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, 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.

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 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 Sightilne and TMS for many customers.

Solution

The ability to proactively identify high-risk or compromised infrastructure is becoming an increasingly important concern for network operators, as this capability allows them to more effectively manage risk and clean-up their environments. Sightline with Sentinel has a roadmap which will significantly help through FY '21.

Sentinel will use a combination of reputation data within the ATLAS® Intelligence Feed (AIF) and NETSCOUT® Smart Data to allow network operators to identify compromised devices at scale by matching intelligence to application layer DNS data. This will allow network operators to identify botnets building out within their networks.

Sentinel will also use a new component of AIF that incorporates ASERT Internet scan data. This will notify operators of open reflection amplification infrastructure within their networks, so that they can monitor these systems more proactively.

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 all expect 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. The only practical solution today is deployments of smart visibility at scale across the entire network. Sightline with Sentinel leveraging the ATLAS Intelligence Feed (AIF) and NETSCOUT Smart Data provide both the required visibility and the intelligence to effectively mitigate the problem.

Summary

Maintaining network availability against the onslaught of massive IoT botnets distributed both across the global internet and also within Internet Service Provider networks is no small task. The arms race of attacker capabilities versus network operator defenses will certainly continue. As these attacks become more ubiquitous so must our defenses. For this reason, NETSCOUT has continued to improve the scalability, reliability and performance of DDoS detection and mitigation systems. The Arbor Threat Mitigation System (TMS) is a highly scalable, surgical mitigation tool that can work seamlessly with other network infrastructure to stop DDoS attacks from taking down network capacity, critical services, and applications. Sightline with Sentinel enables network visibility on a massive scale while using intelligent automation to mitigate at scale across the entire network.

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

SECUC_009_EN-2001 05/2020