EXTRAHOP™

WHITE PAPER

RevealX™ and the MITRE ATT&CK® Framework

How RevealX Differentiators Fuel Breadth and Depth of MITRE ATT&CK Coverage

For security teams looking to take a structured, proactive approach to cybersecurity, the MITRE ATT&CK Matrix for Enterprise has become the industry standard since its introduction in 2013. The collection of adversarial tactics, techniques, and procedures (TTPs) constitutes an assessment framework that organizations can use to benchmark their security operations. Furthermore, the collective body of knowledge has, in many ways, come to serve as a *de facto* industry reference guide for security professionals.

However, in the effort to create a widely applicable framework that's easy to understand, MITRE sometimes identifies a single data source–such as scanning results, process monitoring, or sensor telemetry–for detecting certain techniques, when other data sources may also detect those same techniques. For example, MITRE identifies 60 techniques in the ATT&CK framework that it deems network addressable, meaning they can be detected using network data. But ExtraHop® verified via its own tests and via a third-party 51 additional techniques that can also be detected using network data, including brute force, traffic signaling, resource hijacking, and many others.

The danger, then, for organizations taking the techniques that MITRE defines as network addressable as gospel is that they may not realize other tools in their cyber defense arsenal are capable of detecting these techniques, and therefore, they may miss out on detections and mitigations.

This white paper provides a technical overview of how the ExtraHop RevealX network detection and response platform not only detects and enables investigation of a broad range of "network-addressable" TTPs cataloged by MITRE ATT&CK, but is capable of uncovering further TTPs using network data that are not documented in the framework. It serves to demonstrate the breadth and depth of ATT&CK framework coverage that RevealX can provide, above and beyond other NDR providers in the marketplace.

Table of Contents

What Is the MITRE ATT&CK Framework?

MITRE ATT&CK is a globally accessible knowledge base of TTPs that cybersecurity researchers have observed in attacks attributed to advanced persistent threats (APTs) and less sophisticated actors around the world.

The ATT&CK framework describes how adversaries penetrate networks, move laterally, escalate their privileges, and evade organizations' defenses. It looks at the technical goals adversaries are trying to achieve, articulated as 14 high-level tactics, and the methods (or techniques) they use to achieve those objectives. The framework currently catalogs 234 techniques across 14 tactics.

Organizations of all sizes and security maturity levels can use the framework to understand how different adversaries tend to launch and execute attacks, so that they can plan how to detect, hunt for, and stop those behaviors, as well as identify gaps in their security coverage.

What Is Network Detection & Response (NDR)?

Network detection and response (NDR) solutions ingest network traffic, then apply machine learning and behavioral analysis to monitor for security risks, identify exposure, and detect malicious activities. Security teams can leverage NDR for a wide variety of use cases, from stopping in-progress attacks before they result in data theft or business disruption, to inventorying and classifying all of the devices communicating on their network. By definition, NDR solutions must also perform traffic decryption and protocol parsing in order to detect and investigate adversary behavior and associated TTPs. These solutions may also sometimes be categorized as network analytics and visibility (NAV), but the required capabilities remain the same.

Because the RevealX NDR platform is passive, operates in real time, and is able to see transaction payloads and decrypt traffic, it is the ideal solution for detecting the TTPs listed in this paper, often without adversaries even knowing they are being watched.

There's No XDR Without NDR

Extended detection and response (XDR) is a strategy that integrates NDR, endpoint detection and response (EDR), security information and event management (SIEM), and other security products into a cohesive security operations system. XDR collects threat data from previously siloed security tools across the network, cloud workloads, email, endpoints, log data, and more, so SOC teams can prioritize, investigate, and respond to incidents quickly and efficiently.

NDR complements EDR and log-based solutions by covering unmanaged devices and those that cannot be instrumented with an EDR agent. According to research from ExtraHop, fewer than 50% of assets in an enterprise have EDR coverage. In addition, NDR resists counter-incident-response (IR) activities and defense evasion techniques used by attackers who target the endpoint agent itself, or disable logging processes that would feed a SIEM or other correlation engine. EDR tools also miss activities that RevealX sees, like red team tests and protocol tunneling. So even if your organization has an EDR solution that addresses some of these same TTPs, you would still benefit from RevealX.

How RevealX Enables MITRE ATT&CK Coverage

RevealX fills visibility gaps and provides investigative coverage right out of the box for 126 techniques across 12 of the 14 MITRE ATT&CK framework tactics: Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Exfiltration, Command and Control (C2), and Impact. No special configuration or integrations are needed to get this coverage from RevealX.

The platform provides especially strong coverage of late-stage TTP categories, with 89% coverage of the TTPs in the Lateral Movement, Command and Control, and Exfiltration stages, and 92% coverage of TTPs deemed network addressable.

Our breadth of coverage is demonstrated by the number of techniques RevealX is capable of addressing. Not only does RevealX detect 55 of the 60 techniques that MITRE deems network addressable, the platform also provides coverage for an additional 51 techniques that MITRE does not yet consider network addressable, and ExtraHop regularly develops and releases new detections and detectors. The additional techniques for which RevealX provides coverage but that MITRE does not consider network addressable have been independently verified and are italicized throughout the tables that follow. (20 of the techniques RevealX addresses apply to more than one tactic, so when you group those techniques by tactic and add them all up across the 12 tactics, you get 126 techniques, all of which are listed in Appendix A.)

Our depth of coverage is defined by the number of ways we have to detect each technique and the number of detectors RevealX offers out of the box, which you can see in the tables on the following pages.

The capabilities that differentiate RevealX and enable it to go above and beyond other NDR products in detecting and investigating MITRE ATT&CK techniques include:

- Out-of-band processing of network traffic up to 100 Gbps to ensure consistent performance with enterprise data volumes and to maintain the integrity of packet data.
- Advanced, strategic decryption capabilities that allow for parsing of more than 70 different protocols, including SSL/TLS 1.3, SMBv3, WIN-RM, and MS-RPC, and that result in higher fidelity detections and higher quality data for investigations–without relying on “man-in-the-middle” or “break-and-inspect” approaches.
- Access to packet-level transaction records, enabling rapid detections across data link, network, transport, and application OSI layers, with storage for the past 90 days.
- Metric- and behavioral-based detections driven by machine analysis of more than 5,000 different attributes to detect multiple variations of techniques and advanced attacks, like those that rely on the use of valid credentials.

RevealX MITRE ATT&CK Coverage by Category

Initial Access

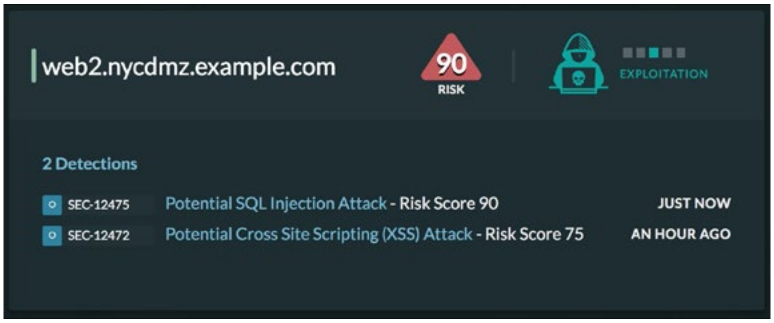
Following preliminary reconnaissance, attackers attempt to gain a foothold in the network without being detected. RevealX provides MITRE-recommended detection capabilities for the following initial access tactics:

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
External Remote Services	T1133	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. ExtraHop detects the malicious use of External Remote Services with the VPN Gateway Access from an Unusual Location detector.	10	Use of IP Spoofing, VPN Tunnel Hijacking, VPN Access from an Unusual Location, Man-In-The-Middle Attacks, Social Engineering/Phishing, Malware/Ransomware Attacks, Unauthorized Access via VPN Software Vulnerabilities, Dictionary and Brute-Force Attacks, Session Cookie Theft, Traffic Analysis
Exploit Public-Facing Application	T1190	Adversaries may attempt to exploit a weakness in an internet-facing host or system to initially access a network.	6	Exploitation of Public Facing Applications with the SQL Injection (SQLi) Attack, Outbound Log4Shell Activity, Log4Shell JNDI Injection Attempt by a Scanner, Shellshock HTTP Exploit Attempt by a Scanner, Shellshock DHCP Exploit Attempt, Log4Shell JNDI Injection Attempt
Valid Accounts	T1078	Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.	3	Anonymous FTP Auth Enabled, Anonymous FTP Login, Unusual LDAP Plaintext Authentication
Phishing	T1566	Adversaries may send phishing messages to gain access to victim systems.	10	Multiple Email Errors, Spike in Email Traffic Volume, HTTP Request to a Suspicious URL, HTTP Request to a Suspicious Host, DNS Request to a Suspicious Host, Outbound Connection to a Suspicious IP Address, SSL/TLS Connection to a Suspicious Host, Past Connection to a New Suspicious Domain, Past Connection to a New Suspicious IP Address, Sliver C&C Connection
Drive-by Compromise	*T1189*	*Adversaries may gain access to a system through a user visiting a website over the normal course of browsing.*	*8*	*HTTP Request to a Suspicious URI, HTTP Request to a Suspicious Host, DNS Request to a Suspicious Host, Suspicious HTTP File Received, Outbound Connection to a Suspicious IP Address, SSL/TLS Connection to a Suspicious Host, Past Connection to a New Suspicious Domain, and Past Connection to a New Suspicious IP Address*
Hardware Additions	*T1200*	*Adversaries may introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access.*	*1*	*New SSH Device*

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Supply Chain Compromise	*T1195*	*Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.*	*2*	*Kaseya VSA Activity, REvil Suspicious Connection (Kaseya Supply Chain)*



2 Detections

SEC-12475 Potential SQL Injection Attack - Risk Score 90 JUST NOW

SEC-12472 Potential Cross Site Scripting (XSS) Attack - Risk Score 75 AN HOUR AGO

RevealX analyzes SQL and HTTP payloads to detect exploits of public-facing applications.

Execution

Techniques that allow attackers to execute malicious code on hosts inside the target network. This step makes nearly every other step in the attack chain easier. Attackers may use this ability to pursue persistence, exfiltrate data, evade defenses, establish command and control channels, and more.

Many execution TTPs either rely on payloads that are delivered across the network, or rely on network-based remote management tools to execute malicious actions on compromised endpoints. RevealX is able to detect PowerShell, PSexec, Windows Management Instrumentation, and many other mechanisms often deployed by adversaries at this stage of an attack.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Scheduled Task/Job	T1053	Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code.	1	Scheduled Task Activity (ITaskSchedulerService)
Command and Scripting Interpreter	T1059	Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.	1	Unusual Interactive Traffic from an External Endpoint
Native API	T1106	Adversaries may interact with the native OS application programming interface (API) to execute behaviors.	1	BloodHound Enumeration Activity

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Inter-Process Communication	T1559	Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution.	1	SMB/CIFS Privileged Pipe
System Services	T1569	Adversaries may abuse system services or daemons to execute commands or programs.	3	Remote Service Launch, Database Takeover Attack, New WSMan Remote Administration Activity, Impacket SMBExec Activity
Windows Management Instrumentation	*T1047*	*Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads.*	*1*	*New WMI Method Launch*
Exploitation for Client Execution	*T1203*	*Adversaries may exploit software vulnerabilities in client applications to execute code.*	*1*	*Cross-Site Scripting (XSS) Attack*
User Execution	*T1204*	*An adversary may rely upon specific actions by a user in order to gain execution.*	*6*	*Request to External NFS Server, Unusual HTML Application (HTA) File Download, Unusual Executable File Download, Unusual Executable Script Download, Unusual Archive File Download, Sliver C&C Connection*

Persistence

Once an attacker has gained initial access, they commonly try to create mechanisms that will allow them to maintain access, or regain it through various channels, so that being discovered in any one channel doesn't end their entire operation.

Persistence activities frequently require communication across the network. This creates activity evidence that RevealX will record, detect, and alert on. Attackers may use the remote access capabilities established in the Initial Access step to transmit malware, insert code into local processes, or to gain access to legitimate remote access services such as VPNs or virtual desktop/thin client systems to maintain access to the target network through multiple channels.

Note: The following table listing ATT&CK techniques and RevealX detections represenst point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
External Remote Services	T1133	Adversaries may leverage external-facing remote services to initially access and/or persist within a network.	1	VPN Gateway Access from an Unusual Location
Create Account	T1136	Adversaries may create an account to maintain access to victim systems.	1	Unusual User Creation (in Windows and Active Directory Environments)
Create or Modify System Process	T1543	Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence.	2	Remote Registry Modification, New Windows Registry Modification Activity

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Server Software Component	T1505	Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems.	2	Unusual Interactive Traffic from an External Endpoint, SUPERNOVA Web Shell
Browser Extensions	*T1176*	*Adversaries may abuse internet browser extensions to establish persistent access to victim systems.*	*1*	*Command-and-Control Beaconing*
Boot or Logon Initialization Scripts	*T1037*	*Adversaries may use scripts automatically executed at boot or logon initialization to establish persistence.*	*1*	*Remote Registry Modification*

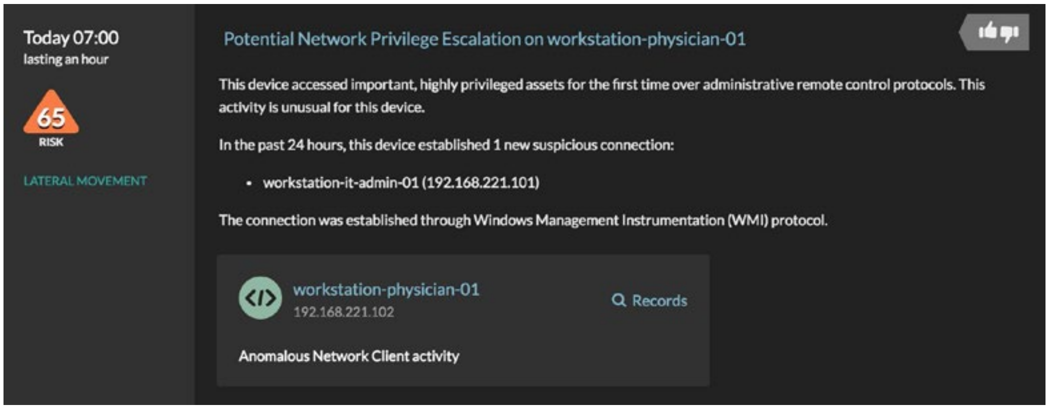
Privilege Escalation

Attackers often gain first access to a target network through a low-privilege user account. From there, they will attempt to either increase the privilege level of that account, or use that account to gain access to further accounts with administrative/root access privileges.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Exploitation for Privilege Escalation	T1068	Adversaries may exploit software vulnerabilities in an attempt to elevate privileges.	1	Exploitation for Privilege Escalation (e.g., CVE-2020-1301 SMBv1 exploit)
Event Triggered Execution	T1546	Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.	2	Remote Registry Modification, New Windows Registry Modification Activity
Boot or Logon Autostart Execution	T1547	Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.	3	Remote Registry Modification, New Windows Registry Modification Activity, File Transfer to Windows Autostart Path



Today 07:00
lasting an hour

65
RISK

LATERAL MOVEMENT

Potential Network Privilege Escalation on workstation-physician-01

This device accessed important, highly privileged assets for the first time over administrative remote control protocols. This activity is unusual for this device.

In the past 24 hours, this device established 1 new suspicious connection:

- workstation-it-admin-01 (192.168.221.101)

The connection was established through Windows Management Instrumentation (WMI) protocol.

workstation-physician-01
192.168.221.102

Records

Anomalous Network Client activity

RevealX builds privilege models for each device on the network to identify privilege escalation activity in real time.

Defense Evasion

Attackers are aware of common controls and countermeasures that may be in place on target networks and will work proactively to evade them, including concealing their activity afterwards.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Obfuscated Files or Information	T1027	Adversaries may obfuscate data in order to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit.	1	SUPERNOVA web shell
BITS Jobs	T1197	Adversaries may abuse Windows Background Intelligent Transfer Service (BITS) to persistently execute code and perform various background tasks.	1	BITS Download
System Binary Proxy Execution	T1218	Adversaries may bypass process and/or signature-based defenses by proxying execution of malicious content with signed, or otherwise trusted, binaries.	5	Unusual HTML Application (HTA) File Download, Koadic C&C Stager Connection, Koadic C&C Beaconing Activity, Koadic C&C Implant Activity, Remote Service Launch Attempt to Run a LOLBAS
Hijack Execution Flow	T1574	Adversaries may execute their own malicious payloads by hijacking the way operating systems run programs.	1	IP Exploit Attempt (e.g., hijacking TCP/IP execution flow)
Exploitation for Defense Evasion	*T1211*	*Adversaries may exploit a system or application vulnerability to bypass security features.*	*1*	*CVE-2022-0543 Redis Exploit*

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Indicator Removal	*T1070*	*Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses.*	*1*	*Remote Log Deletion*
Modify Registry	*T1112*	*Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution.*	*3*	*Windows Registry Enumeration, Remote Registry Modification, New Windows Registry Modification Activity*
Trusted Developer Utilities Proxy Execution	*T1127*	*Adversaries may take advantage of trusted developer utilities for proxy execution of malicious payloads.*	*1*	*CVE-2020-6207 SAP Solution Manager Exploit Attempt*
Rogue Domain Controller	*T1207*	*Adversaries may register a rogue Domain Controller to enable manipulation of Active Directory data.*	*1*	*DCShadow Activity (based on MSRPC traffic)*
Impair Defenses	*T1562*	*Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms.*	*3*	*Overlapping IP Fragmentation, Remote Registry Modification, New Windows Registry Modification*
Network Boundary Bridging	*T1599*	*Adversaries may bridge network boundaries by compromising perimeter network devices or internal devices responsible for network segmentation.*	*1*	*Unconventional Internal Connection*
Build Image on Host	*T1612*	*Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry.*	*1*	*Unconventional External Connection*

Credential Access

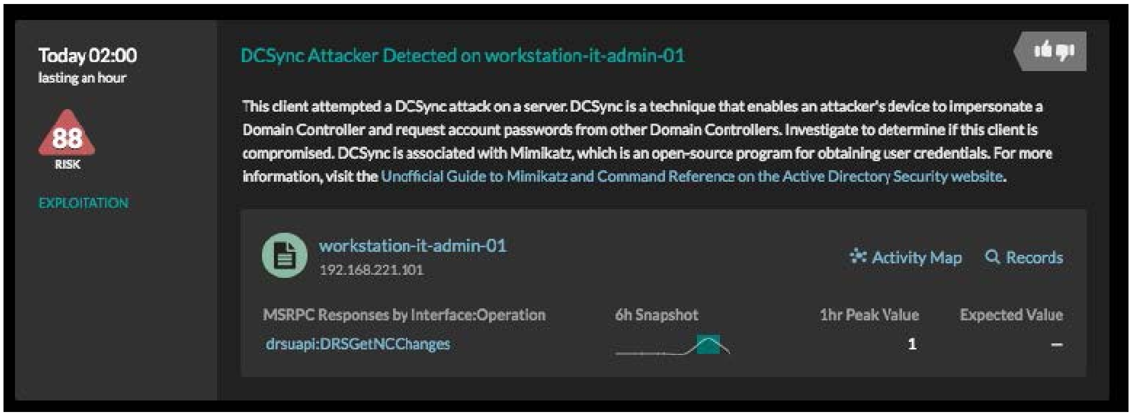
Accessing and abusing legitimate credentials is a standard procedure for attackers.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
OS Credential Dumping	T1003	Credential Dumping is a common method used by attackers to retrieve credential material, which can enable later steps of the attack chain.	4	DCSync Activity, Impacket SecretsDump MMCExec Activity, Registry Hive Transfer Over SMB/CIFS, DPAPI Backup Key Export Attempt
Unsecured Credentials	T1552	Adversaries may search compromised systems to find and obtain insecurely stored credentials.	2	AWS Instance Metadata Service (IMDS) Proxy, Group Policy Preferences (GPP) Password Enumeration
Credentials from Password Stores	T1555	Adversaries may search for common password storage locations to obtain user credentials.	1	DPAPI Backup Key Export Attempt
Modify Authentication Process	T1556	Adversaries may modify authentication mechanisms and processes to access user credentials or enable otherwise unwarranted access to accounts.	1	Oracle WebLogic Exploit
Adversary-in-the-Middle	T1557	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique.	7	NBT-NS Poisoning, LLMNR Poisoning, New DHCP Activity, NTLM Relay Attack, NTLMv1 Authentication, NTLMv1 Authentication, Unusual NTLMv1 Authentication
Steal or Forge Kerberos Tickets	T1558	Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable Pass the Ticket attacks.	6	Unusual Kerberos Fingerprint, Weak Kerberos Encryption, Kerberos Silver Ticket Attack, Kerberos Golden Ticket Attack, AS-REP Roasting Activity, Kerberoasting Activity
Brute Force	*T1110*	*Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained.*	*7*	*SMB/CIFS Brute Force, RDP Brute Force, FTP Brute Force, Database Brute Force, WordPress Brute Force, Spike in AAA Failed Login Attempts, Unconventional SSH Behavior*
Network Sniffing	*T1040*	*Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network.*	*2*	*Unencrypted Zoom Data, LDAP Plaintext Authentication*

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Exploitation for Credential Access	*T1212*	*Adversaries may exploit software vulnerabilities in an attempt to collect credentials. ExtraHop detects exploitation of software vulnerabilities for credential collection with the HTTP Path Traversal Attempt detector.*	*1*	*HTTP Path Traversal Attempt*
Forced Authentication	*T1187*	*Adversaries may gather credential material by invoking or forcing a user to automatically provide authentication information through a mechanism that they can intercept.*	*1*	*New External SMB/CIFS Connection*



DCSync Attacker Detected on workstation-it-admin-01

This client attempted a DCSync attack on a server. DCSync is a technique that enables an attacker's device to impersonate a Domain Controller and request account passwords from other Domain Controllers. Investigate to determine if this client is compromised. DCSync is associated with Mimikatz, which is an open-source program for obtaining user credentials. For more information, visit the Unofficial Guide to Mimikatz and Command Reference on the Active Directory Security website.

workstation-it-admin-01
192.168.221.101

MSRPC Responses by Interface:Operation	6h Snapshot	1hr Peak Value	Expected Value
drsuapi:DRSGetNCChanges		1	–

RevealX analyzes MSRPC Responses to detect credential dumping activity, such as DCSync attacks.

Discovery

Discovery is the process an attacker goes through as they attempt to scan a target network to learn about its structure, where valuable data is kept, usernames, applications, and other information that a savvy attacker can use to navigate laterally and take actions on objectives.

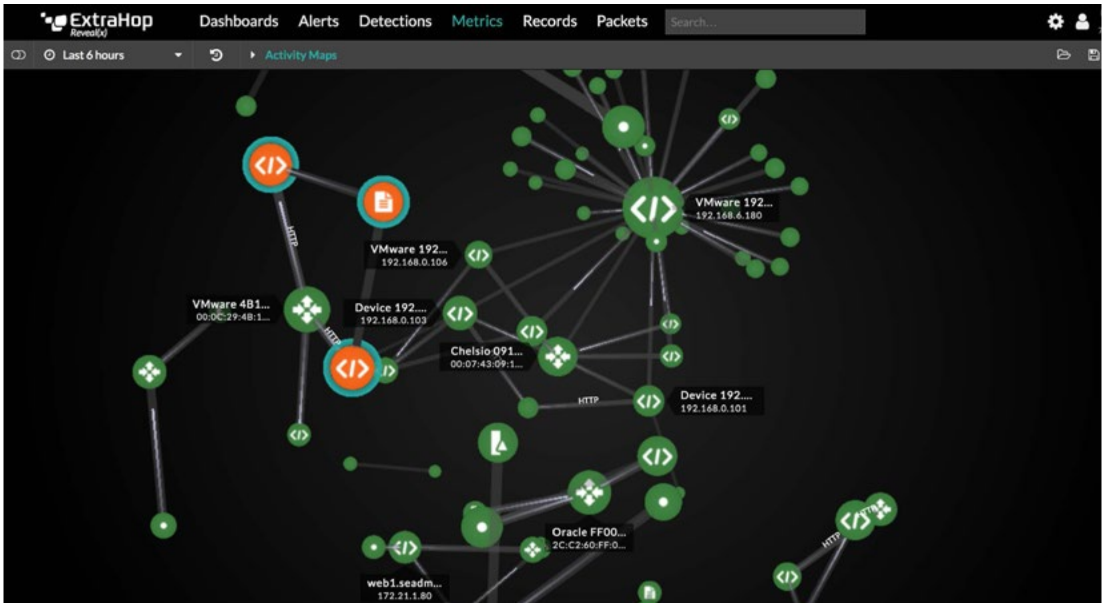
While many discovery activities are conducted directly on an endpoint, using local command line tools or other local utilities, these activities are also often conducted remotely in ways that require communication across a network. Since RevealX automatically discovers all assets communicating across the network, as well as identifying what type of asset they are and which protocols they're using to communicate, RevealX can often detect these activities when they are executed remotely.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Account Discovery	T1087	Adversaries may attempt to get a listing of valid accounts, usernames, or email addresses on a system or within a compromised environment.	7	LDAP SPN Scan, Kerberos User Enumeration, Windows Account Enumeration, Spike in LDAP Requests, Domain Admin Enumeration, AdFind Activity, Bloodhound Enumeration Activity
Query Registry	T1012	The registry contains a significant amount of information about the operating system, configuration, software, and security on a Windows machine. Attackers may remotely query the registry in order to enumerate information about a device.	1	Windows Registry Enumeration
System Network Configuration Discovery	T1016	Adversaries may look to enumerate details about the network configuration of systems they access or through information discovery of remote systems.	2	DNS Zone Transfer, AdFind Activity
System Network Connections Discovery	T1049	Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network.	1	RDP Session Enumeration
Domain Trust Discovery	T1482	Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments.	5	Domain Trusts Enumeration, Domain Trust Enumeration, BloodHound Enumeration Activity, Unusual LDAP Query Activity, AdFind Activity
Cloud Service Discovery	T1526	An adversary may attempt to enumerate the cloud services running on a system after gaining access.	1	AWS Cloud Service Enumeration

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Group Policy Discovery	T1615	Adversaries may gather information on Group Policy settings to identify paths for privilege escalation, security measures applied within a domain, and to discover patterns in domain objects that can be manipulated or used to blend in the environment.	2	LDAP GPO Enumeration, Unusual LDAP Query Activity
Network Service Discovery	*T1046*	*Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation.*	*1*	*TCP SYN Scan*
Network Share Discovery	*T1135*	*Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.*	*1*	*SMB/CIFS Share Enumeration*
File and Directory Discovery	*T1083*	*Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.*	*2*	*Web Directory Scan, Unconventional Internal Connection*
Password Policy Discovery	*T1201*	*Adversaries may attempt to access detailed information about the password policy used within an enterprise network or cloud environment.*	*2*	*BloodHound Enumeration Activity, New External NFS Connection*
Permission Groups Discovery	*T1069*	*An adversary may attempt to discover group and permission settings.*	*3*	*Windows Account Enumeration, Group Member Enumeration, Domain Group Enumeration*
Remote System Discovery	*T1018*	*Attackers might attempt to enumerate information about remote systems that can be used for later parts of the attack chain, such as lateral movement.*	*2*	*DNS Internal Reverse Lookup Scan, Domain Controller Enumeration*
System Owner/User Discovery	*T1033*	*Adversaries may attempt to enumerate one or more users associated with or actively using a computer.*	*1*	*Logged-On User Enumeration*
System Information Discovery	*T1082*	*An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.*	*2*	*Scheduled Task Enumeration, New WMI Enumeration Query*
Software Discovery	*T1518*	*Adversaries may attempt to get a listing of software and software versions that are installed on a system or in a cloud environment.*	*1*	*Web Directory Scan*



RevealX maps devices communicating on the network, automatically classifying them according to their observed role. Scanning activity can be easily discerned with these live activity maps.

Lateral Movement

The lateral movement phase of an attack is when the attacker moves outward from their original beachhead or compromised host and starts to locate valuable assets to steal or destroy. This may involve using the original compromised host to remotely access other devices in the network, steal admin credentials, or otherwise increase access to internal assets in the target network.

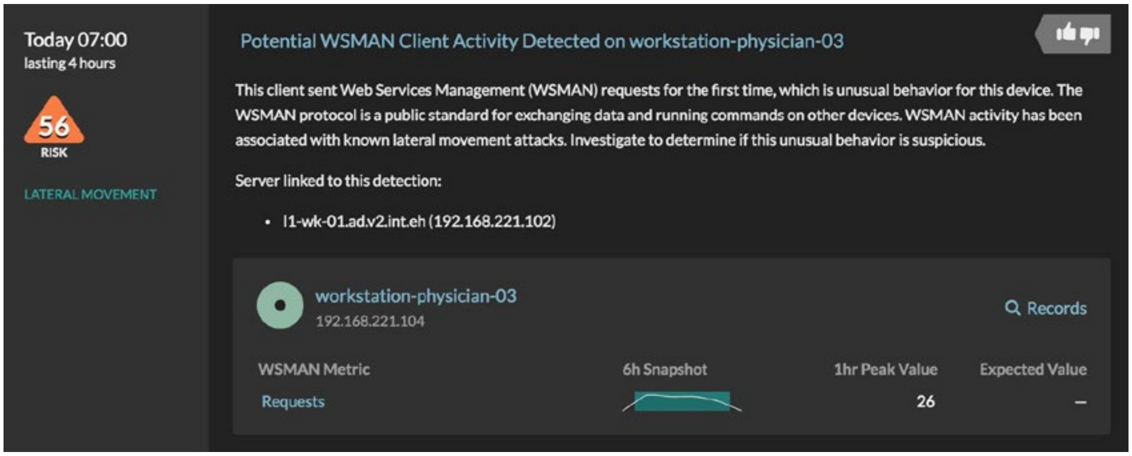
Because NDR focuses on analyzing internal traffic and detecting behavioral anomalies, it is well suited to detecting lateral movement.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Lateral Tool Transfer	T1570	Adversaries may transfer tools or other files between systems in a compromised environment.	5	Unusual SMB/CIFS Executable File Transfer, File Transfer to Windows Autostart Path, New SMB/CIFS Executable File Transfer, Cobalt Strike Beacon Transfer, Unusual Executable File Transfer
Taint Shared Content	T1080	Adversaries may deliver payloads to remote systems by adding content to shared storage locations, such as network drives or internal code repositories.	2	Unusual SMB/CIFS Executable File Transfer, New SMB/CIFS Executable File Transfer

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Use Alternate Authentication Material	T1550	Adversaries may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.	3	Kerberos Attack Tool Activity, Kerberos Silver Ticket Attack, Kerberos Golden Ticket Attack
Remote Services	*T1021*	*Adversaries might interact with remote services for many reasons such as exploitation or lateral movement.*	*3*	*Network Privilege Escalation, PowerShell Remoting Attempt, File Transfer to Windows Autostart Path*
Exploitation of Remote Services	*T1210*	*Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network.*	*10*	*Spike in VNC Sessions, Remote Service Launch, New WMI Method Launch, Spike in RDP Sessions, EternalBlue Exploit, HTTP Path Traversal Attempt, Unconventional Internal Connection, HTTP Desync Attack, New WMI Process Creation, Java Deserialization Exploit Attempt*



Potential WSMAN Client Activity Detected on workstation-physician-03

This client sent Web Services Management (WSMAN) requests for the first time, which is unusual behavior for this device. The WSMAN protocol is a public standard for exchanging data and running commands on other devices. WSMAN activity has been associated with known lateral movement attacks. Investigate to determine if this unusual behavior is suspicious.

Server linked to this detection:

- l1-wk-01.ad.v2.int.eh (192.168.221.102)

workstation-physician-03
192.168.221.104

WSMAN Metric	6h Snapshot	1hr Peak Value	Expected Value
Requests		26	–

RevealX detects suspicious use of remote management services such as WSMAN and PSexec.

Collection

The collection stage is when attackers begin accessing the data they plan to steal. This may involve moving the data into staging areas for exfiltration, copying data into more easily accessible locations, or establishing new paths to accessing data that will eventually be stolen.

Many, but not all TTPs in this stage involve moving data across the network in ways that would look suspicious to RevealX.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Data from Local System	T1005	Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.	1	CVE-2021-22991 F5 BIG-IP Exploit
Data from Information Repositories	T1213	Adversaries may leverage information repositories to mine valuable information before exfiltrating it.	2	Rare Database Table Access, Database Enumeration
Data from Cloud Storage	T1530	Adversaries may access data from cloud storage.	1	Unusual Download from S3 Bucket
Archive Collected Data	T1560	An adversary may compress and/or encrypt data that is collected prior to exfiltration. BloodHound is known to compress collected data into a zip file before exfiltrating it to be analyzed.	1	BloodHound Enumeration Activity
Data from Network Shared Drive	T1039	Adversaries may search network shares on computers they have compromised to find files of interest that can be exfiltrated at a later time.	1	Suspicious SMB/CIFS File Reads
Data Staged	*T1074*	*Adversaries may stage collected data in a central location or directory prior to Exfiltration.*	*6*	*Unconventional SSH Data Transfer, Suspicious NFS File Reads, Unconventional RDP Data Transfer, Unconventional SMB/CIFS Data Transfer, Unconventional Data Transfer, Unusual Download from S3 Bucket*
Email Collection	*T1114*	*Adversaries may target user emails to collect sensitive information.*	*2*	*Increase in Internal SMB/CIFS File Transfers, Increase in Internal Database Data Transfers*
Data from Configuration Repository	*T1602*	*Adversaries may collect data related to managed devices from configuration repositories.*	*1*	*SNMP Reconnaissance Activity*

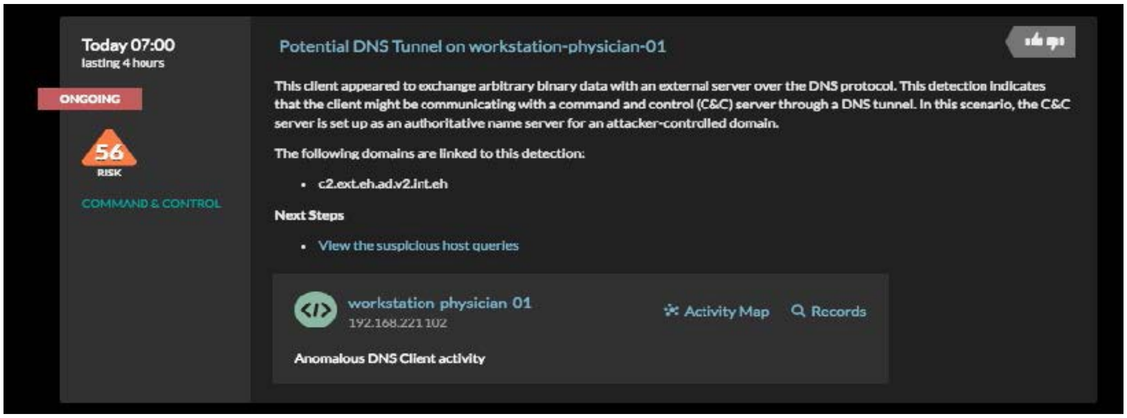
Command and Control (C2)

Command and Control is the stage when attackers cultivate channels for manipulating data and using compromised endpoints to expand their reach and establish a persistent toehold in the target network. This may involve installing malware on a compromised host that can execute commands on that host or control other rootkitted hosts on the network to coordinate attack activities across multiple hosts.

Many common C2 TTPs require communication across the network, often using common ports. With RevealX watching the traffic on those ports, it becomes much easier to detect C2 activity. For example, an attacker using a commonly open port for C2 may be transmitting using a protocol that is not usual for that port. By detecting which ports and protocols are in use and decrypting and analyzing the behavior patterns in this traffic, RevealX is able to detect C2 activity in spite of the many tactics adversaries have developed to cover their tracks.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.



Potential DNS Tunnel on workstation-physician-01

This client appeared to exchange arbitrary binary data with an external server over the DNS protocol. This detection indicates that the client might be communicating with a command and control (C&C) server through a DNS tunnel. In this scenario, the C&C server is set up as an authoritative name server for an attacker-controlled domain.

The following domains are linked to this detection:

- c2.ext.eh.ad.v2.int.eh

Next Steps

- View the suspicious host queries

Anomalous DNS Client activity

RevealX detects DNS tunneling activity, a subtle method that attackers use to hide their C2 communications.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Data Obfuscation	T1001	Adversaries may obfuscate command and control traffic or data within it to hide its meaning.	3	HTTP Tunnel, Command-and-Control Beaconing, DoublePulsar SMB/CIFS Implant Activity
Fallback Channels	T1008	Attackers may utilize one or more C2 channels to maintain redundant access to a victim's environment.	3	Unusual Interactive Traffic from a Remote Desktop, Remote Control SSH Traffic, SUNBURST C&C Activity
Non-Application Layer Protocol	T1095	Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network.	6	ICMP Tunnel, Unusual Protocol for Enterprise Software, Unusual Protocol Connection from a High Value Device, Unusual Host Connection from a High Value Device, Redline Stealer TCP Activity, ICMP Tunnel

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Multi-Stage Channels	T1104	Adversaries may create multiple stages for command and control that are employed under different conditions or for certain functions.	2	Command-and-Control Beaconing, Unusual Interactive Traffic from a Remote Desktop
Ingress Tool Transfer	T1105	Adversaries may transfer tools or other files from an external system into a compromised environment.	1	Suspicious FTP Download
Remote Access Software	T1219	An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks.	7	Unconventional VNC Behavior, New External RDP Connection, New External SSH Connection, Unusual Interactive Traffic from a Remote Desktop, Unusual Interactive Traffic from an External Endpoint, Remote Control SSH Traffic, New Remote Access Software Activity
Dynamic Resolution	T1568	Adversaries may dynamically establish connections to command and control infrastructure to evade common detections and remediations.	4	Domain Generation Algorithm, DGA Domain Queries, DGA Domain Resolution, SUNBURST C&C Activity
Encrypted Channel	T1573	Adversaries may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.	15	HTTP Request to a Suspicious Host, Outbound Connection to a Suspicious IP Address, Command-and-Control Beaconing, Unusual Interactive Traffic from a Remote Desktop, Unusual Interactive Traffic from an External Endpoint, Remote Control SSH Traffic, DoublePulsar SMB/CIFS Implant Activity, DoublePulsar RDP Implant, SSL/TLS Connection to a Suspicious Host, New DNS over HTTPS (DoH) Activity, SUNBURST C&C Activity, Confirmed OnePercent Group Ransomware IOC, Past Connection to a New Suspicious Domain, Past Connection to a New Suspicious IP Address, Sliver C&C Connection
Application Layer Protocol	*T1071*	*Adversaries may communicate using OSI application layer protocols to avoid detection/ network filtering by blending in with existing traffic.*	*2*	*SMB/CIFS Named Pipe Beaconing, Cobalt Strike DNS Beaconing*
Proxy	*T1090*	*Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure.*	*5*	*Domain Fronting, Inbound Tor Node Connections, Outbound Connection to a Tor Node, New Outbound SOCKS Connection, Inbound Connection from a Tor Node*
Web Service	*T1102*	*Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system.*	*1*	*Command-and-Control Beaconing*

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Data Encoding	*T1132*	*Adversaries may encode data to make the content of command and control traffic more difficult to detect.*	*1*	*Command-and-Control Beaconing*
Non-Standard Port	*T1571*	*Adversaries may communicate using a protocol and port pairing that are typically not associated.*	*10*	*Rare SSH Port, Non-standard HTTP Port, Command-and-Control Beaconing, Caldera C&C Sandcat Beaconing, Caldera C&C Ragdoll Beaconing, Caldera C&C Manx Beaconing, Koadic C&C Stager Connection, Koadic C&C Beaconing Activity, Koadic C&C Implant Activity, Emotet SSL/TLS Certificate*
Protocol Tunnelling	*T1572*	*Adversaries may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems.*	*6*	*Unusual Interactive Traffic from a Remote Desktop, Unusual Interactive Traffic from an External Endpoint, Remote Control SSH Traffic, Metasploit C&C SSL/TLS Connection, Meterpreter C&C Session, SessionManager Malware Activity*

Exfiltration

The Exfiltration stage is when attackers move data off of the target network. Attackers often try to hide this behavior by transferring small amounts of data over long periods of time and by using unexpected protocols and encrypted channels to transfer data.

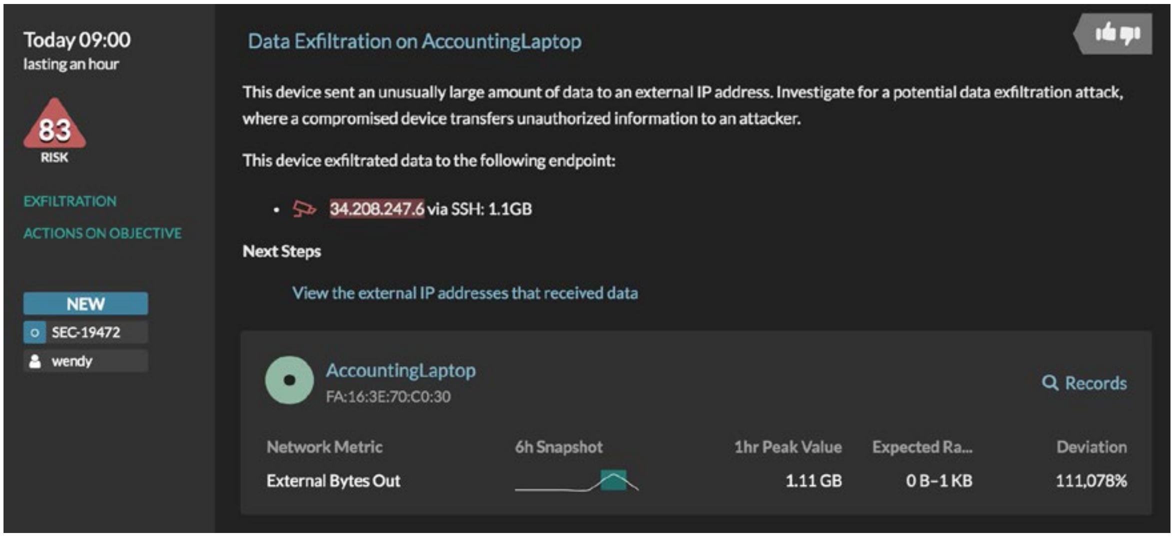
Exfiltration almost always involves sending data across the network, often to never-before-seen destinations. RevealX can detect when data transfers from inside the network to outside are occurring, and whether the protocols, traffic patterns, and even contents are suspicious.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Scheduled Transfer	T1029	Adversaries may schedule data exfiltration to be performed only at certain times of day or at certain intervals.	1	Data Exfiltration
Transfer Data to Cloud Account	T1537	Adversaries may exfiltrate data by transferring the data, including backups of cloud environments, to another cloud account they control on the same service to avoid typical file transfers/downloads and network-based exfiltration detection.	2	Data Exfiltration to Unknown S3 Bucket, Data Exfiltration to S3 Bucket

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Exfiltration over Web Service	T1567	Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.	5	Data Exfiltration, Data Exfiltration to Unknown S3 Bucket, Data Exfiltration to S3 Bucket, Unusual Sensitive Data Transfer, Rclone File Upload to MEGA
Exfiltration over Other Network Medium	*T1011*	*Adversaries may choose to exfiltrate data over a separate network medium than the primary command and control channel.*	*1*	*Data Exfiltration*
Automated Exfiltration	*T1020*	*Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.*	*1*	*Unusual Sensitive Data Transfer*
Data Transfer Size Limits	*T1030*	*An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds.*	*1*	*DNS Tunnel*
Exfiltration over Command and Control Channel	*T1041*	*Adversaries may steal data by exfiltrating it over an existing command and control channel.*	*1*	*Data Exfiltration*
Exfiltration over Alternative Protocol	*T1048*	*Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.*	*1*	*Increase in Internal Database Data Transfers*


Today 09:00
lasting an hour

83
RISK

EXFILTRATION
ACTIONS ON OBJECTIVE

NEW
SEC-19472
wendy

Data Exfiltration on AccountingLaptop

This device sent an unusually large amount of data to an external IP address. Investigate for a potential data exfiltration attack, where a compromised device transfers unauthorized information to an attacker.

This device exfiltrated data to the following endpoint:

- 34.208.247.6 via SSH: 1.1GB

Next Steps

View the external IP addresses that received data

AccountingLaptop
FA:16:3E:70:C0:30

Records

Network Metric	6h Snapshot	1hr Peak Value	Expected Ra...	Deviation
External Bytes Out		1.11 GB	0 B–1 KB	111,078%

RevealX automatically detects data exfiltration by analyzing network connections and applying behavioral analysis and matching known-bad IPs against threat intelligence feeds.

Impact

This category represents “techniques whose primary objective directly reduces the availability or integrity of a system, service, or network.” According to MITRE, these techniques “may represent an adversary’s end goal, or provide cover for a breach of confidentiality.” Essentially, these techniques are at the far-right end of the attack chain, and their occurrence is highly likely to affect business or operations. Of the 14 techniques added to the MITRE ATTACK Framework in this category, three are well suited to detection via network traffic analysis.

Note: The following table listing ATT&CK techniques and RevealX detections represents point-in-time coverage. ExtraHop releases cloud-updated detectors weekly in response to novel attacks and new attack variants, so our coverage of the ATT&CK framework continues to expand.

Tactics covered by RevealX that are not yet recognized by MITRE as network-addressable are in italics.

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Data Destruction	T1485	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources.	2	Suspicious SMB/CIFS File Share Access, Database Data Deletion Activity
Inhibit System Recovery	T1490	Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.	2	Kaseya VSA Activity, REvil Suspicious Connection (Kaseya Supply Chain)
System Shutdown/ Reboot	T1529	Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems.	1	Remote System Shutdown
Account Access Removal	T1531	Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users.	3	LDAP Invalid Credentials Error, Kerberos Revoked Credentials Errors, Kerberos Wrong Password Errors
Data Encrypted for Impact	*T1486*	*Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.*	*5*	*Ransomware Activity, Suspicious SMB/CIFS File Share Access, Kaseya VSA Activity, REvil Suspicious Connection (Kaseya Supply Chain), Confirmed OnePercent Group Ransomware IOC*
Resource Hijacking	*T1496*	*Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability.*	*3*	*Cryptocurrency Mining, DNS Request for a Cryptocurrency Mining Pool, SSL/TLS Connection to a Cryptocurrency Mining Pool*
Network Denial of Service	*T1498*	*Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users.*	*14*	*DNS Timeouts, Delayed Citrix Data Transfer, Delayed Data Transfer, Delayed Email Data Transfer, Stalled Data Transfer, Delayed Database Data Transfer, Delayed Redis Data Transfer, Delayed LDAP Data Transfer, Delayed HTTP Data Transfer, DNS Request Timeouts, Delayed Kerberos Data Transfer, Interrupted Citrix Data Transfer, HTTP Gateway Timeout Error, Delayed Memcache Data Transfer*

Technique	ID	Definition	Associated Detectors in RevealX	Detections
Endpoint Denial of Service	*T1499*	*Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users.*	*13*	*Overwhelmed HTTP Data Transfer, Overwhelmed FTP Data Transfer, Overwhelmed LDAP Data Transfer, DNS Timeouts, Overwhelmed Data Transfer, Overwhelmed Email Data Transfer, Overwhelmed Memcache Data Transfer, Overwhelmed Database Data Transfer, Overwhelmed Citrix Data Transfer, DNS Request Timeouts, Overwhelmed Kerberos Data Transfer, Overwhelmed Redis Data Transfer, HTTP Gateway Timeout Error*

Conclusion

As you can see, RevealX offers broad coverage across a wide range of TTPs in the MITRE ATT&CK framework, and numerous ways to detect adversary behavior. The platform provides especially strong coverage of late-stage TTP categories, with 89% coverage of the TTPs in the Lateral Movement, Command and Control, and Exfiltration stages, and 92% coverage of TTPs deemed network addressable.

RevealX detects more MITRE ATT&CK TTPs with fewer false positives because it performs full-stream reassembly of L7 transactions at scale, real-time TLS 1.3 decryption, and offers guided investigations featuring direct links to relevant ATT&CK TTP listings. This accelerates mean-time-to-detect, investigate, and respond.

Although the MITRE ATT&CK Framework is currently quite endpoint focused, our assessment is that RevealX can at a minimum provide telemetry to security teams, even as it often also provides alerts and enrichment for many of the TTPs listed in this paper on their behavior and actions on the network. Representing defense-in-depth for endpoint solutions and incremental detection to offset typical blind spots and gaps in network security, this powerful visibility and detection linked to our guided investigations will help RevealX play a crucial role in your security architecture.

Appendix A: RevealX Coverage Matrix

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

MITRE ATT&CK Category	Techniques for Which RevealX Provides Detection, Telemetry, or Enrichment
Initial Access	1. Exploit Public-Facing Application (T1190) 2. External Remote Services (T1133) 3. Phishing (T1566) 4. Valid Accounts (T1078) *5. Hardware Additions (T1200)* *6. Supply Chain Compromise (T1195)* *7. Drive-by Compromise (T1189)*
Execution	1. Scheduled Task/Job (T1053) 2. Command and Scripting Interpreter (T1059) 3. Native API (T1106) 4. Inter-Process Communication (T1559) 5. System Services (T1569) *6. Exploitation for Client Execution (T1203)* *7. User Execution (T1204)* *8. Windows Management Instrumentation (T1047)*
Persistence	1. Scheduled Task/Job (T1053) 2. Valid Accounts (T1078) 3. External Remote Services (T1133) 4. Create Account (T1136) 5. BITS Jobs (T1197) 6. Server Software Component (T1505) 7. Create or Modify System Process (T1543) 8. Event Triggered Execution (T1546) 9. Boot or Logon Autostart Execution (T1547) 10. Modify Authentication Process (T1556) 11. Hijack Execution Flow (T1574) *12. Boot or Logon Initialization Scripts (T1037)* *13. Browser Extensions (T1176)* *14. Traffic Signaling (T1205)*
Privilege Escalation	1. Scheduled Task/Job (T1053) 2. Exploitation for Privilege Escalation (T1068) 3. Valid Accounts (T1078) 4. Create or Modify System Process (T1543) 5. Event Triggered Execution (T1546) 6. Boot or Logon Autostart Execution (T1547) 7. Hijack Execution Flow (T1574) *8. Boot or Logon Initialization Scripts (T1037)*

Appendix A: RevealX Coverage Matrix, Cont.

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

MITRE ATT&CK Category	Techniques for Which RevealX Provides Detection, Telemetry, or Enrichment
Defense Evasion	1. Obfuscated Files or Information (T1027) 2. Valid Accounts (T1078) 3. BITS Jobs (T1197) 4. System Binary Proxy Execution (T1218) 5. Use Alternate Authentication Material (T1550) 6. Modify Authentication Process (T1556) 7. Hijack Execution Flow (T1574) *8. Indicator Removal (T1070)* *9. Modify Registry (T1112)* *10. Trusted Developer Utilities Proxy Execution (T1127)* *11. Traffic Signaling (T1205)* *12. Rogue Domain Controller (T1207)* *13. Exploitation for Defense Evasion (T1211)* *14. Impair Defenses (T1562)* *15. Network Boundary Bridging (T1599)* *16. Build Image on Host (T1612)*
Credential Access	1. OS Credential Dumping (T1003) 2. Unsecured Credentials (T1552) 3. Credentials from Password Stores (T1555) 4. Modify Authentication Process (T1556) 5. Adversary-in-the-Middle (T1557) 6. Steal or Forge Kerberos Tickets (T1558) *7. Network Sniffing (T1040)* *8. Brute Force (T1110)* *9. Forced Authentication (T1187)* *10. Exploitation for Credential Access (T1212)*

Appendix A: RevealX Coverage Matrix, Cont.

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

MITRE ATT&CK Category	Techniques for Which RevealX Provides Detection, Telemetry, or Enrichment
Discovery	1. Query Registry (T1012) 2. System Network Configuration Discovery (T1016) 3. System Network Connections Discovery (T1049) 4. Account Discovery (T1087) 5. Domain Trust Discovery (T1482) 6. Cloud Service Discovery (T1526) 7. Group Policy Discovery (T1615) *8. Remote System Discovery (T1018)* *9. System Owner/User Discovery (T1033)* *10. Network Sniffing (T1040)* *11. Network Service Discovery (T1046)* *12. Permissions Groups Discovery (T1069)* *13. System Information Discovery (T1082)* *14. File and Directory Discovery (T1083)* *15. Network Share Discovery (T1135)* *16. Password Policy Discovery (T1201)* *17. Software Discovery (T1518)*
Lateral Movement	1. Taint Shared Content (T1080) 2. Use Alternate Authentication Material (T1550) 3. Lateral Tool Transfer (T1570) 4. Remote Service Session Hijacking (T1563) *5. Exploitation of Remote Services (T1210)* *6. Remote Services (T1021)*
Collection	1. Data from Local System (T1005) 2. Data from Information Repositories (T1213) 3. Data from Cloud Storage (T1530) 4. Adversary-in-the-Middle (T1557) 5. Archive Collected Data (T1560) *6. Data from Network Shared Drive (T1039)* *7. Data Staged (T1074)* *8. Email Collection (T1114)* *9. Data from Configuration Repository (T1602)*

Appendix A: RevealX Coverage Matrix, Cont.

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

MITRE ATT&CK Category	Techniques for Which RevealX Provides Detection, Telemetry, or Enrichment
Command and Control	1. Data Obfuscation (T1001) 2. Fallback Channels (T1008) 3. Non-Application Layer Protocol (T1095) 4. Multi-Stage Channels (T1104) 5. Ingress Tool Transfer (T1105) 6. Remote Access Software (T1219) 7. Dynamic Resolution (T1568) 8. Encrypted Channel (T1573) *9. Application Layer Protocol (T1071)* *10. Proxy (T1090)* *11. Web Service (T1102)* *12. Data Encoding (T1132)* *13. Traffic Signaling (T1205)* *14. Non-Standard Port (T1571)* *15. Protocol Tunneling (T1572)*
Exfiltration	1. Scheduled Transfer (T1029) 2. Transfer Data to Cloud Account (T1537) 3. Exfiltration over Web Service (T1567) *4. Exfiltration over Other Network Medium (T1011)* *5. Automated Exfiltration (T1020)* *6. Data Transfer Size Limits (T1030)* *7. Exfiltration over C2 Channel (T1041)* *8. Exfiltration over Alternative Protocol (T1048)*
Impact	1. Data Destruction (T1485) 2. Inhibit System Recovery (T1490) 3. System Shutdown/Reboot (T1529) 4. Account Access Removal (T1531) *5. Data Encrypted for Impact (T1486)* *6. Resource Hijacking (T1496)* *7. Network Denial of Service (T1498)* *8. Endpoint Denial of Service (T1499)*

Appendix B: TTP Coverage Enabled by Decryption

In some cases, decrypting traffic makes the difference in whether you can confidently detect a particular TTP in action. Here are a few examples of TTPs that RevealX excels at detecting, where other vendors cannot, because RevealX decrypts traffic for analysis.

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

ATT&CK TTP	Why Layer 7 Visibility & Decryption Matter
SQL Injection (See T1190, Exploit Public-Facing Application)	SQL Injection involves transmitting SQL commands via user input fields transmitted across HTTPS. An NDR tool that cannot decrypt will only see a totally legitimate-looking transaction. RevealX, by decrypting the traffic, can see that a user has typed a SQL command into the input box instead of the intended content such as their username or password.
Kerberos Golden Ticket (T1078)	Kerberos implements its own encryption mechanism and should be configured to leverage TLS as a means of ensuring the security of data as it traverses the network. Without this protocol, user credentials and authentication tickets sent across the network are vulnerable to eavesdropping attackers. Active Directory (AD) services (from printers to production servers) rely on these protocols to authenticate and authorize users, meaning that most connections between AD-joined clients and servers in modern Windows networks should be encrypted. A golden ticket is a forged ticket-granting ticket (TGT) that provides an attacker with unlimited access to an entire AD domain. RevealX detects golden ticket attacks by automatically checking the Kerberos requests for TGS tickets (TGS_REG) sent over the network that include indicators of a forged TGT, when Domain Controller-assisted decryption is enabled.
Kerberos Silver Ticket (T1078)	Every domain controller (DC) in an AD domain has a Kerberos Key Distribution Center (KDC) service for issuing ticket-granting tickets (TGTs) and a ticket-granting service (TGS) service for creating TGS tickets. These tickets act as a cryptographic proof of identity. A user must have valid TGT and TGS tickets to access services such as file shares and printers. A valid TGS ticket is encrypted with a service account key. If an attacker manages to steal a service account key, the attacker can bypass the TGS to create a forged TGS ticket, which is known as a silver ticket. A silver ticket is created by running a command in a Windows exploit tool, such as Mimikatz or Impacket. The silver ticket is encrypted with the stolen account key and might include fake domain administrator credentials. When the attacker wants to access a service, they send a Kerberos AP_REQ message with the silver ticket to the service. The service trusts the silver ticket and gives access to the attacker posing as a domain administrator. RevealX detects silver ticket attacks by automatically checking for AP_REQ in the Kerberos message type sent over the network that include indicators of a forged TGS ticket, when Domain Controller-assisted decryption is enabled.

Appendix B: TTP Coverage Enabled by Decryption, Cont.

In some cases, decrypting traffic makes the difference in whether you can confidently detect a particular TTP in action. Here are a few examples of TTPs that RevealX excels at detecting, where other vendors cannot, because RevealX decrypts traffic for analysis.

Note: TTPs for which RevealX provides coverage, but are not considered network-addressable by MITRE, are in italics.

ATT&CK TTP	Why Layer 7 Visibility & Decryption Matter
Brute Force (T1110)	*Brute force attacks across the network create a large number of transactions that can be detected. However, in large, high-traffic environments, that may not be enough of a signal to trigger an alarm. By decrypting the traffic for analysis, RevealX is able to detect brute force attacks more confidently by looking at transaction details, rather than just transaction volume used by many tools.*
Drive-by Compromise (T1189)	*RevealX is able to detect and alert on cross-site scripting, a common mechanism for delivering malicious code in a drive-by compromise.*
CVE-2023-3519 Citrix NetScaler ADC and NetScaler Gateway Exploit Attempt (T1210 - *Exploitation of Remote Service* & T1190 - Exploit Public Facing Application)	The Citrix products, NetScaler Application Delivery Controller (formerly Citrix ADC), and NetScaler Gateway (formerly Citrix Gateway), have an HTTPS web application that includes a DoS and remote code execution (RCE) vulnerability. An unauthenticated attacker sends a malicious HTTP request to the victim. This request includes a path that ends with /gwtest/formssso. The request also includes query parameters with two specific key-value pairs: The event key is paired with the start value and the target key is paired with a malicious payload. The payload content is tailored to the specific version and desired outcome. If HTTPS is enabled on the device, which is highly likely, SSL/TLS decryption via RevealX is required to inspect the path and payload in the attacker's malicious HTTPS request.
CVE-2023-46747 F5 BIG-IP Exploit Attempt (T1210 & T1190)	CVE-2023-46747 is an authentication bypass vulnerability that affects the Traffic Management User Interface (TMUI) in the F5 BIG-IP system. Unauthenticated attackers can exploit this vulnerability and gain full administrator privileges, leading to full remote code execution. After initial exploitation of CVE-2023-46747, an attacker could send an HTTP POST request to the /mgmt/tm/util/bash endpoint to run commands as the newly created administrative user. RevealX detects attempts to smuggle a malicious AJP message within an HTTP POST request through the vulnerable TMUI endpoint. If HTTPS is enabled on devices, which is highly likely, SSL/TLS decryption via RevealX is required to inspect the POST requests.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at **extrahop.com**.

EXTRAHOP™

info@extrahop.com
extrahop.com