CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

FY23 RISK AND VULNERABILITY ASSESSMENTS (RVA) RESULTS

MITRE ATT&CK™ TACTICS AND TECHNIQUES

The percent noted for each technique represents the success rate for that technique across 145 RVA assessments.

Mitigations reference CISA Cyber Performance Goals (CPGs). CPGs are a prioritized subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks and are applicable across all Critical Infrastructure sectors.

CLICK TO REVIEW COMPANION ANALYSIS

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Initial Access

Threat actors attempt to obtain unauthorized initial access into a victim’s network. Actors use techniques, such as Valid Accounts T1078 or Spear Phishing Link T1566.002s, to gain this access. After obtaining initial access, actors can then execute other techniques to move about the network.

Mitigations

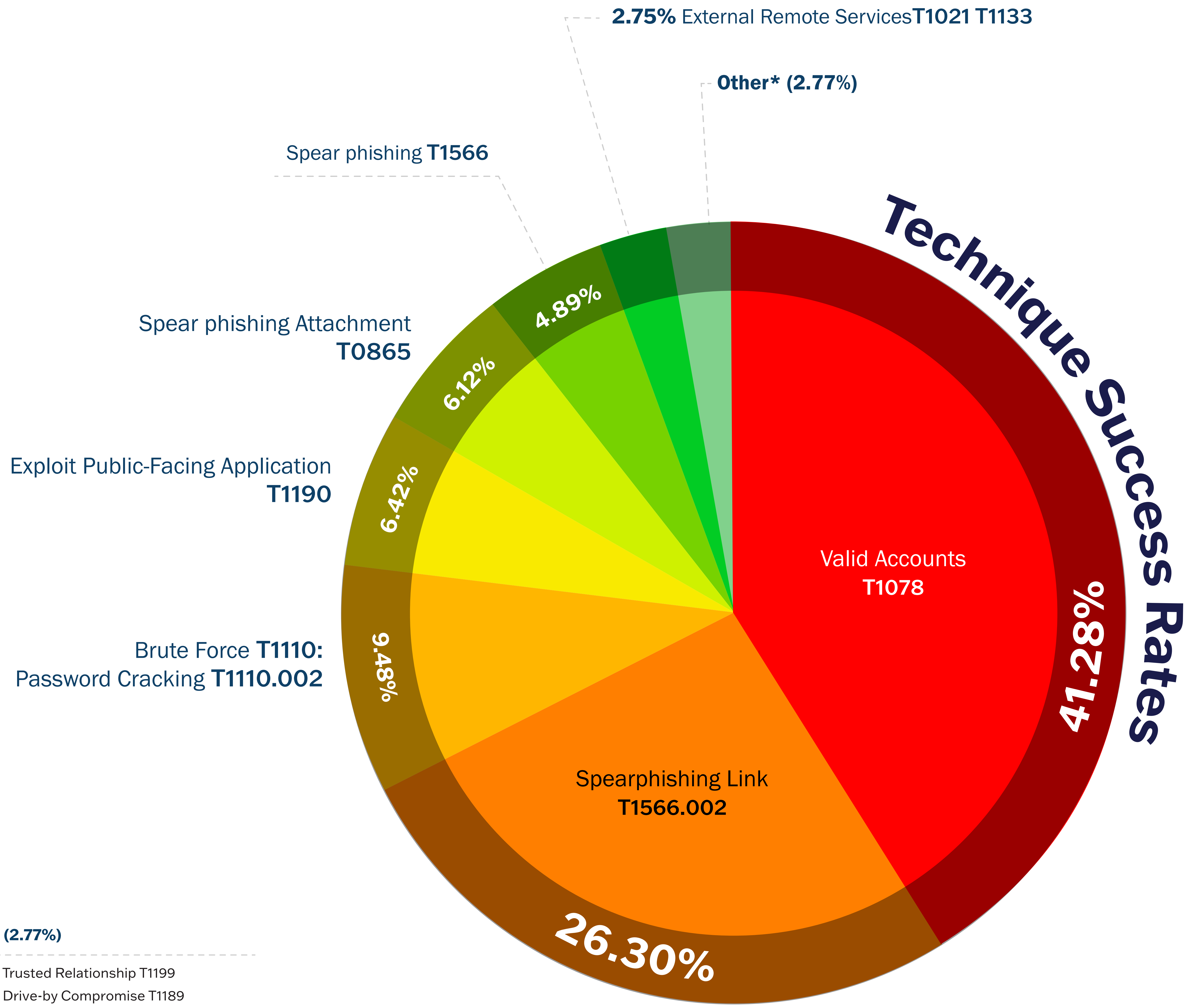
Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 1.E Mitigating Known Vulnerabilities CPG 2.A Changing Default Passwords

CPG 2.H Phishing-Resistant Multifactor Authentication CPG 2.M Email Security

CPG 2.N Disable Macros by Default

CPG 2.W No Exploitable Services on the Internet



*Other (2.77%)

0.92%	Trusted Relationship T1199
0.92%	Drive-by Compromise T1189
0.31%	Hardware Additions T1200
0.31%	Replication Through Removable Media
0.31%	Process Injection T1631 T1055

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Execution

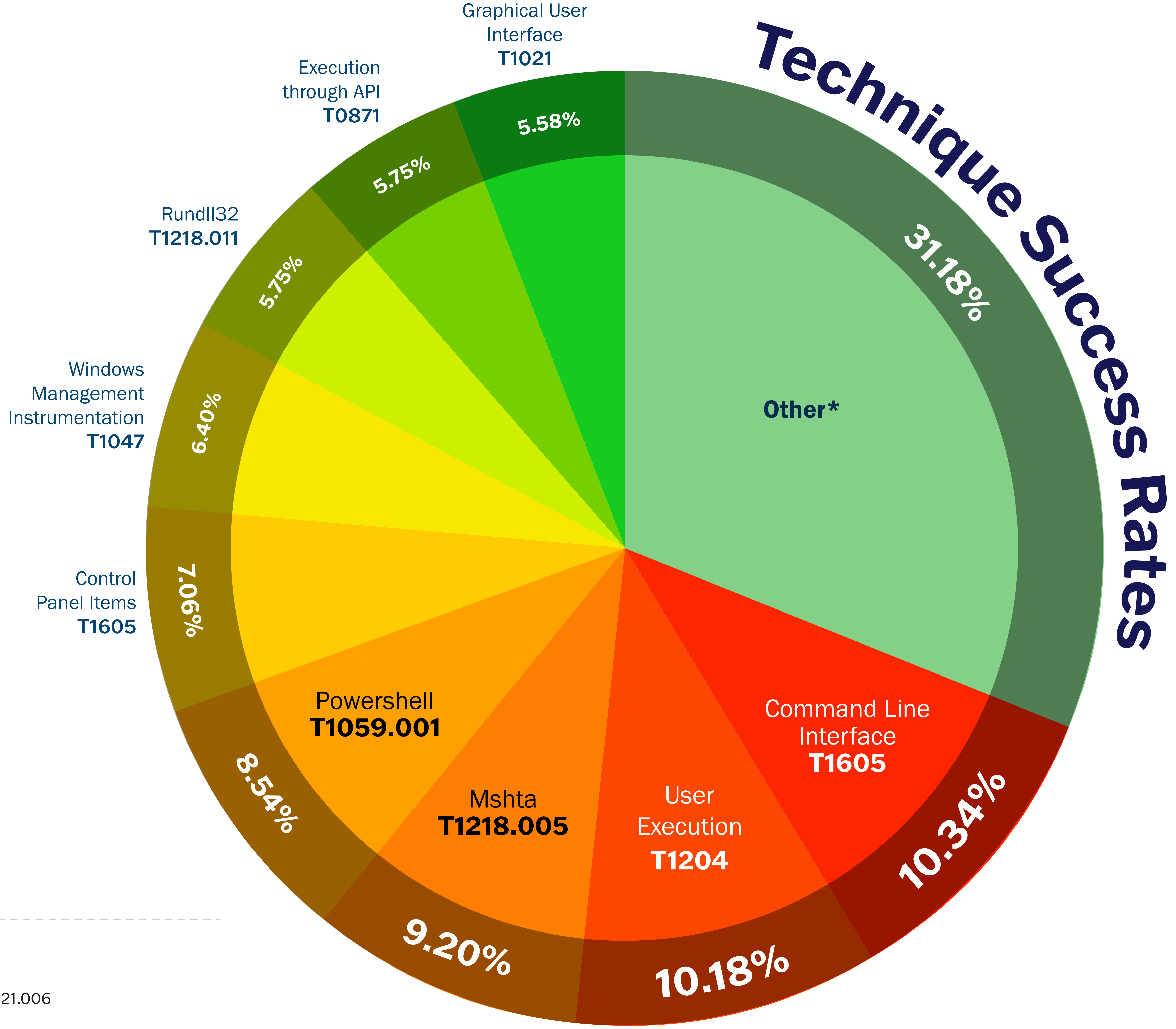
After obtaining initial access, threat actors use a variety of tools to execute malicious code that further compromises victim systems and networks. For example, threat actors may execute Powershell T1059.001 scripts to run commands and payloads.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.Q Hardware and Software Approval Process CPG 2.T Log Collection

CPG 3.A Detecting Relevant Threats and TTPs



***Other (31.18%)**

4.11%	Compiled HTML File T1218.001
3.78%	Scripting T0853
3.45%	Windows Remote Management T1021.006
3.45%	Regsvcs/Regasm T1218.009
2.46%	LSASS Driver T1547.008
1.81%	Service Execution T1569.002
1.81%	Execution through Module Load T1129
1.48%	Exploitation for Client Execution T1203
1.48%	Signed Binary Proxy Execution T1218
1.15%	Trusted Developer Utilities T1127
0.82%	Third Party Software T1072
0.82%	Pass the Hash T1550.002
0.82%	Regsvr32 T1218.010
0.66%	Windows Admin Shares T1021.002
0.49%	Remote Desktop Protocol T1021.001
0.49%	Remote File Copy T1105
0.49%	Pass the Ticket T1550.003
0.33%	Scheduled Task T1053
0.16%	Space after Filename T1036.006
0.16%	Account Discovery T1087
0.16%	Network Service Scanning T1046
0.16%	Exploitation of Remote Services T1021
0.16%	Signed Script Proxy Execution T1218
0.16%	Remote Services T1021
0.16%	Exploitation for Credential Access T1212
0.16%	Proxy Execution T1218

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Persistence

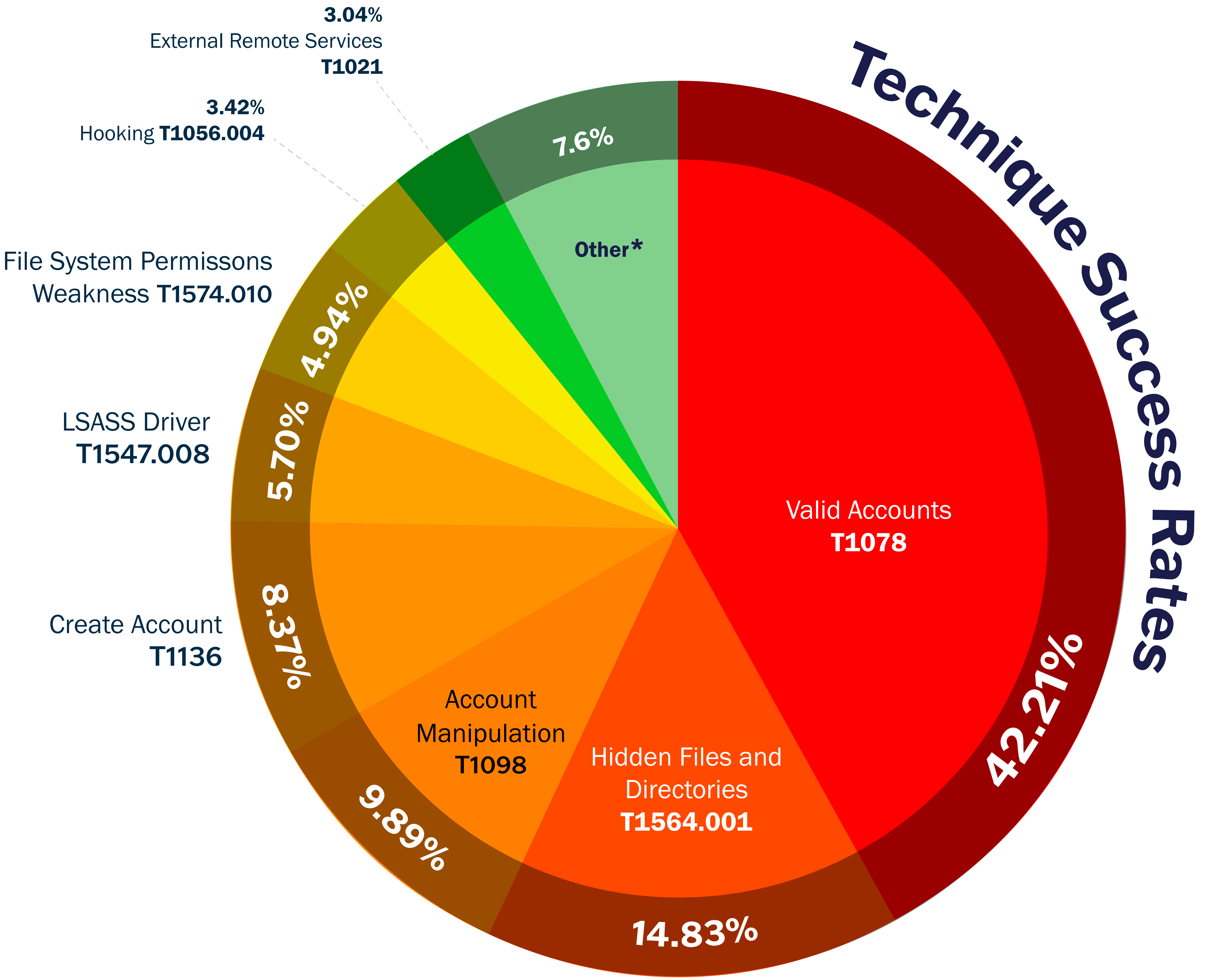
Threat actors maintain persistence or foothold in a network or system by changing credentials or modifying configuration files to maintain continued access. Threat actors may also monitor and manipulate reports observed in the Server Manager Performance Monitor to remain undetected.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.T Log Collection



***Other (7.6%)**

1.52%	Web Shell T1505.003	0.38%	New Service
1.14%	DLL Search Order Hijacking T1574.001	0.38%	Event Subscription T1546.003
0.76%	Redundant Access	0.38%	Office Application Startup T1137
0.76%	Login Item T1547.015	0.38%	Windows Management Instrumentation T1047
0.38%	Hypervisor	0.38%	Image File Execution Options Injection T1546.012
0.38%	Service Registry Permissions Weakness	0.38%	Scheduled Task T1053
0.38%	Modify Existing Service		

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Privilege Escalation

Threat actors attempt to obtain escalated privileges to further compromise a network. Actors search systems for hard-coded or default credentials. When carrying out an attack, threat actors conduct extensive reconnaissance and credential harvesting to identify administrator accounts.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.C Unique Credentials

CPG 2.L Secure Sensitive Data

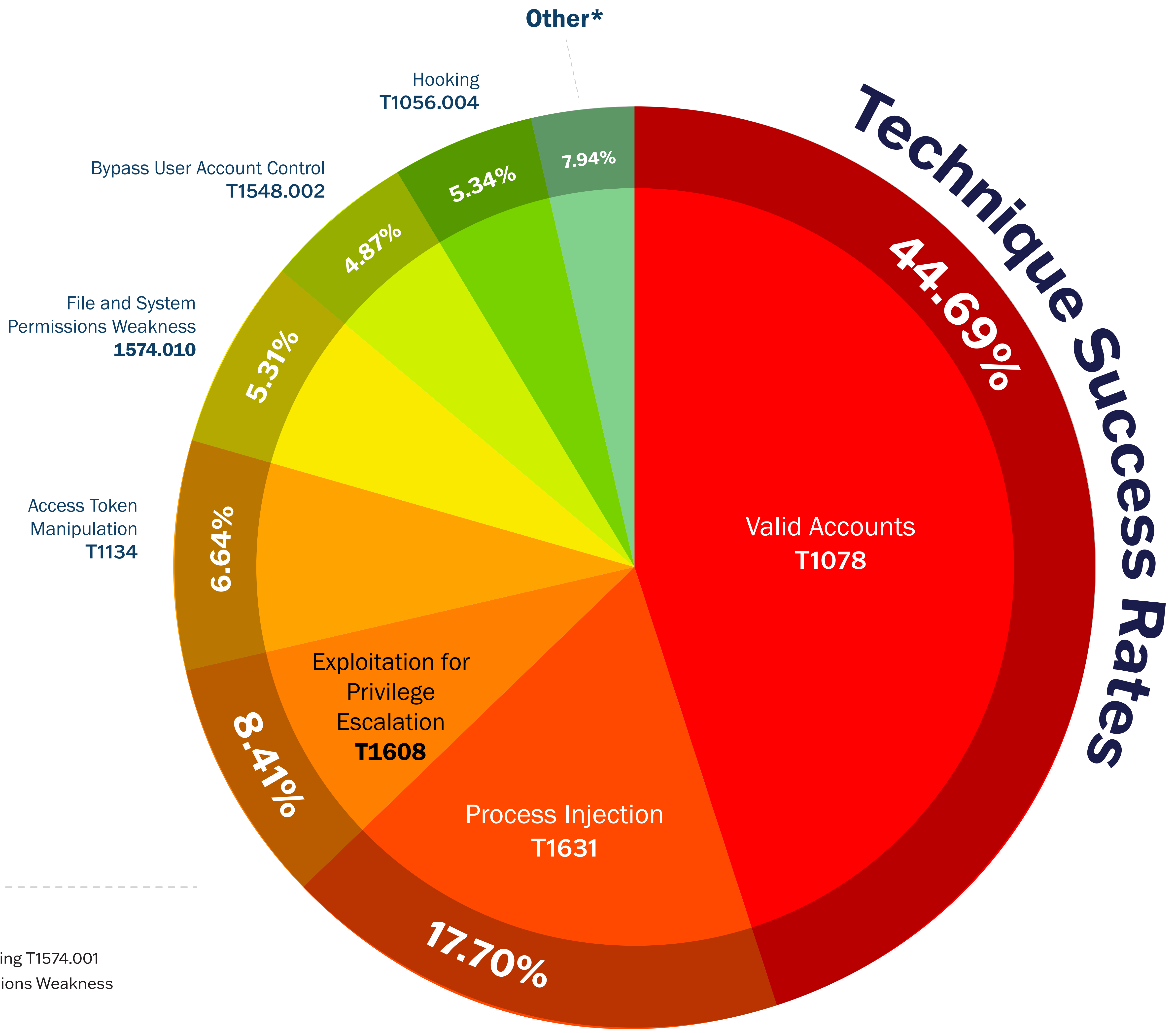
CPG 2.F Network Segmentation

CPG 2.G Detection of Unsuccessful Login attempts

CPG 3.A Detecting Relevant Threats and TTPs

ATT&CK®

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 **cisa.gov**.



***Other (7.94%)**

1.77%	Web Shell T1505.003
1.33%	Scheduled Task T1053
0.44%	DLL Search Order Hijacking T1574.001
0.44%	Service Registry Permissions Weakness
0.44%	Masquerading T1036
0.44%	Rundll32 T1218.011
0.44%	Virtualization/Sandbox Evasion T1497
0.44%	Sudo T1548.003
0.44%	Web Accounts
0.44%	Image File Execution Options Injection T1546.012
0.44%	Extra Window Memory Injection T1055.011
0.44%	Web Service T1102
0.44%	New Service
0.44%	Control Panel Items T1605
0.44%	Mshta T1218.005

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Defense Evasion

Threat actors utilize defense evasion techniques, such as disabling security software or obfuscating data.

Mitigations

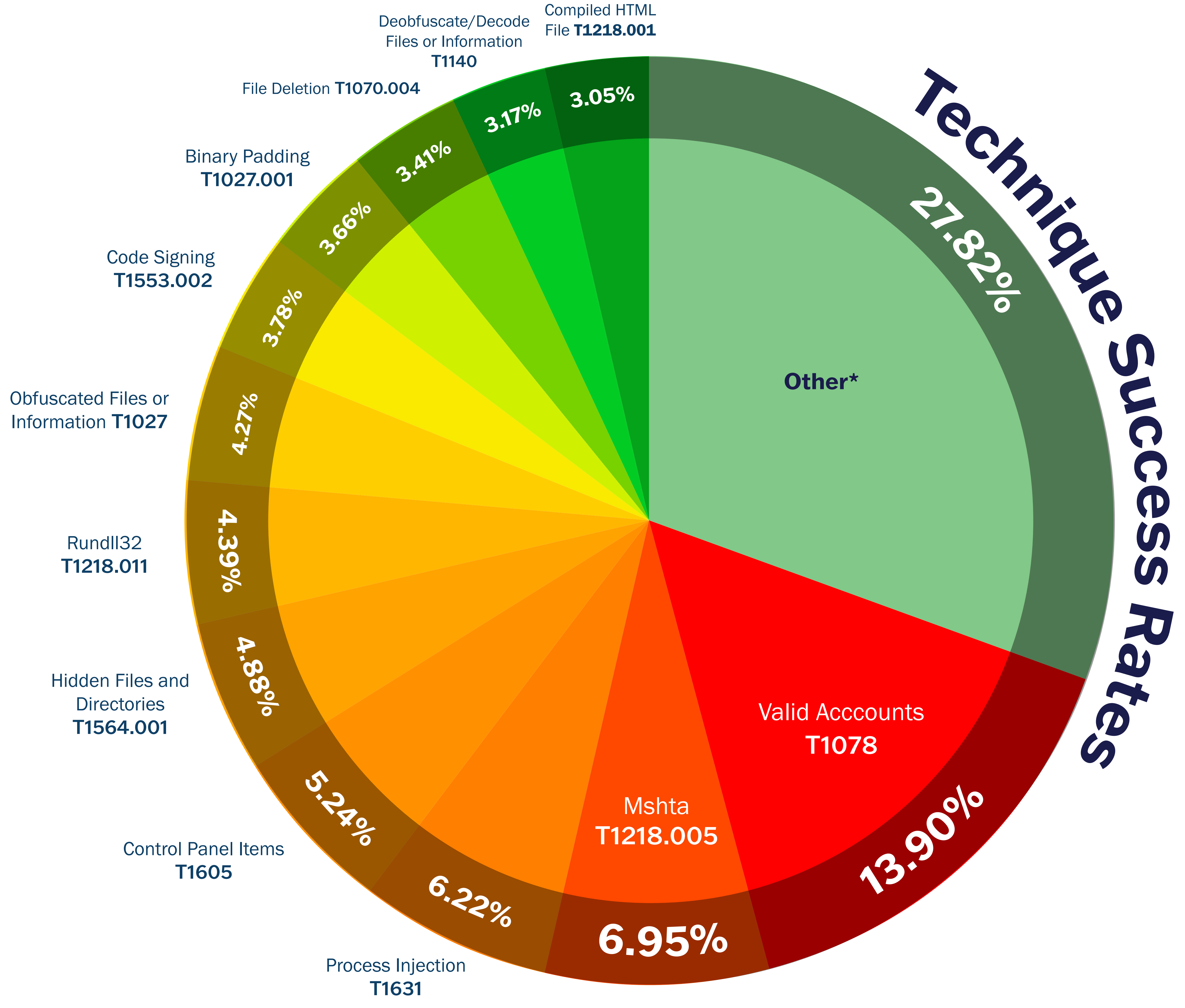
Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.A Changing Default Passwords

CPG 2.E Separating User and Privileged Accounts

CPG 2.T Log Collection

CPG 2.U Secure Log Storage



***Other (27.82%)**

2.93%	Web Service T1102	1.22%	ZSigned Binary Proxy Execution T1218	0.24%	New Service
2.80%	Scripting T0853	0.85%	Trusted Developer Utilities T1127	0.24%	Credential Dumping T1003
2.68%	Regsvcs/Regasm T1218.009	0.73%	Indicator Removal on Host T1070	0.12%	Network Sniffing T1040
2.32%	Virtualization/Sandbox Evasion T1497	0.73%	Execution Guardrails T1480	0.12%	Group Policy Modification T1021
2.32%	Hidden Window T1564.003	0.61%	Regvr32 T1218.010	0.12%	Extra Window Memory Injection T1055.011
2.32%	Indicator Blocking T1562.006	0.61%	Exploitation for Defense Evasion T1211	0.12%	Credentials in Files T1552.001
2.20%	Access Token Manipulation T1134	0.61%	DCShadow T1207	0.12%	Credentials In Registry T1552.002
1.95%	Indicator Blocking T1562.006	0.49%	Template Injection T1221	0.12%	Signed Script Proxy Execution T1218
1.83%	DLL Side-Loading T1574.002	0.49%	Indirect Command Execution T1202	0.12%	Image File Execution Options Injection T1546.012
1.83%	Process Hollowing T1055.012	0.49%	File Permissions Modification T1222.002	0.12%	Disabling Security Tools T1629.003
1.59%	Software Packing T1027.002	0.37%	Masquerading T1036	0.12%	Space after Filename T1036.006
1.59%	Compile After Delivery T1027.004	0.37%	DLL Search Order Hijacking T1574.001	0.12%	Powershell T1059.001
1.46%	Bypass User Account Control T1548.002				

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Credential Access

Threat actors steal credentials to gain access to internal resources, obfuscate their movements, and escalate privileges. Actors use a variety of techniques, such as keylogging or Credential Dumping T1003. Some threat actors target Ntdsutil, a Windows utility that stores Active Directory data, including usernames and passwords.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

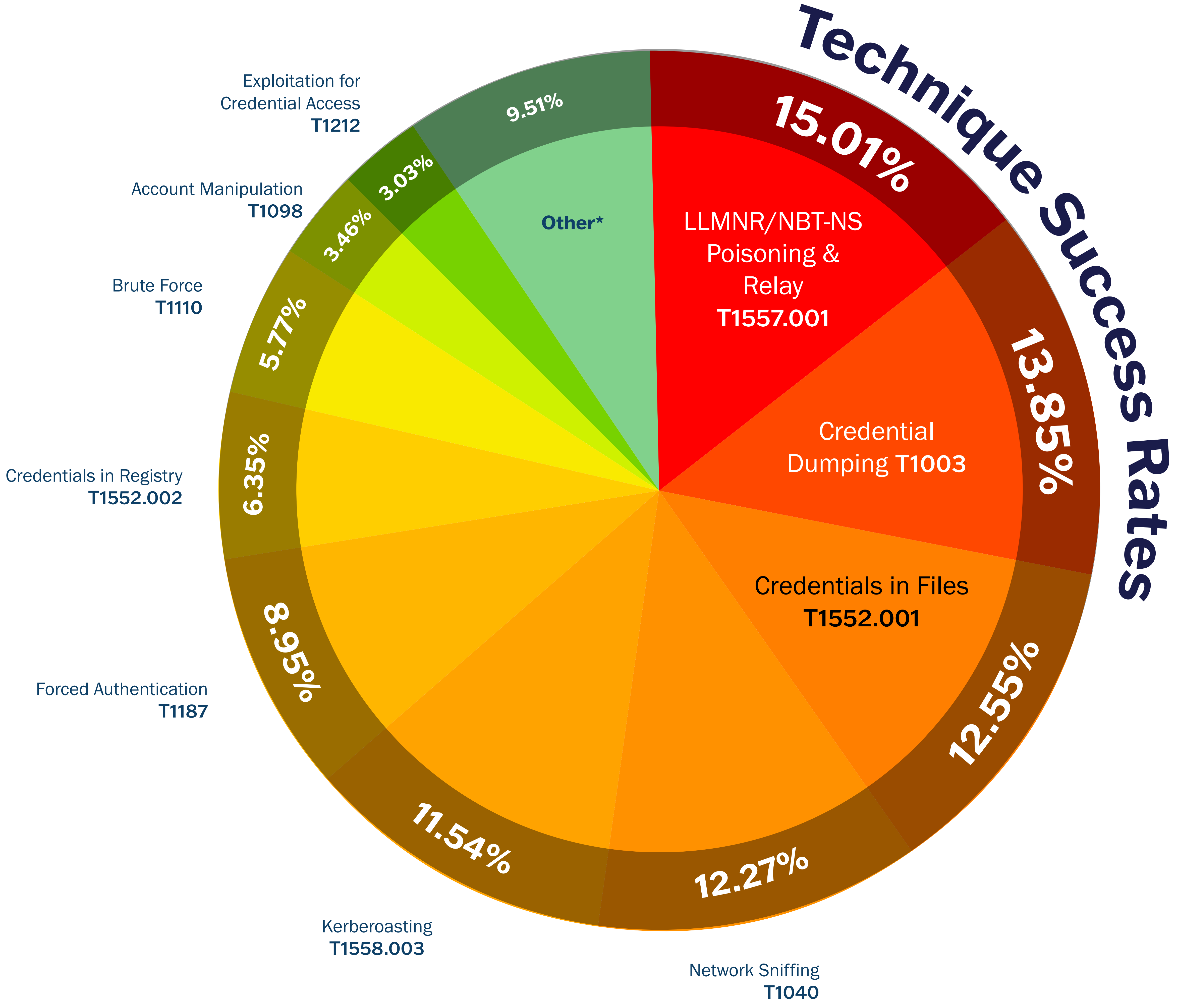
CPG 2.C Unique Credentials

CPG 2.D Revoking Credentials for Departing Employees

CPG 2.E Separating User and Privileged Accounts

CPG 2.G Detection of Unsuccessful (Automated) Login Attemps

CPG 3.A Detecting Relevant Threats and TTPs



***Other (9.51%)**

2.02%	Web Shell T1505.003
1.44%	DLL Search Order Hijacking T1574.001
1.30%	Redundant Access
0.58%	Login Item T1547.015
0.43%	Hypervisor
0.29%	Service Registry Permissions Weakness T1574.011
0.29%	Modify Existing Service T1629.003
0.29%	New Service
0.14%	Event Subscription T1546.003
0.14%	Office Application Startup T1137
0.14%	Windows Management Instrumentation T1047
0.14%	Image File Execution Options Injection T1546.012

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Discovery

Threat actors use the system information discovery technique to learn about victim systems, networks, and data. For example, actors can use a system information tool to determine whether a system, firmware, or open port is a good candidate to target.

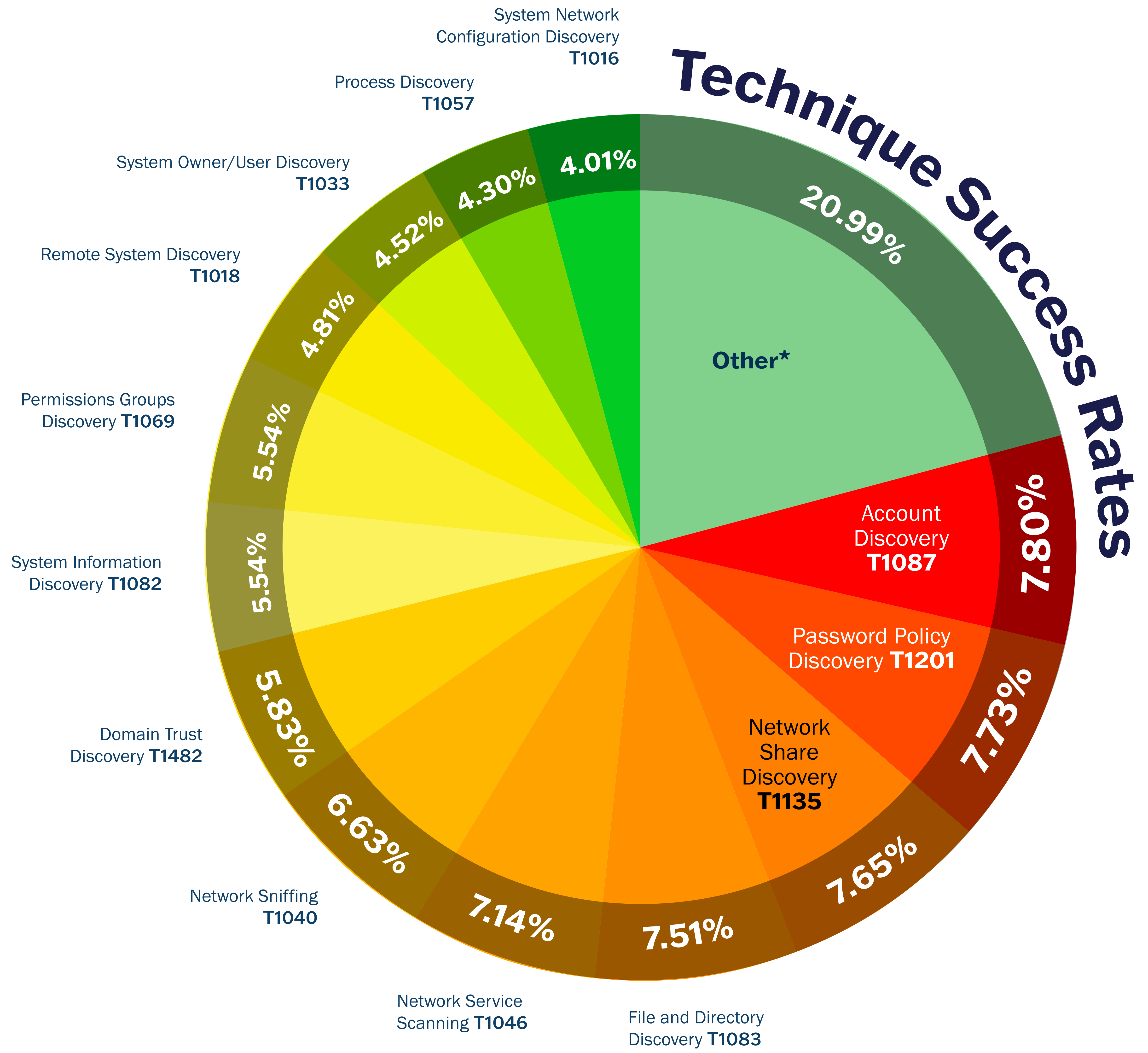
Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.F Network Segmentation

CPG 2.T Log Collection

CPG 3.A Detecting Relevant Threats and TTPs



***Other (20.99%)**

3.50%	System Network Connections Discovery T1421
3.50%	Security Software Discovery T1418.001
3.43%	System Service Discovery T1007
2.99%	Query Registry T1012
1.82%	Application Window Discovery T1010
1.82%	Browser Bookmark Discovery T1217
1.46%	System Time Discovery T1124
1.38%	Virtualization/Sandbox Evasion T1497
1.09%	Peripheral Device Discovery T1120

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Lateral Movement

Threat actors move laterally in a network to reposition, supplement, or spread their active foothold. Actors frequently move from host to host until they reach the location within the target environment necessary to conduct further attack steps.

Mitigations

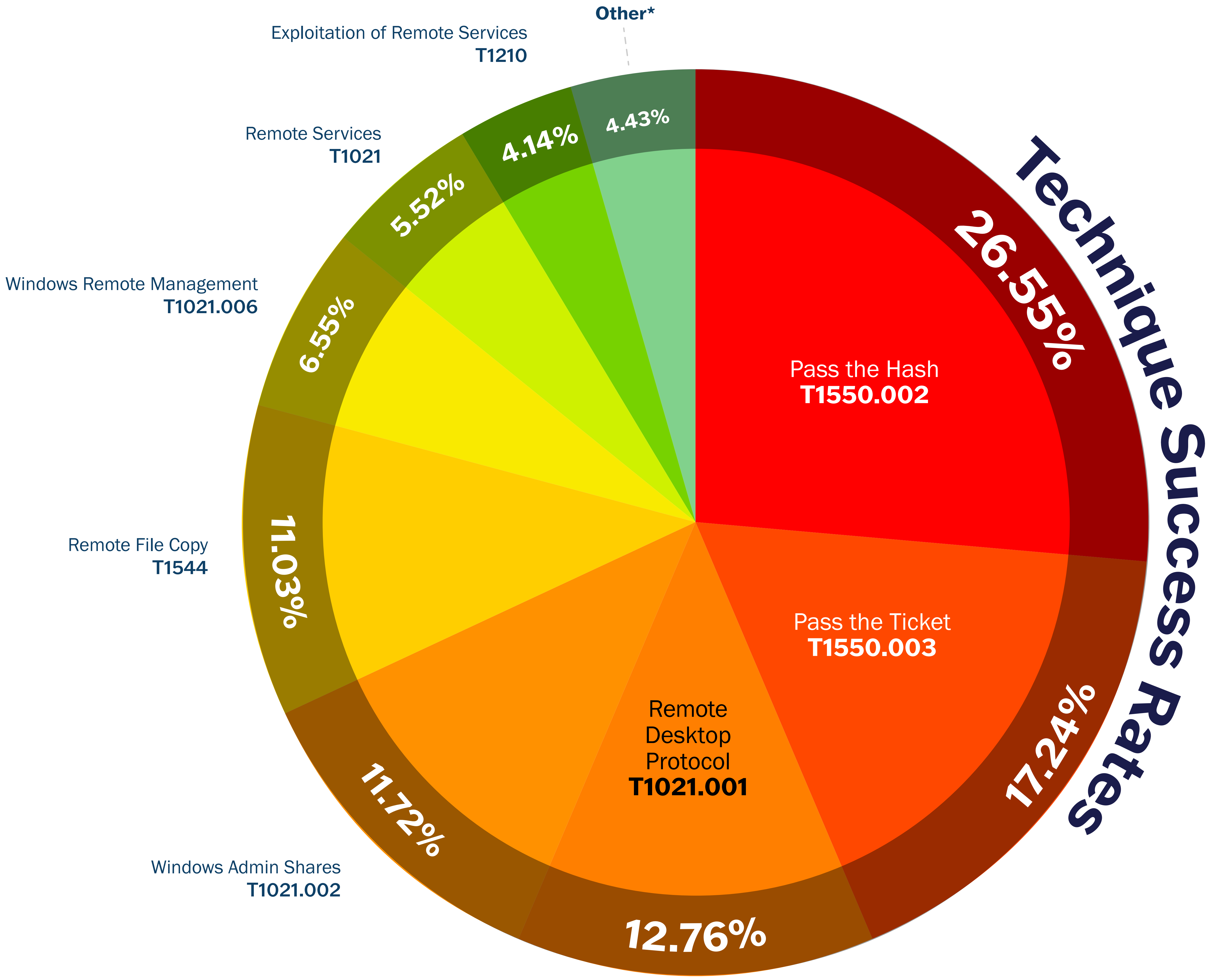
Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.C Unique Credentials CPG 2.F Network Segmentation

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.F Network Segmentation

CPG 2.T Log Collection



***Other (4.43%)**

1.03%	Third Party Software T1072
0.34%	Windows Management Instrumentation T1047
0.34%	User Execution T1204
0.34%	Control Panel Items T1605
0.34%	Taint Shared Content T1080
0.34%	Replication Through Removable Media T1091
0.34%	Powershell T1059.001
0.34%	Rundll32 T1218.011
0.34%	Mshta T1218.005
0.34%	Regsvcs/Regasm T1218.009
0.34%	Shared Webroot

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Collection

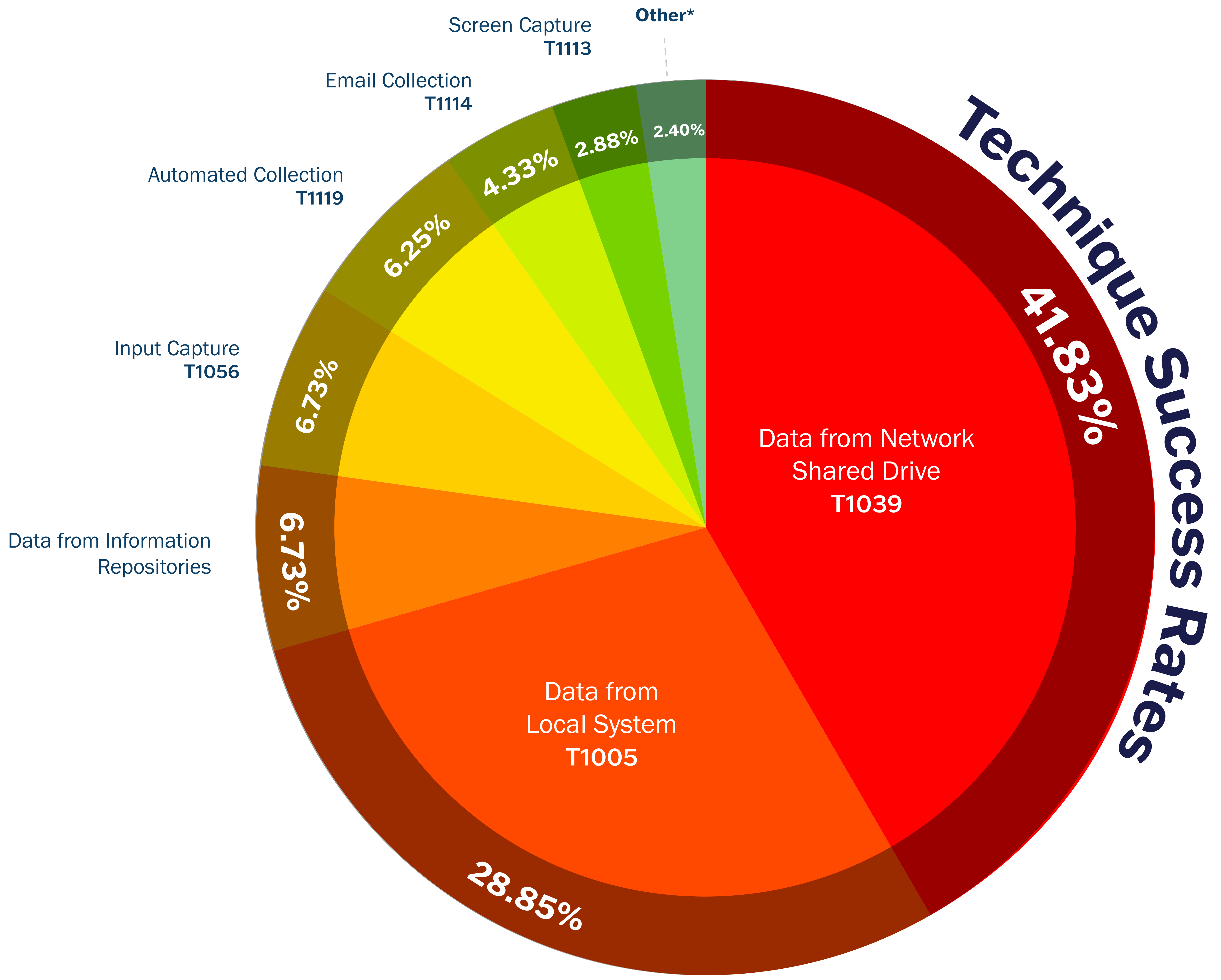
Threat actors use a variety of techniques to collect sensitive internal data, such as capturing screenshots and keyboard inputs. They often collect data by accessing shared drives.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 1.3 Log Collection

CPG 8.2 Detecting Relevant Threats and TTPs



***Other (2.40%)**

0.96%	Data Staged T1074
0.96%	Data from Removable Media T1025
0.48%	Man in the Browser T1185

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Command and Control

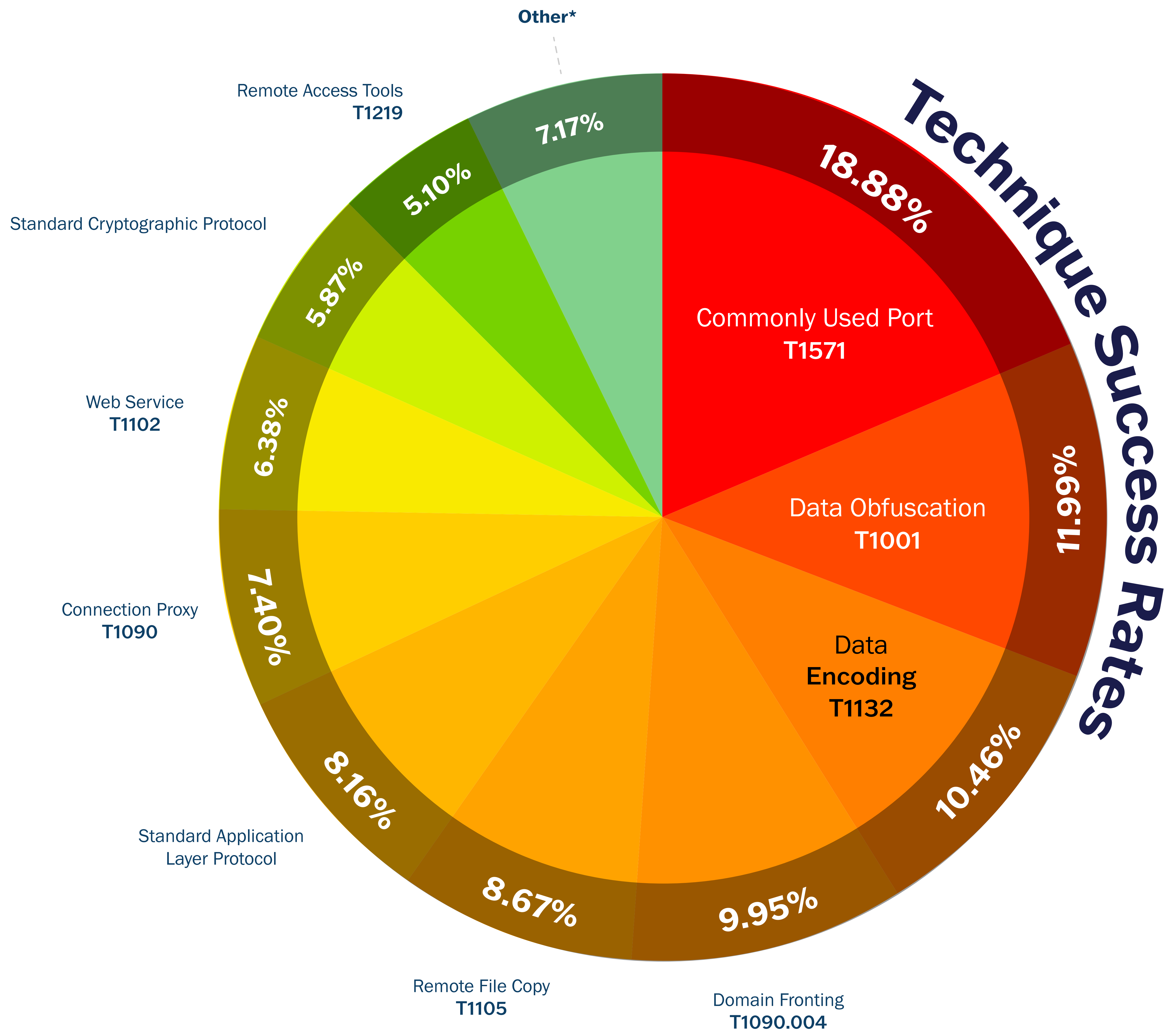
Threat actors use hidden communication channels between their remote servers and compromised systems within a targeted network to conduct internal activity without detection. Through backdoors or commonly used ports, threat actors can gain command and control of the compromised system.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 3.1 Log Collection

CPG 8.2 Detecting Relevant Threats and TTPs



***Other (7.17%)**

2.30%	Multilayer Encryption	0.26%	Custom Cryptographic Protocol
1.79%	Custom Command and Control Protocol T1095	0.26%	Uncommonly Used Port
1.02%	Multi-hop Proxy T1090.003	0.26%	Application Layer Protocol T1071
0.51%	Fallback Channels T1008	0.26%	Standard Non-Application Layer Protocol
0.51%	Input Capture T1056		

ATT&CK®

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 **cisa.gov**.

FY23 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Exfiltration

Threat actors often exfiltrate sensitive data from victim networks. Actors sometimes remove data over command-and-control channels and hex encode the data. By exfiltrating the data, threat actors can analyze it from the safety of their remote locations.

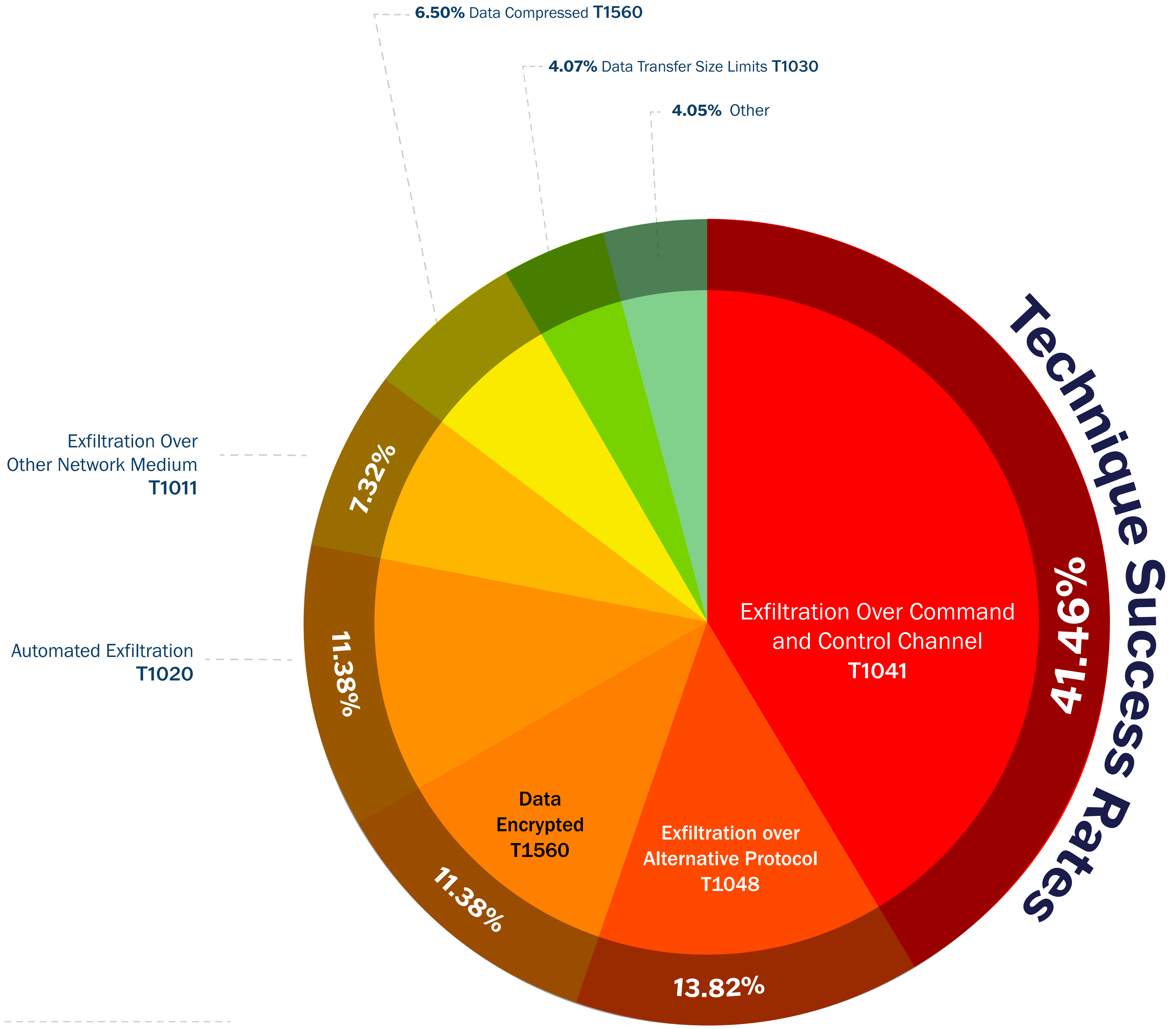
Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following CPGs:

CPG 2.T Log Collection

CPG 2.R System Backups

CPG 3.A Detecting Relevant Threats and TTPs



***Other (4.05%)**

0.81%	Pass the Hash T1550.002
0.81%	Exfiltration Over Alternative Protocol T1048
0.81%	User Execution T1204
0.81%	Exfiltration for Client Execution T1203
0.81%	Exfiltration Over Physical Medium T1052

ATT&CK®

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 **cisa.gov**.