Arista NDR Covers the Spectrum of the MITRE ATT&CK Framework

Get a Holistic View of Your Entire Environment

The MITRE ATT&CK Framework is an important collection of adversary tactics, techniques, and procedures (TTPs) that are used in launching attacks against organizations. The framework was developed out of a need to first understand these common TTPs and to then enable the creation of solutions that can detect and mitigate the threats in both enterprise and mobile environments.

While the framework has been developed with a primarily endpoint-focused view of the world, it is evolving over time as MITRE works with more industry researchers, such as those from Arista NDR, to broaden the scope of known TTPs and the relevant detection capabilities. This evolution acknowledges that tools that operate with the purview of an entire network can detect threats that exist beyond the scope of the endpoint. Such tools have a distinctly strong advantage in detecting attacks on unmanaged infrastructure, including shadow IT, Internet of Things (IoT), and Operational Technology (OT) networks as well as the cloud.

The MITRE ATT&CK Framework essentially maps TTPs across different aspects of attack stages and activities—from initial access, to data exfiltration and every activity in between. Many of these activities go far beyond the endpoint, particularly in the later stages and this is where many existing security tools have their limitations. But Arista NDR has the view of the entire network and the ability to understand whether a particular activity makes sense for a specific environment. With a deep ability to understand network behaviors, Arista NDR fills the gaps left by endpoint and log-based detection tools. For example, Arista NDR has insight into an attacker learning the network from the inside when moving around laterally.

Mapping Detections by The Arista NDR Platform to MITRE ATT&CK

The rest of this document dives into detail with examples of techniques Arista NDR detects and how they map to the MITRE ATT&CK Framework.

Initial Access

Consists of techniques that use various entry vectors to gain an initial foothold within a network. Initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

Example Techniques:

phishing attack, drive-by download, compromised application

Arista NDR often finds IoT and other non-traditional devices targeted for initial access. These devices frequently run an outdated operating system that is easily exploitable and provides a foothold within the organization from where the attacker can spread their tentacles. For instance, Arista NDR recently uncovered an HVAC system controller being accessed from the internet using Microsoft's Remote Desktop Protocol (RDP).

Another very common scenario that Arista NDR detects is when a user visits a website that is compromised or that has an advertising framework with malware injected into it. In the latter case, the malware redirects the user to a new page where an exploit kit or other malware might be used to compromise the victim. In both scenarios, the goal is to surreptitiously plant malware on the endpoint device in furtherance of the attack.

Execution

Consists of techniques that result in adversary-controlled code running on a system. Techniques that run malicious code are often paired with those from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does remote system discovery.

Example techniques:
command line interface (CLI), execution through APIs

PowerShell is a built-in tool on most Microsoft systems that enables the user to perform administrative-type activities. The use of PowerShell is not inherently malicious, but the tool can be made to conduct malicious acts. This is why Arista NDR monitors communications involving PowerShell and uses various techniques to analyze the behavior and highlight only those activities that exhibit malicious intent.

Persistence

Consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

Example Techniques:
Browser extensions, BITS jobs, External Remote Services

An example of creating persistence is through a scheduled task on a system. For example, an attacker can schedule a task to open a port that they can later connect to in order to, say, exfiltrate data that they have been collecting on the system. Another common activity Arista NDR observes frequently is the abuse of a built-in system tool to create persistence. For example, the Windows diagnostics tool BITS can be used to access external domains that aren't controlled by Microsoft. This bypasses various controls that might be in place to protect web traffic.

Arista NDR also has detected persistence using network-accessible services such as SSH running on unmanaged devices.

Privilege Escalation

Consists of techniques that adversaries use to gain higher-level permissions on a system or network. Adversaries can often enter and explore a network with unprivileged access but require elevated permissions to follow through on their objectives. Common approaches are to take advantage of system weaknesses, misconfigurations, and vulnerabilities.

Example techniques:
SYSTEM/root level, local administrator, user accounts with access to a specific system

One activity that Arista NDR detects quite frequently is someone attempting to brute force or crack the password of a network user or administrator. If the password can be derived by such measures, the attacker obviously can gain illicit access to resources.

Defense Evasion

Consists of techniques that adversaries use to avoid detection throughout their compromise. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware.

Example Techniques:
uninstalling/disabling security software, obfuscating/encrypting data and scripts

A classic example of a defense evasion maneuver is to disable the security controls on a system. Arista NDR detected this specific action in a recent attempt to conduct a ransomware attack on a manufacturing company. The attacker attempted to disable User Account Control on a number of Microsoft Windows devices remotely.

Credential Access

Consists of techniques for stealing credentials like account names and passwords. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

Example techniques:
keylogging, credential dumping

This is a case where behavior analytics are especially helpful. Arista NDR understands the "normal" behavior of people associated with specific credentials and can flag activity that appears to be unusual for a set of credentials; for example, logging into the network with administrative credentials from a device that doesn't typically perform administrative functions.

Discovery

Consists of techniques an adversary may use to gain knowledge about the system and internal network. These techniques, which often use native OS tools, help adversaries observe the environment, and orient themselves before deciding how to act. They also allow the attacker to explore what they can control and what's around their entry point to discover how it could benefit their current objective.

Example Techniques:
network sniffing, file and directory discovery, account discovery

Arista NDR frequently sees protocols like SMB and LDAP used for the purpose of mapping the network; for instance, the enumeration of entire subnets of systems or network file shares.

Lateral Movement

Consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. This involves pivoting through multiple systems and accounts to ultimately get to the crown jewels. Adversaries might install their own remote access tools to accomplish lateral movement or use legitimate credentials with native network and operating system tools, which may be stealthier.

Example techniques:
pass the hash, internal spearphishing, remote services

Arista NDR can detect if a user is moving laterally on the network in a way that indicates malintent e.g. the use of Windows Admin Shares for copying malicious payloads and having those run on the remote device. A recent discovery involved lateral movement from a workstation to the customer's cloud infrastructure, accomplished by stealing credentials for the cloud service provider from the victim's browser. Arista NDR has also observed hardware implants using the Raspberry Pi or BeagleBone platforms to establish a foothold and then using protocols like SSH to move within the environment.

Command and Control (C&C)

Consists of techniques that adversaries may use to communicate with systems under their control within a victim network. Adversaries commonly attempt to mimic normal, expected traffic to avoid detection.

Example techniques:
port knocking, domain generation algorithms, commonly used port

Attackers are increasingly using malicious browser extensions/add-ons as a way to gain unfettered access to devices. One use for this technique is to set up communications with C&C destinations. Endpoint security solutions typically don't report on browser add-ons as a threat because they aren't traditional malware. Arista NDR autonomously identifies risky browser plug-ins based on what destination they are communicating with, and whether they are legitimate extensions.

Exfiltration
Consists of techniques that adversaries may use to steal data from the network. Once they've collected data, adversaries often package it to avoid detection while removing it. This can include compression and encryption.

Example techniques:
transferring it over a command and control channel and batching the transfer to stay under file limits

DNS data exfiltration is a way to exchange data between two computers without any direct connection. During the exfiltration phase, the client makes a DNS resolution request to an external DNS server address. Instead of responding with an A record in response, the attacker's name server will respond back with a CNAME, MX or TXT record, which allows a large amount of unstructured data to be sent between attacker and victim. Arista NDR inspects DNS at a granular level to uncover such a threat, whereas with other detection tools, the attacker flies under the radar by taking advantage of a common blind spot given how prevalent DNS traffic is. Another example Arista NDR recently uncovered was a Wi-Fi enabled USB keystroke logger that was uploading information to an external location.

Impact
Consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. In some cases, business processes can look finebut may have been altered to benefit the adversaries' goals.

Example techniques:
destroying or tampering with data, firmware corruption

Arista NDR commonly detects two types of attacks in the Impact category: cryptomining and ransomware. Arista NDR is able to detect TTPs relevant to such attacks, including attempts at network share encryption, credential abuse, privilege escalation, and lateral movement. Arista NDR also identifies the disabling of security measures and uncovers the use of tools like PowerShell for ransomware distribution.

Compliance (currently not part of the Framework)
Arista NDR considers this an important pre-attack condition that must be factored into an organization's security program. We define compliance as consisting of conditions that make an organization susceptible to an attack. For example, suppose a user or even a system administrator keeps a clear-text document that contains account user IDs and passwords. Though this activity in itself is not malicious, it poses a risk in the event that the file is stolen. The exposure of this data makes the organization much more vulnerable to attack. Another example is having extremely out-of-date systems, such as a server running Windows 2003 that hasn't been patched in years. The very existence of this device on the network creates a high level of vulnerability to attack.

The existence of a file with passwords or an outdated server is not, in itself, malicious. However, it can be a precursor to malicious activity, and Arista NDR can detect the presence of these risky conditions network-wide and notify security personnel about them so that they can be addressed before they are exploited by a bad actor.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062