WHITEPAPER

Attivo NETWORKS®

ATTIVO NETWORKS® THREATDEFEND® PLATFORM AND THE MITRE ATT&CK MATRIX

INTRODUCTION

The MITRE Corporation Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) Matrix provides a model for cyber adversary behavior, reflecting various phases of an adversary's lifecycle and the platforms they are known to target. Initiated five years ago, it is designed to help determine which technologies work or fail, identify gaps to improve security posture and processes, prioritize work on detecting and deterring techniques, and to evaluate new security technology. ATT&CK is useful for understanding security risk against known adversary behavior, planning security improvements, and verifying defenses work as expected. The goal of ATT&CK is to break down and classify attacks in a consistent and clear manner that can make it easier to compare them to find how the attacker exploited networks and endpoints in a successful compromise. More information is available at https://attack.mitre.org/wiki/.

THE ATT&CK MATRIX

ATT&CK for Enterprise is an adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network. The model can be used to characterize and describe post-compromise adversary behavior better. It both expands the knowledge of network defenders and assists in prioritizing network defense by detailing the tactics, techniques, and procedures (TTPs) cyber threats use to gain access and execute their objectives while operating inside a network.

ATT&CK for Enterprise is an adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network.

The 12 tactics categories within ATT&CK for Enterprise were derived from the later stages of the Lockheed Martin Cyber Kill Chain® (Exploit, Control, Execute, Maintain). These are:

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control
- Impact

Each category contains a list of techniques that an adversary could use to perform that tactic. Techniques are broken down to provide a technical description, indicators, useful defensive sensor data, detection analytics, and potential mitigations. Applying intrusion data to the model helps focus defense on the commonly used techniques across groups of activity and helps identify gaps in security.

ATT&CK for Enterprise incorporates details from multiple operating system platforms commonly found within enterprise networks, including Microsoft Windows, macOS, and Linux. ATT&CK provides a matrix for each of these systems, as well as a separate matrix for mobile systems. The framework and higher-level categories may also apply to other platforms and environments.

There is also a PRE-ATT&CK Matrix that covers the early stages of the Lockheed Martin Cyber Kill Chain (Recon, Weaponize, Deliver). This matrix is a growing common reference for pre-compromise techniques that brings greater awareness of what actions may be seen prior to a network intrusion. It enables a comprehensive evaluation of computer network defense (CND) technologies, data, processes, and policies against a common enterprise threat model. It is based on publicly available and submitted data, and not meant to be comprehensive.

> Deception Technology is a powerful threat detection mechanism that bridges gaps left open and exploitable by attackers when adversaries successfully penetrate a perimeter defense.

ATTIVO NETWORKS SUPPORT FOR THE MITRE ATT&CK MATRIX

The Attivo Networks ThreatDefend® Deception and Response Platform provides extensive capabilities to detect many of the techniques outlined in the ATT&CK Matrix. It includes the Attivo BOTsink® Deception server, ThreatStrike® Endpoint Deception Suite, ThreatPath® Visibility solution, DecoyDocs for Data Loss Tracking, and ThreatOps® Incident Response Playbooks.

With the most comprehensive deception solution covering the widest attack surfaces, the ThreatDefend Platform efficiently and accurately detects attackers already inside the network, early in the attack cycle through network, endpoint, application, and data decoys. These deceptions project onto user networks, datacenters, and specialized environments such as ICS-SCADA, IoT, or POS, whether on-premises, in the cloud, or at remote or branch offices. The platform automatically learns the environment and crafts mirror-match decoys for the highest authenticity.

The Attivo Networks solution is easy to deploy and operate, requiring little effort to manage, while providing unparalleled visibility to credential-based attacks, Man-in-the-Middle activity, Active Directory attacks, reconnaissance, and attacker lateral movement. It can detect known and unknown attacks with engagement-based, forensic-backed alerts that reduce mean-time-to-detect with high fidelity and accuracy. The platform's numerous third-party integrations reduce mean-time-to-respond, accelerating the incident response process while providing offense-based intelligence for a proactive defense.

In evaluating the ThreatDefend Platform against the ATT&CK Matrix, Attivo Networks compared the solution against the techniques to identify how it would detect each one for initial compromise. The table below contains the analysis as of Q3 2019, mapping to the techniques the ThreatDefend Platform can successfully detect and how it can detect each.

PRIVILEGE ESCALATION	
File System Permissions Weakness	The Attivo ThreatPath solution can detect if attackers replace legitimate service binaries with malicious binaries.
Path Interception	The Attivo ThreatPath solution detects if the attacker starts services exploiting path interception.
Service Registry Permissions Weakness	The Attivo ThreatPath solution detects endpoints that can be targeted by attackers who can exploit such weaknesses in service registry permissions.

LATERAL MOVEMENT	
AppleScript	The ThreatStrike Suite and BOTsink appliance decoys can detect lateral movement when performed using Apple scripts against the decoys.
Application Deployment Software	BOTsink appliance decoys can deploy as part of the enterprise domain and add to software deployment systems. The BOTsink appliance detects malicious code deployment on decoys added to an enterprise software distribution system.
Distributed Component Object Model	The BOTsink appliance allows for loading custom images with Office software installed as decoys. Customers can submit phishing mail and documents to these decoys. Attivo monitors and alerts on DDE execution from malicious documents.
Exploitation of Remote Services	The BOTsink appliance hosts real operating systems as decoys which are as vulnerable as production systems. Customers can also deploy unpatched versions of vulnerable operating systems to engage and detect attacks inside the network.
Logon Scripts	The BOTsink appliance decoys can deploy as part of an enterprise domain and add them to Active Directory.
Pass the Hash	The BOTsink appliance decoys are vulnerable to pass-the-hash methods and detect attackers using pass-the-hash on decoys.
Pass the Ticket	The ThreatStrike Suite can deploy deceptive Kerberos tickets in user machines. Attackerdumping memory or Kerberos tickets instead see deceptive Kerberos tickets.

LATERAL MOVEMENT CONT.	
Remote Desktop Protocol	The BOTsink appliance supports hosting Windows decoys with RDP. The ThreatStrike Suite can install RDP credentials to decoys in endpoint caches and lure attackers to decoy systems. The ThreatPath solution can monitor and raise an alert for all active sessions that are under Domain Admin or Privileged Admin.
Remote File Copy	The BOTsink appliance decoys allows users to perform remote file copy operations. The ThreatStrike Suite leaves deceptive lures to the BOTsink appliance decoy file and ftp servers in user endpoints to redirect attackers towards the decoys.
Remote Services	The BOTsink appliance decoys hosts production applications (for example, SSH Servers, VNC, RDP servers, and others). The ThreatStrike Suite distributes SSH keys and credentials to these decoy servers.
Shared Webroot	The ThreatPath solution will detect open and misconfigured network file shares that could lead to this attack specifically.
Taint Shared Content	The ThreatStrike Suite can deploy decoy network shares on endpoints mapping to decoy servers. These redirect attackers to tamper with decoy shares instead of production shares.
Third-party Software	The BOTsink appliance decoy systems can be added to software deployment tools like SCCM, Altris, and others. The adversary can execute malicious code on endpoint systems. The BOTsink appliance decoys will detect remote code execution and provide an early detection mechanism.
Windows Admin Shares	ThreatPath solution will detect open and misconfigured network shares (C$, ADMIN$, and such). Customers can deploy decoy SMB servers with such open shares to detect attackers targeting them.
Windows Remote Management	The BOTsink appliance decoys allows remote connection attempts using WinRM. Users can deploy decoys or ThreatDirect forwarders and engage attackers exploiting WinRM commands for persistence and lateral movement.

DISCOVERY	
System Time Discovery	The BOTsink appliance decoys can be queried to gather time and time zone information. The BOTsink appliance detects remote activity and attempts to install scheduled tasks on its decoys.
Network Share Discovery	The ThreatStrike Suite installs decoy network shares. The network shares are customizable, and users can upload custom folders and files to the shares. On Windows, the ThreatPath solution can be used to monitor and detect the exposure of data on various folders and systems that are important and key to the Enterprise's business.
System Network Configuration Discovery	The BOTsink decoy resources (IPs, SMB shares, DNS entries, AD entries, and such) can be discovered as part of a network discovery process. Similarly, BOTsink decoys send multicast and broadcast traffic as standard images.
Remote System Discovery	The BOTsink decoy resources (IPs, SMB shares, DNS entries, AD entries, and such) that attackers can discover as part of a network discovery process. Similarly, BOTsink decoys send multicast and broadcast traffic as standard images.

DISCOVERY CONT.	
File and Directory Discovery	The ThreatStrike solution installs scripts and decoys documents in endpoints containing sensitive information like hostnames, user accounts, and passwords. Attempts to use the data lead the attacker towards the decoys for engagement. The ThreatPath solution can monitor and detect the exposure of data on various folders and systems that are critical to the Enterprise's business.
Browser Bookmark Discovery	The ThreatStrike Suite can install bookmarks to the browser's profile that point to decoys, detecting attackers who follow these bookmark lures. Bookmark lures can also cache the credentials that point to customer production images, which the platform can import as decoys.
Network Service Scanning	Installing network decoys across VLANs is a very important step in detecting network scans. Any attempt to discover services on a decoy hosted by the Attivo ThreatDefend platform will identify the attackers during the network fingerprinting phase.
Account Discovery	Attivo offers a tight integration with Active Directory. The BOTsink platform, in combination with the ThreatStrike Endpoint Suite, can add deceptive user and privileged groups to Active Directory for attackers to use high value accounts that lead them to decoys.
Permission Groups Discovery	The ThreatPath solution will flag an alert if a domain user is part of the local admin group.

CREDENTIAL ACCESS	
Brute Force	The Attivo ThreatDefend Platform monitors attempts to login for any deceptive credentials by integrating with SIEM technologies within the enterprise. Any brute force attempt using deceptive users will be detected as stolen credentials attack.
Credential Dumping	The ThreatStrike Suite is used to inject deceptive credentials across the enterprise at the real endpoints. These credentials are cached/ saved/injected to be discovered by attackers which can lead the attackers towards decoys. The ThreatPath solution will scan and report on the endpoints that store cleartext credentials in LSA memory.
Credentials in Files	ThreatStrike Suite can deploy scripts, configuration files, passwords in text files, and documents across the endpoints.
Forced Authentication	The ThreatPath solution scans and alerts if WebDAV is enabled at any endpoint. WebDAV is prone to several attacks and vulnerabilities.
Kerberoasting (roadmap)	The Attivo ThreatDefend Platform will deploy lures that alerts against Kerberoasting attacks.

COLLECTION	
Data from Information Repositories	Attivo Decoy Documents can detect attempts to exfiltrate data from repositories. Customers can deploy document decoys in key information repositories and monitor if attackers exfiltrate the documents outside of these systems.

COLLECTION CONT.	
Data from Local System	Attivo Decoy Documents can detect the collection of such information. Customers can deploy document decoys in key repositories like Sharepoint, Confluence, File Servers, Box.com, and others, and monitor if attackers exfiltrate them outside of these systems.
Data from Network Shared Drive	Attivo Decoy Documents can detect the collection of such information. Customers can deploy document decoys in network shared drives and monitor if attackers exfiltrate the documents outside of these systems.

SUMMARY

Deception Technology is a powerful threat detection mechanism that bridges gaps left open and exploitable by attackers when adversaries successfully penetrate a perimeter defense. By adding the Attivo Networks® ThreatDefend® Platform to the security stack, organizations gain early and accurate eyes-inside-the-network visibility to attack techniques documented in the MITRE ATT&CK Matrix, that either bypass existing controls or are perpetrated by malicious actors already inside the network.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in network attacks. The Attivo ThreatDefend Deception Platform offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 100 awards for its technology innovation and leadership.

www.attivonetworks.com