TLP:WHITE

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

FISCAL YEAR 2020 (FY20)

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

+ POTENTIAL ATTACK PATHS

Attack Path 1: Seems “Phishy” to Me

Initial Access » Phishing Link and MSHTA
Execution » PowerShell
Defense Evasion » Process Injection and MSHTA
Discovery » Network Sniffing
Collection » Data from Local System
Command & Control » Remote Access Software

Attack Path 2: Where is the Poison Control?

Initial Access » Valid Accounts
Execution » Windows Management Instrumentation
Credential Access » LLMNR/NBT-NS Poisoning and Relay
Discovery » Permission Groups Discovery
Collection » Data from Network Shared Drives
Command & Control » Standard Application Layer Protocol

Attack Path 3: Discover & Unlock

Initial Access » Trusted Relationship
Execution » Windows Management Instrumentation
Discovery » Permission Groups Discovery
Collection » Data from Local System
Command & Control » Remote Access Software

Attack Path 4: Take Into Account: Good Guy or Bad Guy?

Initial Access » User Execution
Execution » Windows Management Instrumentation
Discovery » Account Discovery
Collection » Data from Local System/
Data from Network Shared Drive
Command & Control » Remote Access Software
Exfiltration » Exfiltration over C2 Channel

Attack Path 5: Credential Convenience Has Its Cost

Initial Access » Valid Accounts
Execution » Windows Management Instrumentation
Credential Access » OS Credential Dumping
Discovery » Account Discovery
Collection » Data from Local System/
Data from Network Shared Drive
Command & Control » Remote Access Software

FY20 RVA RESULTS

MITRE ATT&CK Tactics and Techniques

This page is a breakout of the top three most successful techniques in each tactic. The percent noted for each technique represents the success rate for that technique across all RVAs. For example, a phishing link was used to gain initial access in 49% of the FY20 RVAs.

Note: see https://www.cisa.gov/publication/rva for *CISA Analysis: FY2020 Risk and Vulnerability Assessments*, which provides a sample attack path that could compromise an organization that has weaknesses that are representative of those in the FY20 RVAs.

*CISA encourages organizations to request the assessment services available on the **CISA Cyber Resource Hub**. The more assessment data CISA can collect, the better the analysis we can share with partners to help them gain visibility into vulnerability trends, adversarial activities and, most importantly, effective mitigations to implement for better protection of their networks.*

37 Total Number of Assessments

Initial Access

Phishing Link	49%
Exploit Public-Facing Application	11.8%
Phishing Attachment	9.8%

Credential Access

OS Credential Dumping	17%
LLMNR/NBT-NS Poisoning & SMB Rekay	17%
Kerberoasting	13.2%

Execution

PowerShell	24.4%
Windows Management Instrumentation	13%
Command & Scripting Interpreter	12.2%

Discovery

Account Discovery	12.1%
Network Service Scanning	10.9%
File & Directory Discovery	8.1%

Privilege Escalation

Valid Accounts	37.5%
Exploitation for Privilege Escalation	21.9%
Make & Impersonate Token	15.6%

Lateral Movement

Pass the Hash	29.8%
Remote Desktop Protocol	25%
Exploitation of Remote Services	11.9%

Command & Control

Web Protocols	42%
Remote Access Software	15.9%
Standard Application Layer Protocol	8.7%

Defense Evasion

Process Hollowing	18.5%
Mshta	12.3%
Valid Accounts	12.3%

Collection

Data from Local System	32.2%
Data from Network Shared Drive	30.5%
Screen Capture	22%

Exfiltration

Exfiltration Over C2 Channel	68.2%
Archive Collected Data	9.1%
Automated Exfiltration	9.1%

This advisory uses the MITRE ATT&CK® v9.0 and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks at https://attack.mitre.org/versions/v9/ for referenced threat actor techniques. For more information about CISA assessment services, please visit https://www.cisa.gov/cyber-resource-hub.

TLP:WHITE

TLP:WHITE

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

FISCAL YEAR 2020 (FY20)

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

MITIGATIONS FOR TOP TECHNIQUES

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

M1013 Application Developer Guidance

Provide secure software best practice guidance and training to application developers to avoid introducing security weaknesses through code.

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.

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

Configure Network Intrusion Prevention systems to block malicious file signatures and file types at the network boundary.

M1042 Disable or Remove Feature or Program

Remove or deny access to unnecessary and potentially vulnerable software to prevent abuse by adversaries.

M1049 Antivirus/Antimalware

Maintain Antivirus/Antimalware software up to date and configured to recognize and remove malicious files that have been downloaded or created on the host.

M1051 Update Software

Periodically perform software updates, including vendor patches, OS updates, and firmware upgrades, to mitigate exploitation risk.

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

FY20 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, a phishing link was used to gain initial access in 49% of the FY20 RVAs.

37 Total Number of Assessments

Initial Access

49.0%	Phishing Link
11.8%	Exploit Public-Facing Application
9.8%	Phishing Attachment
11.8%	Valid Accounts
5.88%	User Execution
3.92%	Trusted Relationship
1.96%	Drive-by Compromise
1.96%	Exploitation of Remote Application
1.96%	Exploitation of Remote Services

Execution

24.4%	PowerShell
13.0%	Windows Management Instrumentation
12.2%	Command and Scripting Interpreter
11.4%	Service Execution
11.4%	Windows Command Shell
8.9%	User Execution
7.3%	Mshta
3.3%	Remote Services
2.4%	Exploitation for Client Execution
1.6%	Rundll32
0.8%	Native API
0.8%	Regsvr32
0.8%	Remote Desktop Protocol
0.8%	Shared Modules
0.8%	Windows Remote Management

Privilege Escalation

37.5%	Valid Accounts
21.9%	Exploitation for Privilege Escalation
15.6%	Make & Impersonate Token
9.4%	Process Injection
6.3%	Sudo and Sudo Caching
3.1%	Access Token Manipulation
3.1%	Bypass User Account Control
3.1%	Default Accounts

Defense Evasion

18.5%	Process Hollowing
12.3%	Mshta
12.3%	Valid Accounts
10.8%	Obfuscated Files or Information
9.2%	File Deletion
6.2%	Default Accounts
4.6%	Access Token Manipulation
4.6%	Web Service
3.1%	Hidden Window
3.1%	Bypass User Account Control
3.1%	Process Injection
3.1%	Rundll32
1.5%	DLL Side-Loading
1.5%	Group Policy Modification
1.5%	Masquerading
1.5%	Software Packing
1.5%	Indicator Removal from Tools
1.5%	Regsvr32

Credential Access

17.0%	OS Credential Dumping
17.0%	LLMNR/NBT-NS Poisoning & SMB Relay
13.2%	Kerberoasting
9.4%	Credentials in Files
8.8%	Password Cracking
7.5%	Password Guessing
7.5%	Network Sniffing
6.9%	Forced Authentication
3.1%	Exploitation of Credential Access
3.1%	Credentials in Registry
1.9%	Brute Force
1.3%	Bash History
0.6%	Unsecured Credentials
0.6%	Private Keys
0.6%	Pass the Ticket
0.6%	Input Prompt
0.6%	Two-Factor Authentication Interception

Discovery

12.1%	Account Discovery
10.9%	Network Service Scanning
8.1%	File & Directory Discovery
8.1%	Permission Groups Discovery
7.7%	Password Policy Discovery
6.9%	Remote System Discovery
6.0%	Network Share Discovery
6.0%	Process Discovery
5.6%	Domain Trust Discovery
4.4%	Network Share Discovery
4.0%	System Owner/User Discovery
4.0%	System Service Discovery
3.6%	System Network Connections Discovery
3.2%	System Information Discovery
2.4%	Security Software Discovery
2.4%	System Network Configuration Discovery
2.0%	Query Registry
1.2%	System Time Discovery
0.8%	Network Sniffing
0.4%	Browser Bookmark Discovery

Lateral Movement

29.8%	Pass the Hash
25.0%	Remote Desktop Protocol
11.9%	Exploitation of Remote Services
10.7%	Remote Services
10.7%	SMB/Windows Admin Shares
6.0%	Windows Admin Shares
2.4%	Pass the Ticket
2.4%	Windows Remote Management
1.2%	Ingress Tool Transfer

Collection

32.2%	Data from Local System
30.5%	Data from Network Shared Drive
22.0%	Screen Capture
5.1%	Keylogging
1.7%	Data from Information Repositories
3.4%	Man-in-the-Middle
1.7%	Man in the Browser
3.4%	Automated Collection

Command & Control

42.0%	Web Protocols
15.9%	Remote Access Software
8.7%	Standard Application Layer Protocol
8.7%	Data Obfuscation
7.2%	Data Encoding
5.8%	Encrypted Channel
4.3%	Proxy
2.9%	Web Service
1.4%	Custom Command & Control Protocol
1.4%	Standard Cryptographic
1.4%	Protocol
1.4%	Ingress Tool Transfer

Exfiltration

68.2%	Exfiltration over C2 Channel
9.1%	Archive Collected Data
9.1%	Automated Exfiltration
9.1%	Scheduled Transfer
4.5%	Data Transfer Size Limits

This advisory uses the MITRE ATT&CK® v9.0 and Pre-ATT&CK frameworks. See the ATT&CK for Enterprise and Pre-ATT&CK frameworks at https://attack.mitre.org/versions/v9/ for referenced threat actor techniques. For more information about CISA assessment services, please visit https://www.cisa.gov/cyber-resource-hub.

TLP:WHITE