Network Traffic Analysis Meets MITRE ATT&CK

APRIL 2019

Expand and Reinforce Detection Coverage For Late-Stage Attack Behaviors

Faced with an array of seemingly identical products, many enterprises are turning to MITRE ATT&CK to evaluate the potential contribution of a new detective tool. The MITRE knowledge base of adversary tactics, techniques, and procedures (TTPs) is based on real-world observations. The TTPs included in the framework are in use globally by advanced persistent threat groups as well as far less sophisticated adversaries. When a mechanism works, it will appear over and over, affecting organizations of all sizes and security postures.

In modern, multi-stage attacks, there is little way to avoid communicating on the network at some point. The framework lists many exploits and behaviors that are likely to generate subtle, yet unusual network traffic patterns on the east-west corridor inside an enterprise network, as well as traversing north-south through the nominal perimeter at multiple times over the course of the attack.

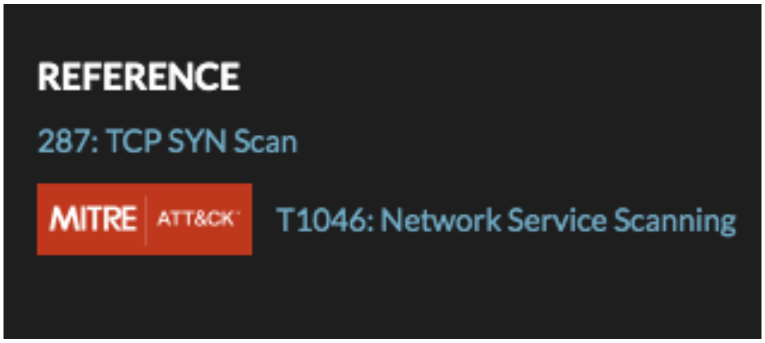
Network traffic analysis (NTA) tools offer passive monitoring, protocol parsing, and real-time examination of data in flight across a network. By detecting and investigating adversary behaviors and attack TTPs that leave evidence on the network, NTA offers the best chance of detecting more of the 11 categories that represent the links in the chain of an attack. Together, this rich evidence helps SOC analysts put together a more complete, actionable picture of what is happening to mount a meaningful response.

Why Reveal(x)?

NTA as a category offers baseline detection. As an enterprise-class solution, specific capabilities differentiate Reveal(x) and enable it to go beyond other NTA products in detecting and investigating MITRE ATT&CK TTPs:

- Instant access to application transaction contents at Layer 7 enables rapid detection and investigation of suspected threats, even those hidden in legitimate traffic.
- Real-time detection of threats based on machine-learning driven behavioral analysis to catch unknown unknowns in ways that rules-based detection can't.
- Decryption capabilities, including for Perfect Forward Secrecy (PFS), enable detection of TTPs in use that would otherwise escape detection by hiding in legitimate traffic.
- Out-of-band, passive processing of network traffic at scale (up to 100Gbps). Many vendors top out at 40Gbps, which is not enough for today's enterprises.

In addition, as part of its guided investigations, Reveal(x) includes a reference and link to MITRE whenever a detection matches a MITRE ATT&CK TTP. This permits immediate recognition of the significance of the threat and direct access to context and recommendations about mitigations.



REFERENCE

287: TCP SYN Scan

MITRE ATT&CK T1046: Network Service Scanning

Get Started

By incorporating enterprise-class Reveal(x) Network Traffic Analysis into your security operations, you can improve the range and completeness of detections and better defend against and investigate data breaches, malicious attacks, and insider threats. For more information on how Reveal(x) identifies these TTPs, refer to the full-length technical overview.

To learn more about network traffic analysis as a category, download a complimentary copy of Gartner Market Guide for Network Traffic Analysis, in which ExtraHop is listed as a representative vendor.*

*Gartner, "Market Guide for Network Traffic Analysis," by Lawrence Orans, Jeremy D'Hoinne, and Sanjit Ganguli. February 28, 2019.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

MITRE ATT&CK Category	Tactics, Techniques, and Procedures Covered by Reveal(x)
Initial Access	Drive-by Compromise, Exploit Public-Facing Application, Hardware Additions, Valid Accounts
Execution	Command-Line Interface, Dynamic Data Exchange, Graphical User Interface, PowerShell, Third-party Software, Windows Remote Management, Windows Management Instrumentation
Persistence	Browser Extensions, Create Account, External Remote Services, Logon Scripts, Netsh Helper DLL, Port Monitors
Privilege Escalation	Access Token Manipulation, Bypass User Account Control, Port Monitors, Web Shell
Defense Evasion	DCShadow, Exploitation for Defense Evasion, File Deletion, File Permissions Modification, Network Share Connection Removal, Web Service, Port Knocking
Credential Access	Account Manipulation, Brute Force, Credential Dumping, Credentials in Files, Exploitation for Credential Access, Forced Authentication, Input Prompt, Kerberoasting, LLMNR/NBT-NS Poisoning, Network Sniffing
Discovery	Application Window Discovery, Network Service Scanning, Network Share Discovery, File and Directory Discovery, Browser Bookmark Discovery, Password Policy Discovery, Permission Groups Discovery, Query Registry, Remote System Discovery, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Service Discovery, System Time Discovery
Lateral Movement	Application Deployment Software, Distributed Component Object Model, Exploitation of Remote Services, Logon Scripts, Pass the Hash, Pass the Ticket, Remote File Copy, Remote Desktop Protocol, Remote Services, Shared Webroot, SSH Hijacking, Taint Shared Content, Windows Admin Shares, Windows Remote Management
Collection	Data from Network Shared Drive, Data Staged, Automated Collection, Data from Information Repositories, Email Collection, Man in the Browser
Exfiltration	Automated Exfiltration, Data Transfer Size Limits, , Data Compressed, Data Encrypted, Exfiltration over Alternative Protocol, Exfiltration over Command & Control Channel, Scheduled Transfer
Command & Control	Commonly Used Port, Connection Proxy, Custom Command & Control Protocol, Custom Cryptographic Protocol, Data Encoding, Data Obfuscation, Domain Fronting, Fallback Channels, Multi Stage Channels, Multi-Hop Proxy, Multiband Communication, Multilayer Encryption, Port Knocking, Remote File Copy, Remote Access Tools, Standard Application Layer Protocol, Standard Cryptographic Protocol, Uncommonly Used Port, Standard Non-Application Layer Protocol, Web Service