HC3: Threat Actor Profile

August 20, 2024 TLP:CLEAR Report: 202408201700

Threat Actor Profile: Everest Ransomware Group

Executive Summary

The Everest ransomware group has been active since 2020, and has engaged in data extortion and ransomware operations, along with initial access broker (IAB) activity. The group has increasingly targeted the healthcare industry since 2021, and claimed responsibility for a recent incident impacting a surgical facility in the United States. The group leverages a variety of common publicly available tools in its attacks, and is known to obtain initial access via various remote access tools and methods. The ransomware strain was previously linked to a Russia-based ransomware operation.

Background

The Everest ransomware group has been around since at least December 2020, and has gone through multiple iterations as a group. The group has targeted organizations across various industries and regions, with some high profile victims including NASA and the Brazilian government. The group originally focused on data exfiltration, before shifting to ransomware operations. In May 2021, the Everest data leak site (DLS) became unreachable following a high profile ransomware attack against the U.S. fuel transport company Colonial Pipeline. The group has then increasingly specialized as an Initial Access Broker (IAB) in 2023. Everest was first observed acting as an IAB as far back as November 2021. The ransomware strain has previously been linked to the EverBe 2.0 family and, based on more recent analysis of its ransomware, researchers have also linked Everest to the Russia-based ransomware group BlackByte.

In October 2023, open source reports indicated that threat actors associated with Everest ransomware and extortion operations were seeking to offer corporate insiders cash payments in return for remote access. Mandiant has previously observed the actor Everest and/or actors associated with Everest extortion operations seeking accesses to organizations' networks. In a previous advertisement on the Everest data leak site (DLS), they stated they were looking for access to corporate networks of organizations based in the United States, Canada, and Europe. The advertisement included a broad list of access types that the group is interested in, such as shell, vnc, hvnc, RDP with VPN, or via various remote access software tools. It should be noted that these types of accesses are commonly purchased and/or obtained from other malicious actors that conduct initial access operations into corporate networks, and do not necessarily indicate that Everest actors are leveraging and/or explicitly seeking out corporate insiders.

Technical Details

For lateral movement, the group uses legitimate compromised user accounts and Remote Desktop Protocol (RDP) to move laterally across networks. By exploiting weak or stolen credentials, they can access multiple systems within a target organization. Everest utilizes tools like `ProcDump` to create copies of the LSASS process, allowing them to extract additional credentials. They also create copies of the NTDS database, containing valuable Active Directory data. To avoid detection, Everest routinely removes tools, reconnaissance output files, and data collection archives from compromised hosts. This helps to cover their tracks and maintain persistence within the network. Upon compromising a new host, Everest conducts network discovery using tools such as `netscan.exe`, `netscanpack.exe`, and `SoftPerfect Network Scanner`. These tools enable the group to identify further targets within the network and plan subsequent stages of the attack. The group installs `WinRAR` on file servers to archive data for exfiltration. This archived data is then transferred out of the network for ransom or sale. Everest

primarily uses Cobalt Strike for command and control (C2) communications. They execute `Cobalt Strike beacons` on compromised hosts through `PowerShell` commands and also deploy secondary C2 methods using remote access tools like `AnyDesk`, `Splashtop Remote Desktop`, and `Atera`. Data exfiltration is conducted using the file transfer capabilities of tools like Splashtop. This ensures that sensitive information is moved out of the network before encryption or other malicious activities are initiated. Data is encrypted using the AES and DES algorithms while encrypted files are renamed with the ".EVEREST" file extension. Ransom demand messages are usually displayed as a pop-up window or a text file that appears on the desktop or in folders containing encrypted files. There is currently no public decryptor available for Everest ransomware.

Leveraged Tools

See **Table 1** for publicly available tools and applications used by Black Basta affiliates. This includes legitimate tools repurposed for their operations. **Disclaimer**: Use of these tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

Table 1: Tools Used by Everest Affiliates

Tool Name	Description
ProcDump	A legitimate Microsoft Sysinternals tool that is commonly used to dump the contents of Local Security Authority Subsystem Service, LSASS.exe.
netscan.exe	Tool used for network discovery.
netscanpack.exe	Tool used for network discovery.
SoftPerfect	A network scanner (netscan.exe) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
WinRAR	A popular archiving tool that supports encryption.
Cobalt Strike	A penetration testing tool used by security professions to test the security of networks and systems. Everest affiliates have used it primarily for command and control (C2) communications.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
AnyDesk	A legitimate remote desktop application that provides remote control, file transfer, and VPN functionality.
Splashtop	Remote desktop software that allows remote access to devices for support, access, and collaboration.
Atera	A legitimate remote monitoring management (RMM) software tool.

Industry Targeting

In total, the Everest Ransomware Group has claimed 120 victims on its Data Leak Site (DLS) as of July 15, 2024, according to a trusted third party. The victims are primarily located in the United States (around 34% of victims) with the most targeted industries being construction and engineering, financial services, legal and professional services, healthcare, and government, respectively. The healthcare industry accounts for around 10% of all victims worldwide (see **Figure 1**), while around 27% of victims in the United

HC3: Threat Actor Profile

August 20, 2024 TLP:CLEAR Report: 202408201700

States alone are in the healthcare industry.

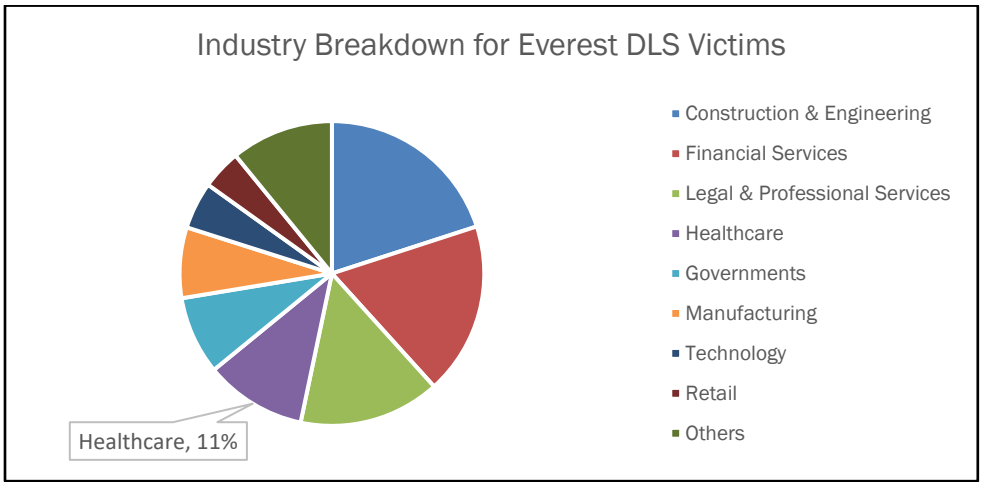

Figure 1. Global industry breakdown for victims listed on Everest Ransomware data leak site (DLS) as of July 15, 2024.

Impact to the Health Sector

There are nearly 20 historical incidents targeting the health sector associated with the Everest Ransomware Group from April 2021 to July 2024. The group has disproportionately targeted medical imaging providers in the United States. Most recently, the group claimed the compromise of a New York-based surgery center with a revenue of USD $17 million, in which the attackers claimed to possess more than 450 GB of data allegedly exfiltrated from the victim, including comprehensive details about the center's physicians and patients, encompassing personal and medical records. The attackers gave the victim 24 hours to initiate negotiations, threatening to disclose the data publicly if their demands are not met. While relatively low compared to other ransomware operations, the number of Everest ransomware incidents in the HPH sector has steadily trended upward since 2021, increasing by around one incident per year.

Mitigations

The following resources and guidance are provided by various elements of the federal government to assist the health sector in defending against, mitigating the effects of, and reporting ransomware attacks:

- DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
- FBI Cybercrime: https://www.fbi.gov/investigate/cyber
- FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
- FDA - Medical Device Security Information: https://www.fda.gov/medical-devices/digital-healthcenter-excellence/cybersecurity
- H-ISAC White Papers: https://h-isac.org/category/h-isac-blog/white-papers/
- 405(d) Resource Library: https://405d.hhs.gov/resources
- HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Furthermore, the FBI recommends the following steps:

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password-protect backup copies offline. Ensure copies of

critical data are not accessible for modification or deletion from the system where the data resides.

- Review Task Scheduler for unrecognized scheduled tasks. Additionally, manually review operating system-defined or system-recognized scheduled tasks for unrecognized "actions." (For example, review the steps each scheduled task is expected to perform.)
- Review anti-virus logs for indications that they were unexpectedly turned off.
- Implement network segmentation.
- Require administrator credentials to install software.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as updates/patches are released.
- Use multi-factor authentication where possible.
- Regularly change the passwords to network systems and accounts and avoid re-using passwords for different accounts.
- Implement the shortest acceptable timeframe for password changes.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a virtual private network (VPN).
- Consider adding an email banner to emails received from outside your organization.
- Disable hyperlinks in received emails.

Indicators of Compromise (IOCs)

Indicator	Type	Description
netscan.exe	File name	SoftPerfect Network Scanner
netscanpack.exe	File name	This was unable to be analyzed during the investigation.
svcdsl.exe	File name	SoftPerfect Network Scanner Portable
Winrar.exe	File name	Popular archiving tool, which supports encryption.
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

HC3: Threat Actor Profile

August 20, 2024 TLP:CLEAR Report: 202408201700

MITRE ATT&CK Tactics & Techniques

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 utilized PowerShell to execute malicious commands.
Execution	Command and Scripting Interpreter: Windows Command Shell	T1059.003	Threat actor utilized Windows Command Shell to execute malicious commands.
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	Lateral movement was observed utilizing 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.
Defense Evasion	Indicator Removal on Host: File deletion	T1070.004	Threat actor routinely deleted tooling and output.
Discovery	Network Service Discovery	T1046	Threat actor utilized 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 utilized 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.

Relevant HC3 Products

- June 18, 2024 – Qilin/Agenda Ransomware Threat Profile
- January 18, 2024 - Ransomware & Healthcare

References

SOCRadar. “Dark Web Profile: Everest Ransomware.” May 22, 2024. https://socradar.io/dark-web-profile-everest-ransomware/

GoldSparrow. “Everbe 2.0 Ransomware.” EnigmaSoft. https://www.enigmasoftware.com/everbe20ransomware-removal/

Jones, Connor. “Everest cybercriminals offer corporate insiders cold, hard cash for remote access.” The Register. October 12, 2023.
https://www.theregister.com/2023/10/12/everest_courting_corporate_insiders/

Searchlight Cyber. “Everest Ransomware Group Increases Initial Access Broker Activity.” June 26, 2023.
https://www.slcyber.io/everest-ransomware-group-increases-initial-access-broker-activity/

Shekhar, Shashank. “Everest Ransomware Group Targets Gramercy Surgery Center, Threatens to Release 465 GB of Data.” CloudSEKNews. https://news.cloudsek.com/2024/07/everest-ransomware-group-targets-gramercy-surgery-center-threatens-to-release-465-gb-of-data/

Salvage Data. “Everest Ransomware: Complete Guide.” October 4, 2023.
https://www.salvagedata.com/everest-ransomware/

Meskauskas, Tomas. “Everbe Ransomware.” November 29, 2021. PCRisk.
https://www.pcrisk.com/removal-guides/12790-everbe-ransomware

NCC Group. “Climbing Mount Everest: Black-Byte Bytes Back?” July 13, 2022.
https://www.nccgroup.com/us/research-blog/climbing-mount-everest-black-byte-bytes-back/

Satter, Rachel. “More ransomware websites disappear in aftermath of Colonial Pipeline hack.” Reuters. May 16, 2021. https://www.reuters.com/article/us-usa-products-colonial-pipeline-ransom/more-ransomware-websites-disappear-in-aftermath-of-colonial-pipeline-hack-idUSKCN2CX0KT/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback