Weaponization of Internet Infrastructure

We have all seen the media around the ever growing IoT threat, with DDoS, data-theft and other nefarious activities all making the headlines. The DDoS attacks targeting Krebs and DYN back in 2016, launched by DVR and Camera systems compromised by Mirai, brought the IoT threat into sharp focus for everyone given the impact.

Since then the IoT threat has evolved with a broader range of devices being targeted, compromised and subsumed into botnets. These botnets can be built quickly and used for a variety of different purposes. ASERT research has indicated that an IoT device connected to the internet will be scanned within 5 minutes of connection and may be targeted by a specific exploit within its first 24 hours.

Challenge

Unfortunately, the IoT security situation has NOT improved since 2016. Many devices are still poorly secured and configured, many cannot be patched, plus many run extraneous and vulnerable services. In short, IoT devices remain a potent resource for bad actors to exploit. The risks will increase as IoT is used more widely in mission- and safety-critical environments like autonomous vehicles and medical applications, etc. Further, the number of devices deployed will grow exponentially with 5G roll-outs.

IoT is not the only area that attackers are exploiting. In the DDoS realm, various forms of reflection amplification attacks have been behind most of the largest DDoS attacks seen on the internet over the past decade. Reflection amplification uses poorly secured or configured internet infrastructure to amplify and obfuscate the true source of a DDoS attack. Many protocols can be used for reflection amplification, including DNS, NTP, SSDP, and SNMP. Recently, attackers have also used TCP-based (SYN-ACK) reflection amplification, which adds a stateful element to the attack impact affecting infrastructure like firewalls, NAT, and load-balancers. At the same time, attackers have been identifying and weaponizing new protocols like WS-Discovery, COAP, and ARMS, circumventing existing defenses and growing their capabilities. In fact, ASERT research indicates that the rate at which attackers are identifying and weaponizing new protocols has doubled in the last year.

Architecture	Sample Count
ARM	67,165
MIPS	38,431
Intel 80386	26,180
PowerPC or Cisco 4500	19,723
SPARC	13,816
Motorola m68k	11,761
Renesas SH	11,702
ARC Core Tangent-A5	243
Xilinz MicroBlaze 32-bit RISC	82
ARM aarch64	82
Altera Nios II	43
Tensilica Xtensa	35
OpenRISC	33
unknown arch 0xc3 version 1 (SYSV)	23
UCB RISC-V	5
Version 1 (SYSV)	1

Figure 1: Mirai is the premier IoT malware family circulating in the wild and boasts a lot of success To continue that trend, malware operators not only were responsible for a 57% increase in the number of unique Mirai variants circulating in the wild, but also managed to port the malware to 16 different OS Architectures (Listed Above)to ensure the malware propagates successfully.

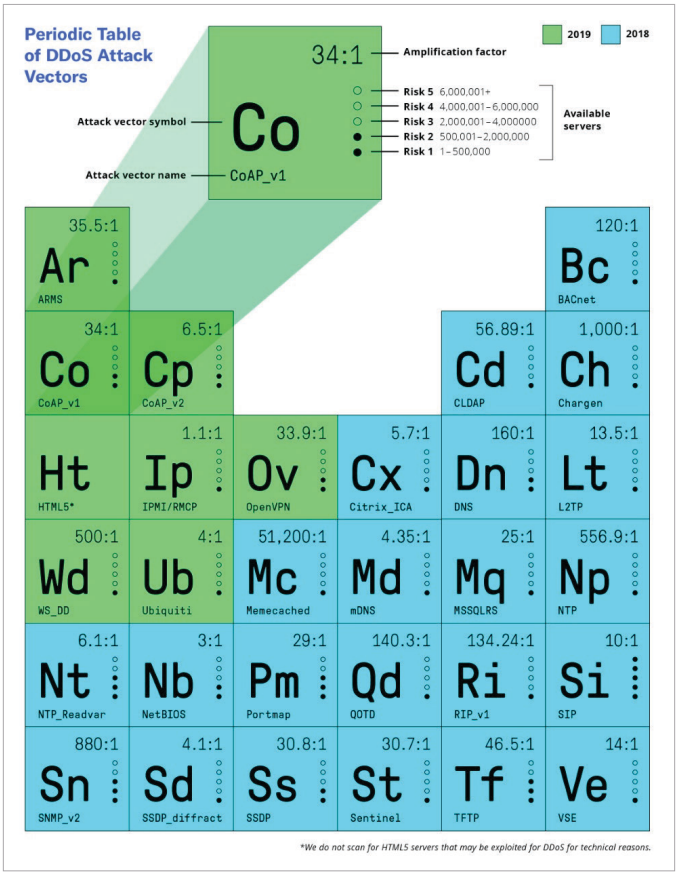

Figure 2: A large portion of DDoS attacks today leverage UDP Reflection/Amplification to send volumetric attacks at their targets. To date, NETSCOUT scans for and tracks 27 different UDP Reflection/ Ampflication vectors as notated in our Period Table of DDoS Attack Vectors, which showcases the number of available reflectors/ amplifiers exist and their amplification factor.

Risk

The combination of IoT and reflection-amplification attack vectors has been an issue for network operators for some time-leading them to reconsider and redesign their DDoS defenses. Traditionally, many operators defended solely against attacks coming from outside of their networks. Now they have to worry just as much about attacks originating inside their networks. Even if the target is outside of the network, the traffic levels can have a local impact. This has led to a significant second wave of investment in Arbor Sightline and Arbor Threat Mitigation System (TMS) for many customers.

Solution

Network operators need every assistance to get ahead of the threats they face. New features and capabilities are being added to Sightline and Sentinel to help in this battle.

Sentinel correlates flow, and later this year DNS information from Smart Data, with threat intelligence from the ATLAS® Intelligence Feed (AIF). This allows the identification of compromised populations of devices within networks of any scale, giving network operators the visibility they need to manage their risk from IoT botnets.

Knowing that the threat of IoT-based botnets will only continue to increase in the future, network operators must be prepared to discover, defend and mitigate this rapidly escalating threat. It is clearly not practical to expect all IoT device manufacturers to fully secure and protect their devices today. Even if this problem were solved tomorrow, there are still billions of devices already deployed that may never be remediated.

Sightline and TMS 9.3 also use a new component of AIF, from ATLAS Security Engineering and Response Team (ASERT), that distributes lists of known reflector / amplifier infrastructure actively being used in current attacks. This new feed of information will further assist network operators in dealing with any attack more efficiently, protecting the availability of their services, infrastructure and customers. Sightline and Sentinel leverage the ATLAS Intelligence Feed (AIF) and NETSCOUT® Smart Data to provide both the required visibility and the intelligence to effectively mitigate the threat from weaponised Internet infrastructure.

Summary

Maintaining network availability against the onslaught of weaponised infrastructure across the global internet is no small task. The arms race of attacker capabilities versus network operator defenses continues. For this reason, NETSCOUT is continuously evolving and innovating to deliver the scalability, reliability, and performance within the features of Sightline, Sentinel and TMS. The Arbor Threat Mitigation System (TMS) is a highly scalable, intelligent mitigation system that can work seamlessly with other network infrastructure to stop DDoS attacks. Sightline With Sentinel delivers Layer 7 visibility across terabit scale networks, and orchestrates and automates DDoS defense across the network edge.

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

© 2020 NETSCOUT SYSTEMS, INC. All rights reserved. NETSCOUT, the NETSCOUT logo, Guardians of the Connected World, Adaptive Service Intelligence, Arbor Networks, the Arbor Networks logo, ATLAS, InfiniStream, InfiniStreamNG, nGenius, and nGeniusONE are registered trademarks or trademarks of NETSCOUT SYSTEMS, INC., and/or its subsidiaries and/or affiliates in the USA and/or other countries. Third-party trademarks mentioned are the property of their respective owners.