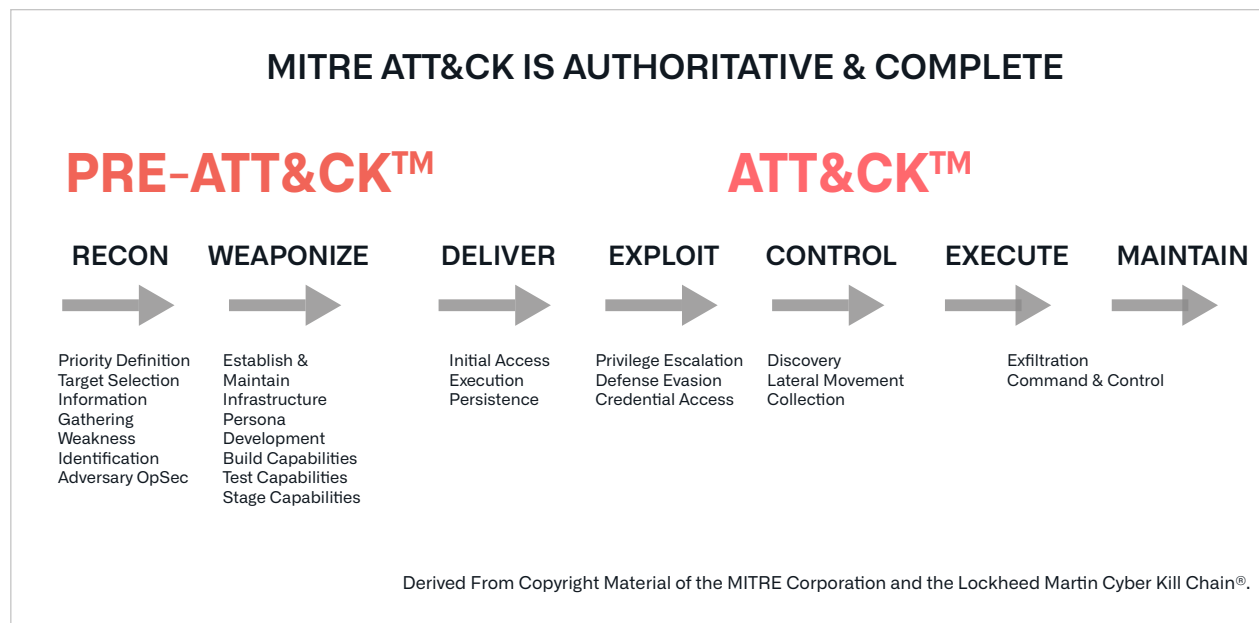


SOLUTION NOTE

MITRE ATT&CK AND DNS SECURITY

This solution brief will share an overview of the MITRE ATT&CK framework and why it is compelling for modern enterprise and government institutions. We overview the large accessible and highly vulnerable attack surface available when DNS is unprotected. We illustrate this by defining the MITRE ATT&CK Tactics, Techniques (& Sub-Techniques), and Procedures (TTPs) which use DNS. BloxOne Threat Defense DNS security can provide protection against a multitude of cyberattacker techniques.



THE MITRE ATT&CK FRAMEWORK

The MITRE ATT&CK™ framework, developed by The MITRE Corporation, is a comprehensive knowledge base of cyberattacker tactics and techniques gathered from the observation of attacker behavior. MITRE is a non-profit organization that does work for the U.S. Government agencies in a wide variety of areas. MITRE ATT&CK (Adversarial Tactics, Techniques, And Common Knowledge) was developed and released by Mitre Corp. in 2015.

As an important knowledge base, MITRE ATT&CK enables anyone on the cyber defense team to review and contrast attacker activity, and then understand the best options for defense. So you know, there is also MITRE PRE-ATT&CK, which helps cyber defenders prevent an attack before the attacker can gain access to the network. The 15 top-level tactic categories for PRE-ATT&CK correlate to the first two stages of the Lockheed Martin Cyber Kill Chain®. PRE-ATT&CK presents the tactics, underlying techniques, and procedures that a cyberattacker will use to define targets, gather information, and then launch an attack.

MITRE ATT&CK brings a common lexicon to describe the activities of cyberattackers, and the step-by-step tactics and techniques which they will use. This enables you to communicate clearly with others on the exact details of the threat. ATT&CK also provides a consistent way to describe your current security controls and processes. MITRE ATT&CK allows the cyber defenders to clearly identify the nature of a threat, map that threat back to the controls that should protect against it, and then ultimately determine whether that control is effective.

The MITRE ATT&CK framework also provides a comprehensive taxonomy to post-exploitation cyberattacker behavior. A detailed focus on attacker behavior, such as provided by MITRE ATT&CK, is the best way to find and stop an ongoing attack before data exfiltration or destructive behavior can be achieved. MITRE ATT&CK can help organizations make better decisions about assessing risks, deploying new security controls, and better defending its networks.

MAPPING THE DNS ATTACK SURFACE WITH MITRE ATT&CK

Everything on your networks whether on premise, in the cloud, IOT, or mobile will need to use DNS services. DNS provides better-centralized visibility and control of all computing resources, including users and servers in a micro-segment, all the way to an individual IP address. There are a multitude of ways that cyberattackers can leverage unprotected DNS services.

The following MITRE ATT&CK techniques and sub-techniques explicitly define how cyberattackers will target and use DNS services. The Tactic represents the goal the attacker is trying to achieve. The Techniques and Sub-Techniques represent the different ways that cyberattackers can achieve the goals and objectives of the tactic. Mitigation of these techniques require comprehensive DNS security solutions.

MITRE ATT&CK TECHNIQUES WHICH USE DNS

TACTIC	GOAL OF ATTACKER	TECHNIQUES USING DNS	SUB-TECHNIQUE
Reconnaissance		T1590 Gather Victim Network Information	.001 Domain Properties
			.002 DNS
			.004 Network Topology
			.005 IP Address
			.003 Spearphishing Link
Resource Development		T1583 Acquire Infrastructure	.001 Domains
			.002 DNS Server
		T1584 Compromise Infrastructure	.001 Domains
			.002 DNS Server

“ MITRE ATT&CK has segmented attacks in a very consistent way that makes it easy to compare them and to determine how an attacker might have exploited your network. Attacker analysis predominantly focuses on their activities in terms of perimeter defense. MITRE ATT&CK takes a much closer look at them once they get in.”

Anthony James
Vice President of Product Marketing
Infoblox

TACTIC GOAL OF ATTACKER	TECHNIQUES USING DNS	SUB-TECHNIQUE
	T1608 Stage Capabilities	.002 Upload Tool
Initial Access	T1189 Drive-by Compromise	
	T1190 Exploit Public-Facing Application	
	T1566 Phishing	.002 Spearphishing Link
Execution	T1204 User Execution	.001 Malicious Link
Credential Access	T1557 Adversary-in-the-Middle	
	T1040 Network Sniffing	
Command and Control	T1071 Application Layer Protocol	.004 DNS
	T1132 Data Encoding	
	T1568 Dynamic Resolution	
	T1573 Encrypted Channel	
	T1008 Fallback Channels	
	T1105 Ingress Tool Transfer	
	T1572 Protocol Tunneling	
	T1090 Proxy	.001 Internal Proxy
		.002 External Proxy
Exfiltration	T1030 Data Transfer Size Limits	
	T1048 Exfiltration Over Alternative Protocol	.001 Exfiltration Over Symmetric Encrypted Non-C2 Protocol
		.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
		.003 Exfiltration Over Unencrypted Obfuscated Non-C2 Protocol
	T1041 Exfiltration Over C2 Channel	

Let's take a close look at the **Reconnaissance Tactic**. In the case of Reconnaissance, the attacker is trying to gather information they can use to plan future attacks. There are two Techniques (and multiple Sub-Techniques) used extensively by attackers to utilize DNS as defined by MITRE ATT&CK:

T1590. Gathering Victim Network Information. Adversaries may gather information about the victim's networks that can be used during targeting. Information about networks may include a variety of details, including administrative data (ex: IP ranges, domain names, etc.) as well as specifics regarding its topology and operations.

- **001 Domain Properties.** Adversaries may gather information about the victim's network domain(s) that can be used during targeting. Information about domains and their properties may include a variety of details, including what domain(s) the victim owns as well as administrative data (ex: name, registrar, etc.) and more directly actionable information such as contacts (email addresses and phone numbers), business addresses, and name servers.
- **002 DNS.** Adversaries may gather information about the victim's DNS that can be used during targeting. DNS information may include a variety of details, including registered name servers as well as records that outline addressing for a target's subdomains, mail servers, and other hosts
- **004 Network Topology.** Adversaries may gather information about the victim's network topology that can be used during targeting. Information about network topologies may include a variety of details, including the physical and/or logical arrangement of both external-facing and internal network environments. This information may also include specifics regarding network devices (gateways, routers, etc.) and other infrastructure.
- **005 IP Addresses.** Adversaries may gather the victim's IP addresses that can be used during targeting. Public IP addresses may be allocated to organizations by block, or a range of sequential addresses. Information about assigned IP addresses may include a variety of details, such as which IP addresses are in use. IP addresses may also enable an adversary to derive other details about a victim, such as organizational size, physical location(s), Internet service provider, and or where/how their publicly-facing infrastructure is hosted.




T1598. Phishing for Information. Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](#) in that the objective is gathering data from the victim rather than executing malicious code.

- **003 Spearphishing Link.** Adversaries may send spearphishing messages with a malicious link to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](#) or [Compromise Accounts](#)) and/or sending multiple, seemingly urgent messages.

All of these MITRE ATT&CK DNS-related techniques and sub-techniques define areas of potential risk for your organization. If your DNS, DHCP, and IPAM infrastructure is undefended, modern attackers will quickly discover and utilize these attack surface vulnerabilities.

BLOXONE® THREAT DEFENSE

BloxOne Threat Defense secures traditional networks, as well as SD-WAN, IoT, the cloud, and the move to mobile devices. BloxOne Threat Defense brings all of your DNS controls, administration, and management into one hybrid architecture. Everything on your networks whether on premise, in the cloud, IOT, or mobile will need to use DNS services. This gives you one architecturally efficient, centralized point of control and visibility to any traffic that requires resolution of a domain name with DNS services for all of your on-premises and cloud-based resources. Once you assert this control, you have very effectively enabled the defensive build-out of DNS.

 <p>VISIBILITY & AUTOMATION</p>	 <p>PROTECTION EVERYWHERE</p>	 <p>REDUCING COST OF THREAT DEFENSE</p>
<p>Identify all devices across the enterprise and improve productivity of SecOps through automated data sharing</p>	<p>DNS as a “signal” for security events and control point for security enforcement ACROSS EVERYTHING</p>	<p>Offload blocking of known threats and preserve processing power of perimeter security</p>

Organizations must always be in control of their DNS traffic

CONCLUSIONS AND RECOMMENDATIONS

MITRE ATT&CK is an important tool to identify, analyze, and communicate consistently about malicious cyber activity. There are a multitude of attacker vectors identified within MITRE ATT&CK that utilize and impact DNS. DNS security core network services such as DNS, DHCP, and IPAM provide deep visibility as incredibly valuable security controls and threat intelligence assets. You can rapidly investigate a threat or anomalous behavior and share valuable data with the rest of your security ecosystem. Using DNS security and leveraging DNS related data can bring risk reduction for every cloud and on-premise data center used by your organization.

ABOUT INFOBLOX

Infoblox delivers the next-level network experience with its Secure Cloud-Managed Network Services. As a pioneer in providing the world’s most reliable, secure, and automated networks, we are relentless in our pursuit of next-level network simplicity. A recognized industry leader, Infoblox has more than 12,000 customers, including more than 80% of the Fortune 500. To learn more, please visit our website via www.infoblox.com.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com