WHITEPAPER

Attivo NETWORKS

DISRUPT AN ATTACKER'S ABILITY TO DISCOVER NETWORKS AND MOVE LATERALLY

EXECUTIVE SUMMARY

After gaining initial access in an enterprise, attackers will want to move deeper inside the network to expand their foothold, access critical data, and move to high-value targets. They must discover internal networks, systems, and applications to achieve their objective. Attackers use fingerprinting to identify targets, decide which vulnerabilities to exploit, and determine how to interact with them successfully. They can accomplish much of this reconnaissance with native operating systems tools and simple scripts.

Attempts by attackers to fingerprint an endpoint are regularly missed due to the complexity of tracking, analyzing, and alerting on all of an endpoint's communications traffic. Many traditional detections typically generate a high volume of false positives, making them unusable. Research shows that only 4% of reconnaissance activity generates an alert, and security controls missed 54% of techniques used to test lateral movement detection.

This white paper discusses key use cases of the Endpoint Detection Net's Deflect function that prevent attackers from fingerprinting an endpoint to identify security weaknesses and conducting reconnaissance.

WHAT IS THE DEFLECT FUNCTION?

The Attivo Networks® ThreatDefend® Platform enhances an organization's defenses by providing visibility and early detection into in-network lateral movement and other attack activities that have evaded existing security controls. The Endpoint Detection Net (EDN) suite strengthens endpoint defensive capabilities by early detection of attacker's Tactics, Techniques, and Procedures (TTPs). The EDN suite includes the Deflect function that misdirects attackers attempting to fingerprint and compromise vulnerable ports and services. It redirects any attack connection attempt targeting non-existing services on endpoints to network decoys that engage with them, recording all activity and capture Indicators of Compromise (IoCs) and TTPs. The Deflect function prevents attackers from accurately fingerprinting endpoints and closes any opportunity to move laterally inside the network.

The Deflect function is easy to deploy and does not require any extra privileges at the endpoint. It redirects inbound or outbound attacker attempts to fingerprint or laterally move to a system, forcing an engagement with a decoy that records TTPs and captures forensic data.

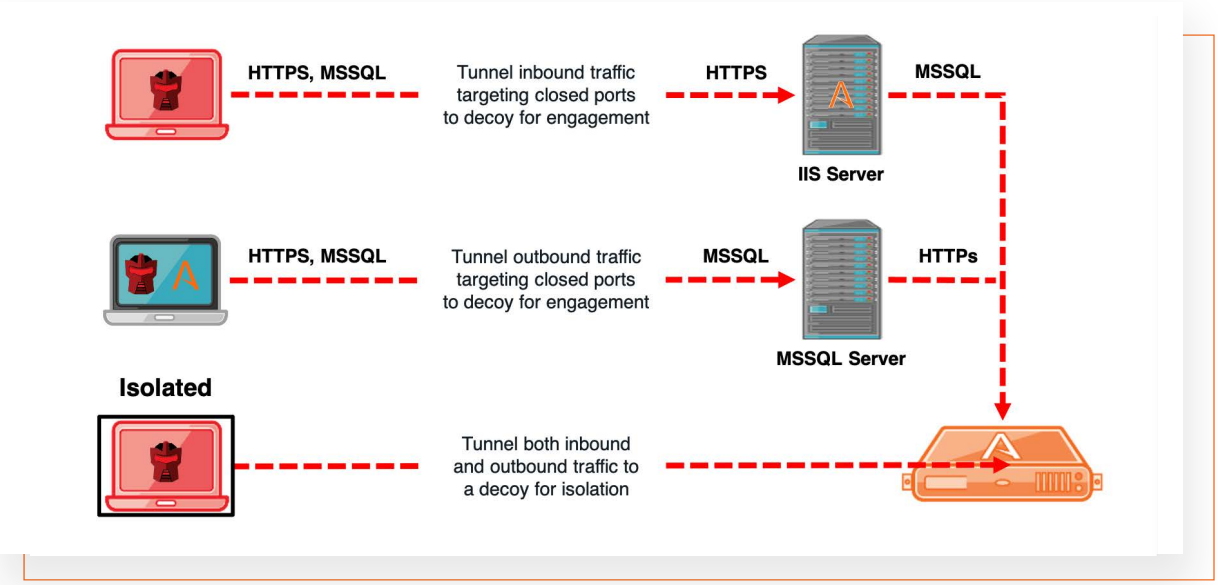
KEY CAPABILITIES OF THE EDN DEFLECT FUNCTION:

- Redirects scans touching closed ports on protected hosts to decoys for engagement.
- Makes every endpoint a decoy and prevents accurate host fingerprinting.
- Provides active detection and prevention capabilities at both the source and destination endpoints.
- Can quarantine infected endpoints away from the production network.

USE CASES FOR THE DEFLECT FUNCTION

Identifying vulnerable targets for remote software exploitation in applications and misconfigurations is a popular method that attackers use to move further inside the organization. They can accomplish this easily with readily available tools that scan for ports and vulnerabilities. APT32, APT39, FIN6, and many other attack groups are known o perform network reconnaissance to search for operating systems and services to exploit. Exploitation examples include zero-day and unpatched vulnerabilities in protocols like SMB or RDP, Database services, misconfigured SMB shares, and weak passwords.

The following lists typical use cases for the Deflect function, which helps monitor the attacker's connection attempts and redirect them to decoys for engagement, isolating the attack without interfering with production services or ports.



LATERAL MOVEMENT PREVENTION

The Deflect function continuously learns the open services on any protected endpoint, redirecting both illicit inbound and outbound attempts to connect to closed ports to decoys for engagement. Attackers will often interrogate an endpoint for any available services in a fingerprinting process to determine the server type. Once they identify any open services, they can use exploits that take advantage of vulnerabilities to gain access and compromise the endpoint. The Deflect function effectively disguises the endpoint because any closed port will respond as if it were open since the traffic gets redirected to a corresponding decoy running the service. Any subsequent connection attempts will engage with the decoy services, preventing lateral movement by misdirecting the attack away from production assets. The Deflect function covers the following scenarios:

Inbound Deflect

The Deflect function monitors the attacker's reconnaissance techniques as they scan for ports and services to exploit on the endpoints. It detects suspicious inbound connection attempts that touch non-existent services and redirects the traffic to a decoy while raising an alert. For example, when an attacker targets a web server and probes for a database service, the Deflect function redirects the attack to the database service hosted on a decoy, capturing the attack's IOCs and TTP's, as well as any forensic evidence, including packet captures.

Outbound Deflect

The Deflect function can also redirect an attacker's outbound traffic from a compromised protected endpoint, even if the destination endpoint is unprotected. The Deflect function triggers alerts on suspicious activity and forwards the failed outbound connection attempts on non-existing services to the decoys. For example, when an attacker initiates web traffic against a database server, the Deflect function will redirect the attacker to a web server hosted on a decoy.

QUARANTINE INFECTED ENDPOINT

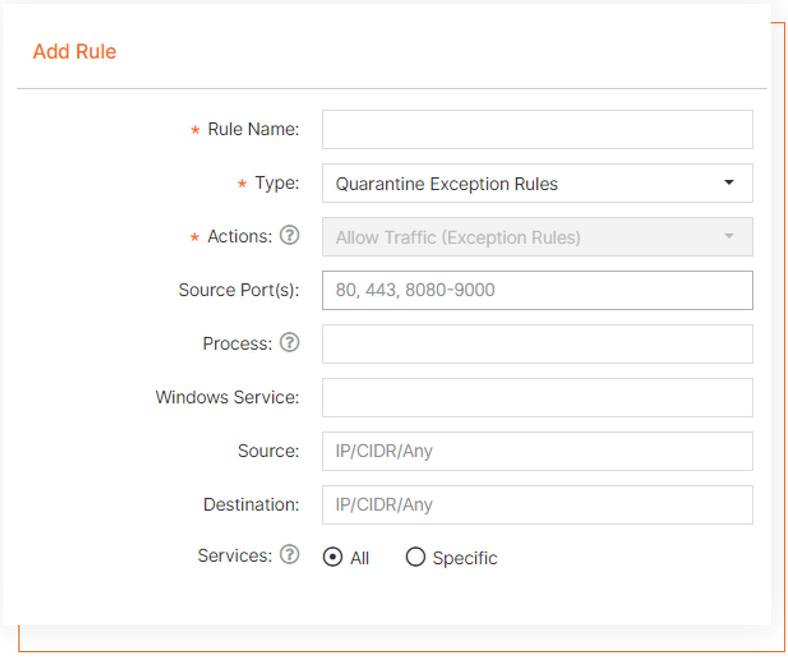
An infected endpoint connected to the network can spread the infection to other vulnerable systems. It is essential to prevent further malware compromises by promptly quarantining the system. The Deflect function quarantine modes include: limiting suspicious traffic only to the decoy environment for engagement and preventing the attacker from communicating with any production system.

Quarantine with Deflect

This method enables native isolation for infected endpoints to prevent the system from compromising other systems and contacting the Command and control (C2) server. Critical business applications are not interrupted and will continue to function and communicate with the rest of the network.

Redirect with Deflect

This method redirects traffic from an infected endpoint to decoys for engagement, providing the opportunity to study the attack. The attacker cannot access any internal or external systems other than the decoys. Critical business applications can continue to function and communicate with the rest of the network to ensure continued operations.



Monitor Mode

This method allows customers to observe the events the Deflect function would generate without actually redirecting any traffic to identify critical business applications it may affect. In this mode, the Deflect function does not block or redirect any traffic and instead generates security events related to potentially malicious network attempts.

DEPLOYING DEFLECT IN KUBERNETES NODES

Protecting widely used cloud environments, containers, and microservices is critical to the security team. Deploying the Deflect function allows organizations to detect suspicious activity and attacker attempts to discover services running on other cloud endpoints. The Deflect function detects fingerprinting and redirects both inbound and outbound connection attempts to decoys for engagement.

MITRE ATT&CK® COVERAGE

The Attivo Endpoint Detection Net Suite's Deflect function offers detection capabilities that cover the MITRE ATT&CK framework across on-premises and cloud environments. The following table shows MITRE ATT&CK TTPs mapped to different attack phases and how the Deflect function supports the use cases discussed.

MITRE ATT&CK Techniques	Tactic	EDN: Deflect Function Capabilities
T1046 - Network Service Scanning	Discovery	Detects and triggers an event on attacker reconnaissance techniques as they scan for ports and services to exploit.
T1016 - System Network Configuration Discovery	Discovery	Detects and alerts when attackers query system network information from an infected endpoint.
T1018 - Remote System Discovery	Discovery	Detects and triggers an event on attackers attempting to list other systems by IP address, hostname, or other logical identifiers on a network they can use to move laterally from the current system.
T1021 - Remote Services	Lateral Movement	Detects and triggers an event when an attacker attempts multiple inbound/outbound access attempts to non-existing services.

CONCLUSION

Cyber-crime has become a big business opportunity, and criminals are using many advanced attack techniques, including exploiting software vulnerabilities to advance their attacks. IT security teams should prioritize detecting suspicious traffic indicating attacker attempts to discover running services and open ports to compromise or exploit. Organizations can achieve this capability by deploying the Attivo Networks EDN Suite across on-premises, remote worksites, and cloud infrastructure. They can also take advantage of the native isolation of infected systems capabilities by quarantining attacks away from production systems and limiting the damage they can do. This quarantine function can also be beneficial in accelerating incident response and strengthening security across the entire enterprise.

REFERENCES

https://investors.fireeye.com/news-releases/news-release-details/mandiant-security-effectiveness-report-2020-now-available
https://attivonetworks.com/documentation/Attivo_Networks-Deflect_Datasheet.pdf

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE Shield, and its capabilities tightly align to the MITRE ATT&CK Framework. Attivo has won over 130 awards for its technology innovation and leadership. www.attivonetworks.com