REDSHIFT
NETWORKS

SIP BotNet Threat Intelligence Report

redshiftnetworks.com/resources/condor-labs-security-threat-research

Q3 2020 | Condor Labs Team

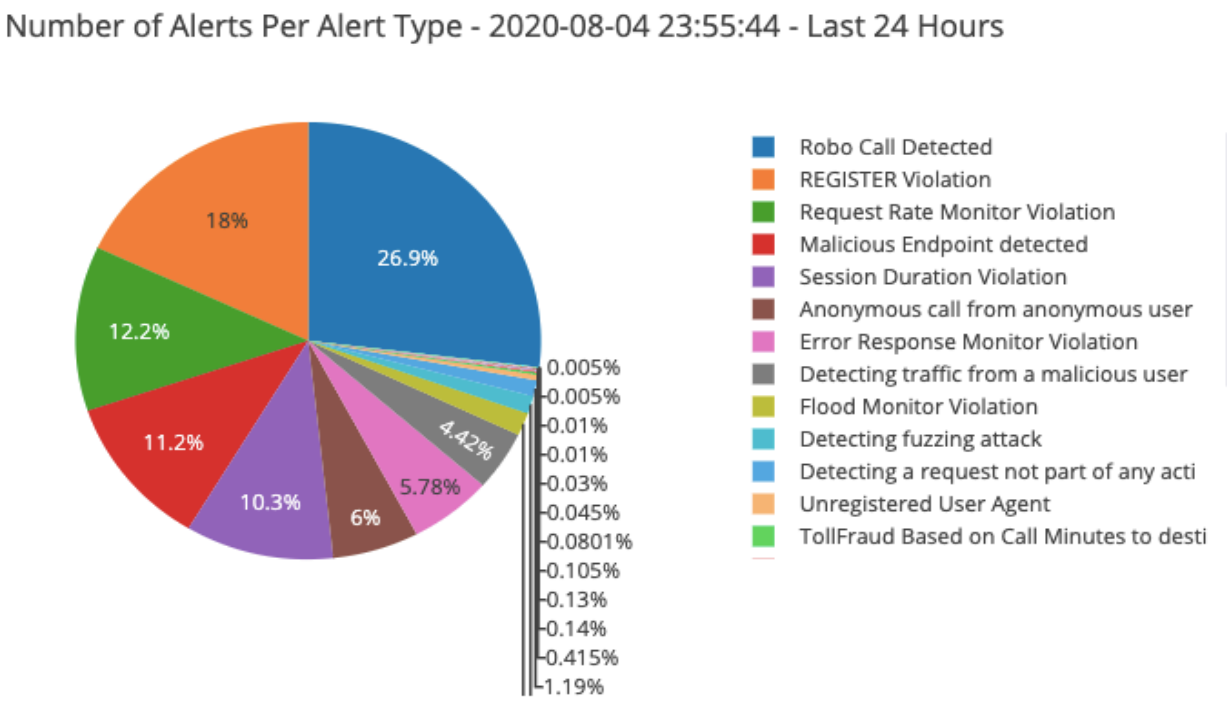
OBJECTIVE

RedShift Networks (RSN) offers a cloud-based SIP Threat Intelligence Service comprised of customer RSN Unified Communications Threat Management (UCTM) installations and Honeypots (security mechanism set to detect security attacks) installed in locations around the world to detect SIP Botnets. These Botnets are compromised systems servers, mostly in ISPs that offer hosting services, that generate special attack scripts installed by fraudsters and hackers from around the world.

Bots are a particular aggressive form of attacker. They are the root cause behind many major cyber security meltdowns in the past few years. Trillions of dollars have been lost to bot attacks. This particular variant is a SIP bot attack that are specifically targeted towards voice, video, collaboration, Unified Communications, IMS, VoLTE and telephony systems.

This report is a graphical representation and summary of SIP Botnets attacks globally impacting enterprise and carrier customers.

(a) Types of SIP Attacks over the last 24 hours by RedShift Networks



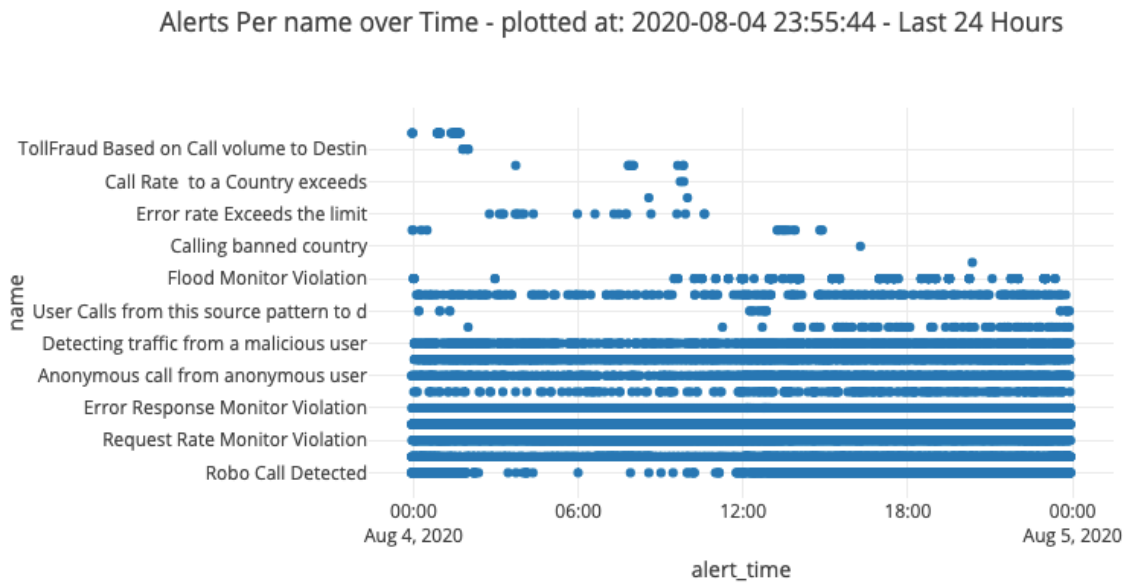
Robocalls are the most frequent type of attack visible globally in our customer base and honeypots.. These are SPAM callers causing nuisance and telemarketing calls inundating the US over the last few years. It is estimated that 40% of all calls in the US are now Robocalls and $9.5B of loss in productivity and other metrics.

The 2nd most frequent type of attacks are Register Violation attacks. In this attack, the hacker attempts to take control of the IP phone and falsely “register” in the customers network as a legitimate user. Once the hacker becomes a legitimate user, they launch a costly myriad of attacks and fraudulent calls impersonating someone else. Fraud is a major problem in the US. Last year, the CFCA research showed that over $29B was lost to Telecom Fraud that is an enormous amount of loss.

The 3rd most frequent type of attack is ‘Request Rate Monitor’. This is a type of Distributed Denial of Service (DoS) attack including Telephony Denial of Service (TDoS). TDoS operates by sending an

overwhelming quantity of SIP packets are sent to a customer's target IP address. Here we see many TDoS attacks targeting our customer base and honeypots.

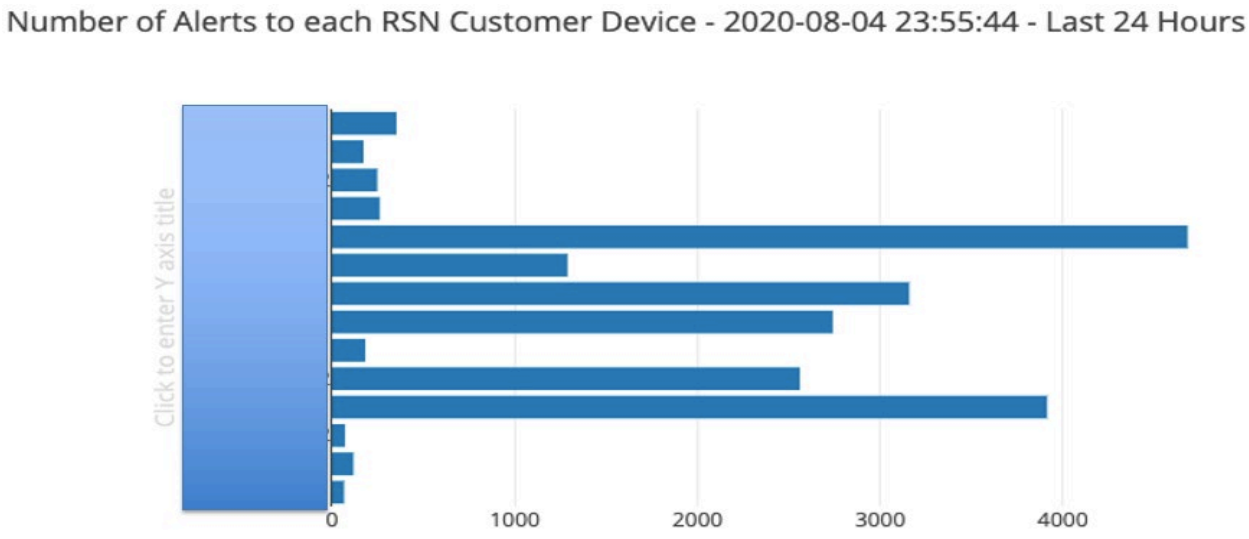
(b) Type of attacks within a 24 hour window showing time of day



The screen above shows the type of attacks targeting RedShift customers and honeypots within a 24-hour window and the frequency of these attacks. The attackers target the customers at different times of the day. There is a noticeable lull in Robocall attacks during the early hours of the morning. Typically, Robocalls are made from Asia starting around noontime in North America. Therefore, we see an increase of Robocallers from noon until the late hours of the night.

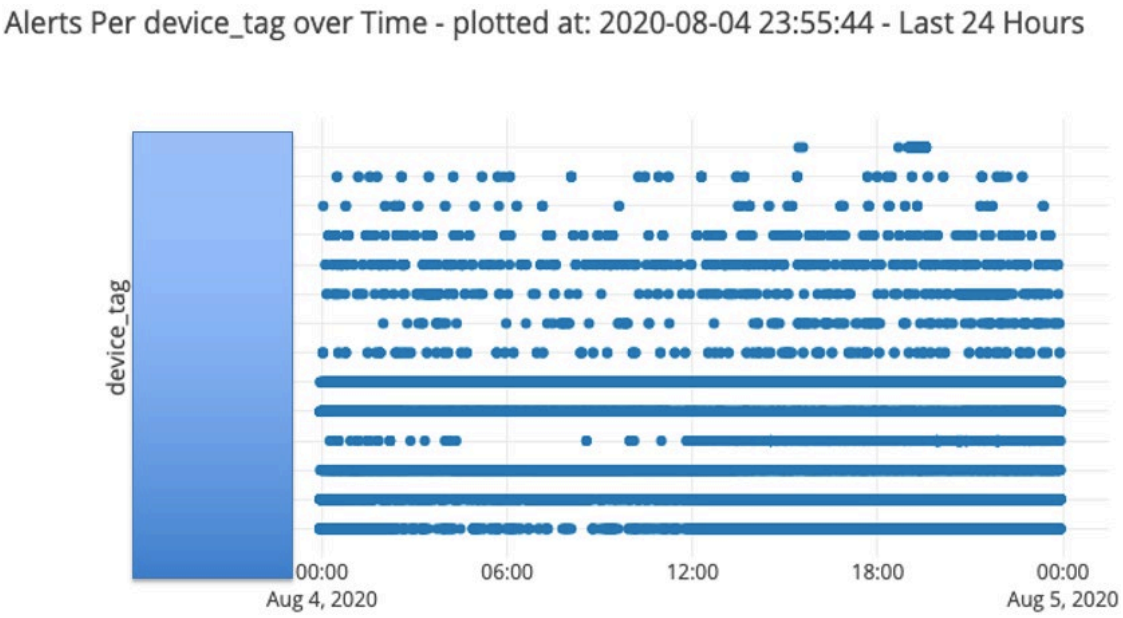
Some attacks are made during work hours – 9 am to 5 pm – other attacks target customers in the evening hours. Those attempting to target customers in the evening hours are typically reconnaissance attacks where they are studying the targets. These attackers study their targets for days, months and often a year or more to find an opening before they generate a large-scale attack.

(c) Number of attacks per customer or honeypot in the last 24 hours



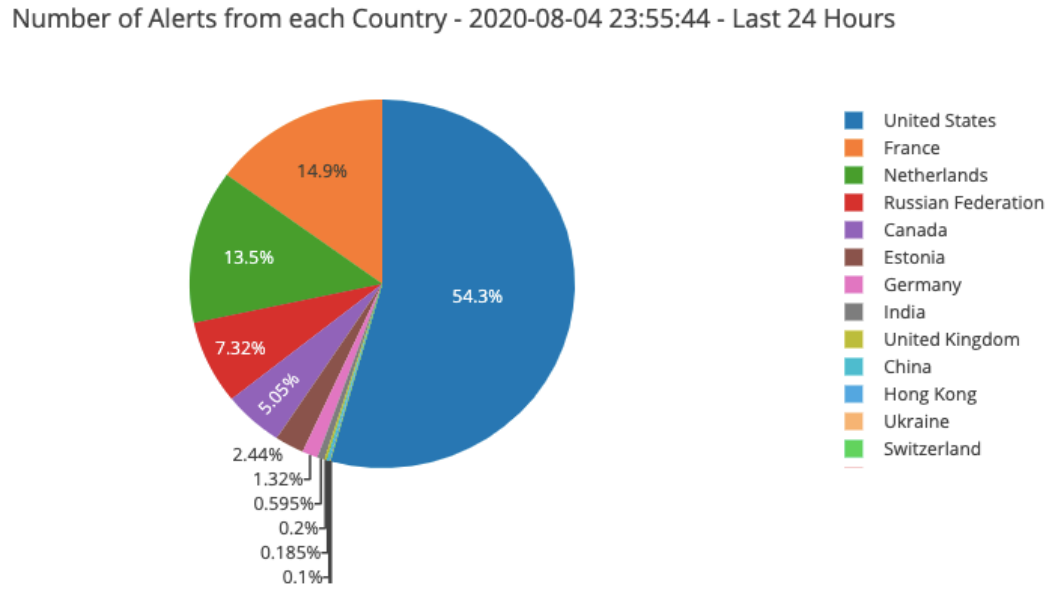
In this diagram, there is a growing number of attacks on a select set of customers and honeypot nodes. Some nodes experienced more than 4000 attacks in a single 24-hour period. Depending on the target, enterprise or carrier the frequency of the attack can become more severe.

(d) Type of attacks per customer/honeypot during a 24-hour period



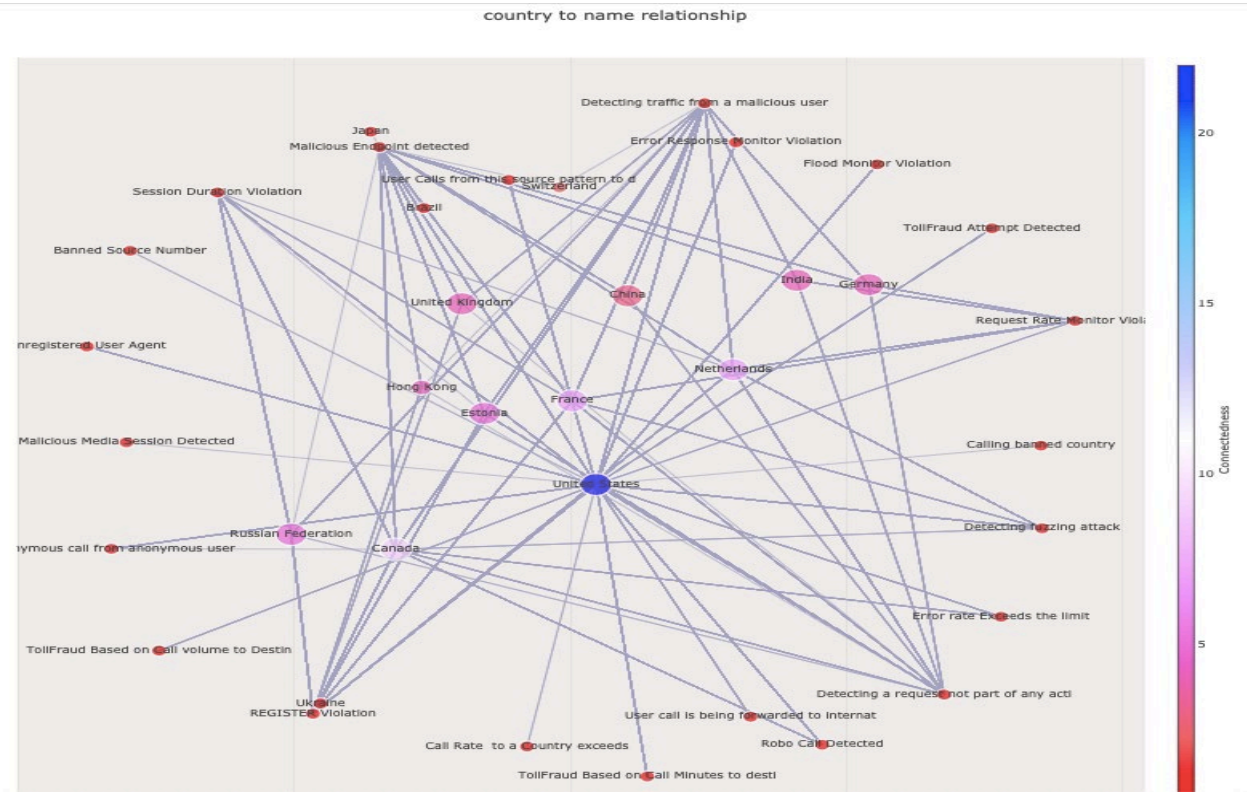
This diagram shows attacks on a specific RedShift Networks customer or honeypot. The attacker is active during different times in the day. Sometimes during business hours and other times during the night based on the type of attack.

(e) Where are the attackers coming from – which countries?



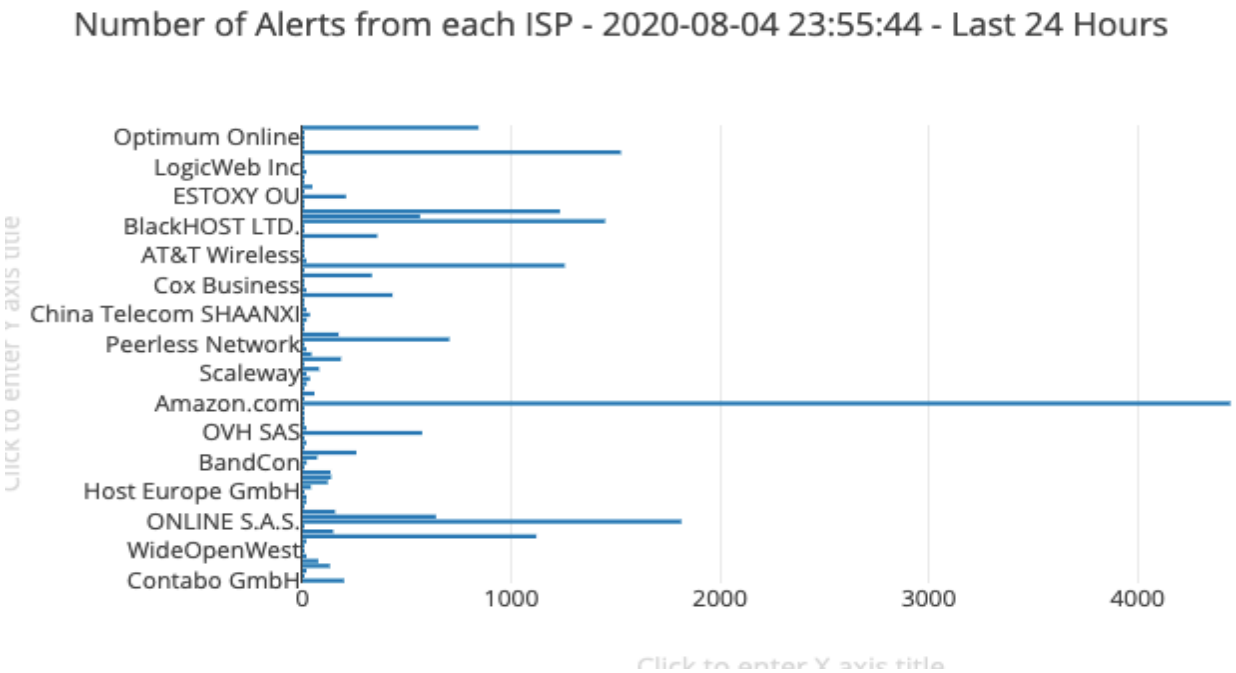
Most SIP Botnet attacks originate in the US where we have our largest installed base of customers. Attacks also arrive from Western Europe – France, Netherlands, Russian Federation, and Asia.

(f) Types of SIP attacks from each country – What kind of SIP attacks is each country generating?



This attack map above shows a sample of the myriad of types of attacks coming from different countries. Each attack is unique and at times the attack may have compromised systems in different countries generating additional attacks.

(g) **Where are the attacks coming from – ISPs, Carriers, Enterprises?**



The above names are of ISPs and Carriers that are located in the US and around the world. Hackers compromise servers in these networks by installing their attack scripts. Interestingly, even servers in Amazon are compromised and generate attacks. Some of these names are well-known carriers and ISPs, others are not well known. Unfortunately, these hackers are experts in taking control of these servers. The hacker runs the 'Command & Control Center' and from these C&CC's they hijack or compromise the servers in these ISPs, which are then instructed to generate attacks. This is the definition of a Bot.

Conclusion

Through this SIP botnet threat intelligence report RedShift Networks is visually educating enterprises and carriers in the US and around the world about the myriad of attacks generated by application-savvy Bots. While protecting enterprise data communications is now commonplace, offering security to an increasingly distributed workforce dependent on SIP-based Unified Communication applications is a new domain. These users and applications require RedShift Networks relevant real-time protection to avoid fraud, malicious exploits and various denial of service attacks. For more information, please visit www.redshiftnetworks.com.