DDoS Attack Used As Smokescreen

NETSCOUT AED is The First and Last Line of Defense

When an advanced cyber-adversary decides to target your organization, they will customize an attack campaign consisting of multiple tactics, techniques and procedures (TTPs); that will be strategically executed during multiple phases of a process known as the Cyber Attack Kill Chain[1]. DDoS is an attack vector that is used during multiple stages of the Kill Chain.

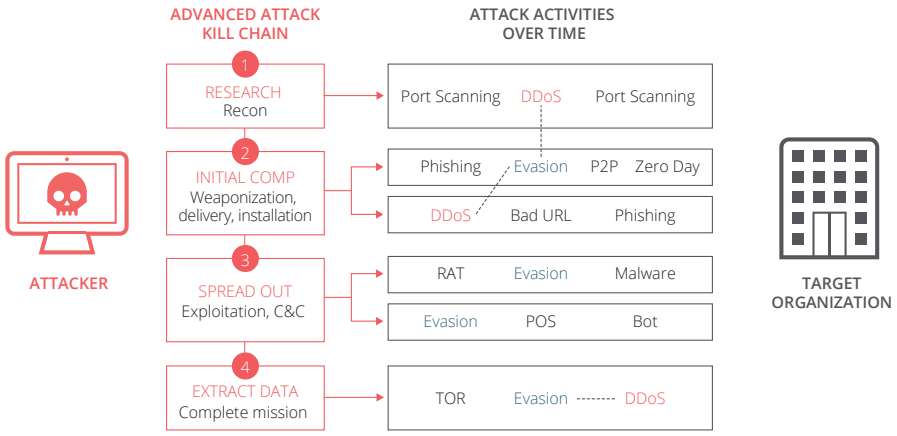

Figure 1: DDoS used during various stage of attack kill chain. Source: Arbor, Inc.

- The early Reconnaissance stage to test an organization's ability to respond to a DDoS attack or cover up port scanning activity.
- The Weaponization or malware Delivery stage, where the DDoS attacks are used to produce extraneous security forensic log and data files; making the search for the planted malware much more challenging.
- The Data Extraction stage where the DDoS attack is used as a diversionary tactic or smokescreen to cover up the exfiltration of confidential data.

DDoS as a smokescreen has been documented by various security research firm such as:

- NETSCOUT[2] – 14th annual Worldwide Infrastructure Security Report noted that the motivation behind 24% of all DDoS attacks was to be used as a diversionary tactic.
- Kapersky Labs[3] – Reported 36% of business are confident that DDoS has been used as a smokescreen for other kinds of cybercrime.

KEY FEATURES AND BENEFITS

First & Last Line of Defense

AED's unique location on the network edge, its stateless packet processing engine and ATLAS® global threat intelligence feed allow it to stop inbound threats and outbound communication from compromised hosts.

Always On, In-Line, Advanced DDoS Protection

Out of the box, on-premise protection from all types of advanced DDoS attacks including volumetric, state-exhaustion, application-layer which can be used as a smokescreen.

Intelligently Automated, Hybrid DDoS Protection

The intelligently automated, fully managed combination of in-cloud (via Arbor Cloud) and on-premises (via AED) is continuously armed with ATLAS global threat intelligence; offers the most comprehensive form of protection from the modern-day DDoS attack.

Blocking Outbound IoCs

AED's can also act as the last line of defense as it blocks outbound communication from internal compromised to known bad sites (i.e. IP addresses, domains, URLS etc.) helping to stop further proliferation of malware or data breach.

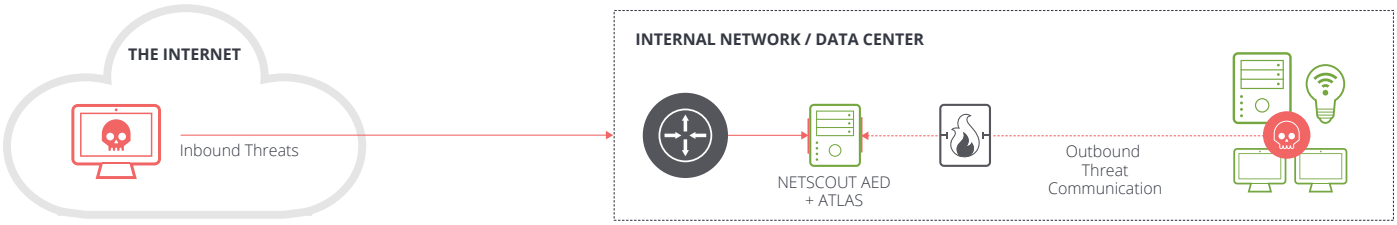

Figure 2: AED and ATLAS act as First and Last Line of Defense, providing organizations protection during multiple stages of the Kill Chain.

NETSCOUT Arbor Edge Defense (AED) Acts as First and Last Line of Defense

NETSCOUT® AED is a deployed at the network perimeter (i.e. between the Internet router and firewall). Using a stateless packet processing engine and armed with continuous highly curated, reputation-based threat intelligence it receives from NETSCOUT ATLAS Threat Intelligence or 3rd parties via STIX/TAXII, AED is a network perimeter enforcement point that can automatically detect and stop both inbound threats (e.g. DDoS attacks and other threats in bulk) and outbound communication from internal compromised hosts that have been missed by other components in the security stack – essentially acting as the first and last line of defense for organizations. In other words, the NETSCOUT AED can help during all phase of the Cyber Attack Kill Chain.

First Line of Defense

In an appliance or virtual form factor, NETSCOUT Arbor Edge Defense (AED) is deployed at the network perimeter (i.e. between the Internet router and firewall) where it provides first line of defense from DDoS attacks and inbound threat connection attempts. AED Provides Best of Breed DDoS Attack Protection: Based upon Arbor' 20-year heritage, proven technology and global threat intelligence from NETSCOUT ATLAS. AED delivers best of breed and comprehensive DDoS attack protection.

- AED can automatically detect and stop inbound application layer, TCP-state exhaustion and DDoS attacks as large as 40 Gbps.
- In the event of larger DDoS attack, AED's Cloud Signaling will automatically reroutes traffic to Arbor Cloud or a MSSP's cloud-based DDoS attack mitigation center.
- Arbor Cloud provides protection from the largest DDoS attacks via 12 worldwide scrubbing centers providing over 14 Tbps of mitigation capacity.
- AED stays abreast of the latest DDoS threats via the ATLAS Threat Intelligence Feed.

Last Line of Defense

In a world where security stacks are still missing Indicators of Compromise (IoCs), AED can act as the last line of defense. Armed with highly curated Indicators of Compromise (IoCs) it receives from NETSCOUT ATLAS Threat Intelligence and/or 3rd parties via STIX/TAXII, AED can act as an outbound network enforcement point by detecting and automatically blocking outbound communication to known attacker C2 infrastructures (i.e. IP addresses, domains, URLs, C2C infrastructure). By acting as this last line of defense, AED can help organizations stop the proliferation of stage 2 malware within their networks and ultimately avoid the data breach.

Contextual Threat Intelligence

AED and NETSCOUT ATLAS Threat Intelligence can also help security teams by providing more context to IoCs that it has blocked. For example, when AED blocks an outbound IoC, it sends an alert NETSCOUT ATLAS Security Engineering Research Team (ASERT). Using Machine learning and other technology, ASERT automatically analyzes its vast database of threat intelligence to provide more context related to the IoC. This additional context is then automatically delivered to the security analyst via the AED UI who then can determine the true risk to their organization or proactively hunt using their other security tools.

LEARN MORE

For more information about NETSCOUT AED and how it can be used to protect organizations during multiuple stages of the Kill Chain visit:

https://www.netscout.com/products/netscout-aed

[1] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[2] https://www.netscout.com/report/
[3] https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business

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

SECSB_010_EN-1901 05/2019