Blocking C2 Communication from Compromised Internal Devices

Command-and-control infrastructure, also called C2, is employed by cyber criminals to maintain communications with compromised devices within a target network. Compromised devices often connected via the internet are what constitute zombie armies or botnets that execute instructions from the cyber criminals. Communications to the botnets or compromised devices can be as simple as maintaining an inventory of the compromised devices within a target network for attack planning or for executing malicious activity, such as data exfiltration or encryption. While the command-and-control server is used to control the system on the inside of the target organization, it is usually the compromised host that initiates the communication from inside the network to a command-and-control server on the internet. Indicators of Compromise (IoCs) are pieces of forensic data left behind, such as data found in system log entries or files, that aid information security and IT professionals in detecting data breaches, malware infections, or other threat activity. By monitoring for IoCs, organizations can detect attacks and act quickly to prevent breaches from occurring or limit damages by stopping attacks in earlier stages. IoCs are the red flags that indicate a potential threat that could lead to a data breach or systems compromise.

Threat

The threat is the malware itself and the potential damage it can inflict. The challenge is reliably detecting the malware when it's present and stopping it by blocking communication to its C2 infrastructure for further instruction. IoCs may not necessarily "indicate" that an attack has occurred. But, if seen early enough, and analyzed, they can indicate that a network breach has occurred that precedes an imminent attack. For example, detecting a dropper prior to a ransom-ware attack.. Confirming the attack, identifying the compromised device and blocking the potential C2 communication from the malware involved requires an in-depth security investigation. One of the things that makes this hard is ensuring you have an accurate and comprehensive list of potential indicators, combined with the necessary data or intelligence to confirm the threat, and take meaningful action to prevent the malware from causing harm.

Risk

Attackers are using stealthy techniques to stay under the radar for longer periods as an Advanced Persistent Threat (APT). This entails maintaining undetected access within a victim's organization to wait for opportunities or to slowly live off the land, move laterally, escalate privileges and exfiltrate information. Opportunities for an attacker could mean stolen data, planting and triggering ransomware or malware, stolen credentials or passwords and the potential for a general DDoS or cyberattack. None of these scenarios are optimal for any organization due to the potential losses in productivity, costs to organizational reputation and damage to critical business applications and processes.

Investigation

IoCs are not always easy to detect; they can be elements within metadata or instances buried in complex code. Some examples of IoCs are:

- Traffic to known bad IP addresses, domains or URLs
- Unusual Outbound Network Traffic
- Geographic Irregularities
- Anomalies in Privileged User Account Activity
- Log-In Anomalies
- Increased Volume in Database Read
- DNS Request Anomalies
- Large Number of Requests for the Same File
- HTML Response Size

Analysts look for correlations between identified IoCs within a network and gathered threat intelligence to analyze them for potential threats or for identifying a previous or future attack. For example, it is well known that the Ryuk ransomware is seeded by the Trickbot Remote Access Trojan. The ransomware attack can be stopped by detecting and blocking malicious communication with the Trickbot malware command and control infrastructure prior to dropping and executing the Ryuk ransomware.

While they are reactive in nature, organizations that diligently monitor for IoCs plus keep up with the latest IoC discoveries and reporting, will improve detection rates and response times significantly.

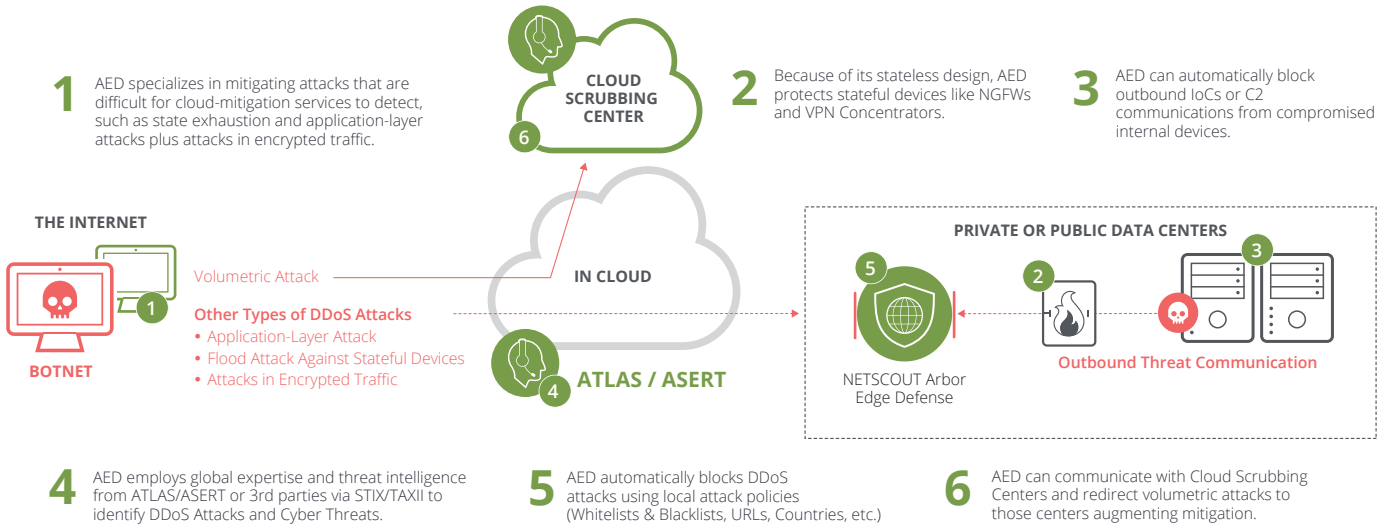

Figure 1: NETSCOUT AED provides a first and last line of network edge defense.

Attackers are also taking advantage of the current exponential growth of Internet of Things (IoT) devices on networks. IoT systems are based on two main components, system hardware and system software, both of which have design flaws. Vulnerabilities are weaknesses in a system or its design, policies and procedures used in the systems, and system users themselves. These can allow an intruder to execute commands and access unauthorized data. Exposure is a problem or mistake in the system configuration that allows an attacker to conduct information-gathering activities. One of the most challenging issues in IoT is resiliency against exposure to physical attacks. In most IoT applications, devices may be left unattended and likely will be placed in location easily accessible to attackers. Such exposure raises the possibility that an attacker might capture the device, extract cryptographic secrets, modify their programming, or replace them with a malicious device under the control of the attacker. For these reasons, monitoring a network for IoC data and analyzing it when found is the key to blocking communication with malicious C2 infrastructure and stopping future cyberattacks.

Mitigation

The most common form of DDoS attack protection today is a cloud-based mitigation service, often from ISPs or independent providers. And while such services are indeed vital to stop large, volumetric DDoS attacks that outstrip the volume of internet circuits, that is only one part of a comprehensive protection strategy. Another important aspect is the on-premises ability to identify and block inbound threats and outbound communication to known malicious C2 infrastructure from compromised devices on the network in real time.

NETSCOUT® Arbor Edge Defense (AED), an on-premises solution that leverages the company's proven market-leading DDoS technology and comprehensive Threat Intelligence via the ATLAS® Intelligence Feed (AIF) as well as other threat intel feeds through its STIX/TAXII feature to provide millions of reputation-based IoCs out of the box, which assist to detect and block the inbound threats and outbound communication from internal compromised hosts that have been missed by other devices in the security stack—helping to stop further proliferation of malware and other tactics used within crimeware and advanced-threat campaigns. Additionally, AED's packet-processing engine uses parameters like confidence ranks and custom-made allow lists to fine tune each blocklist and minimize false positives. Finally, AED can integrate with an existing cybersecurity stack and process. For example, AED can send SYSLOG alerts to a SIEM and can be used by a SOAR for blocking threats at the network edge. AED engages a unique, stateless, packet-processing engine to provide efficient inbound and outbound blocking of malicious traffic without tracking any session state. As a result, NETSCOUT AED can make other perimeter defenses, such as firewalls, more effective by shielding them from DDoS attacks, and offloading the overhead associated with applying millions of IoCs to traffic streams.

Summary

AED is built to combat internet-scale, IoC-based intrusions. The unique combination of stateless filtering, rigorous curation of custom threat intelligence as well as ingestion of third-party feeds, allows NETSCOUT AED to block outbound threats with the same level of confidence they've been blocking inbound DDoS threats for years.

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_019_EN-2101 12/2021