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

FISCAL YEAR 2021 (FY21)

Risk and Vulnerability Assessment: Upon request, CISA can identify vulnerabilitites that adversaries could potentially exploit to compromise security controls. CISA collects data in an on-site assessment & combines it with national threat information to provide customers with a tailored risk analysis report. To schedule a Risk & Vulnerability Assessment or learn more, contact CISAServiceDesk@cisa.dhs.gov.

PHISH AND INTEL CHIPS

"POTENTIAL ATTACK PATH OF KNOWN APTS"

Initial Access>> Spearphishing Link

Execution>> PowerShell

Persistence>> Valid Accounts

Privilege Escalation>> Process Injection

Defense Evasion>> File and Artifact Obfuscation

Credential Access>> Brute Force Attack

Discovery>> Network Sniffing

Lateral Movement>> Pass the Hash

Collection>> Data from Local Systems

Command and Control>> Non-Standard Ports

Exfiltration>> Archive Collected Data

FY21 RVA RESULTS

MITRE ATT&CK Tactics and Techniques

This page is a breakout of the top 3 most successful techniques in each tactic. The percent noted for each technique represents the success rate for that technique across all RVAs. For example, valid accounts were used to gain initial access in 51.5% percent of the FY21 RVAs

112 Total Number of Assessments

Initial Access

Valid Accounts	51.5%
Spearphishing Link	36.0%
Spearphishing Attachment	5.1%

Execution

PowerShell	12.7%
Mshta	12.4%
Windows Management Instrumentation	11.0%

Persistence

Valid Accounts	72.0%
Account Manipulation	6.0%
Create Account	5.0%

Privilege Escalation

Valid Accounts	47.4%
Process Injection	19.7%
Access Token Manipulation	16.4%

Defense Evasion

Valid Accounts	25.0%
Mshta	13.2%
Process Injection	10.4%

Credential Access

LLMNR/NBT-NS Poisoning & SMB Rekay	19.9%
Credentials in Files	15.4%
OS Credential Dumping	13.1%

Discovery

Account Discovery	8.9%
Network Share Scanning	8.4%
File & Directory Discovery	8.2%

Lateral Movement

Pass the Hash	27.3%
Remote Desktop Protocol	17.5%
SMB/Windows Admin Shares	16.5%

Collection

Data from Network Shared Drive	33.1%
Data from Local System	28.7%
Input Capture	13.2%

Command & Control

Non-Standard Port	15.3%
Application Layer Protocol	13.9%
Data Obfuscation	12.9%

Exfiltration

Exfiltration Over C2 Channel	65.6%
Exfiltration Over Alternate Protocol	11.5%
Automated Exfiltration	8.2%

In order to help agencies with making data informed risk decisions, CISA may conduct analysis of assessment data and provide this information to our partners. This is one way requesting CISA services can help the broader cybersecurity community gain visibility with vulnerability trends, adversarial activities and, most importantly, effective mitigations that will better protect their networks. Check out all the services available at the **Cyber Resource Hub**

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.

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

FISCAL YEAR 2021 (FY21)

Risk and Vulnerability Assessment: Upon request, CISA can identify vulnerabilitites that adversaries could potentially exploit to compromise security controls. CISA collects data in an on-site assessment & combines it with national threat information to provide customers with a tailored risk analysis report. To schedule a Risk & Vulnerability Assessment or learn more, contact CISAServiceDesk@cisa.dhs.gov.

MITIGATION FOR TOP TECHNIQUES

The top 10 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.

M1021 Restrict Web-Based Content
Restrict or block certain websites.

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

M1028 Operating System Configuration
Make configuration changes related to the operating system or a common feature of 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 Instrusion Prevention
Configure Network Intrusion Prevention systems to block malicious file signatures and file types at the network boundary.

M1038 Execution Prevention
Block execution of code on a system.

M1041 Encrypt Sensitive Information
Use strong encryption mechanisms to protect sensitive data.

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

M1057 Data Loss Prevention
Use a data loss prevention (DLP) strategy to categorize sensitive data, identify data formats indicative of personally identifiable information (PII), and restrict exfiltration of sensitive data.

FY21 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, valid accounts were used to gain initial access in 51.5% of the FY21 RVAs

112 Total Number of Assessments

Initial Access

51.5%	Valid Accounts
36.0%	Spearphishing Link
5.1%	Spearphishing Attachment
2.2%	Exploit Public-Facing Application
1.5%	External Remote Services
1.5%	Drive-by Compromise
1.5%	Trusted Relationship
0.7%	Spearphishing via Service

Execution

12.7%	Mshta
12.4%	PowerShell
1.0%	Windows Management Instrumentation
9.3%	Command and Scripting Interpreter
6.9%	User Execution
6.2%	Windows Remote Management
5.2%	Rundll32
4.8%	Remote Services
4.5%	Service Execution
4.1%	Scripting
4.1%	Command-Line Interface
2.4%	Native API
2.1%	WIndows Command Shell
1.7%	Exploitation for Client Execution
1.4%	Compiled HTML File
1.4%	Regsvr32
1.4%	Execution Through API
1.0%	Third-Party Software
1.0%	Malicious Link
1.0%	LSASS Driver
0.7%	Scheduled Task/Job
0.7%	Trusted Developer Utilities
0.7%	Control Panel
0.7%	Identify Vulnerabilities in Third-Party Software Libraries
0.7%	Spearphishing Link
0.3%	AppleScript
0.3%	CMSTP
0.3%	Malicious Attachment
0.3%	Signed Binary Proxy Execution
0.3%	GUI Input Capture
0.3%	InstallUtil

Persistence

72.0%	Valid Accounts
6.0%	Account Manipulation
5.0%	Create Account
4.0%	Windows Service
3.0%	Web Shell
3.0%	LSASS Driver
2.0%	Scheduled Task/Job
2.0%	External Remote Services
1.0%	Boot or Logon Initialization Scripts
1.0%	Credential API Hooking
1.0%	Services File Permissions Weakness

Privilege Escalation

47.4%	Valid Accounts
19.7%	Process Injection
16.4%	Access Token Manipulation
4.6%	Exploitation for Privilege Escalation
3.9%	Bypass User Account Control
2.6%	Windows Service
2.0%	Web Shell
1.3%	Scheduled Task/Job
0.7%	Credential API Hooking
0.7%	Token Impersonation/ Theft
0.7%	Services File Permissions Weakness

Defense Evasion

25.0%	Valid Accounts
13.4%	Mshta
10.4%	Process Injection
8.7%	Access Token Manipulation
5.2%	Rundll32
4.9%	Web Service
4.5%	Obfuscated Files or Information
4.2%	Scripting
2.8%	Command and Scripting Interpreter
2.1%	Process Hollowing
2.1%	Bypass User Account Control
2.1%	File Deletion
1.7%	DLL Side-Loading
1.4%	Subvert Trust Controls: Code Signing
1.4%	Compiled HTML File
1.4%	Regsvr32
1.4%	Disable or Modify Tools
1.0%	Deobfuscate/Decode Files or Information
1.0%	Code Signing
0.7%	Compile After Delivery
0.7%	Trusted Developer Utilities
0.7%	Control Panel
0.7%	Virtualizaton/Sandbox Evasion
0.7%	Software Packing
0.3%	CMSTP
0.3%	Signed Binary Proxy
0.3%	InstallUtil
0.3%	Execution Guardrails
0.3%	Windows Service
0.3%	Hidden Window

Credential Access

19.9%	LLMNR/NBT-NS Poisoning and SMB Relay
15.4%	Credentials in Files
13.1%	OS Credential Dumping
11.1%	Kerberoasting
10.1%	Network Sniffing
7.5%	Credential Dumping
6.2%	Input Capture
2.9%	Brute Force
2.3%	Password Guessing
2.3%	Credentials in Registry
2.0%	Account Manipulation
2.0%	Forced Authentication
1.6%	Password Cracking
1.6%	Exploitation for Credential Access
0.3%	Process Injection
0.3%	Process Injection: Process Hollowing
0.3%	Input Capture: Credential API Hooking
0.3%	Vaild Accounts
0.3%	Private Keys
0.3%	Modify Authentication Process

Discovery

8.9%	Account Discovery
8.4%	Network Share Discovery
8.2%	File and Directory Discovery
8.0%	Password Policy Discovery
7.8%	Network Service Scanning
5.8%	Remote System Discovery
5.7%	Permission Groups Discovery
5.4%	System Information Discovery
5.2%	Process Discovery
4.8%	System Owner/User Discovery
4.5%	System Network Connections Discovery
4.5%	Domain Trust Discovery
4.4%	Network Sniffing
4.2%	Security Software Discovery
4.1%	System Service Discovery
4.0%	System Network Configuration Discovery
2.5%	Query Registry
1.2%	System Time Discovery
1.1%	Browser Bookmark Discovery
0.7%	Peripheral Device Discovery
0.4%	Application Window Discovery
0.3%	Virtualization/Sandbox Evasion

Lateral Movement

27.3%	Pass the Hash
17.5%	Remote Desktop Protocol
16.5%	SMB/Windows Admin Shares
9.8%	Remote Services
9.3%	Windows Remote Management
5.7%	Exploitation of Remote Services
3.6%	Ingress Tool Transfer
3.6%	Remote File Copy
2.1%	Pass the Ticket
1.5%	Third-Party Software
1.0%	Identify Vulnerabilities in Third-Party Software Libraries
0.5%	Distributed Component Object Model
0.5%	Boot or Logon Initialization Scripts
0.5%	AppleScript
0.5%	Taint Shared Content

Collection

33.1%	Data From Network Shared Drive
28.1%	Data From Local System
13.2%	Input Capture
10.3%	Screen Capture
4.4%	Automated Collection
4.4%	Email Collection
3.7%	Data From Information Repositories
1.5%	Data From Removable Media
0.5%	Audio Capture

Command & Control

15.3%	Non-Standard Port
13.9%	Data Obfuscation
12.9%	Application Layer Protocol
8.9%	Commonly Used Port
8.9%	Data Encoding
7.4%	Web Service
7.4%	Encrypted Channel
6.9%	Commonly Used Port
4.5%	Remote Access Software
3.5%	Ingress Tool Transfer
3.5%	Remote File Copy
2.5%	Proxy
2.5%	Non-Application Layer Protocol
1.5%	Standard Non-Application Layer Protocol
0.5%	Multi-hop Proxy

Exfiltration

65.6%	Exfiltration Over C2 Channel
11.5%	Exfiltration Over Alternative Protocol
8.2%	Automated Exfiltration
3.3	Data Encrypted
4.9%	Archive Collected Data
4.9%	Data Compressed
1.6%	Exfiltration Over Network Medium

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.