AREA 1®

PHISHING AND THE MITRE ATT&CK™ FRAMEWORK

AREA 1

OVERVIEW

MITRE has developed a framework for cybersecurity that allows organizations to measure and prove the efficacy of security controls.

The MITRE ATT&CK™ framework matrix covers 12 key technique areas, and although phishing is only one technique within the "initial access" area, one successful phish can have a significant impact on the efficacy of a broad range of tactics and techniques across the entire framework.

MITRE ATT&CK MATRIX - Key Areas

- **Initial Access** - The adversary is trying to get into your network.
- **Execution** - The adversary is trying to run malicious code.
- **Persistence** - The adversary is trying to maintain their foothold.
- **Privilege Escalation** - The adversary is trying to gain higher-level permissions.
- **Defense Evasion** - The adversary is trying to avoid being detected.
- **Credential Access** - The adversary is trying to steal account names and passwords.
- **Discovery** - The adversary is trying to figure out your environment.
- **Lateral Movement** - The adversary is trying to move through your environment.
- **Collection** - The adversary is trying to gather data of interest to their goal.
- **Command and Control** - The adversary is trying to communicate with compromised systems to control them.
- **Exfiltration** - The adversary is trying to steal data.
- **Impact** - The adversary is trying to manipulate, interrupt, or destroy your systems and data.

This guide details how Area 1 Security's comprehensive email security can be mapped to the MITRE ATT&CK framework and the importance of anti-phishing to preempt damages within an enterprise. Whether it is malware, ransomware, credential theft, Types 1-4 Business Email Compromise (BEC), it only takes one. Organizations will find that comprehensive email security that integrates seamlessly into their network, SIEMs, and drives SOAR operations, keeping them ahead of emerging threats, 95% of which begin with that one initial access technique — phishing.

WHAT IS MITRE ATT&CK?

Here are some of the areas where a comprehensive email security approach to phishing attacks maps to the MITRE ATT&CK framework.

INITIAL ACCESS

Stop phishing attacks by taking a proactive approach. We utilize our web crawlers to discover newly established phishing infrastructure. Our advanced machine learning engine examines the real text and images of an email, and our gateway functionality blocks malicious emails and rewrites/defangs URLs.

EXECUTION

Stop malicious files from entering the environment by proactively blocking them before delivery. We also defang/rewrite malicious URLs contained in emails to ensure that malicious content isn't executed.

DEFENSE EVASION

Detect BEC, domain mismatches, as well as user and brand impersonation (including malicious phish that bypass SPF/DKIM/DMARC), which are are common attacks to evade detection. With our advanced machine learning and our team of security experts, we stay on top of the latest threats.

CREDENTIAL ACCESS

Proactively prevent spear phishing and other malicious emails from the ability to gain access to credentials by way of credential harvesters and other malicious attacks.

DISCOVERY

Proactively block malicious inbound email. This prevents an attacker from gaining entry and understanding your network environment. With our API integrations in the network and web security tools, we can assist in protecting the entire organization, not just the inbox.

LATERAL MOVEMENT

Detect lateral movement via journaling. Compromised accounts passing phishing emails to internal employees can be detected and stopped via message retraction. Our API functionality can discover network or web phishing in your environment as well.

COMMAND AND CONTROL

Take a comprehensive approach to phishing across web and network traffic. By utilizing recursive DNS, integrating into a next-gen firewall, and an array of other security tools via an extensive array of APIs, Area 1 blocks communication to Command and Control systems.

EXFILTRATION

Utilizing the same approach to exfiltration as it does with Command and Control, Area 1 provides critical value in its holistic email security approach.

IMPACT

Protect your end users by blocking malicious attacks such as ransomware. By proactively blocking the malicious email before it reaches the inbox, Area 1 saves your business from large-scale disruption and impact, as well as reputational damage.

AREA 1

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	EXFILTRATION	IMPACT
🟦 Drive-by Compromise	🟦 Command and Scripting Interpreter	Account Manipulation	▨ Valid Accounts	BITS Jobs	▨ Brute Force	Application Window Discovery	Exploitation of Remote Services	Data from Cloud Storage Object	Application Layer Protocol	Automated Exfiltration	🟦 Account Access Removal
🟦 Exploit Public-Facing Application	🟦 Exploitation for Client Execution	BITS Jobs		🟦 Masquerading	▨ Credentialsfrom Password Stores	Domain Trust Discovery	🟦 Internal Spearphishing	Data from Information Repositories	Data Encoding	Data Transfer Size Limits	🟦 Data Destruction
🟦 External Remote Services	Software Deployment Tools	Create Account		Rogue Domain Controller	🟦 Exploitation for Credential Access	File and Directory Discovery	Lateral Tool Transfer	Data from Local System	Data Obfuscation	Exfiltration Over Alternative Protocol	🟦 Data Encrypted for Impact
🟦 Phishing	System Services	Create or Modify System Process		🟦 Obfuscated Files or Information	🟦 Forced Authentication	Network Service Scanning	Remote Service Session Hijacking	Data from Network Shared Drive	🟦 Dynamic Resolution	Exfiltration Over C2 Channel	🟦 Data Manipulation
🟦 Supply Chain Compromise	🟦 User Execution	Event Triggered Execution		🟦 Template Injection	🟦 Input Capture	Network Share Discovery	🟦 Remote Services	Data Staged	🟦 Encrypted Channel	Exfiltration Over Other Network Medium	🟦 Defacement
🟦 Trusted Relationship	Windows Management Instrumentation	External Remote Services		Traffic Signaling	Man-in-the-Middle	Network Sniffing	Software Deployment Tools	🟦 Email Collection	🟦 Fallback Channels	🟦 Exfiltration Over WebService	🟦 Disk Wipe
▨ Valid Accounts		Traffic Signaling		▨ Valid Accounts	Network Sniffing	Query Registry	Taint Shared Content	🟦 Man in the Browser	Ingress Tool Transfer	Scheduled Transfer	🟦 Endpoint Denial of Service
		▨ Valid Accounts		🟦 Virtualization / Sandbox Evasion	OS Credential Dumping	Remote System Discovery		Man-in-the-Middle	Multi-Stage Channels	🟦 Transfer Data to Cloud Account	🟦 Firmware Corruption
					🟦 Steal Application Access Token	Software Discovery			Non-Application Layer Protocol		🟦 Inhibit System Recovery
						System Information Discovery			Non-Standard Port		🟦 Network Denial of Service
						System Network Configuration Discovery			Protocol Tunneling		🟦 Resource Hijacking
						System Network Connections Discovery			🟦 Proxy		🟦 Service Stop
						System Owner/ User Discovery			Remote Access Software		🟦 System Shutdown / Reboot
						System Service Discovery			Traffic Signaling		
						System Time Discovery			🟦 Web Service		
						🟦 Virtualization / Sandbox Evasion					

TABLE LEGEND

🟦 Area 1 can detect technique or prevent technique from executing

▨ Area 1 can provide an indicator for verification

KONNI MALWARE

EXAMPLE MALWARE PHISHING MAPPED TO MITRE ATT&CK FRAMEWORK

KONNI malware is a remote administration tool (RAT) often delivered via phishing emails as a Microsoft Word document with a malicious VBA macro code. The malicious code can change the font color to fool the user to enable content, check if the Windows operating system is a 32-bit or 64-bit version, and construct and execute the command line to download additional files.

Once the VBA macro constructs the command line, it uses the certificate database tool to download remote files from a given Uniform Resource Locator. It also incorporates a built-in function to decode encoded files. The Command Prompt silently copies an executable file into a temp directory and renames it to evade detection.

The attacker then downloads a text file from a remote resource containing a base64-encoded string that is decoded by CertUtil and saved as a batch file. Finally, the attacker deletes the text file from the temp directory and executes the file.

MITRE ATT&CK TECHNIQUES - According to MITRE, KONNI uses the ATT&CK techniques listed in the Table 1 below.

TABLE 1: KONNI ATT&CK TECHNIQUES

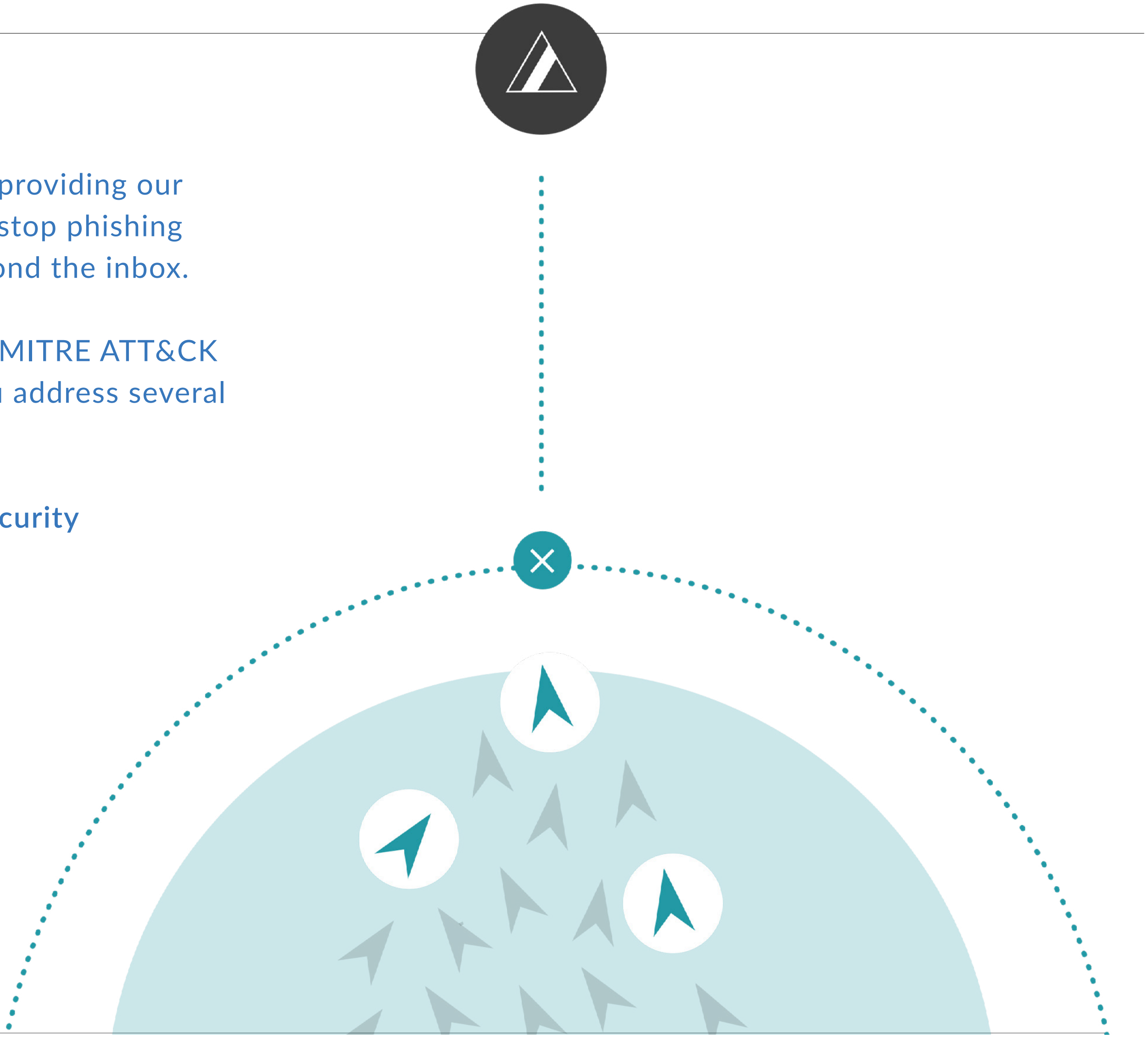
TECHNIQUE	USE
System Network Configuration Discovery [T1016]	KONNI can collect the Internet Protocol address from the victim's machine.
System Owner/User Discovery [T1033]	KONNI can collect the username from the victim's machine.
Masquerading: Match Legitimate Name or Location [T1036.005]	KONNI creates a shortcut called `Anti virus service.lnk` in an apparent attempt to masquerade as a legitimate file.
Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol [T1048.003]	KONNI has used File Transfer Protocol to exfiltrate reconnaissance data out.
Input Capture: Keylogging [T1056.001]	KONNI has the capability to perform keylogging.
Process Discovery [T1057]	KONNI has used `tasklist.exe` to get a snapshot of the current processes' state of the target machine.
Command and Scripting Interpreter: PowerShell [T1059.001]	KONNI used PowerShell to download and execute a specific 64-bit version of the malware.
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	KONNI has used `cmd.exe` to execute arbitrary commands on the infected host across different stages of the infection change.
Indicator Removal on Host: File Deletion [T1070.004]	KONNI can delete files.
Application Layer Protocol: Web Protocols [T1071.001]	KONNI has used Hypertext Transfer Protocol for command and control.
System Information Discovery [T1082]	KONNI can gather the operating system version, architecture information, connected drives, hostname, and computer name from the victim's machine and has used `systeminfo.exe` to get a snapshot of the current system state of the target machine.
File and Directory Discovery [T1083]	A version of KONNI searches for filenames created with a previous version of the malware, suggesting different versions targeted the same victims and the versions may work together.
Ingress Tool Transfer [T1105]	KONNI can download files and execute them on the victim's machine.
Modify Registry [T1112]	KONNI has modified registry keys of ComSysApp service and Svchost on the machine to gain persistence.
Screen Capture [T1113]	KONNI can take screenshots of the victim's machine.
Clipboard Data [T1115]	KONNI had a feature to steal data from the clipboard.
Data Encoding: Standard Encoding [T1132.001]	KONNI has used a custom base64 key to encode stolen data before exfiltration.
Access Token Manipulation: Create Process with Token [T1134.002]	KONNI has duplicated the token of a high integrity process to spawn an instance of cmd.exe under an impersonated user.
Deobfuscate/Decode Files or Information [T1140]	KONNI has used CertUtil to download and decode base64 encoded strings.
Signed Binary Proxy Execution: Rundll32 [T1218.011]	KONNI has used Rundll32 to execute its loader for privilege escalation purposes.
Event Triggered Execution: Component Object Model Hijacking [T1546.015]	KONNI has modified the ComSysApp service to load the malicious DLL payload.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]	A version of KONNI drops a Windows shortcut into the Startup folder to establish persistence.
Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]	A version of KONNI drops a Windows shortcut on the victim's machine to establish persistence.
Abuse Elevation Control Mechanism: Bypass User Access Control [T1548.002]	KONNI bypasses User Account Control with the "AlwaysNotify" settings.
Credentials from Password Stores: Credentials from Web Browsers [T1555.003]	KONNI can steal profiles (containing credential information) from Firefox, Chrome, and Opera.

CONCLUSION

Area 1 Security is dedicated to providing our customers the best solution to stop phishing and protect our customers beyond the inbox.

If your company is utilizing the MITRE ATT&CK framework, Area 1 can help you address several key areas within it.

To learn more from our cybersecurity experts, contact us here.



The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

REFERENCES — https://attack.mitre.org/matrices/enterprise/ • https://www.area1security.com/

About Area 1 Security

Area 1 Security is the only company that preemptively stops Business Email Compromise, malware, ransomware and targeted phishing attacks. By focusing on the earliest stages of an attack, Area 1 stops phish — the root cause of 95 percent of breaches — 24 days (on average) before they launch. Area 1 also offers the cybersecurity industry's first and only performance-based pricing model, Pay-per-Phish.

Area 1 is trusted by Fortune 500 enterprises across financial services, healthcare, critical infrastructure and other industries, to preempt targeted phishing attacks, improve their cybersecurity posture, and change outcomes.

Area 1 is cloud-native, a Certified Microsoft Partner, and Google Cloud Technology Partner of the Year for Security. To learn more, visit **www.area1security.com**, follow us on **LinkedIn**, or subscribe to the **Phish of the Week** newsletter.