



PROFILE

Everest Ransomware

ZEROFOX INTELLIGENCE

Classification: TLP - Amber

Intelligence Requirements: Threat Actors, Vulnerability

P-2022-03-23a

March 23, 2022



Created on: March 23, 2022

Intelligence Cut-off: 9:30 AM (EDT) on March 23, 2022

First Seen: 2020

Origin: Likely Russia

Aliases: Everest Locker

Motivation: Financial

Targeted Industries: Agriculture, Construction, Energy, Finance, Government, Healthcare, Legal, Manufacturing, Insurance, Retail, Packaging, Transportation, Wholesale

Targeted Nations: Argentina, Brazil, Canada, Finland, France, Italy, Portugal, United Kingdom, United States

Background

Everest is a Russian-language ransomware collective that has historically targeted organizations by encrypting and exfiltrating data to be used in ransom demands or to sell to third parties. Everest is believed to have been developed from the Everbe ransomware strain—active between late 2018 to 2020—which has also included Embrace, EvilLocker, Hyena Locker, and PainLocker. However, it is not clear if Everest is a rebrand or just utilizes similar code and tactics. Everest, in its current guise, was identified as early as 2020 but raised its profile significantly in June 2021 after conducting a series of attacks against French companies across multiple industries.¹ This was followed by an uptick in activity with an expanded scope of targets. Everest claims that it has breached several organizations and entities globally towards the end of 2021 and into early 2022, including departments of the UK and U.S. governments. ZeroFox has been unable to confirm the veracity of some of Everest's claims.

Infrastructure

Everest hosts its own data leak site on the dark web where it publicly lists new and claimed data breaches. The leak site is used to record each victim individually and describe the information that can be found within the stolen data, such as root access to servers, employee credentials, and access to the victim's VPN. In some cases, the listings include a sample screenshot, which is likely an attempt to substantiate Everest's offerings.² However, screenshots are not provided for every breach listed on the site.

¹ <https://twitter.com/argevise/status/1407404581395570688?s=20&t=t8KBjJPCS7qxfw2lIm9aSQ>

²

https://www-redhotcyber-com.translate.goog/post/l-italiana-speroni-s-p-a-colpita-dal-ransomware-everest/?_x_tr_sl=it&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc



ZeroFox has also observed Everest using the Sonar Secure Messaging app to communicate with victims, as well as XSS—a Russian-speaking hacking forum used to share knowledge about exploits, vulnerabilities, malware, and network penetration. XSS appears to be used by Everest to provide updates to its services. For example, in February 2022, Everest members communicated that the group had experienced a purported distributed denial of service attack on its servers.³

Tactics, Techniques, and Procedures (TTPs)

Very little information has been publicly disclosed regarding the specific TTPs Everest leverages in intrusions. It is not known how initial compromise is achieved. ZeroFox assesses that extortion collectives of this nature are most likely to leverage phishing campaigns, stolen or weak credentials, and vulnerability exploits within public-facing applications.

Although Everest and its familial strains have historically leveraged AES or DES encryption to lock victims' files, ZeroFox has been unable to verify that operators continue to encrypt files. An October 2021 attack on Italian copyright agency SIAE reportedly involved a ransom of EUR 3 million in Bitcoin.⁴ However, the group may be leveraging “hack-and-leak” tactics—a growing trend among extortion outfits—where non-encrypted data exfiltration occurs and is then released or sold to the public. This can be seen in the approach Everest has taken in its operations since late 2021, whereby it looks to leverage its leak site to monetize stolen data without relying on a ransom payment to be fulfilled. Instead of continuing to pursue unpaid ransoms, the group attempts to sell data and third-party access to a victim's network on the Everest data leak site or via forums.



Search

Everest ransom team



Menu

Società Italiana degli Autori ed Editori

This is customer data, financial documents and other very important documents

A huge number of passports, driver's licenses, payment documents, bank accounts, credit cards and other user data

The company did not make a deal. Price of all data 500000 \$.

Representatives of celebrities, you can contact me and redeem all the data. One-hand sale, after the sale the data is deleted.

SIAE data listed for sale after ransom demand is unfulfilled

Source: Everest data leak site

³ <https://twitter.com/Cyberknow20/status/1498414656524013568>

⁴ <https://www.punto-informatico.it/siae-conferma-furto-numerosi-dati/>



Everest has also previously adopted Black Friday sales logic on its site, offering discounts on exfiltrated data and access to victim networks. This is the first instance of this strategy that ZeroFox has observed from a ransomware group; we assess that Everest aims to position itself as an established access broker. ZeroFox has identified no evidence to suggest Everest's most recent tactics have been successful. However, we assess its overall approach to extortion could be leveraged more frequently by other like-minded groups, as it increases the chances of making profits from exfiltrated data by selling to interested third parties and reduces the reliance on solely receiving ransoms from potential victims.

Black Friday has arrived

Argentina GOV Government access in sale. Access to a variety of services inranet. Database access included with full editing. Including vpn, mysql server and various services. The database is very extensive, includes users A large organization, the documents contain various financial statements.Price 30k\$ MINISTRY OF ECONOMY AND FINANCE Peru Financial documents are present. Vpn includingPrice [...]

Black Friday advertising

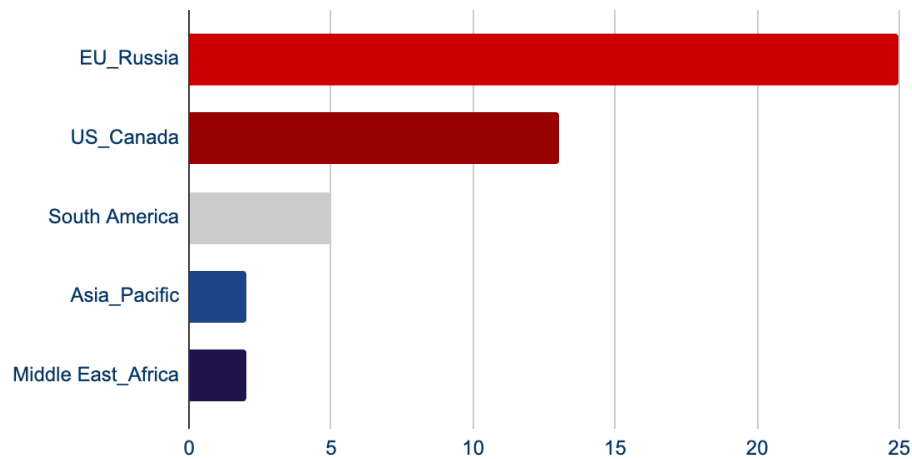
Source: Everest data leak site

ZeroFox data indicates that Everest has directed most of its attacks towards manufacturing, construction, legal, and financial industries across multiple regions in the last year. Everest has also shown a particular interest in targeting government organizations and claims to have network and server accesses for various departments in Argentina, Brazil, Peru, the United Kingdom, and the United States. While Everest has demonstrated capability through previous attacks, ZeroFox has identified no evidence that confirms the majority of its claims and assesses some are likely to be made in an attempt to capture attention and build reputation.



Everest attacks by region

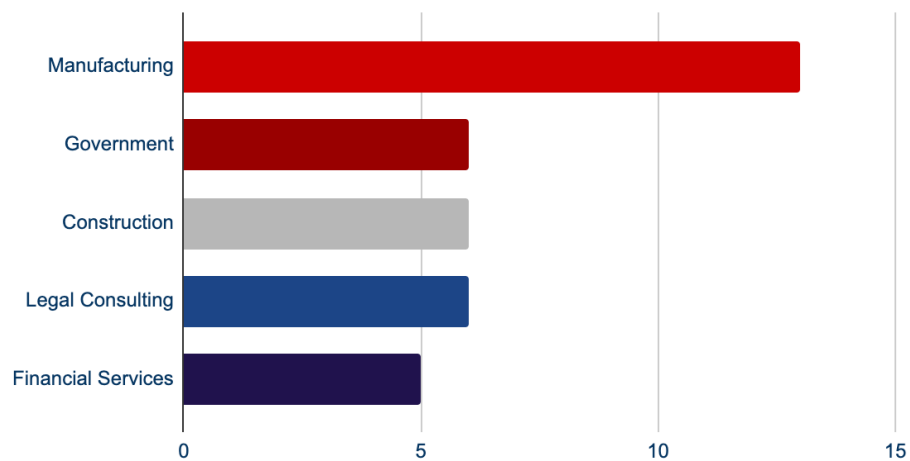
Top five between May 2021 - Present



Source: ZeroFox

Everest attacks by industry

Top five between May 2021 - Present



Source: ZeroFox



State-owned company for generating, transmitting and distributing electricity.

Root access to many servers linux. Databases, backups, employee access to the administration of POS terminals and much more. Multiple settings and developments. You can become the king of electricity the whole country. The largest defense electronic equipment company appears in files and accesses
Price 250k\$

USA GOV

Root access to multiple servers. AD
A lot of confidential information, employee and customer data

Ministry of Economy of Peru

Access to 600 pc. A lot of confidential documents, pst files of employees

Argentina GOV

Root access Mysql,phpmyadmin

France EDU

Employee Access

UK GOV

Access to multiple servers with employee data. A large amount of confidential information. This company is directly related to the country's economy

Claimed access to various government networks and servers

Source: Everest data leak site

Recommendations

- Critical data should be backed up regularly, including password-protected backup copies kept offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, or the cloud).
- Ensure proper network segmentation.
- Never download email attachments from unknown senders or click links from untrusted sources. Provide user-training programs to fight against phishing or social engineering attacks used to obtain critical information that can lead to attacks.
- Enable multi-factor authentication wherever possible.
- Patch disclosed vulnerabilities with updated software versions as quickly as practical.
- Disable PowerShell wherever possible to limit the possibility of operators employing lateral movement modules.



Appendix: Traffic-Light Protocol for Information Dissemination

Color	When Should It Be Used?	How May It Be Shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.