TLP:WHITE

RISK AND VULNERABILITY ASSESSMENT (RVA) MAPPED TO THE MITRE ATT&CK® FRAMEWORK

FISCAL YEAR 2019 (FY19)

Risk and Vulnerability Assessment: Upon request, CISA can identify vulnerabilities that adversaries could potentially exploit to compromise security controls. We collect data in an on-site assessment and combine it with national threat information to provide customers with a tailored risk analysis report.

+ HOW WE LATERAL AND ESCALATE

Attack Path 1: Gone Phishin'

Initial Access » Spearphishing Link and MSHTA
Execution » PowerShell
Defense Evasion » Process Injection and MSHTA
Command & Control » Commonly Used Port

Attack Path 2: You've Poisoned My LLMNR

Credential Access » LLMNR/NBT-NS Poisoning and Relay
Brute Force
Discovery » Network Sniffing

Attack Path 3: The Ol' Discover & Dump

Discovery » Permissions Group Discovery
System Owner/User Discovery
Execution » Windows Management Instrumentation
Persistence/ Defense Evasion/ Privilege Escalation » Valid Accounts

Attack Path 4: I Like My Kerberos Well-Done

Initial Access » Kerberoasting
Brute Force
Persistence/ Defense Evasion/ Privilege Escalation » Valid Accounts

Attack Path 5: Is That a Cleartext Password or SSH Key, I See?

Credential Access » Credentials in Files
Bash History
Private Keys
Valid Accounts
Persistence/ Defense Evasion/ Privilege Escalation » Valid Accounts

FY19 RVA RESULTS

MITRE ATT&CK Tactics and Techniques

The percent noted for each technique represents the success rate for that technique across all RVAs. For example, spearphishing link was used to gain initial access in 45.5% of the FY19 RVAs.

44 Total Number of Assessments

Initial Access

45.5%	Spearphishing Link
4.5%	Exploit Public-Facing Application
2.3%	Spearphishing Attachment

Execution

70.5%	PowerShell
63.6%	Command-Line Interface
45.5%	MSHTA
45.5%	Service Execution
43.2%	Windows Management Instrumentation
18.2%	Graphical User Interface
11.4%	Scripting
9.1%	User Execution
9.1%	Exploitation for Client Execution
2.3%	Execution through API

Persistence

25.0%	Valid Accounts
9.1%	New Service
4.5%	Create Account
2.3%	Windows Management Instrumentation Event Subscription
2.3%	Registry Run Keys/Startup Folder
2.3%	Launch Agent

Privilege Escalation

25.0%	Valid Accounts
20.5%	Exploitation for Privilege Escalation
20.5%	Access Token Manipulation
15.9%	Process Injection
9.1%	New Service
9.1%	Bypass User Account Control
2.3%	Sudo
2.3%	Exploitation of Vulnerability

Defense Evasion

45.5%	MSHTA
36.4%	Process Hollowing
25.0%	Valid Accounts
20.5%	Access Token Manipulation
15.9%	Process Injection
11.4%	Scripting
11.4%	Obfuscated Files or Information
9.1%	Bypass User Account Control
6.8%	Indicator Removal from Tools
6.8%	Hidden Window
6.8%	File Deletion
4.5%	Masquerading
4.5%	DLL Side-Loading
2.3%	Process Doppelgänging
2.3%	Disabling Security Tools

Credential Access

88.6%	Credential Dumping
68.2%	LLMNR/NBT-NS Poisoning
38.6%	Credentials in Files
22.7%	Kerberoasting
20.5%	Brute Force
15.9%	Network Sniffing
11.4%	Input Capture
9.1%	Account Manipulation
4.5%	Exploitation of Credential Access
2.3%	Private Keys
2.3%	Forced Authentication
2.3%	Credentials in Registry
2.3%	Bash History

Discovery

63.6%	Account Discovery
50.0%	Network Service Scanning
47.7%	File & Directory Discovery
45.5%	Network Share Discovery
43.2%	Remote System Discovery
40.9%	Process Discovery
31.8%	Password Policy Discovery
27.3%	System Owner/User Discovery
27.3%	Permission Groups Discovery
18.2%	System Service Discovery
18.2%	Security Software Discovery
13.6%	System Information Discovery
11.4%	System Network Configuration Discovery
4.5%	System Time Discovery
4.5%	System Network Connections Discovery
4.5%	Query Registry
2.3%	Peripheral Device Discovery

Lateral Movement

61.4%	Pass the Hash
52.3%	Remote Desktop Protocol
22.7%	Windows Admin Shares
22.7%	Remote Services
13.6%	Exploitation of Remote Services
9.1%	Pass the Ticket
2.3%	Remote File Copy
2.3%	Distributed Component Object Model

Collection

47.7%	Screen Capture
45.5%	Data from Local System
36.4%	Data from Network Shared Drive
22.7%	Automated Collection
11.4%	Man in the Browser
11.4%	Input Capture
2.3%	Email Collection
2.3%	Data from Information Repositories
2.3%	Clipboard Data

Command & Control

54.5%	Commonly Used Port
20.5%	Data Encoding
18.2%	Remote Access Tools
18.2%	Connection Proxy
11.4%	Standard Application Layer Protocol
9.1%	Data Obfuscation
9.1%	Custom Command & Control Protocol
4.5%	Standard Cryptographic Protocol
2.3%	Remote File Copy
2.3%	Multi-hop Proxy

Exfiltration

18.2%	Scheduled Transfer
13.6%	Exfiltration over Command & Control Channel
11.4%	Data Encrypted
4.5%	Data Compressed
4.5%	Automated Exfiltration

MITIGATIONS FOR TOP TECHNIQUES

The top ten mitigations shown here are widely effective across the top techniques.*

M1017 User Training
Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spear-phishing and social engineering.

M1018 User Account Management
Manage the creation, modification, use, and permissions associated to user accounts.

M1026 Privileged Account Management
Manage the creation, modification, use, and permissions associated to privileged accounts, including SYSTEM and root.

M1027 Password Policies
Set and enforce secure password policies for accounts.

M1028 Operating System Configuration
Make configuration changes to the operating system that result in system hardening against techniques.

M1030 Network Segmentation
Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to sensitive systems and information.

M1031 Network Intrusion Prevention
Use intrusion detection signatures to block traffic at network boundaries.

M1032 Multi-factor Authentication
Use two or more pieces of evidence to authenticate to a system.

M1037 Filter Network Traffic
Use network appliances to filter ingress or egress traffic and perform protocol-based filtering.

M1042 Disable or Remove Feature or Program
Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

M1047 Audit
Perform audits or scans of systems, permissions, software, configurations, etc. to identify potential weaknesses.

**Top techniques and mitigations vary by sector and environment. Organizations should consider additional attack vectors and mitigation strategies based on their unique environment.*

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks for referenced threat actor techniques.
For more information about CISA assessment services, please visit https://www.cisa.gov/

TLP:WHITE