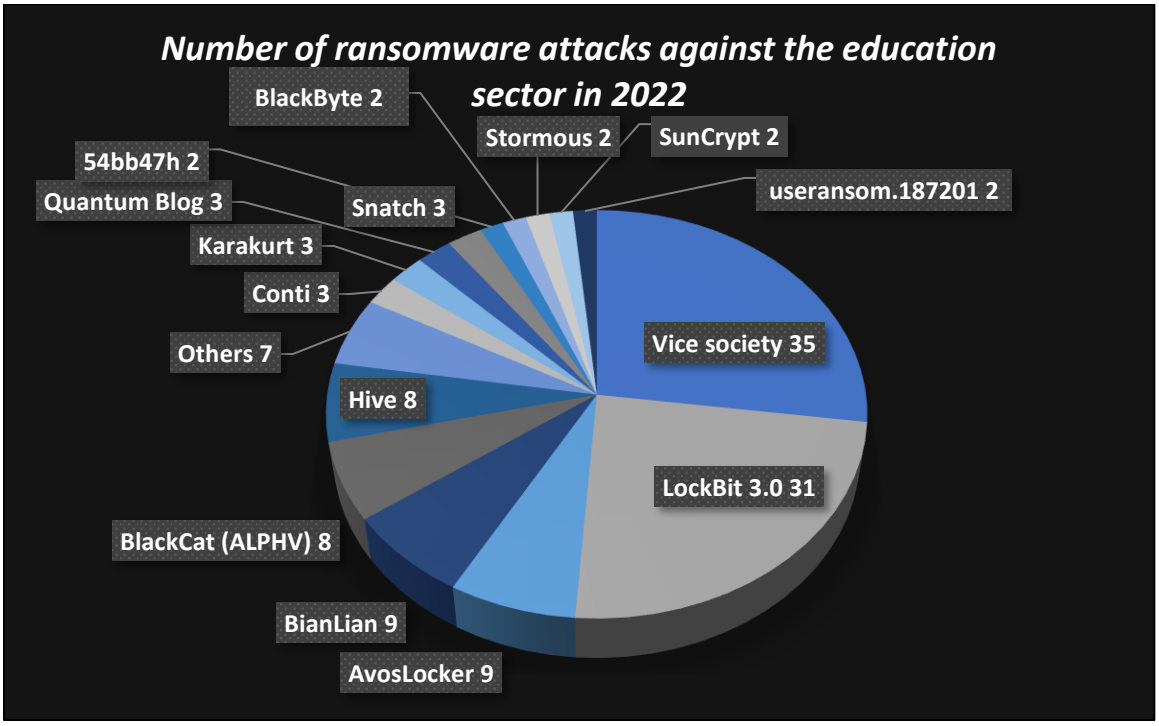

Figure 3: Monitored intrusion sets impacting the Education sector, upon 2022.

Open-source information

1. Analysis of the DLS

Vice Society uses a .onion address to host its Dedicated Leak Site (DLS). Intrinsec's CTI chose not to publish the leak site's address.

As mentioned by Unit42 the latter has been recently under maintenance and endowed with a brand new graphic design and sections.

The most recent header of the Vice Society's DLS is close enough to the logo of the famous video game entitled ''Grand Theft Auto: Vice City", which somewhat matches the brand chosen by this adversary.

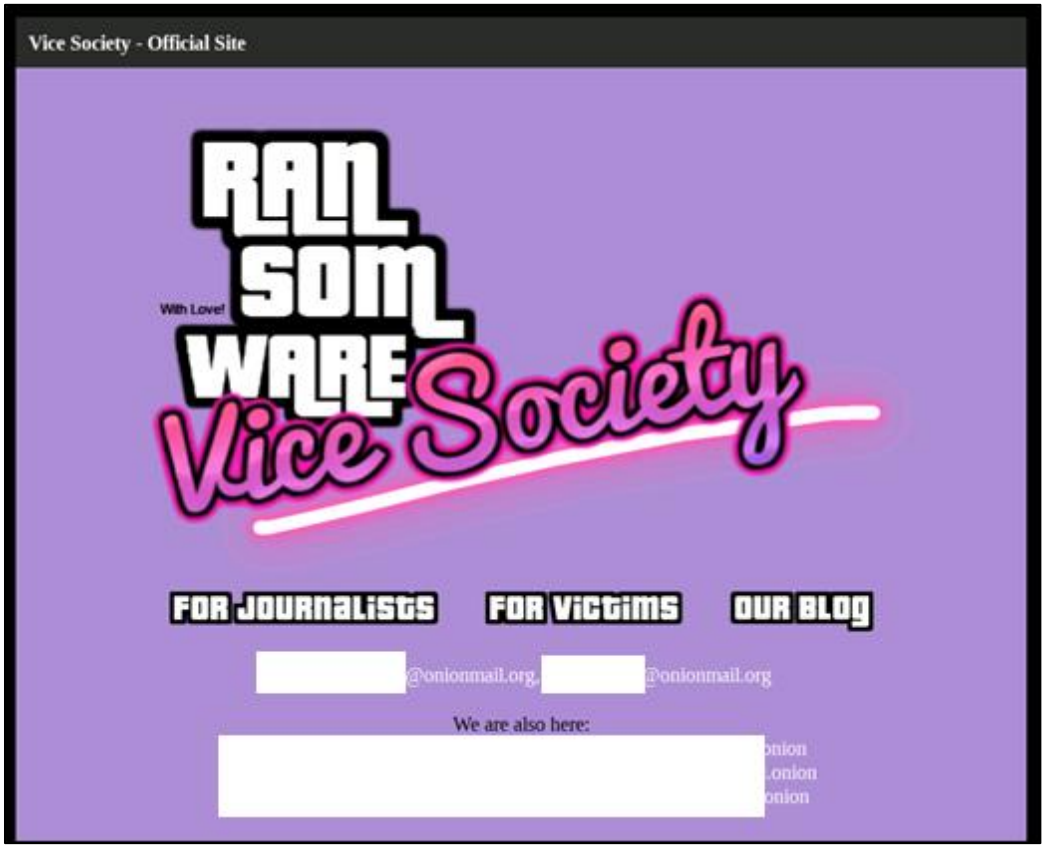

Figure 2: Vice Society's Dedicated Leak Site (DLS) threatening to leak stolen data.

From this website, the operator mentioned other mirror servers being available and aiming at redundancy, some of which being no longer active. It also provides several email contact addresses.

The data of the victims are stored and made available from this anonymized server:

http://[redacted][.]onion/[unique folder]/[a-zA-Z0-9]{14}

The leaked data is stored in the same unique parent folder but sorted in seemingly randomized subfolders for each victim matching the following regex (/[a-zA-Z0-9]{14}). Each victim exposed possesses its own randomized directory.

2. Tooling

Vice Society affiliates are known to abuse legitimate tools such as PowerShell scripting, PsExec, vssadmin, Impacket (especially the wmiexec functionality), Power admin and Rclone or MegaSync (for exfiltration). They have shown to exploit the infamous “PrintNightmare” vulnerabilities for lateral movement:

- CVE-2021-1675
- CVE-2021-34527

According to Microsoft, Vice society affiliates have also exploited a flaw patched in April 2022 identified as CVE-2022-24521 (Windows Common Log File System (CLFS) logical-error vulnerability).

As far as C2 frameworks and backdoors are concerned, the following tools have been reported as leveraged by Vice Society affiliates:

- Cobalt Strike
- SystemBC
- PortStarter
- PowerShell Empire

Code analysis

Intrinsec's CTI team came across suspicious PE files: an executable that we assumed to be a locker, and a DLL file that we thought was a post-exploitation agent.

1. PolyVice locker

We started analysing what we believed to be a locker, by executing it in a controlled environment. We observed debugging messages on top of numerous associated errors displayed to the affiliate upon encryption process. This may suggest that the ransomware is at its early stages of development and will probably be updated in the next releases.

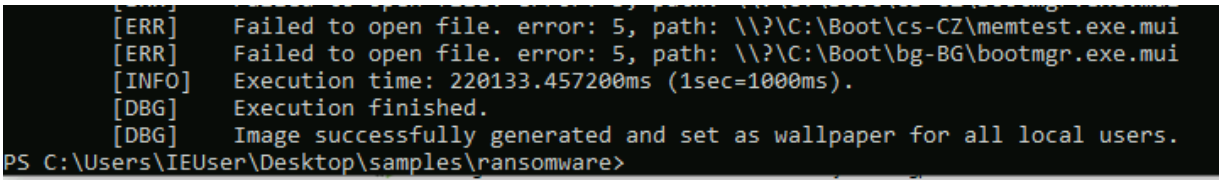

Figure 3: Debugging messages on top of numerous associated errors displayed to the affiliate upon encryption process may suggest that the ransomware is at its early stages of development.

As often encountered with ransomwares, this locker modifies the wallpaper of the victim's desktop after the encryption process has successfully finished with an advertisement depicted in the figure below.

Figure 4: Modified PolyVice variant wallpaper.

A ransom note file named 'AllYFilesAE' is copied in each encrypted directory.

Figure 5: A filename "AllYFilesAE" is found in each encrypted directory.

Its content, stored within the payload, is presented below.

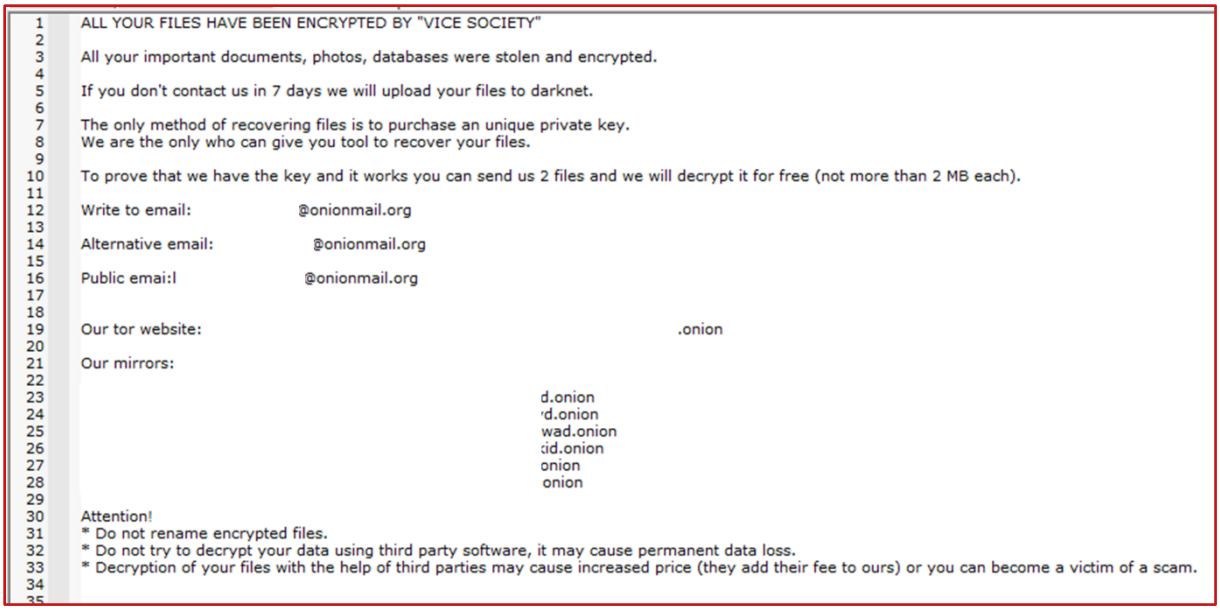

Figure 6: Vice Society ransom note of a PolyVice specimen. The filename is 'ALL YOUR FILES ARE ENCRYPTED'.

On December 22, SentinelOne released a detailed analysis of what they called the PolyVice locker. The article ends with three YARA rules: one for the PolyVice locker, one for Vice Society's version of PolyVice and one for the ransomware variant dubbed as RedAlert.

The binary file found by Intrinsec's CTI team matches both YARA rules from the Sentinelone's article: "MAL_Win_Ransomware_PolyVice" and "MAL_Win_Ransomware_ViceSociety" on all the strings. In contrast, it does not match the RedAlert YARA rule "MAL_Lin_Ransomware_RedAlert".

We can assert with a high level of confidence that the studied file is indeed the same that SentinelOne named PolyVice.

PolyVice uses both asymmetric and symmetric encryption: NTRUEncrypt and ChaCha20-Poly1305. The binary file is uniquely generated per encryption campaign during the build phase, along with a master NTRU key pair (one per build). At runtime, a second NTRU key pair is generated (one per execution). This new private key is encrypted using the master public key that was generated during the build.

It contains multiple optimization ideas, for example the encryption process uses multi-threading allowing to parallelize with multiple worker threads. Another one is applying different strategies depending on the size of the file to be encrypted: if the file size is less than 5MB it will be fully

encrypted, if it is between 5MB and 100MB it will be partially encrypted (only the top 2.5MB and the bottom 2.5M), and if it is larger than 100MB it will also be partially encrypted (2.5MB every 10% of the file).

The files are encrypted using the ChaCha20-Poly1305 symmetric algorithm, the keys are generated at runtime (one per file) and encrypted using the second NTRU public key. The encrypted symmetric key is appended at the end of each file using a specific footer structure.

The combination of NTRUEncrypt and Chacha20-Poly1305 shows advanced comprehension of modern cryptography and good development skills.

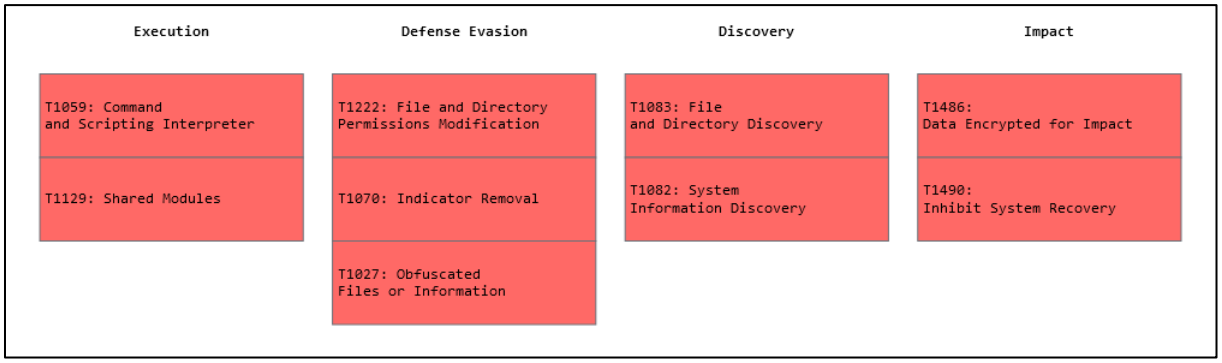

Figure 7: PolyVice's Tactics, Techniques and Procedures (MITRE ATT&CK).

2. PortStarter backdoor

Another interesting file which was spotted by Intrinsec's CTI team seemed to be a post-exploitation agent written in Golang programming language (Go). We were able to confirm it later thanks to the large amount of referred libraries in the PE's strings we could retrieved by a static code analysis.

As a reminder, what we call an agent is the actual malware, the part of the post-exploitation tool that is implanted and executed in the victim's computer. The agent communicates with the C&C (Command and Control) server using a mutual communication protocol.

Malwares written in Go is soaring, particularly embraced by cryptominers; maybe the most famous one is to date Sliver, an open-source Command and Control system written in Go made for red teams and penetration testers. This trend could be explained by several factors, the main one being the intrinsic benefit of Go: simplicity. It allows fast development, provides well documented libraries (networking APIs for example), is easy to learn and offers very handy capabilities such as garbage collection and built-in testing (all of those within a compiled language, thus providing good performance and does not require an interpreter). One other advantage of Go is the detection rate: it is much lower than more standard languages such as C or C++ as it is relatively new. Reversing malwares compiled in Go is usually more challenging due to the numerous embedded libraries with higher associated file sizes.

We then began to analyse the agent, starting with a dynamic analysis using Process Monitor and ProcDOT for user friendly visualisation.

We witnessed the sample running some system commands using native Windows tools, such as:

- Command line:
  ```
  powershell.exe -command "get-wmiobject win32_computersystem | select-object -expandproperty domain"
  ```
  - This command is a reconnaissance technique: T1590.001 Gather Victim Network Information: Domain Properties
  - It leverages the Get-WmiObject PowerShell cmdlet to harvest information about the victim's domain name from the win32_computersystem class
- Command line:
  ```
  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  ```
  - This is a common command line used for example in Cobalt Strike (a very popular post-exploitation framework)
  - The latter will run the conhost.exe binary (Windows Console Host), the "server" behind the Command Prompt "cmd.exe", with specific arguments
  - "0xffffffff" is the Console Host session ID. When the cmd.exe binary is executed without specifying the session ID it will by default be redirected to this session. Thus, running the Console Host with this session ID will receive the commands
  - "-ForceV1" forces the Console Host legacy mode: "conhostV1.dll"
- Command line:
  ```
  powershell.exe -command "& nslookup myip.opendns.com resolver1.opendns.com"
  ```
  - This command will retrieve the public IP address of the victim's computer (the gateway used for internet access if not exposed)
- Command line:
  ```
  powershell.exe -command "new-netfirewallrule -displayname 'windows update' -direction outbound -action allow -protocol tcp -remoteport 80-130,443,2000-2050 -enabled true"
  ```
  - This command is a technique used to impair the victim's defenses: T1562.004 Impair Defenses: Disable or Modify System Firewall
  - It leverages the New-NetFirewallRule PowerShell cmdlet to allow outbound traffic on specific TCP ports, and disguises it as a Windows Update edit

With these elements, we had quite a good idea of the malware's role and functionalities.

It turns out that such capabilities could match with this article from Microsoft that mentions a backdoor written in Go dubbed 'PortStarter'. According to Microsoft analysis, this malware provides functionality such as modifying firewall settings and opening ports to connect to pre-configured command-and-control (C2) servers. This corresponds well to our analysis thus far.

From IOCs provided in Microsoft's paper we could track the evolution of the malware in terms of developments as presented in the table below:

SHA-256	Vhash	Imphash	Entry point	Go version	Timestamp compilation	Size	Name
9f9fefc791e2011d97072382dad9628e0644f2c37a7cd09ded1737396b20d3db	1961476d5555151c051d1az3b14&z2	afec1cff5fa846cfa83f09621ee4da27	5072	1.18.3	2022-07-18 23:50:44 UTC	9095824	[Hash].exe
ca7e91e1c104a1c909ceab85d2c1f188b9fa82a0a58f66c0fc756dc8615e70ea	1961476d5555151c051d1az3b14&z2	afec1cff5fa846cfa83f09621ee4da27	5072	-	2022-08-03 08:08:41 UTC	9103124	AdobeUpdate.dll
8750d579e00d32888920ba9acf38f3ddc2d280f7ae586bc0aafd97c78d14b5b8	1961476d5555151c051d1az3b14&z2	afec1cff5fa846cfa83f09621ee4da27	5072	-	2022-09-05 03:04:23 UTC	9107682	main.dll
e6e957de0cacb333ecf0cbd7049572d1c839d58cadc9f1ede04778f81b19708f	1961476d5555151c051d1az3b12&z2	226f212fbd387a85e62b6b9643a59251	4944	1.18.5	2022-09-27 02:55:54 UTC	9091520	main.dll
8e962d0be1c7ec44574f277942454e581f1f4579743d76dd341893acd64afc60	1961476d5555151c051d1az3b12&z2	226f212fbd387a85e62b6b9643a59251	4944	1.18.5	2022-09-27 03:47:40 UTC	9091520	main.dll

Figure 8: Table depicting the PortStarter RAT release evolution. A substantial change in the compiled code occurred upon September of this year with a different entry point, which generated to a new hash similarity. Of note is the relative common size ranging between 8-9mb.

From the backdoor sample that we found, we tried to pivot on the sample's imphash using VirusTotal search and could identify another sample being similar enough. The latter matches "PortStarter RAT" according to a YARA rule from Nextron Systems.

These two sources of information can let us assume with a quite good level of confidence that the sample we encountered was in fact a new variant of the program that Microsoft named "PortStarter". File sizes are quite different, which requires further analysis to unravel.

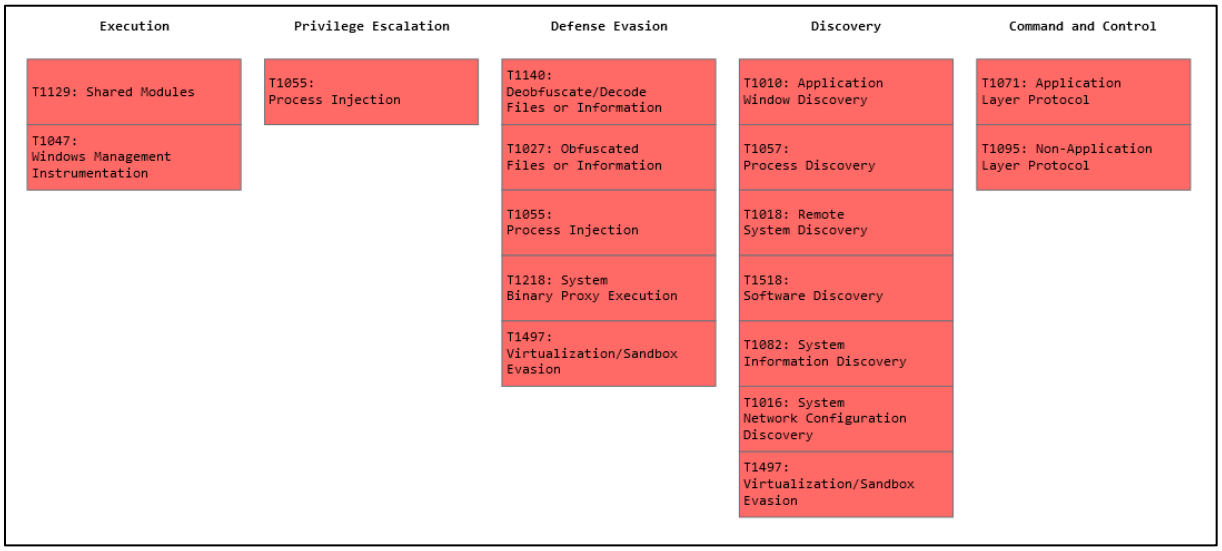

Figure 9: PortStarter's Tactics, Techniques and Procedures (MITRE ATT&CK).

Infrastructure analysis

From the previous client-side analysis of the aforementioned PortStarter backdoor we sought to pivot towards server-side infrastructure. We found a communicating IP from the client towards a potential server (IP address [redacted], with a medium associated confidence level).

By studying historical information for the IP of this server, we found the presence of a reused artefact (hostname: WIN-[redacted]) that turned out be an interesting pivot to reach other potential backdoor servers.

As shown in the figures below, Shodan trends based on historical data provided by this platform shows that a peak of activity occurred around mid-2021. One can observe that the most used ports are 3389, 5985 and 135 respectively leveraged for remote connections RDP, WinRM and RPC, which could be used by a process to remotely create/start services and/or establish persistence mechanism and/or lateralize throughout systems.

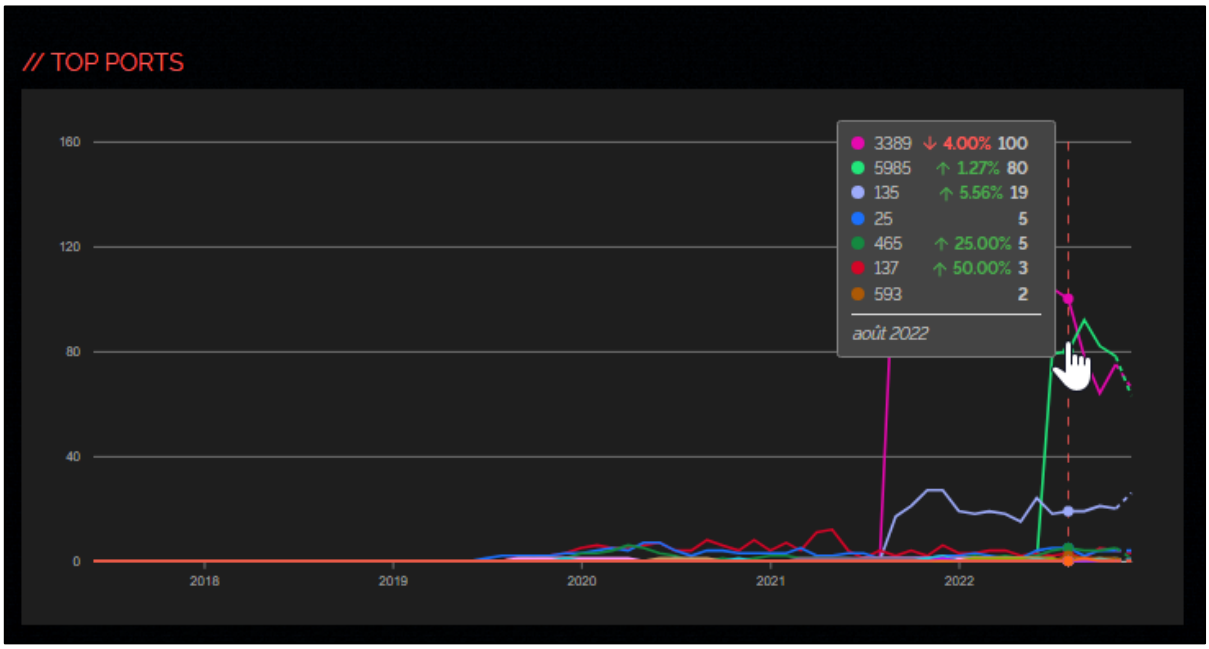

Figure 10: Top ports exposed by servers having endowed by servers with the same hostname WIN-[redacted] found on Shodan (via historical data). The top ports are 3389 (RDP), 5985 (WinRM) and 135 (RPC).

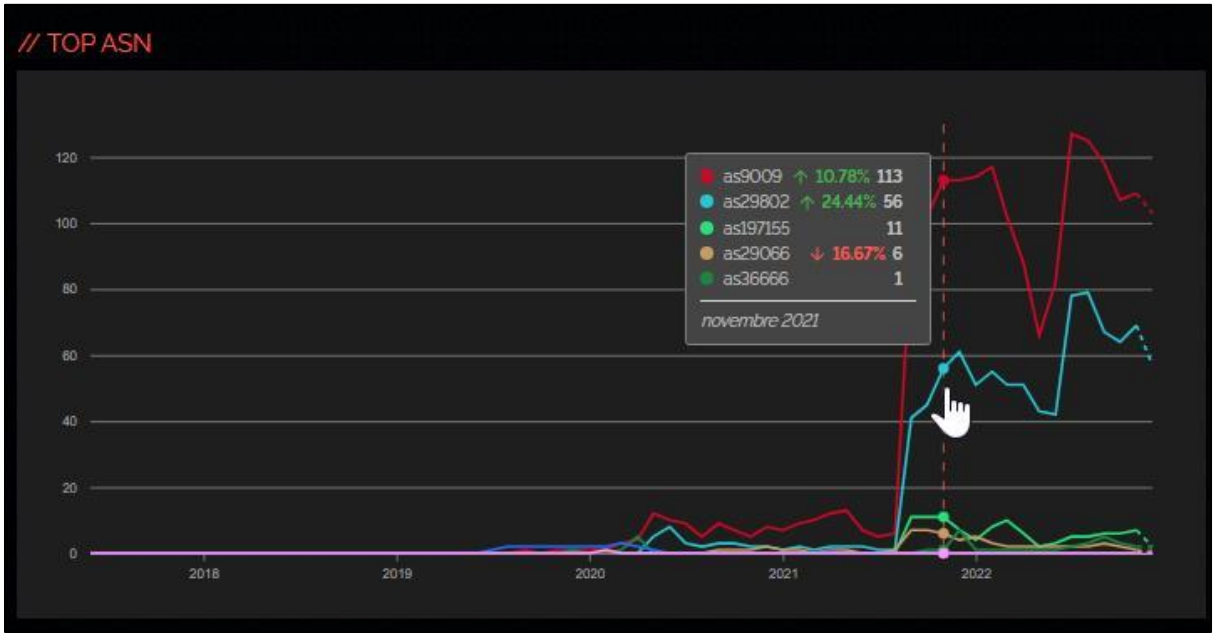

Figure 11: Top ASN of servers having endowed by servers with the same hostname WIN-[redacted] found on Shodan (via historical data). The top ASN are as9009 and as29802 since late 2021.

We found that the server-side infrastructure of Portstarter could be chiefly hosted either by HIVELOCITY, Inc and M247 LTD organizations. This observation is in line with the tweet post of @BushidoToken, who stated that those organizations are often encountered hosting the arsenal of intrusion sets deploying ransomwares.

Attribution

This eCrime adversary conducting extorsion attacks since at least April 2021 has deployed Zepellin ransomware. The source code of Death Kitty, Hello Kitty or Five hands was likely acquired by this group right after. In the meantime, a decryptor was built for Zepellin, which became public in November 2022 and could have coerced them even that date to adopt other commodity ransomwares. Hello Kitty rapidly became the main payload variant deployed upon their operations. Microsoft also reported another ransomware variant adopted by this group Dubbed RedAlert in late September 2022.

In December 2022, SentinelOne revealed that Vice Society operators are building up their own ransomware program likely based on Chily and SunnyDay ransomwares. This new program aiming at being sold (also) to other affiliates was dubbed PolyVice.

In addition, a strong encryption implementation overlap was underlined with the 'RedAlert' ransomware. The latter leverages the NTRUEncrypt (NTRU) library being considered as a Linux locker variant impacting VMware ESXi servers.

The NTRU library, developed in 1996 as an alternative to the RSA and ECC encryption algorithms, has already been used by several ransomware operators; either as the main encryption algorithm for Hello Kitty ransomware or one of the main algorithms for other variants (#Relock / #Hellokitty). Based on

typographical errors in the ransom note, we could trace back to a similar ransom note submitted on August 22 on VirusTotal, whose level of overlap is considered high. From the two email contacts left in this ransom note, we could pivot once again and found several strains that can encrypt non-virtualised Windows environments whose ransom note also contains characteristic typographical errors. To our knowledge, no strains for non-virtualised Windows environments have yet been publicly discussed. Further analysis of these strains could provide information on the genealogy of RedAlert. Researchers at Intezer attribute this strain to the Balaclava malware. Although we found points of similarity in the strain name patterns, their small size (80kb) and the constant evolution of this threat, the level of confidence in the threat attribution remains low at this time.

Though it is possible that those variants (PolyVice, Chily, SunnyDay, Redalert) were developed by at least one common ransomware developer or group, we are not able to date to confirm that information.

Conclusion

Vice Society has shown a striking and versatile evolution since its early stages with the potential to become a very active and impactful ransomware group. It should therefore be considered as a serious threat, certainly against public sectors. Its recent investments in a brand-new locker “PolyVice” and the use of the new Golang backdoor “PortStarter” can be interpreted as a will to continue and expand its operations.

External references

- Vice Society: Profiling a Persistent Threat to the Education Sector
- DEV-0832 (Vice Society) opportunistic ransomware campaigns impacting US education sector
- #StopRansomware: Vice Society
- Custom-Branded Ransomware: The Vice Society Group and the Threat of Outsourced Development

Actionable content

Type	Value	Description	TLP
Script (batch file)	/c vssadmin.exe Delete Shadows /All /Quietreg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" /va /freg delete "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" /freg add "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers"cd %userprofile%\documents\attrib Default.rdp -s -hdel Default.rdp for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"	Malicious hardcoded commands to Inhibit System Recovery, then deletes/resets registry keys aiming to hamper a remote recovery of the affected user.	CLEAR
Stix file	7c26041f8a63636d43a196f5298c2ab694a7fcbfa456278aa51757fd82c237d4 011952038331e398fb18efff89fc0962dbc6e9ed 65a4bf1e61d0d30cb0fa40e89555990b	PolyVice ransomware matching SentinelOne's YARA rule	CLEAR
Stix file	432f91e194973dc214d772d39d228748439839b268f6a62ad529cb4f00203aaa ad5d7c7958a16c918956e9cfc51241ecdc018b12 31053d9eb51bde54e46f764f564b8e0c	PolyVice ransomware matching SentinelOne's YARA rule	CLEAR
Stix file	f366e079116a11c618edcb3e8bf24bcd2ffe3f72a6776981bf1af7381e504d61 342c3be7cb4bae9c8476e578ac580b5325342941 9fda237668200542b7a524afd59c6b48	PolyVice ransomware matching SentinelOne's YARA rule	CLEAR
Stix file	9f9fefc791e2011d97072382dad9628e0644f2c37a7cd09ded1737396b20d3db 4ac75d7f27edd182d8ddfe88409810e18c9387d8 208b2cacc950040402045942c77156e2	PortStarter Golang RAT	CLEAR
Stix file	ca7e91e1c104a1c909ceab85d2c1f188b9fa82a0a58f66c0fc756dc8615e70ea 212f17623b450a5d772c81baa28d95ff7d7555c1 20a636f9e09c900b28207638658ed8ea	PortStarter Golang RAT	CLEAR
Stix file	8750d579e00d32888920ba9acf38f3ddc2d280f7ae586bc0aafd97c78d14b5b8 b3930740f7429a7a9a51103f00d9268de85b5be5 3a40088187165ca5477a1129e3b9478d	PortStarter Golang RAT	CLEAR
Stix file	e6e957de0cacb333ecf0cbd7049572d1c839d58cadc9f1ede04778f81b19708f 5c2247b8d0abb72f3888cf0aac68baa96184689a f44a2ecedf9cc278564bf5bdbed3c0d2	PortStarter Golang RAT	CLEAR
Stix file	8e962d0be1c7ec44574f277942454e581f1f4579743d76dd341893acd64afc60 adb3021a4fa15aa86f48ee6149747acbf3098669 ba4a141fe22513e1431c8b3944dc6fd3	PortStarter Golang RAT	CLEAR