IT Security Spotlight: India

February 2022

Introduction

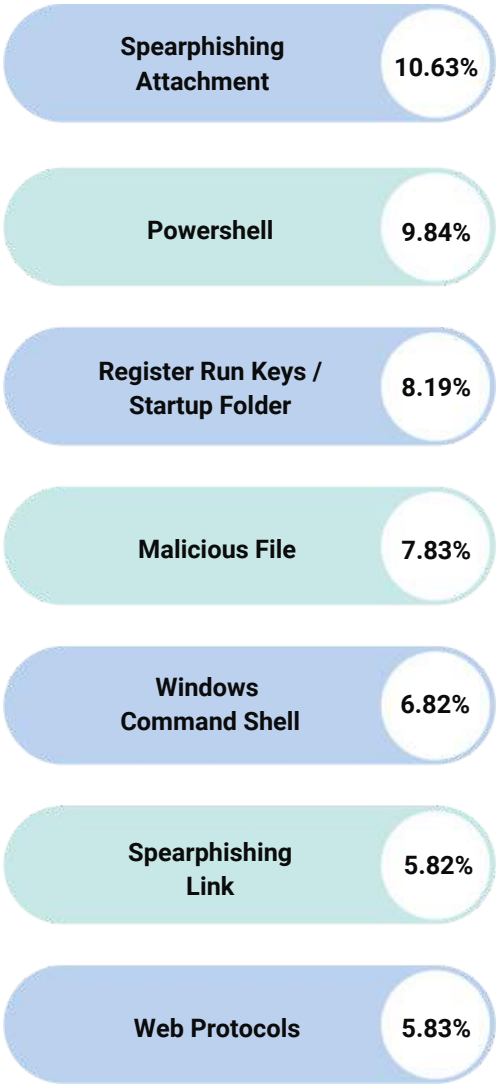
Businesses today are under attack from persistent and sophisticated cybercriminals who can bypass traditional security measures. To combat their attacks, CISOs and CIOs need deeply insightful information that they can take action upon.

To facilitate security, we share with you some key data around the cybersecurity events in the Indian Subcontinent. It reflects the issues we prevented the clients of NTT India from facing. We hope that this localized set of data from our India SOC will be highly relevant to your organization, and help your efforts in keeping your company secure.

Key Trends Seen in Cyber Security Incidents

The analysis seen here features data from our SOC in India observed between 1st to 31st January, 2022.

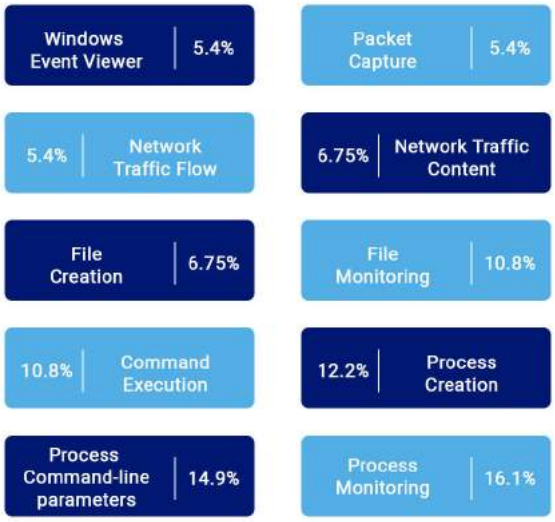
Attack Framework: Top Techniques Used



Incident Tactics

Spearphishing was the top adversarial technique preferred by threat actors.

Attack Framework - Top Log Sources



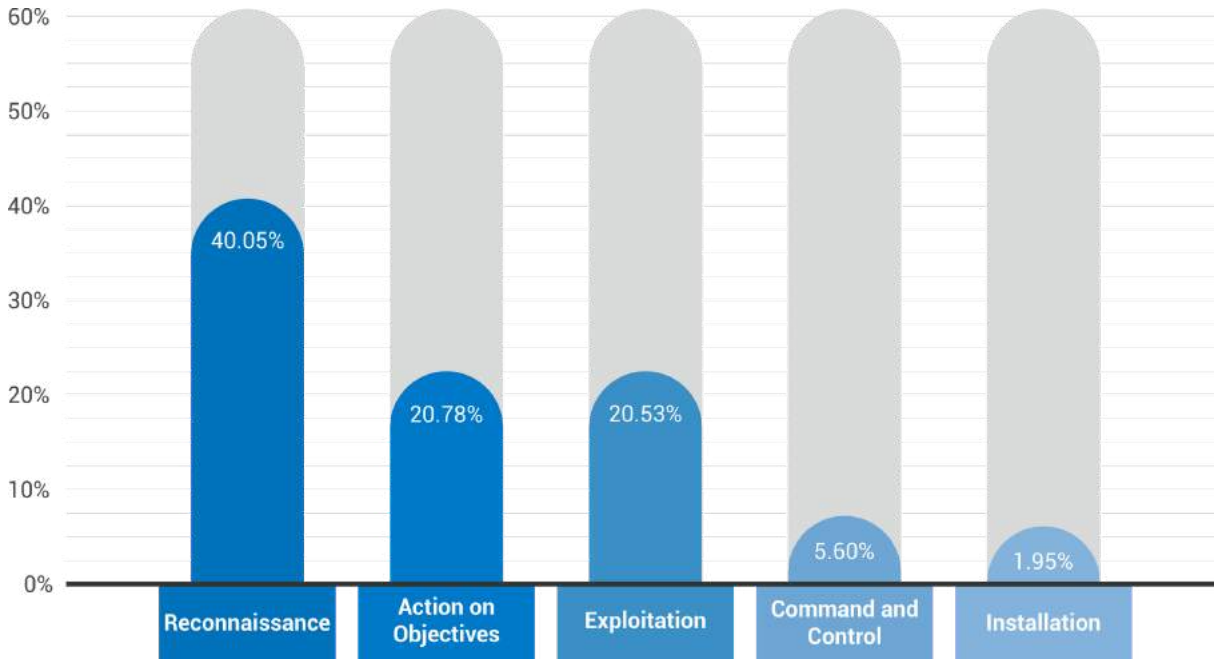
Incident - Type vs. Weekday

	Mon	Tue	Wed	Thurs	Fri	Sat	Sun
Account Anomaly	7.49%	5.11%	5.97%	6.16%	4.33%	2.32%	2.72%
Exploit Activity	0.65%	0.65%	0.86%	0.52%	0.92%	0.74%	0.30%
Malware	0.37%	0.15%	0.27%	0.30%	0.34%	0.40%	0.09%
Network Scanning	0.06%	0.18%	0.21%	0.27%	0.21%	0.12%	0.18%
Policy Violation	0.18%	0.21%	0.21%	0.21%	0	0.27%	0.06%
Suspicious Activity	5.26%	5.29%	5.79%	6.91%	5.48%	3.21%	2.16%
System Health	0.24%	0.43%	0.89%	0.27%	0.58%	0.06%	0.12%

Amongst all the log sources integrated with our Managed Detection and Response, 'process monitoring' proved the most pertinent in detecting attacks.

It is expected to see account anomalies on Monday owing to people forgetting their passwords. However, this month also saw anomalies on Thursday due to a spike in credential harvesting attempts.

Incident - Kill Chain Phase



Malware As A Service: Here's One that is Probably Stealing Your Data

Redline Stealer is a malware that has features for credentials theft, including but not limited to cryptocurrency wallets, browser information, and other authentication data. It also collects information about the targeted machine, such as OS information, system resources, process information, browser credential, and more. Capabilities to inject remote payloads for C2 communication are also included. Redline Stealer is available in the 'Malware As A Service' model from their official telegram channel.

It was recently identified that Omicron news was being exploited to distribute redline malware.

Researchers at multiple cybersecurity companies have said that the use of Redline Stealer started around March of 2020. It quickly became one of the most popular info stealers available on dark web markets.

> Statistics show that **Redline** was used to **steal ~50% of stolen credentials** currently being sold on the dark web.

The snippet of data that Redline malware steals from an endpoint:

- Autofills
- Cookies
- DomainDetects.txt
- ImportantAutofills.txt
- Paswords.txt
- ProcessList.txt
- UserInformation.txt

Our SOC recently saw one such malware, analysis of which is shown below:

Initial Access on the host is observed from a user download which was identified as malicious by End Point Protection Solution.

68532754	MUM-FIN-018	dd9215508a4c60515feef4...	Malicious	2 58 149114	
User: MUM-FIN-018\[redacted]	Certificate: Unsigned	Process path: ...n\Downloads\dd9215508a4c60515feef4a5038aa6dbcc5b3c344d0fac46449765d4af273e8b.exe			

We observe a new process creation post a user download - filename Safewaithand.exe.

Process Create	Win...	1		Process Creation Success	192.168.10.22	0	192.168.10.22

<13>[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4 EventCategory=1 RecordNumber=10345 TimeGenerated=1642253416 TimeWritten=1642253416 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMONEVENT_CREATE_PROCESS Opcode=Info Message=Process Create: RuleName: - UtcTime: ProcessGuid: {8cef9547-cc68-61e2-9203-000000000700} ProcessId: 2888 Image: C:\Users\[redacted]n\Downloads\dd9215508a4c60515feef4a5038aa6dbcc5b3c344d0fac46449765d4af273e8b.exe FileVersion: 1.0.0.0 Description: CrabShooter Product: CrabShooter Company: - OriginalFileName: SafeWaitHand.exe

Registry modification observed and exe added to registry

RegistryEvent (Valve Set)	RegistryEvent (Valve Set)	192.1...	192.1...	**0**	WindowsAuthServer @ MUM-FIN-...	Successful Registry Modification

<13>[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=SYSTEM Domain=NT AUTHORITY EventID=13 EventIDCode=13 EventType=4 EventCategory=13 RecordNumber=10788 TimeGenerated=1642254361 TimeWritten=1642254361 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMONEVENT_REG_SETVALUE Opcode=Info Message=Registry value set: RuleName: InvDB-Path EventType: SetValue UtcTime: [redacted] ProcessGuid: {8cef9547-b598-61e2-b201-000000000700} ProcessId: 9228 Image: C:\Windows\system32\svchost.exe TargetObject: \REGISTRY\A\{253f1b1f-99e5-5aff-3bcc-7a301c6746b1}\Root\InventoryApplicationFile\85f80d0b0a27dc02|bda2fb6dcf6aa7f0\LowerCaseLongPa[redacted] Details: c:\users\john\downloads\85f80d0b0a27dc021b90746ae68fa202534dba28b53d415b1d390a12584c5ceb.exe User: NT AUTHORITY\SYSTEM

New process REGASM.exe spawned which is a legit Windows service associated with Microsoft.Net. However, the outbound communication from this process was identified to be malicious and unknown DNS query to gitlab was initiated by RegASM.exe.

Process Create	192.1...	192.16...	0	WindowsAuthServer @	ProcessCreation Success
Detected Abnormal Parent for a Process	192.1...	192.16..	0	MUM-FIN-... Custom Rule Engine-8 ::	Suspicious Windows Events

68533162 MUM-FIN-018 RegAsm.exe Malicious 2 destinations

User: MUM-FIN-018\[redacted] Certificate: Signed Process path: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

RAW ID	DEVICE	DESTINATION	FIRST SEEN	LAST SEEN	USERS	COUNT
39643538	MUM-FIN-018	172.65.251.78			MUM-FIN-018\[redacted]	
39643510	MUM-FIN-018	185.215.113.57			MUM-FIN-018\[redacted]	

13>J[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=SYSTEM Domain=NT AUTHORITY EventID=22 EventIDCode=22 EventType=4 EventCategory=22 RecordNumber=10797 TimeGenerated=1642254387 TimeWritten=1642254387 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMONEVENT_DNS_QUERY Opcode=Info Message=Dns query: RuleName: - UtcTime: [redacted] ProcessGuid: {8cef9547-d017-61e2-e803-000000000700} ProcessId: 5048 QueryName: gitlab.com QueryStatus: 0 QueryResults: ::ffff:172.65.251.78; Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe User: MUM-FIN-018\[redacted]hn

RegASM.exe is also seen spawning a new proces fl.exe which is downloaded in User-> Appdata-> Temp location, which is identified as Nashbuildminer, used for hogging system resources for XMR mining.

Process Create	192.1...	192.16...	0	WindowsAuthServer @ MUM-FIN-...	Process Creation Success
Detected An Unknown / Unseen Process (Based On The Process Hash)	192.1...	192.16...	0	Custom Rule Engine-8 ::	Suspicious Windows Events
Process Launched from Temp Directory	192.1...	192.16...	0	Custom Rule Engine-8 ::	Misk Malware

<13>[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=SYSTEM Domain=NT AUTHORITY EventID=11 EventIDCode=11 EventType=4 EventCategory=11 RecordNumber=10796 TimeGenerated=1642254385 TimeWritten=1642254385 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMONEVENT_FILE_CREATE Opcode=Info Message=File created: RuleName: EXE UtcTime: [redacted] ProcessGuid: {8cef9547-d017-61e2-e803-000000000700} ProcessId: 5048 Image: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe TargetFilename: C:\Users\J[redacted]n\AppData\Local\Temp\fl.exe CreationUtcTime: [redacted] User: MUM-FIN-018\J[redacted]n

FILELESS LOADING
Process ID: 1480
Source Process: ....ice\HarddiskVolume2\Users\[redacted]\AppData\Local\Temp\fl.exe
Target: nashbuild-miner.exe

Company:
Description:
Version:

Defense evasion using a Bas64 encoded powershell was observed. Upon decoding it was observed that threat actor was attempting to add an exception for *.exe and *.dll to bypass antivirus protection.

```
cmd /c powershell -EncodedCommand
"QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG
4AUABhAHQAaAAgAEAAKAAkAGUAbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABlACwAJABlAG4A
dgA6AFMAeQBzAHQAZQBtAEQAcgBpAHYAZQApACAALQBGAG8AcgBjAGUA" & powershell -
EncodedCommand
"QQBkAGQALQBNAHAAUAByAGUAZgBlAHIAZQBuAGMAZQAgAC0ARQB4AGMAbAB1AHMAaQBvAG
4ARQB4AHQAZQBuAHMAaQBvAG4AIABAACgAJwBlAHgAZQAnACwAJwBkAGwAbAAnACkAIAAtAEYA
bwByAGMAZQA=" & exit
```

```
Add - Mp Preference - Exclusion Path @ ( $ env : User Profile , $ env : System Drive ) - For c e
A d d - M p P r e f e r e n c e - E x c l u s i o n E x t e n s i o n @ ( ' e x e ' , ' d l l ' ) - F o r c e
```

Another malicious file was launched, which was identified as a crypto miner

68533277 MUM-FIN-018 fvnhyyy.exe Malicious In memeory Exe...
User: MUM-FIN-018\[redacted] Certificate: Unsigned Process path: C:\Users\John\AppData\Roaming\ fvnhyyy.exe

```
<13>[redacted]MUM-FIN-018 AgentDevice=WindowsLog
AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-
Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018
User=SYSTEM Domain=NT AUTHORITY EventID=1 EventIDCode=1 EventType=4
EventCategory=1 RecordNumber=10833 TimeGenerated=1642254440
TimeWritten=1642254440 Level=Informational Keywords=0x8000000000000000
Task=SysmonTask-SYSMONEVENT_CREATE_PROCESS Opcode=Info Message=Process Create:
RuleName: - UtcTime: [redacted] ProcessGuid: {8cef9547-d067-61e2-f603-000000000700}
ProcessId: 972 Image: C:\Users\John\AppData\Roaming\ fvnhyyy.exe FileVersion: - Description: - Product:
- Company: - OriginalFileName: - CommandLine: "C:\Users\J[redacted]n\AppData\Roaming\ fvnhyyy.exe"
CurrentDirectory: C:\Windows\system32\ User: MUM-FIN-018\J[redacted]n LogonGuid: {8cef9547-b13b-61e2-
27c8-020000000000} LogonId: 0x2C827 TerminalSessionId: 1 IntegrityLevel: High Hashes:
MD5=560B413ABE765EC7B91056689A9DA571,SHA256=68ABF0B7CA9EAAAA657F2678BA5243809757E7
A19FE1BA87DFF6B081F4CE99BC,IMPHASH=9BFD2DAC39AF50555AE9789117B36B66 ParentProcessGuid:
{8cef9547-d067-61e2-f403-000000000700} ParentProcessId: 6112 ParentImage:[redacted]
C:\Windows\System32\cmd.exe ParentCommandLine: "cmd" cmd /c "C:\Users\John\AppData\Roaming\
fvnhyyy.exe" ParentUser: MUM-FIN-018\J[redacted]n
```

A DNS Query to pool.supportxmr.com was observed, which is a known IOC for Crypto-mining.

A service was installed in a system	192.1...	192.16...	0	WindowsAuthServe...	Service Installed
Driver loaded	192.1...	192.16...	0	WindowsAuthServe...	Information...
RegistryEvent (Value Set)	192.1...	192.16...	0	WindowsAuthServe...	Successful Registry Modification

<13>[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=System PluginVersion=7.3.0.41 Source=Service Control Manager Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=J[redacted]n Domain=MUM-FIN-018 EventID=1073748869 EventIDCode=7045 EventType=4 EventCategory=0 RecordNumber=657 TimeGenerated=1642254470 TimeWritten=1642254470 Level=Informational Keywords[redacted]ventlogClassic Task=None Opcode=Info Message=A service was installed in the system. Service Name: WinRing0_1_2_0 Service File Name: C:\Users\John\AppData\Roaming\Microsoft\Libs\WR64.sys Service Type: kernel mode driver Service Start Type: demand start Service Account:

<13>[redacted] MUM-FIN-018 AgentDevice=WindowsLog AgentLogFile=Microsoft-Windows-Sysmon/Operational PluginVersion=7.3.0.41 Source=Microsoft-Windows-Sysmon Computer=MUM-FIN-018 OriginatingComputer=MUM-FIN-018 User=SYSTEM Domain=NT AUTHORITY EventID=22 EventIDCode=22 EventType=4 EventCategory=22 RecordNumber=10862 TimeGenerated=1642254472 TimeWritten=1642254472 Level=Informational Keywords=0x8000000000000000 Task=SysmonTask-SYSMONEVENT_DNS_QUERY Opcode=Info Message=Dns query: RuleName: - UtcTime: 2022-01-15 12:52:37.008 ProcessGuid: {8cef9547-d085-61e2-fc03-000000000700} ProcessId: 3876 QueryName: pool.supportxmr.com QueryStatus: 0 QueryResults: type: 5 pool-hk.supportxmr.com;::ffff:139.99.124.170;::ffff:139.99.125.38;::ffff:139.99.123.196; Image: C:\Windows\explorer.exe User: MUM-FIN-018\J[redacted]n

WMI Queries trying to gather Sensitive system information like Video controllers, disk information, Operating System and installed software information.

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe WMI Queries: IWbemServices::ExecQuery - root\CIMV2 : SELECT * FROM Win32_VideoController

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe WMI Queries: IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_DiskDrive

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe WMI Queries: IWbemServices::CreateInstanceEnum - root\cimv2 : Win32_ComputerSystem

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe Registry key enumerated: for key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

We also observed attempts to steal browser information and crypto wallet information stored on the Infected machine.

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe File opened:
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe File opened:
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe File opened:
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Cookies

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe File opened:
C:\Users\user\AppData\Roaming\Ethereum\wallets\

Multiple instances of explorer.exe were found to be running in memory, one such process had MZ header and a suspicious encoded command line attached to it, which indicated the malicious behavior of this process.

```
Process: explorer.exe Pid: 3876 Address: 0x140000000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x0000000140000000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000000140000010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000000140000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000000140000030  00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00   ............(...
```

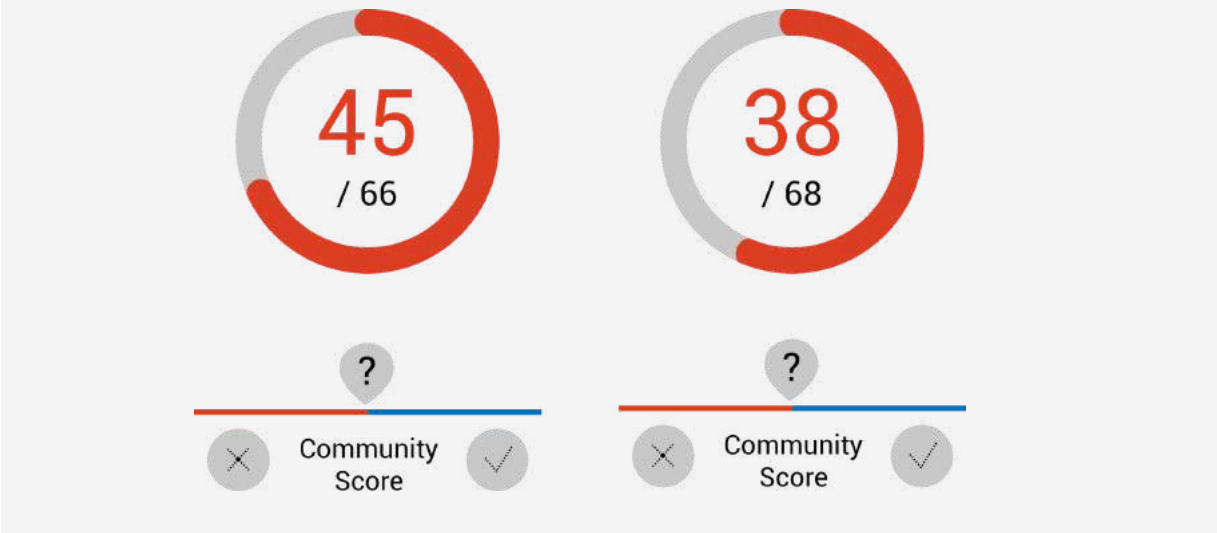
```
**********************************************************************
explorer.exe pid:   3876
Command line : C:\Windows\explorer.exe uynjkkyptxxy1 Xjl3FXYfqqI2timPThbgZueMNpSES88mLhMz2ywydJS6kTcb2sZJ49Q3iSMDc1H0Gsol2ut25e0CiIvlYsuJlRf9cAIWsM5x
Nlv2CpmeSTZ4pQrFWNkEzZPEMfhraeOvsLhWY3jY+xzJ5IosXqgTdD3jVluCpzDi91PFz8FAJKOCtA6KcYwvQwF802MT/V1n/CnG34YKGCYZXIU4zRQW7lEbRoAvFGVxIf4tKfOP3Hf6S6LyTk2je
uhzzf2Zcs/0s5y+xhTpkhMOajNG7ary/m9cgvIxlkbwK4Z5kKm8TURafQOdOA6pYc+FSLPejIrpYVXzGzUYCucc1JnrFsvlMQn0ihvM4UYwSpRyIOiJG/Ku6F7NGOK/Ye1L7T6a3ZENVZhlQpPYYN
gPEbnhEJs092J41opYOyT9/sUeOPXCLeCFLqPwf3W3gaprr6ck+6v8QMjxVDWehenO0tK4Fy+DeQ==

Base                              Size          LoadCount LoadTime                          Path
------------------ ----------------- ---------- ------------------------------ ----
0x0000000140000000           0x787000             0xffff [redacted] UTC+0000   C:\Windows\explorer.exe
```

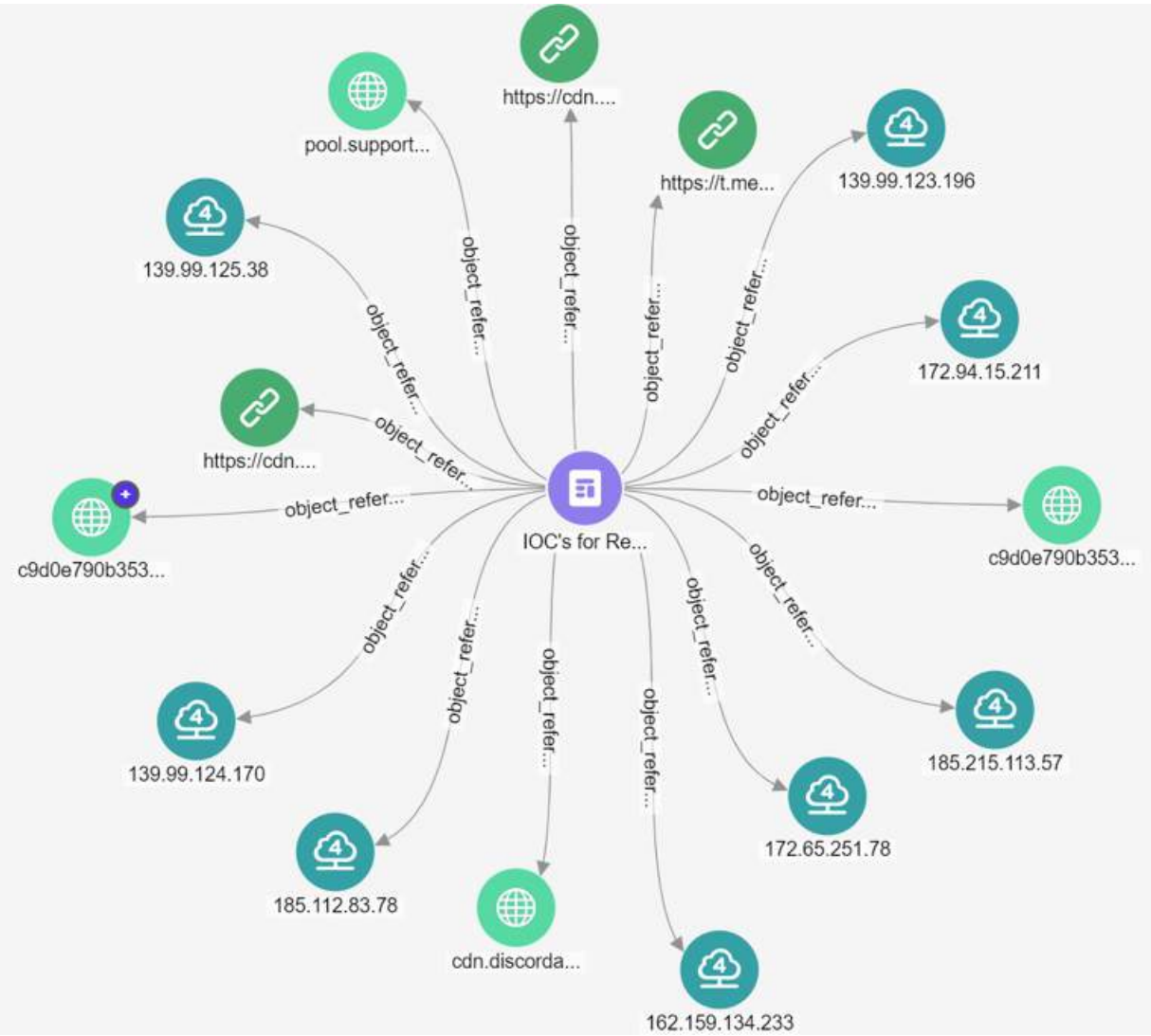
Traffic on Non-Standard Port

101	13.045575	192.168.10.22	185.215.113.57	TCP	66	50335 → 50723 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
103	13.425676	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=1 Ack=1 Win=262656 Len=0
104	13.453428	192.168.10.22	185.215.113.57	TCP	95	50335 → 50723 [PSH, ACK] Seq=1 Ack=1 Win=262656 Len=41
106	13.874770	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=42 Ack=2 Win=262656 Len=0
107	13.935436	192.168.10.22	185.215.113.57	TCP	260	50335 → 50723 [PSH, ACK] Seq=42 Ack=2 Win=262656 Len=206
114	14.359130	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=248 Ack=144 Win=262656 Len=0
148	19.465312	192.168.10.22	185.215.113.57	TCP	208	50335 → 50723 [PSH, ACK] Seq=248 Ack=144 Win=262656 Len=154
153	19.841718	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=402 Ack=3842 Win=262656 Len=0
195	21.250341	192.168.10.22	185.215.113.57	TCP	763	50335 → 50723 [PSH, ACK] Seq=402 Ack=3842 Win=262656 Len=709
199	21.671615	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=1111 Ack=3967 Win=262656 Len=0
228	24.412930	192.168.10.22	185.215.113.57	TCP	445	50335 → 50723 [PSH, ACK] Seq=1111 Ack=3967 Win=262656 Len=391
230	24.845496	192.168.10.22	185.215.113.57	TCP	225	50335 → 50723 [PSH, ACK] Seq=1502 Ack=4095 Win=262400 Len=171
236	25.235048	192.168.10.22	185.215.113.57	TCP	225	50335 → 50723 [PSH, ACK] Seq=1673 Ack=4223 Win=262400 Len=171
239	25.671713	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=1844 Ack=4348 Win=262144 Len=0
240	25.707219	192.168.10.22	185.215.113.57	TCP	252	50335 → 50723 [PSH, ACK] Seq=1844 Ack=4348 Win=262144 Len=198
244	26.156233	192.168.10.22	185.215.113.57	TCP	54	50335 → 50723 [ACK] Seq=2042 Ack=4473 Win=262144 Len=0
251	26.572639	192.168.10.22	185.215.113.57	TCP	228	50335 → 50723 [PSH, ACK] Seq=2042 Ack=4473 Win=262144 Len=174
254	26.959120	192.168.10.22	185.215.113.57	TCP	491	50335 → 50723 [PSH, ACK] Seq=2216 Ack=4601 Win=261888 Len=437

Multiple AV Scanner detections for fl.exe and fvnhyyy.exe



NTT Threat Intel Relation Graph combining all IOCs for Redline Stealer



Indicators of Compromise & YARA Rules

The below indicators of compromise and YARA rules might help you with the early detection of this threat.

YARA Rules Triggered

- spyeye_plugins
- RooterStrings
- Rooter
- Njrat
- win_exe_njRAT
- CAP_HookExKeylogger
- WimmieStrings
- Wimmie
- Insta11Strings
- Insta11

File Hashes

2864336E07CD5C83D65AE61B730577D5B87310DD

9E03F443962FDF5C5A5C9A8A2C6847169461F20B

BF14044D9DF67B55811EF1147D0ED081DB6713B8

EE068F233C553DC8760050D1CDB91047B30FF462

1494545E3B5DE16E63ACCC078C4670482F082C1C

File Names

dd9215508a4c60515feef4a5038aa6dbcc5b3c344d0fac46449765d4af273e8b.exe

RegAsm.exe

fl.exe

fvnhyyy.exe – Nashbuild miner

sihost64.exe

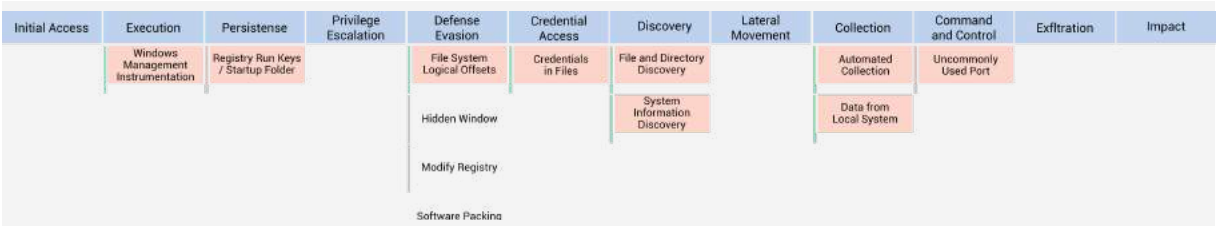
IPs:

- 172.94.15[.]211
- 139.99.125[.]38
- 185.215.113[.]57
- 139.99.124[.]170
- 172.65.251[.]78
- 185.215.113[.]57

Domains

pool.supportxmr[.]com

MITRE ATT&CK Mapping



Conclusion

The Redline malware targets popular browsers such as Chrome and Edge; hence storing your passwords in browsers is not considered a best practice. Even though browsers encrypt passwords while storing, since the malware runs using the same account used to store the passwords, threat actors can decrypt the passwords.

Threat actors use these passwords for credential stuffing, which helps them break into complex networks.

Employee security awareness and multi-factor authentications remain essential for protection from these threats.

Visibility at multiple layers and cross-correlation is required to detect and protect against this malware.

Note: We trust that this data will help you to keep your system secured. Do use the above information to check for breaches in your system. If you think our team can help, feel free to reach out to us at nttin.support@global.ntt.