Calling from the Underground: An alternative way to penetrate corporate networks

seqrite.com/blog/calling-from-the-underground-an-alternative-way-to-penetrate-corporate-networks

Sathwik Ram Prakki January 11, 2023

11 January 2023

Written by Sathwik Ram Prakki

Cybersecurity, Malware, Phishing

Estimated reading time: 5 minutes

Threat actors use multiple methods to distribute malware to infect specific targets. Even though various phishing methods are actively used and evolving, an alternative approach to increase their success rate is to call the target corporate companies. Techniques like BazaCall have been observed since 2021. In this technique, a call is made to the target to make them click on malicious links, leading them to install malware unknowingly.

Threat actors like affiliates of ransomware groups have started to utilize this technique to infect targets across the world. They recruit callers who work on phishing campaigns, called the “Callback phishing” technique. With the emergence of such methods, the search for so-called callers is also increasing. Additionally, new callers are making themselves available on the underground forums. The figure below illustrates an advertisement in one of the underground forums wherein the threat actor can be seen posting details of the “job” and inviting callers to join with a promise of revenue-sharing.

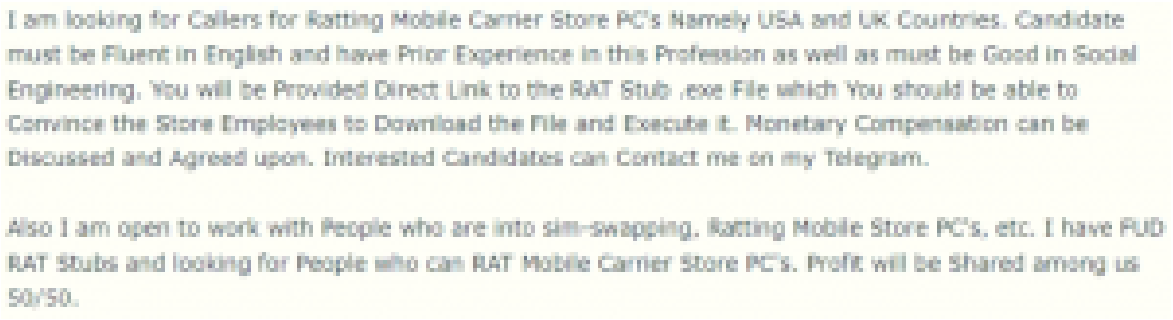


Fig. 1 – Threat actor in search of caller services

As evident from the above advertisement, RAT (Remote Administration Tool) stubs are provided to be installed specifically targeting carriers in the USA and UK.

A Caller's Perspective

Callers provide their services based on the target and are willing to call as many times as necessary to succeed in their mission. Most services offer English callers as the US and UK are the most targeted locations by cybercrime groups, and they work actively every week. They compel the victims to click on malicious links and install a malicious executable through social engineering and phishing.

Another technique explicitly used by these callers targeting various sectors is called Callback Phishing. They make phone calls through various SIM cards registered to different geographical locations. One such threat actor on telegram has multiple Russian SIM cards offering a higher success rate.

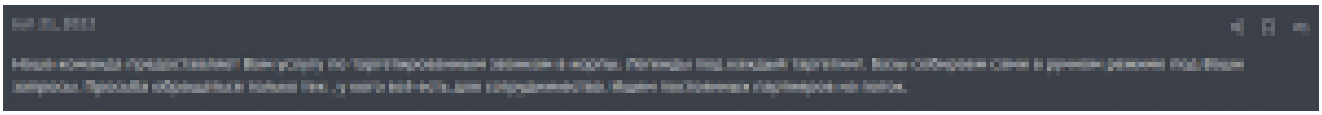
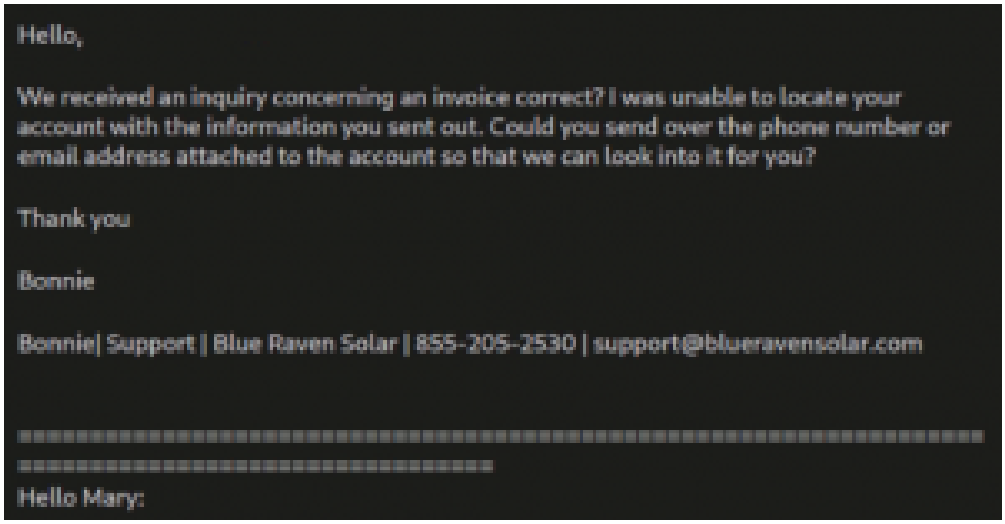


Fig. 2 – Threat actor offering caller services

Some of these callers don't send phishing links to individual targets but operate on bulk orders based on the database provided to them. They make these calls from toll-free numbers like 800 or 888 for more credibility rather than using suspicious SIMs that might get blocked. The threat actors demand a premium price, the lowest being a thousand dollars that includes these toll-free numbers and a connection fee. A big chunk of the money goes as salaries to the operators who sit and call for "long and efficient" communication to make the target install the malicious payloads or click the phishing links that redirect to them.

An Affiliate's Perspective

The threat actors on the forums eagerly seek to hire callers to encrypt the victim's network. We have observed ransomware affiliates, working with Hive and Quantum, target companies in the manufacturing and legal sectors in the USA and Canada with more than $10M in revenue. Manufacturing being the most attacked sector doesn't come as a surprise. However, targeting the legal industry is not regular, indicating that threat actors will also pivot their victims based on their financial motives and geopolitical interests.


Hello,

We received an inquiry concerning an invoice correct? I was unable to locate your account with the information you sent out. Could you send over the phone number or email address attached to the account so that we can look into it for you?

Thank you

Bonnie

Bonnie| Support | Blue Raven Solar | 855-205-2530 | support@blueravensolar.com

Hello Mary:

Fig. 3 – Spam Mail to fetch phone details

These affiliates agree on a percentage of the ransom amount and provide a salary based on a long-term partnership. Sometimes even spam email formats are provided to get the target's name, contact number, email, and property address, where it imitates people from various companies such as Blue Raven Solar, and Zillow home loans, among others, to lure them. Once the target falls for the scam and provides these details, the callers start engaging conversations where they convince the victims to install payloads provided by these affiliates.

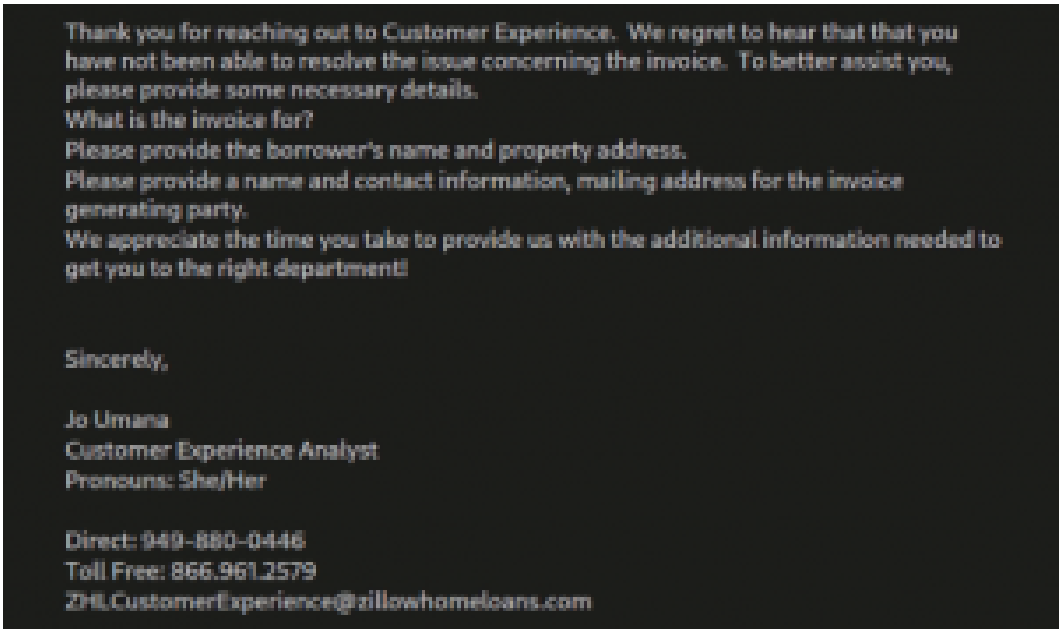


Fig. 4 – Spam Mail to fetch personal details

Instead of sending documents that contain malicious links, the affiliates provide ISO files as attachments, carrying the actual ransomware payloads in an encrypted format that can bypass detections. In some cases, the affiliates do not get the ISO files to distribute them seamlessly. Instead, they get the encrypted ransomware payloads converted to ISO format using a separate set of coders.

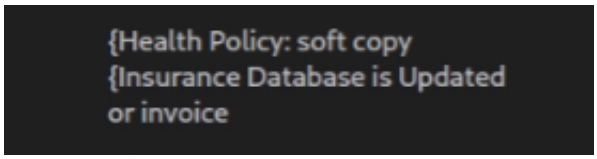


Fig. 5 – Spam Mail randomization (1)

Spammers demand at least 100,000 emails be sent out in bulk to work for a long-term partnership that gives options to randomize the email format, as shown below, where most of them are related to insurance data to lure the targets easily.

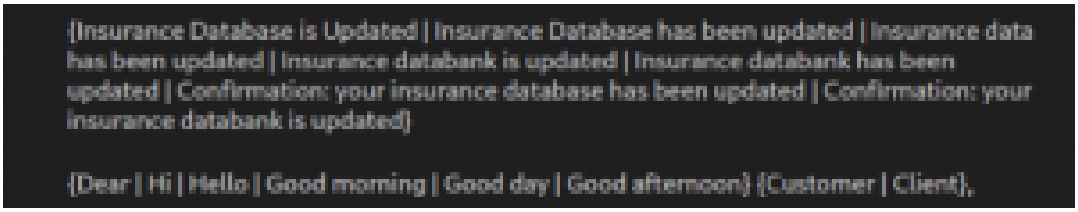


Fig. 6 – Spam Mail randomization (2)

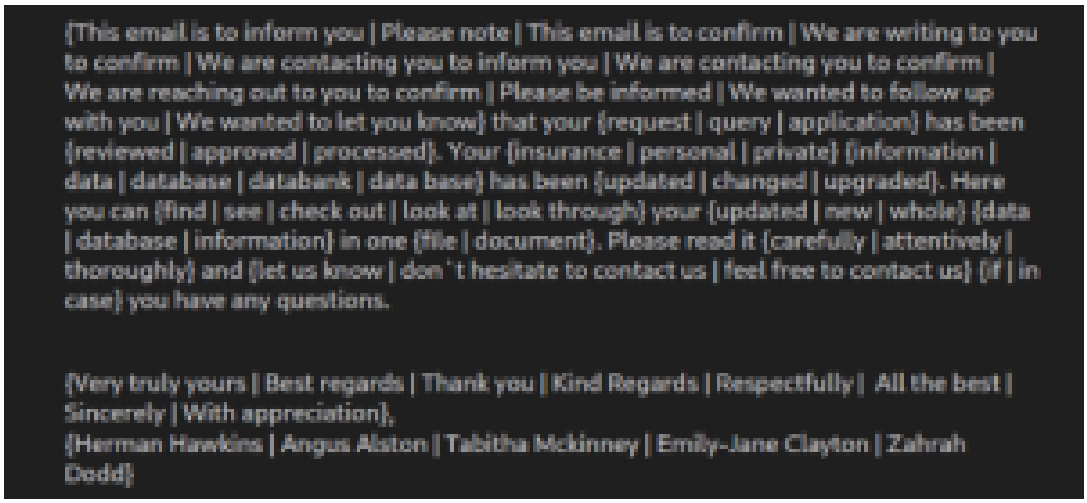


Fig. 7 – Spam Mail randomization (3)

Recent Campaigns

The recent BazarCall campaign, utilized by new groups that rose from Conti, sends out emails with phone numbers that read that the target has subscribed to a service with auto-renewal. As the victims contact the provided number to cancel the subscription, the operators convince them to allow remote access to their devices. While the conversation continues, a network operator sneaks into the target's network to fetch initial access to the device to maintain a remote session later used to install a backdoor. Malware such as BazaarLoader, Trickbot, and IcedID was delivered as BazarCall's tactics evolved that primarily target the US, Canada, and some Asian countries.

Threat actors are not only looking for English callers but other spoken languages like Spanish, Italian, German, and Norwegian, too, so that they can expand their targets.

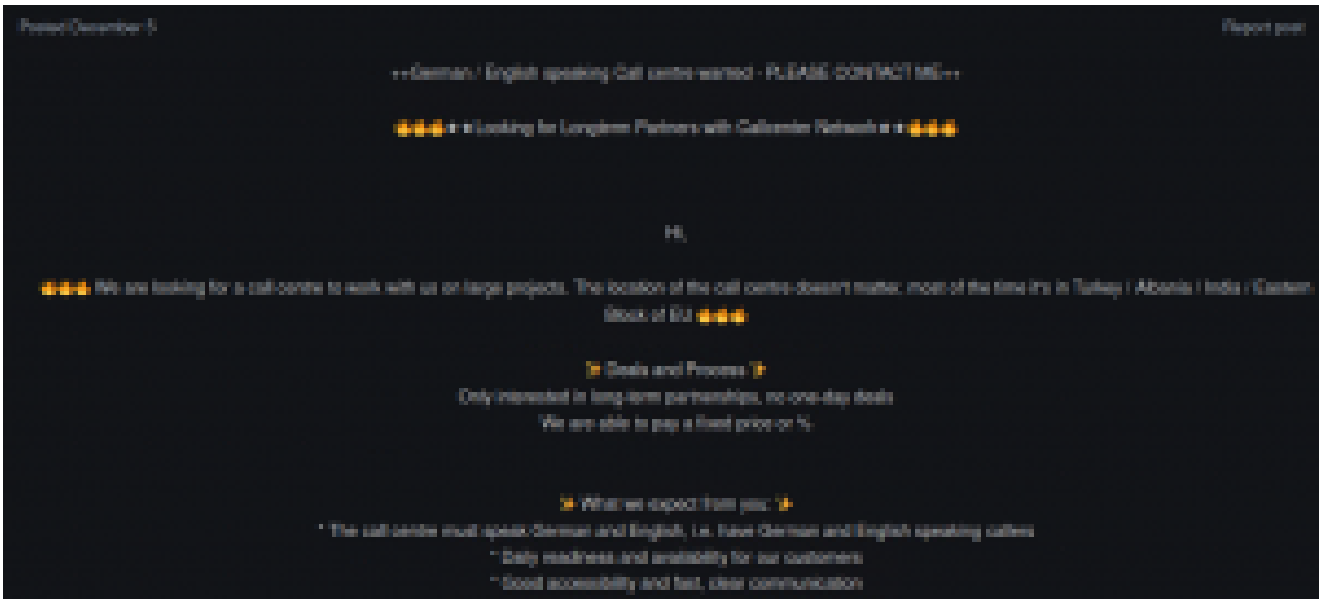


Fig. 8 – Job search for callers

Conclusion

Corporate companies should be aware that threat actors are using caller services as a new way to infect their systems with payloads such as ransomware and other types of malware. These services provide multi-language operators who work with email spammers to spread malicious links. To protect against such attacks, it is crucial to take caution when receiving suspicious or unknown emails with URLs or attachments and to avoid clicking or opening them.

Sathwik Ram Prakki is working as a Security Researcher in Security Labs at Quick Heal. His focus areas are Threat Intelligence, Threat Hunting, and writing about...

Articles by Sathwik Ram Prakki »

No Comments

Leave a Reply.Your email address will not be published.