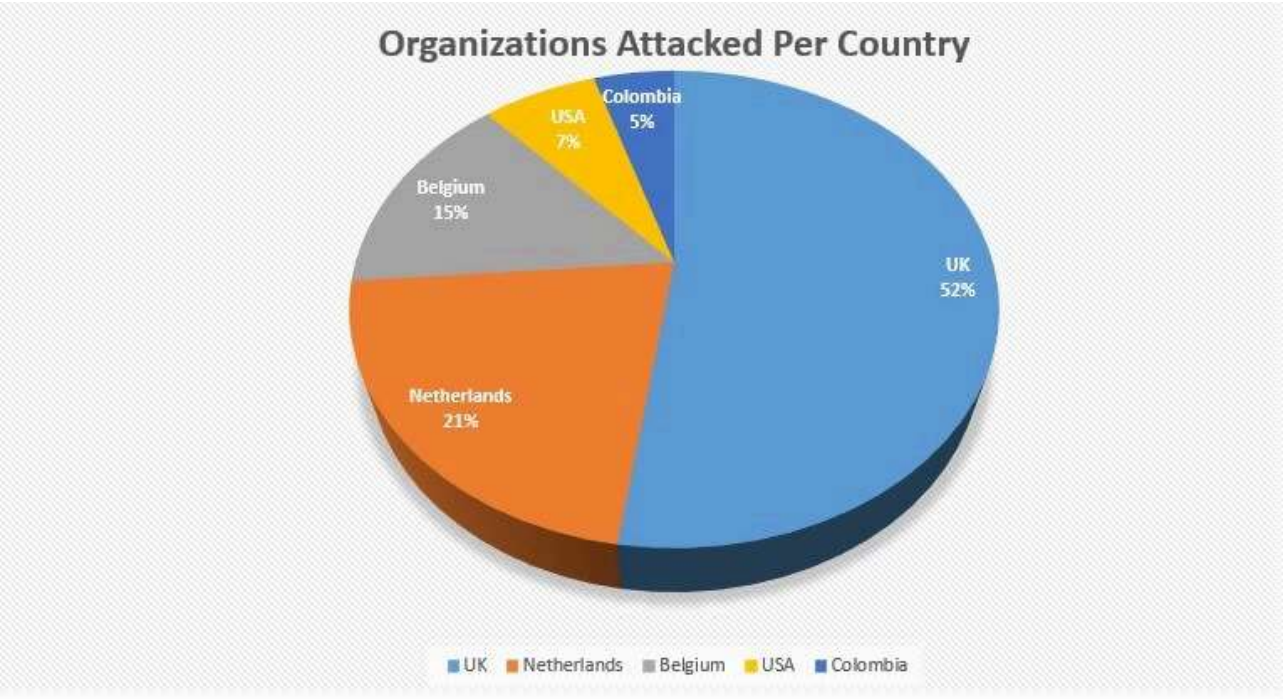
Who's Calling? Gaza and West-Bank Hackers Exploit and Monetize Corporate VoIP Phone System Vulnerability Internationally

By **Check Point Research Team**

- ***Hackers have targeted Sangoma and Asterisk VoIP phone systems at nearly 1,200 organizations worldwide in past 12 months***
- ***Main purpose of hacking campaign is to sell phone numbers, call plans, and live access to compromised VoIP services.***
- ***Losses from global telecoms fraud exceed 28 Billion USD, according to CFCA (Communications fraud control association), with VoIP PBX hacking being one of the top 5 fraud methods used.***
- ***Asterisk is one of the most popular VoIP PBX systems, used by many Fortune 500 companies for their telecommunications.***

Background

Recently, Check Point Research encountered a series of worldwide attacks targeting to VoIP (Voice over Internet Protocol), specifically Session Initiation Protocol (SIP) servers globally. Based on information provided by ThreatCloud, Check Point's threat intelligence engine, researchers found systematic exploitation of SIP servers from different manufactures. Further investigation revealed that this exploitation is part of a large, profitable business model run by hackers which has targeted the corporate VoIP phone systems at nearly 1,200 organizations worldwide over the past 12 months.



During our research, we discovered a new campaign targeting Sangoma PBX, an open-source, web GUI that manages Asterisk. Asterisk is the world's most popular VoIP phone system for businesses used by many Fortune 500 companies for their national and international telecommunications. The attack exploits CVE-2019-19006, a critical vulnerability in Sangoma PBX, which grants the attacker admin access to the system and gives them control over its functions.

Throughout the first half of 2020, we observed numerous attack attempts worldwide. We were able to expose the attacker's entire attack flow, from the initial exploitation of the CVE-2019-19006 flaw which grants administrator rights to the Sangoma VoIP phone system, to uploading encoded PHP files and to leveraging the compromised system.

Hacking the SIP servers which run the VoIP phone system and gaining control of them allows hackers to abuse them in several ways. One of the more complex and interesting hacking methods being used involves abusing the servers to make outgoing phone calls without the company that owns the VoIP system being aware – for example to premium-rate phone numbers set up by the hackers to earn revenues at the company's expense. Because making calls is a legitimate use of the corporate phone system, it is hard to detect when a server is being exploited.

While investigating the exploitations, researchers identified several online profiles associated with private Facebook groups that deal with VoIP, and more specifically, SIP server exploitation. After close

examination of the admins, active users and carriers seen in the Facebook groups, we found that most of them were located in Gaza, the West Bank and Egypt.

How the hackers dial up profits

Our research indicates that the group's main purpose is to sell phone numbers, call plans, and live access to compromised VoIP services from targeted organizations to the highest bidders, who can then exploit those services for their own purposes.

Unrestricted access to a company's telephone system can allow the attackers to make calls using the compromised company's resources and eavesdrop on legitimate calls. They can also use the compromised systems for further attacks, such as using the system resources for cryptomining, spreading laterally across the company network, or launching attacks on outside targets, while masquerading as representatives from the compromised company.

A common practice associated with these attacks, known as International Revenue Share fraud (IRSF), enables attackers to inflate traffic by calling the premium rate numbers they own from the hacked VoIP phone system. The more traffic hits these premium rate numbers, the more revenue their owners receive. This motivates attackers to look for ways to boost and inflate traffic volume in any way possible.

Although the attackers are not targeting specific industries, they are continuously scanning and attacking vulnerable SIP servers with the vulnerability CVE-2019-19006.

Getting a line on the threat actors

Check Point's global network of sensors helped researchers to obtain unique strings during the exploitation of CVE-2019-19006. Perhaps purposely, the threat actor left a "calling card" using the name **"inje3t0r3-seraj"**, which appears to be a variation of the Pastebin script uploader's name.

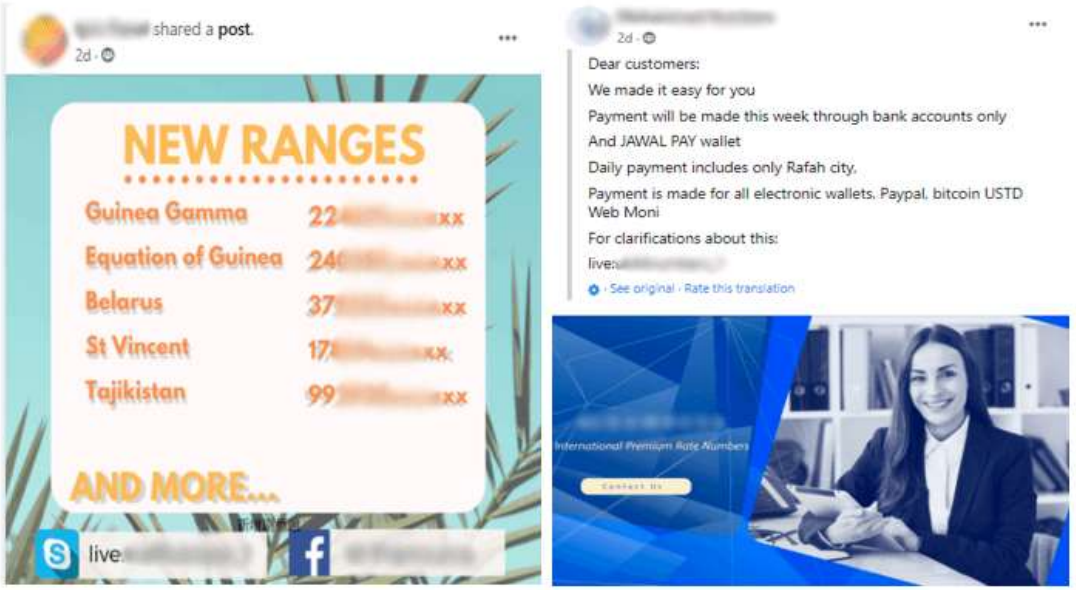
Through further investigation, the names eventually led to multiple private Facebook groups that deal with VoIP, and more specifically, SIP server exploitation. The "voip__sip__inje3t0r3_seraj" group is the most active, sharing admins with different relevant groups, including an admin named "injctor-seraj-rean".

Figure 2: Many admins are active in multiple groups.

The group shares a number of tools related to SIP server exploitation: scanners, authentication bypass, and remote code execution scripts.

Among these scripts, we found a variant of the brute-force script seen in the Pastebin of INJ3CTOR3.

The research shows that the attackers publish guides and videos via social media that explain how others can create such attacks and make money from them.



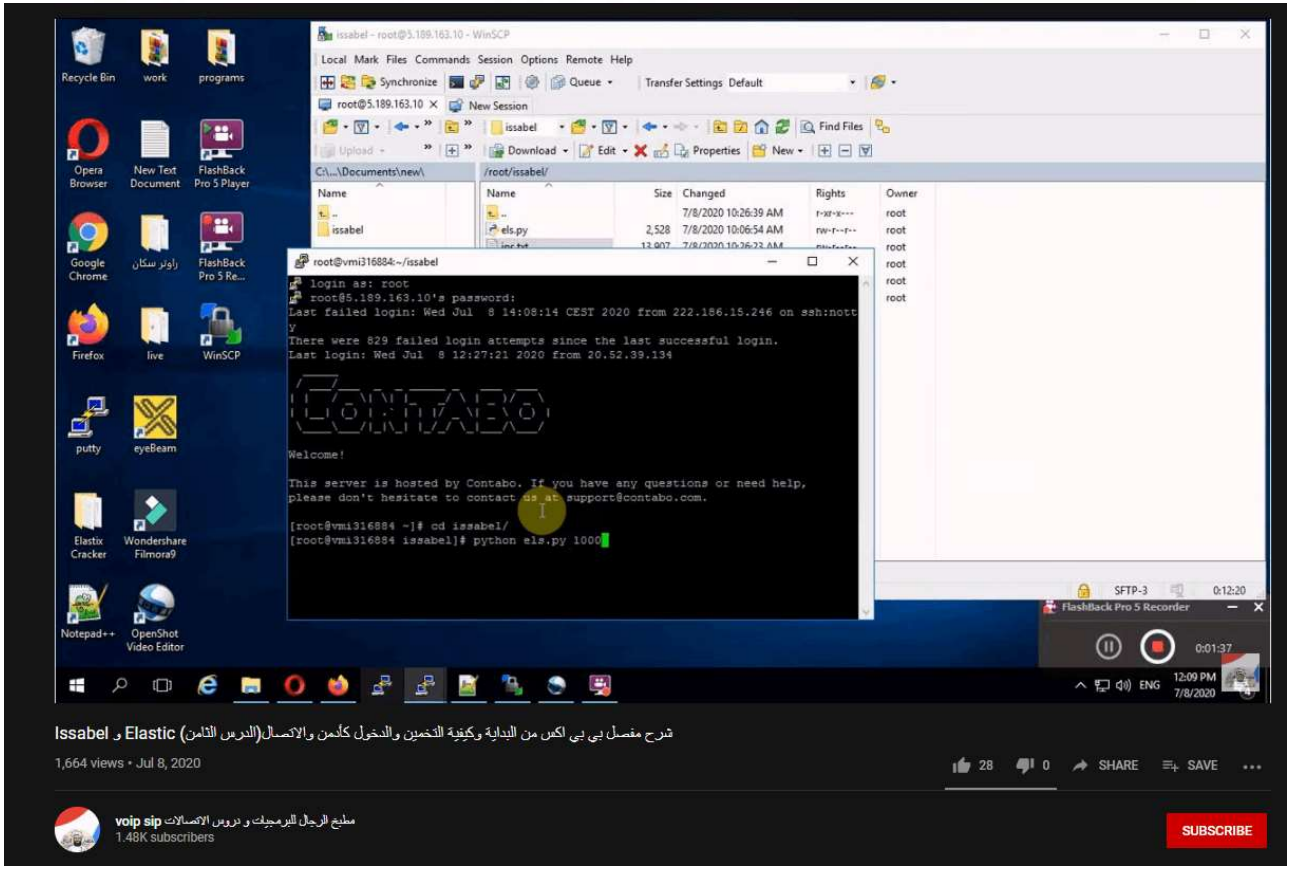
Injctor Seraj Rean is with **Mostafa Ahmed**.
Admin · May 12, 2019 ·

كل عام وانتم بخير جميعا ورمضان كريم
خليك فى المضمون وابدأ الترافيك الخاص بك وإنت مرتاح ومتيقن من إستلام فاتورتك فى مواعيد محدده بدون أى خصومات أو مصاريف نهائيا.
شركة بريميم ريت نمبر هدفها الرئيسي هو كسب ثقة العملاء وضمان إستمرار التعامل معهم إلى المدى البعيد..
خدمة العملاء الخاصة بنا تعمل بأقصى جهدها لتلبية احتياجات عملائنا وضمان ارضائهم..
نتواجد جميع أيام الاسبوع لمدة 24 ساعة فلا تتردد بمراسلتنا إذا كان لديكم أى استفسار أو للمساعدة

Arabic Support
Email:Arabic@premium-rate-numbers.com
Skype:live:arabic_74
==========
Sales English
Email:Sales@premium-rate-numbers.com
Skype:premium-rate-numbers.sales

https://premium-rate-numbers.com
http://ivrreport.com

every year you are fine for everyone .....
Do you want to succeed !!!! and start your Trafic and you are very happy to receive the invoice on time, without any discounts or expenses.
The company's main goal is to win the trust of customers and ensure that they continue to deal with them in the long run.
Our customer service works to the best of our ability to meet the needs of our customers and ensure their satisfaction ..
We are available 24 hours a day. Please feel free to contact us if you have any questions or assistance
Arabic Support
Email: Arabic@premium-rate-numbers.com
Skype: live: arabic_74



Targeted 20 countries and industries

- Targeted 631 enterprises in Great Britain
  - Industries such as government/Military/ Insurance/Finance/Manufacturing
- Targeted 255 enterprises in the Netherlands





    - Industries such as education/research/ Government/Military/Manufacturing
- Targeted 171 enterprises in Belgium
    - Industries such as Retail/Healthcare/Government/Finance
- Targeted 93 enterprises in the U.S.
    - Industries such as Communications/Finance/Banking/Insurance/Banking
- Targeted 57 enterprises in Colombia
    - Industries such as education/research/Government/military/Finance
- Along with ***15 other Countries*** and their targeted attacks*:* Germany (52), France (27), India (27), Italy (27), Brazil (25), Canada (24), Turkey (21), Australia (15), Russia (13), Switzerland (13), Czechia (12), Portugal (11), Denmark (10), Sweden (10) and Mexico (9).

How organizations can stay protected from PBX Hacking

- Analyze call billings on a regular basis. Be aware of call destinations, volumes of traffic and suspicious call patterns – especially to premium-rate numbers
- Analyze international calling patterns and make sure destinations are recognized
- Maintain password policy and change all default passwords
- Look for calls traffic made outside of regular business hours
- Cancel unnecessary/unused voice mails
- Apply patches to close the CVE-2019-19006 vulnerability that hackers are exploiting
- Intrusion Prevention Systems detect or prevent attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking threats

Conclusion

This VoIP system hacking utilizes an easily exploitable vulnerability to compromise Asterisk SIP servers around the world. In-depth details regarding the vulnerability were never publicly released, yet the threat actors behind the attack managed to weaponize and abuse it for their

own gain. As our research shows, the threat actors, who are located in the Palestinian Gaza Strip, share and sell their scripts. This is a phenomenon of an established operation that sets the attacks, finds the targets, and initiates the traffic to premium rate service numbers in order to inflate traffic and gain revenue.

The attack on Asterisk servers is also unusual in that the threat actors' goal is to not only sell access to compromised systems, but also use the systems' infrastructure to generate profit. The concept of IPRN allows a direct link between making phone calls and making money. This means that further attacks can be launched from these systems. So organizations using Sangoma or Asterisk VoIP systems should ensure they have applied all relevant patches, to avoid being exploited for costly calls.

Staying Protected

Check Point customers are protected by these IPS protections:

- SIPVicious Security Scanner

- Sangoma FreePBX Authentication Bypass (CVE-2019-19006)
- Command Injection Over HTTP
- Command Injection Over HTTP Payload