SEARCHLIGHT CYBER

RANSOMWARE SPOTLIGHT

EVEREST GROUP FOCUSES ON INITIAL ACCESS BROKERAGE

BACKGROUND ON THE EVEREST GROUP

Everest was originally a data exfiltration group, before becoming a ransomware operator, and now increasingly specializing as an initial access broker (IAB) - which is the focus of this report.

It targets organizations across a number of industries and regions but with a particular concentration in the Americas (**Figure 1**) and focused on capital goods, health, and public sector (**Figure 2**).

Its ransomware strain was historically linked to the EverBe 2.0 family and, based on more recent analysis of its ransomware, researchers have also linked Everest to the ransomware group BlackByte.

FIRST ACTIVE

December 2020

TOTAL LISTED VICTIMS

Total number of victims on its leak site: 92

KNOWN FORUM ALIASES

Everest (XSS)
Everest (BreachForums)

NOTABLE VICTIMS

Dates reflect when the victims were listed on the Everest leak site:

- AT&T (October 2022)
- Ministerio de Economía Argentina (September 2022)
- Speroni (July 2022)
- Ministry of Economy and Finance Peru (December 2021)
- Brazil Police (November 2021)

DARK WEB PRESENCE

Like many ransomware groups, Everest uses a dark web leak site hosted on Tor to post about its victims. For Everest, this serves a dual purpose of extorting the victim and also advertising its attacks to potential buyers - especially in the case of its data exfiltration and IAB posts.

Everest is also active on dark web hacking forums. For example an actor using the Everest handle joined the XSS cybercrime forum Feb. 2, 2021 and, according to their profile information, they have made 65 posts, mostly advertising their dark web leak blog (**Figure 3**). The actor has also been observed leaking files and data from impacted entities via several forum threads. Everest has accrued a reputation score of 48 points on XSS, with a total of 50 positive reactions and two negative reactions. Some of the positive reactions were obtained from highly reputable forum members such as the threat actor Vespiar, a notorious seller of compromised data and access, and from DataFor, a respected threat actor engaging in leaking stolen data. Everest's profile also revealed one completed Escrow deal, indicating that it successfully sold at least one of its products.

Everest generally uses the Russian language on XSS but the English language was also used on some occasions. During a private conversation with our source on the XSS cybercrime forum, the actor appeared to be exclusively financially motivated and communicated in English. The actor was happy to provide screenshots as proof of access to one of the impacted entities, but heavily sanitized the images and claimed that without a large forum deposit, sensitive information would not be revealed. The actor insisted on using an Escrow service when dealing, increasing the credibility of their claims. Furthermore, during the engagement, we were able to confirm that the actor behind the XSS cybercrime handle was the same as the operator from the Everest dark web blog, therefore suspicion of an impersonation attempt was eliminated.

Starting in May 2022, the actor was also observed using the Everest handle on the now defunct BreachForums. The actor used the English language for communication on BreachForums. According to the information captured from the forum, the actor had an "M.V.P" status and authored 273 posts and opened 28 threads. The actor's last known reputation score was 98.

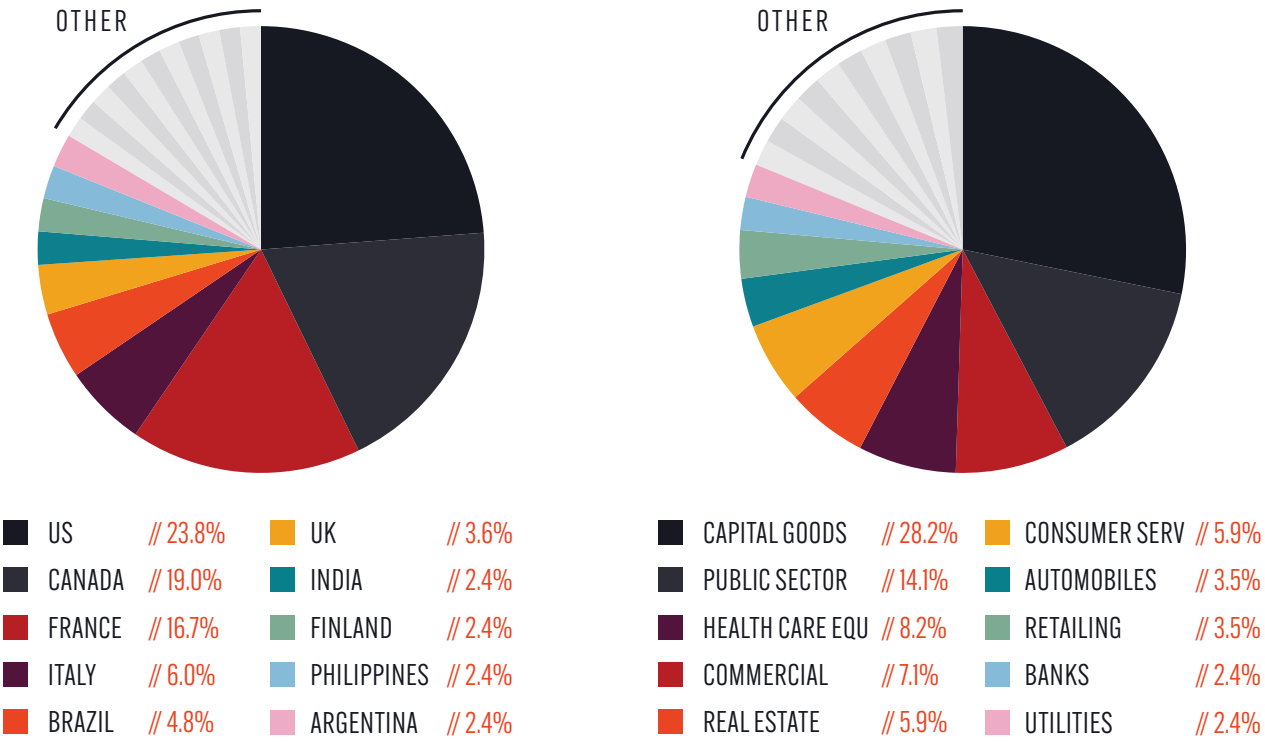


FIGURE 1: VICTIMS POSTED ON EVEREST'S DARK WEB LEAK SITE BY GEOGRAPHY.

FIGURE 2: VICTIMS POSTED ON EVEREST'S DARK WEB LEAK SITE BY SECTOR

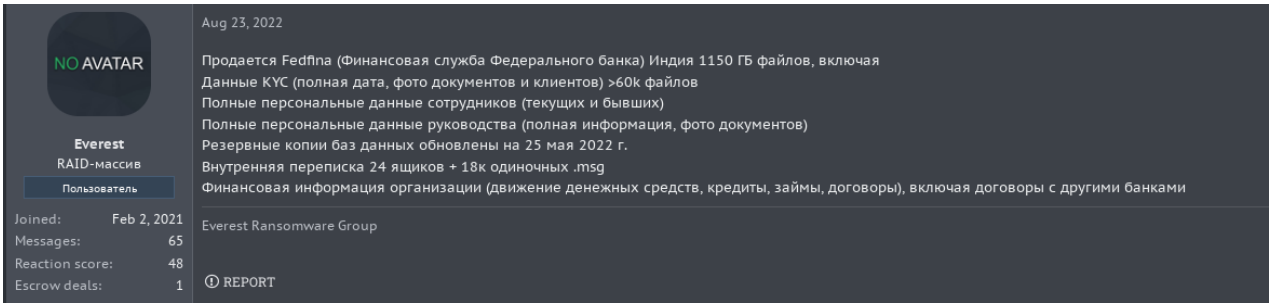


FIGURE 3: AN EVEREST POST ON THE DARK WEB FORUM XSS.

SUMMARY OF SEARCHLIGHT CYBER FINDINGS

- Searchlight Cyber researchers have observed that the Everest group has increased its output as an Initial Access Broker (IAB). This IAB activity, first observed by researchers in November 2021, is extremely rare among ransomware groups.
- Everest frequently deletes its access advertisements from its leak site, which could misrepresent how frequently it is acting as an IAB.
- By capturing deleted posts in our dark web investigation platform, Cerberus, our analysts have observed a marked increase in IAB activity.
- There are several reasons why Everest group may have moved towards being an IAB, including trying to keep a low profile from law enforcement, a loss of personnel, or as a different monetization tactic.

INITIAL ACCESS BROKER VS RANSOMWARE OPERATOR

The Everest ransomware group is unusual in using its dark web leak site to sell initial access to organizations, as well as for the more "traditional" use of extorting ransomware victims. Consequently, the threat group can be classed as an Initial Access Broker (IAB) as well as a ransomware operator.

This IAB activity was observed by NCC Group researchers as far back as November 2021. Perhaps the most notorious instance of Everest selling initial access was the October 2022 listing of the multinational telecommunications company AT&T (see **Figure 4**).

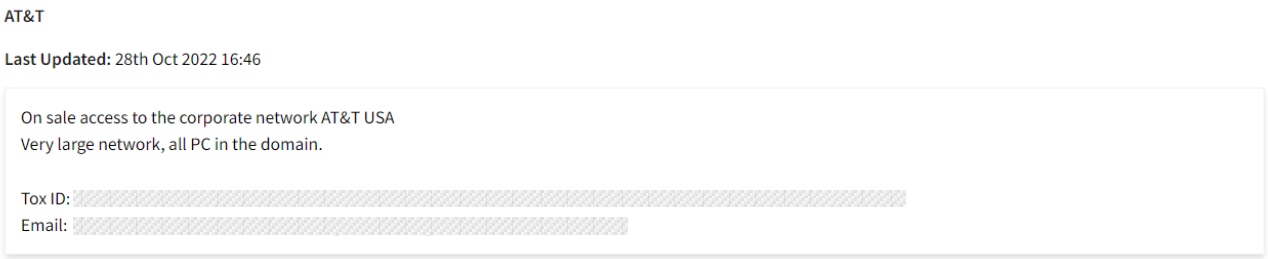


FIGURE 4: THE TEXT OF EVEREST'S AT&T LISTING, DISPLAYED THROUGH SEARCHLIGHT CYBER'S DARK WEB INTELLIGENCE PLATFORM CERBERUS.

Searchlight Cyber researchers have observed that the group has increased the proportion of its attacks as an IAB, recently publishing more IAB posts than extortion posts. (**Figures 5 & 6**).[1]

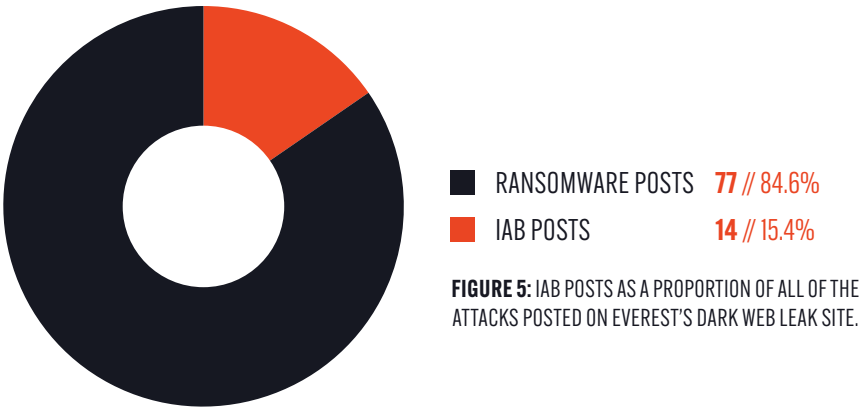


FIGURE 5: IAB POSTS AS A PROPORTION OF ALL OF THE ATTACKS POSTED ON EVEREST'S DARK WEB LEAK SITE.

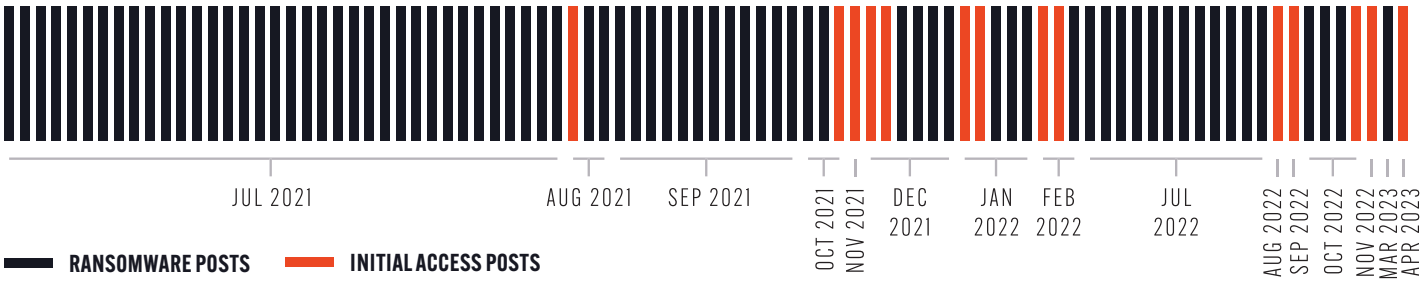


FIGURE 6: A TIMELINE OF EVEREST'S DARK WEB LEAK SITE POSTS, WITH INITIAL ACCESS POSTS INDICATED IN ORANGE, DEMONSTRATING INCREASED FREQUENCY OVER THE PAST 18 MONTHS.

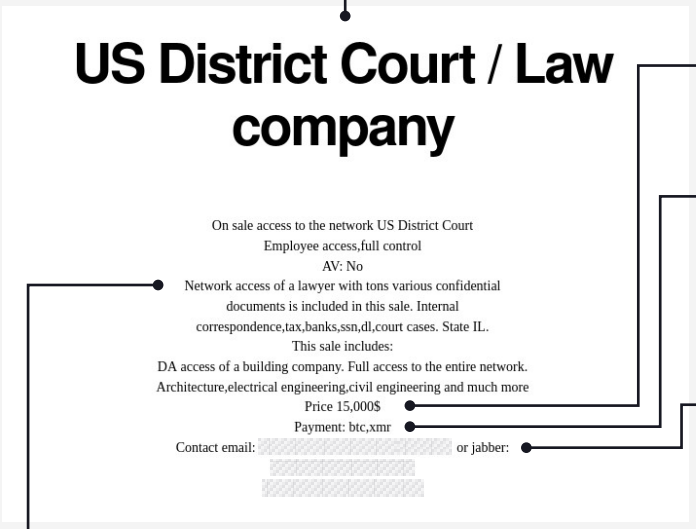
[1] The authors note that Everest often duplicates posts on its dark web leak site, posting the same victim more than once. In particular, there are multiple instances of IAB posts being reposted over time. We have removed those duplicate reposts from the data used in these graphs for the sake of accuracy.

EXAMPLE: US DISTRICT COURT

Figure 7 shows the homepage of the Everest group's dark web leak site, which features the initial auction post for its latest victim: an unnamed US District Court. It is worth noting some details:

THE VICTIM IS NOT NAMED IN THIS CASE

Which indicates that they may not want to alert the victim that they have been compromised. However, in other cases (such as AT&T in Figure 4) the victim is named.



THE PRICE

$15,000 is significantly less than a ransomware group typically extorts from a victim. However, this is higher than comparative access we observe being auctioned on hacking forums such as Exploit.

CRYPTOCURRENCY PAYMENT

Payment is accepted in the cryptocurrencies Bitcoin (btc) or Monero (xmr).

CONTACT DETAILS

Everest provides a contact email address and Jabber instant messengers addresses, which we have redacted.

THE POTENTIAL "BOUNTY"

The advertisement promises "various confidential documents", "full access to the network", and "DA access of a building company" - which refers to "Domain Admin", the highest level of administrative privileges within a Windows Active Directory domain. The group also provides ample documents as proof of access, including files from court cases, scans of identification cards and driving licenses, a screenshot of files on the network, and a screenshot of the remote gateway that has been established (**Figure 8**):

FIGURE 7: A RECENT INITIAL ACCESS POST ON EVEREST'S DARK WEB LEAK SITE.

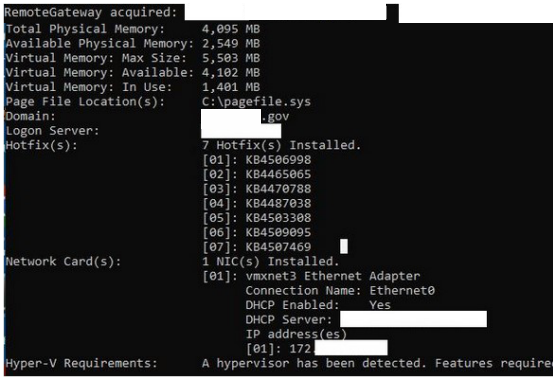


FIGURE 8: A SCREENSHOT SHARED BY EVEREST OF THE REMOTE GATEWAY THAT HAS BEEN ESTABLISHED INTO THE VICTIM NETWORK.

DELETED POSTS

Another noteworthy aspect is that Everest has been observed to remove IAB posts, so if you visit its dark web leak site it is not apparent that it has undertaken this activity. Our dark web investigations platform Cerberus archives the text from dark web sites, even if the posts are deleted, which means we have the collection to demonstrate the frequency of this activity (see examples in **Figure 9**).

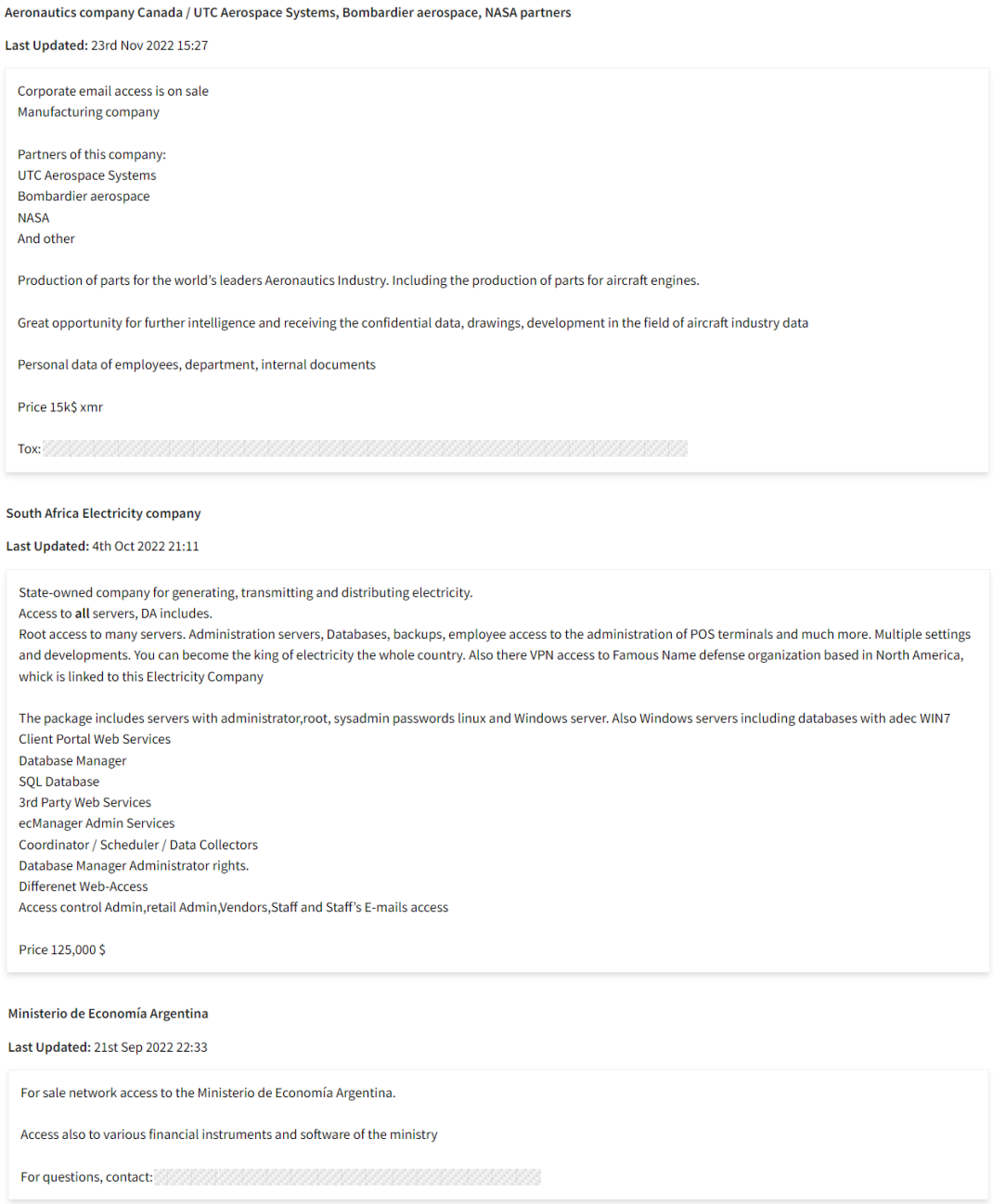


FIGURE 9: EXAMPLES OF INITIAL ACCESS POSTS THAT THE EVEREST GROUP HAS PUBLISHED AND SUBSEQUENTLY DELETED FROM ITS DARK WEB LEAK SITE. POST DISPLAYED THROUGH THE CERBERUS DARK WEB INTELLIGENCE PLATFORM.

It is not clear why the initial access posts are being deleted but there are four possible hypotheses:

1. The initial access has been sold.
2. The victim paid a ransom to have the post taken down.
3. The group couldn't sell the access.
4. The victim discovered the intrusion and remediated the access before it could be sold.

WHY IS EVEREST ACTING AS AN INITIAL ACCESS BROKER?

It is not possible to assert with any confidence exactly why Everest is acting as an IAB. All we can provide are hypotheses to explain this activity, which could frame further research by the cyber threat intelligence community into the group.

HYPOTHESIS 1: LOWER-RISK CYBERCRIMINAL ACTIVITY

It is possible that the Everest group is undertaking IAB in order to not attract too much "heat". Tackling ransomware is high-priority for international law enforcement, and many notable groups such as Conti, DarkSide, and BlackMatter have been forced to disband as a consequence of attracting too much attention with high-profile attacks. It is possible that the Everest group is taking on IAB between ransomware attacks as a comparatively low-risk activity. While the group doesn't make as much money as it could in a ransomware attack, as the examples in **Figure 9** show the group is charging thousands - and in some cases more than $100k - for access. So the group can maintain a profit while the risk of executing the attack is passed on to the purchaser.

HYPOTHESIS 2: A GAP IN THE MARKET

Another possibility is that law enforcement seizures of dark web hacking forums has created a gap in the market for initial access that has made it commercially advantageous for Everest to specialize as an IAB. For example, BreachForums, which was seized in March 2023, had been a popular forum for IAB auctions. Everest could potentially trade on its established reputation as a ransomware group to charge more for the access it provides.

HYPOTHESIS 3: TALENT ATTRITION

It is also a possibility that a change of personnel within the group has forced it to change its tactics from ransomware. For example, infighting within cybercriminal groups is common, and it is within the realms of possibility that the person involved in the encryption part of the ransomware attack has left, leaving less technical ability and skills to carry out full blown ransomware attacks. If the group members involved in initial access remain, that would explain why the group has mostly been undertaking IAB over the past few months.

HYPOTHESIS 4: "DOUBLE DIPPING"

There is some evidence to suggest that Everest is using IAB as an initial tactic for generating revenue from a victim, before moving onto other methods such as selling the stolen data.

For example, in October 2021 Everest published an IAB post on its leak site for the 'Ministry of Economy Peru' (**Figure 10**).

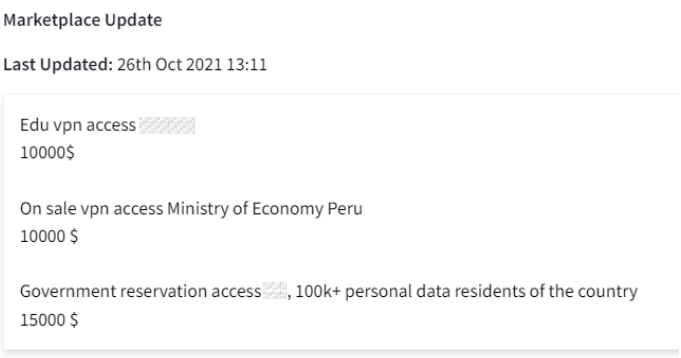


FIGURE 10: EVEREST ADVERTISE INITIAL ACCESS TO THE 'MINISTRY OF ECONOMY PERU' IN OCTOBER 2021. POST DISPLAYED THROUGH THE CERBERUS DARK WEB INTELLIGENCE PLATFORM.

Everest subsequently listed the same victim three times between December 2021, twice in posts that list a number of its victims (**Figure 11**) and once in its own post (**Figure 12**). However, in each of these three times it appears to be offering initial access and data:

FIGURE 11: EVEREST LISTS THE MINISTRY OF ECONOMY AND FINANCE PERU AMONG OTHER VICTIMS IN POSTS IN DECEMBER 2021 AND FEBRUARY 2021. POST DISPLAYED THROUGH THE CERBERUS DARK WEB INTELLIGENCE PLATFORM.

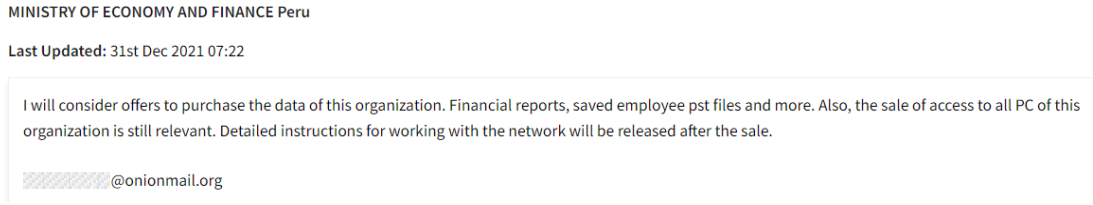


FIGURE 12: EVEREST PUBLISHES A NEW POST ON THE MINISTRY OF ECONOMY AND FINANCE PERU IN DECEMBER 2021, SAYING IT WILL "CONSIDER PURCHASE OF THE DATA" AS WELL AS "PC ACCESS". POST DISPLAYED THROUGH THE CERBERUS DARK WEB INTELLIGENCE PLATFORM.

Finally, in July 2022 Everest leaked the data it had stolen from the victim (**Figure 13**).

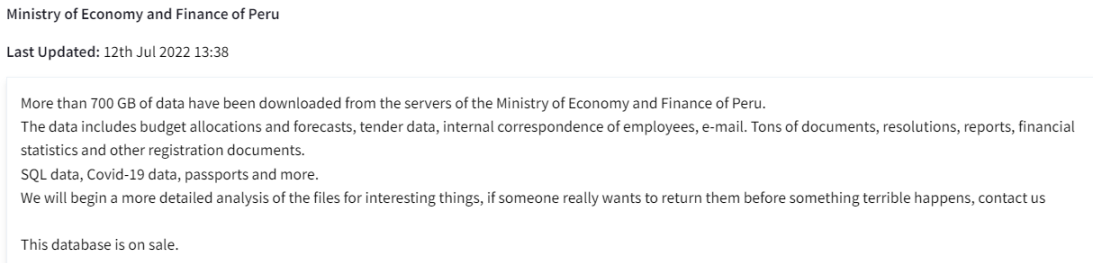


FIGURE 13: EVEREST GROUP LEAKS DATA FROM THE 'MINISTRY OF ECONOMY AND FINANCE OF PERU' IN JULY 2022. POST DISPLAYED THROUGH THE CERBERUS DARK WEB INTELLIGENCE PLATFORM.

This, and other examples of Everest posting data after failing to sell access, may indicate that Everest is using IAB as its "opening gambit" to monetize a victim. If it doesn't find a buyer, Everest then resorts to extracting and selling the data itself.

KEY TAKEAWAYS

Regardless of the group's motivation, the evidence from Everest's dark web leak site demonstrates that it is increasingly acting as an IAB for other criminals. It is important that cybersecurity professionals are aware of these types of changes in how ransomware groups and other threat actors operate to inform their threat models and proactively prepare their defenses based on intelligence on their adversaries.

As always, we publish these findings with the knowledge that dark web intelligence only makes up a part of the picture and call on the wider cybersecurity and threat intelligence community to collaborate with Searchlight Cyber to help us improve our collective understanding of the TTPs of ransomware groups like Everest.

APPENDIX: MITRE ATT&CK TACTICS, TECHNIQUES AND PROCEDURES (TTPS) OBSERVED FOR THE EVEREST GROUP

- Using a strain of the Everbe 2.0 ransomware family and the Black-Byte ransomware variant developed using the C# programming language. [T1486]
- Using compromised access credentials and remote desktop protocol (RDP). [T1133] [T1078] [T1021.001]
- Using the SoftPerfect Network Scanner network administration tool. [T1046]
- Using the ProcDump application monitoring tool to obtain the local authority subsystem service process (lsass.exe) allowing the exfiltration of access credentials. [T1003.001]
- Dumping the NT directory services (ntds.dit) file, the main Active Directory database. [T1003.003]
- Using the Cobalt Strike and Metasploit penetration testing tools as command and control (C2) mechanisms. [1071.001]
- Using WinRAR and Splashtop for collection and exfiltration of data. [T1041]
- Using Atera and AnyDesk as secondary C2 and persistence methods. [T1219]