CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

FY22 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 121 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. CPGs are applicable across all Critical Infrastructure sectors.

FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

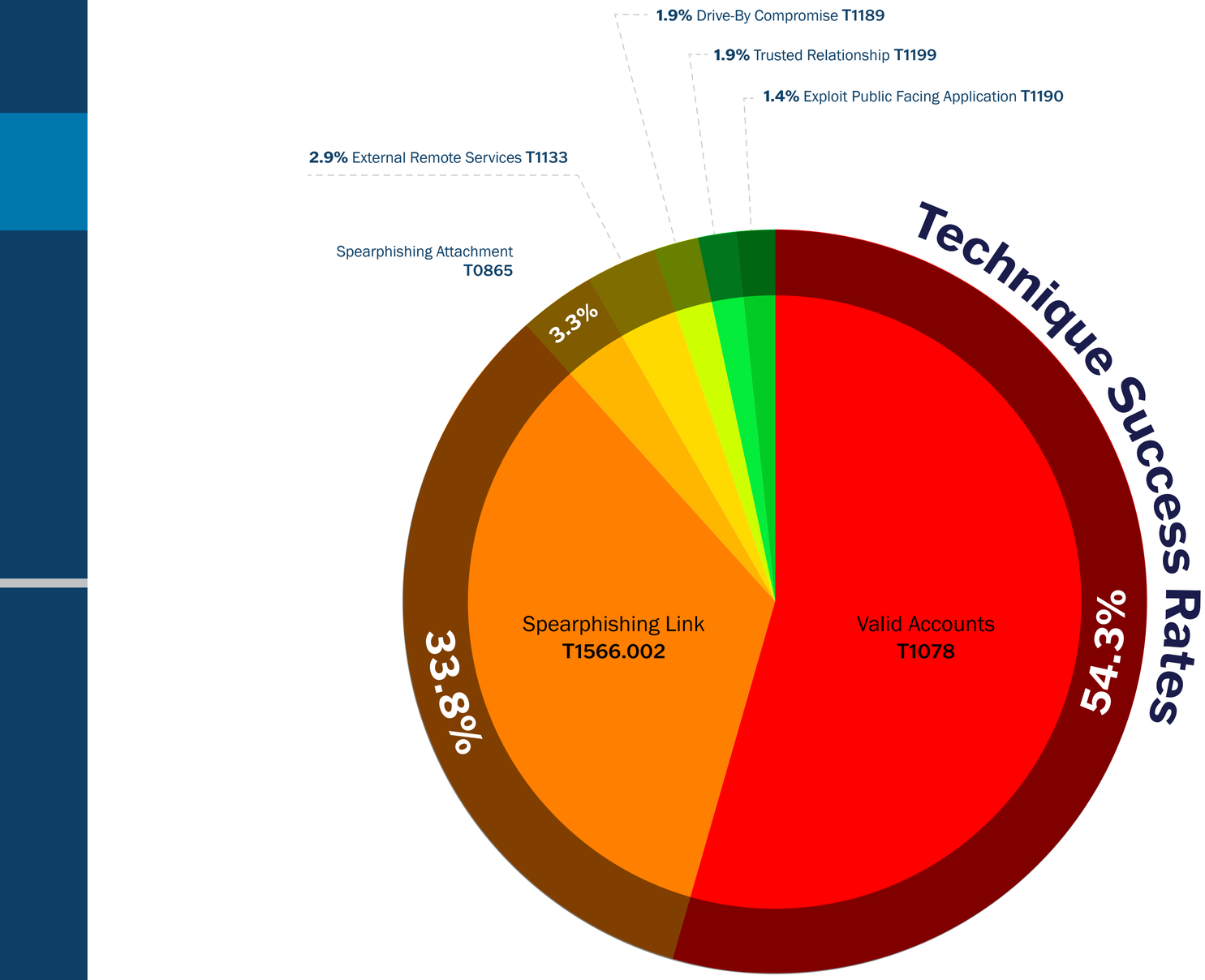
Initial Access

Threat actors attempt to obtain unauthorized initial access into a victim's network. Actors use techniques, such as valid accounts or spearphishing links, 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 Cyber Performance Goals (cisa.gov/cpg):

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



FY22 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 scripts to run commands and payloads.

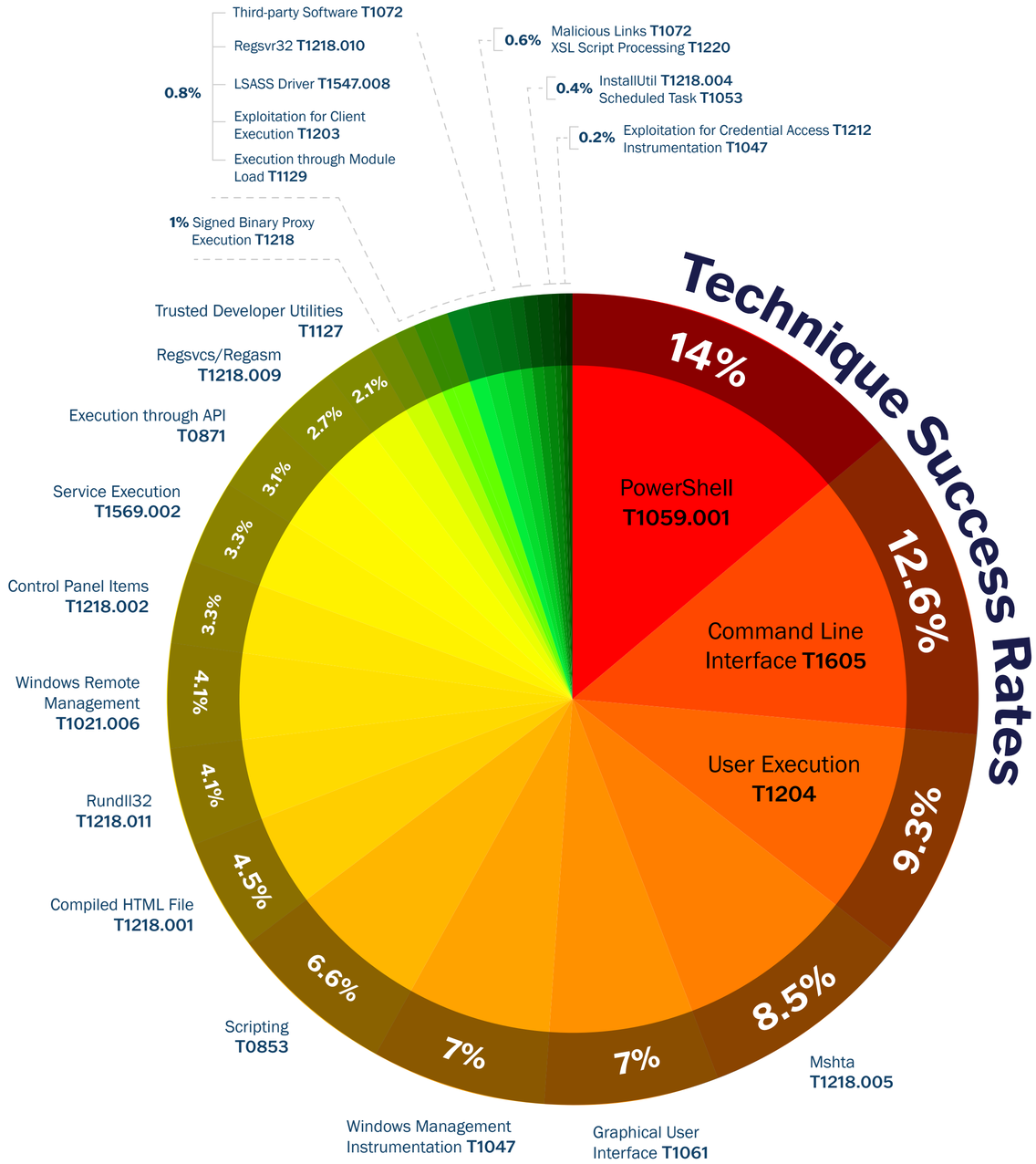
Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.Q Hardware and Software Approval Process

CPG 2.T Log Collection

CPG 3.A Detecting Relevant Threats and TTPs



FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Persistence

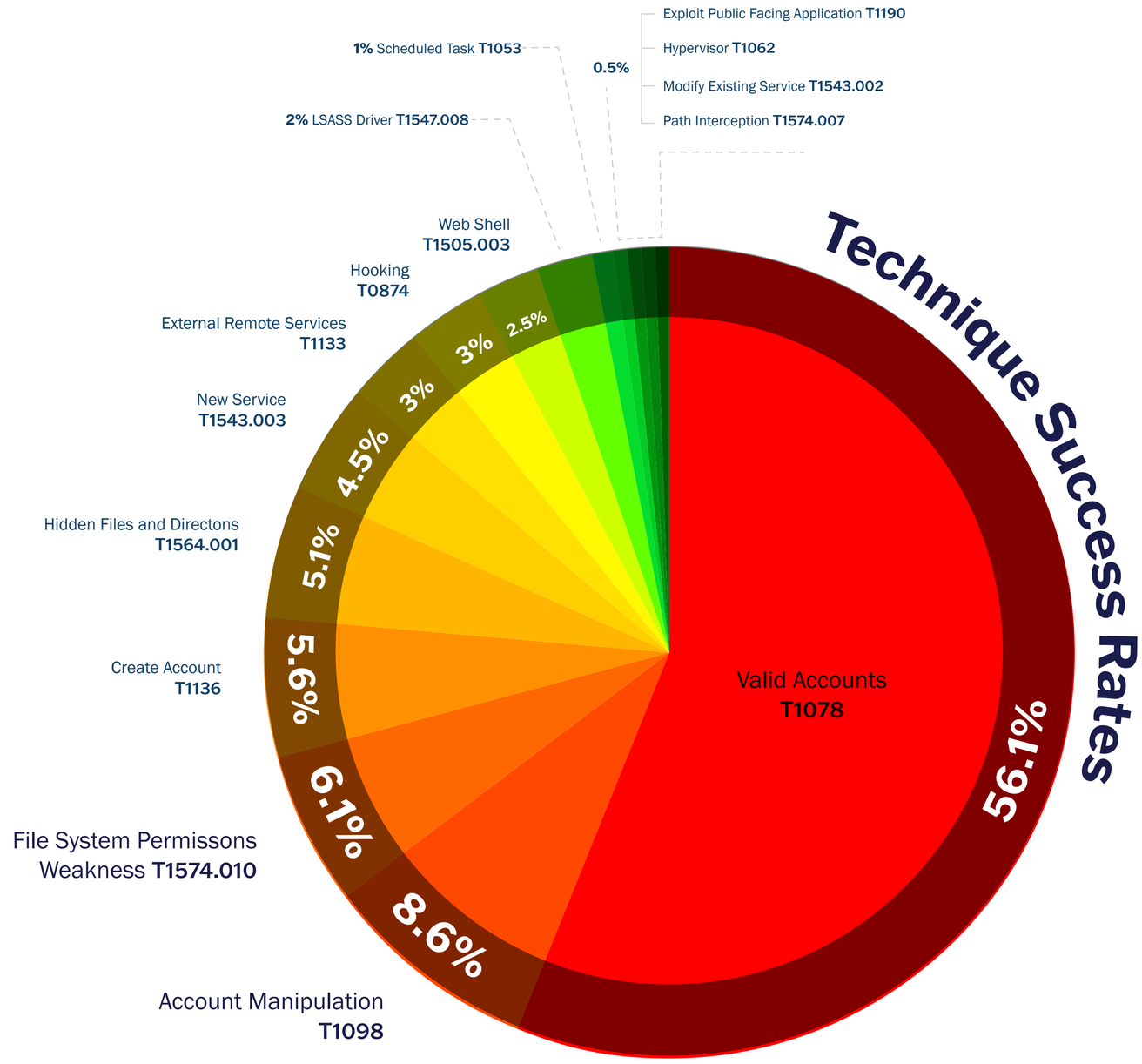
Threat actors maintain persistence or foothold in a network or system by changing credentials or modifying configuration files to maintain continued access. Threat actors may also monitor and manipulate reports observed in the Server Manager Performance Monitor to remain undetected.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.T Log Collection



FY22 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.

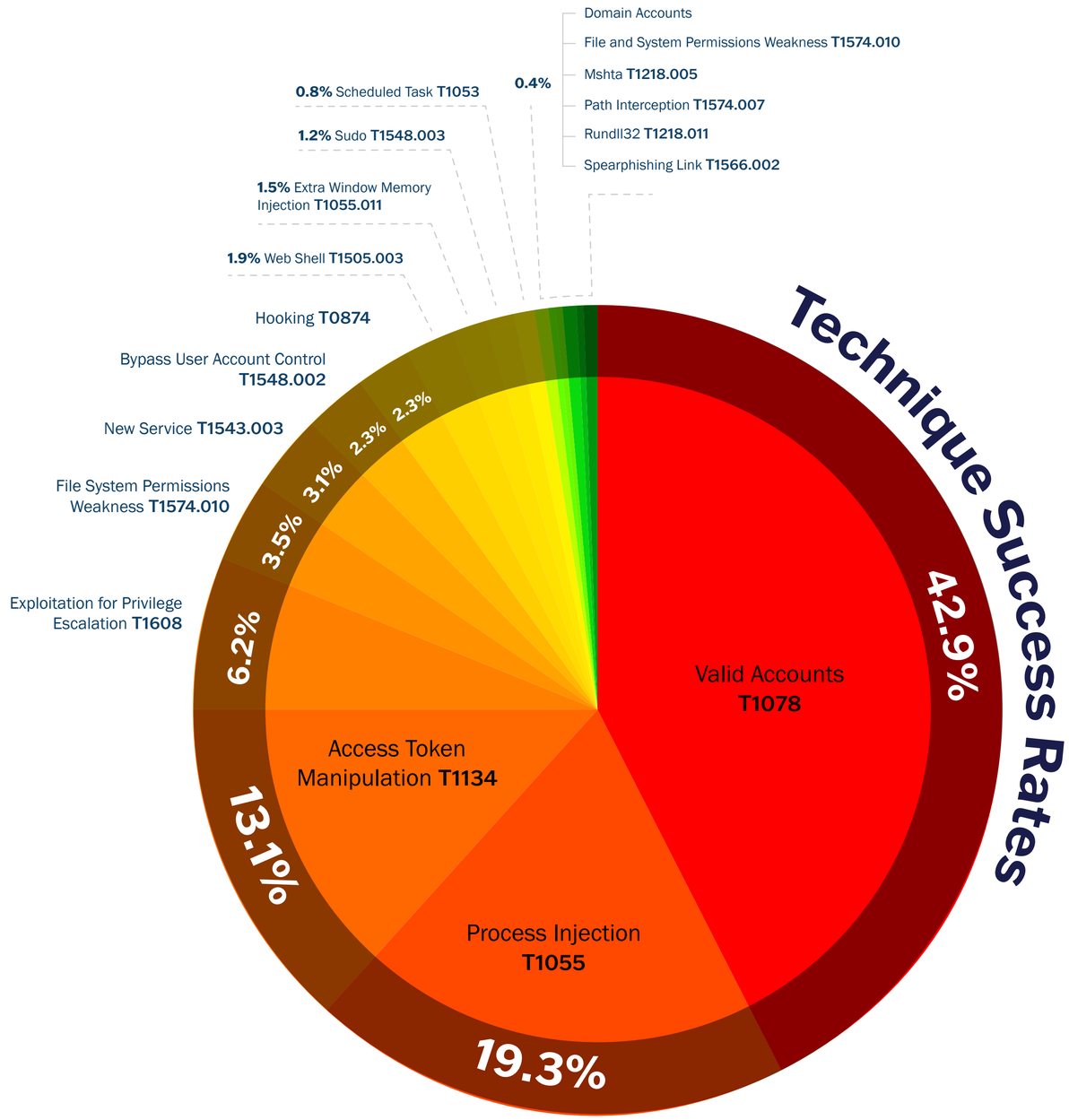
Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.C Unique Credentials

CPG 2.L Secure Sensitive Data

CPG 3.A Detecting Relevant Threats and TTPs



FY22 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

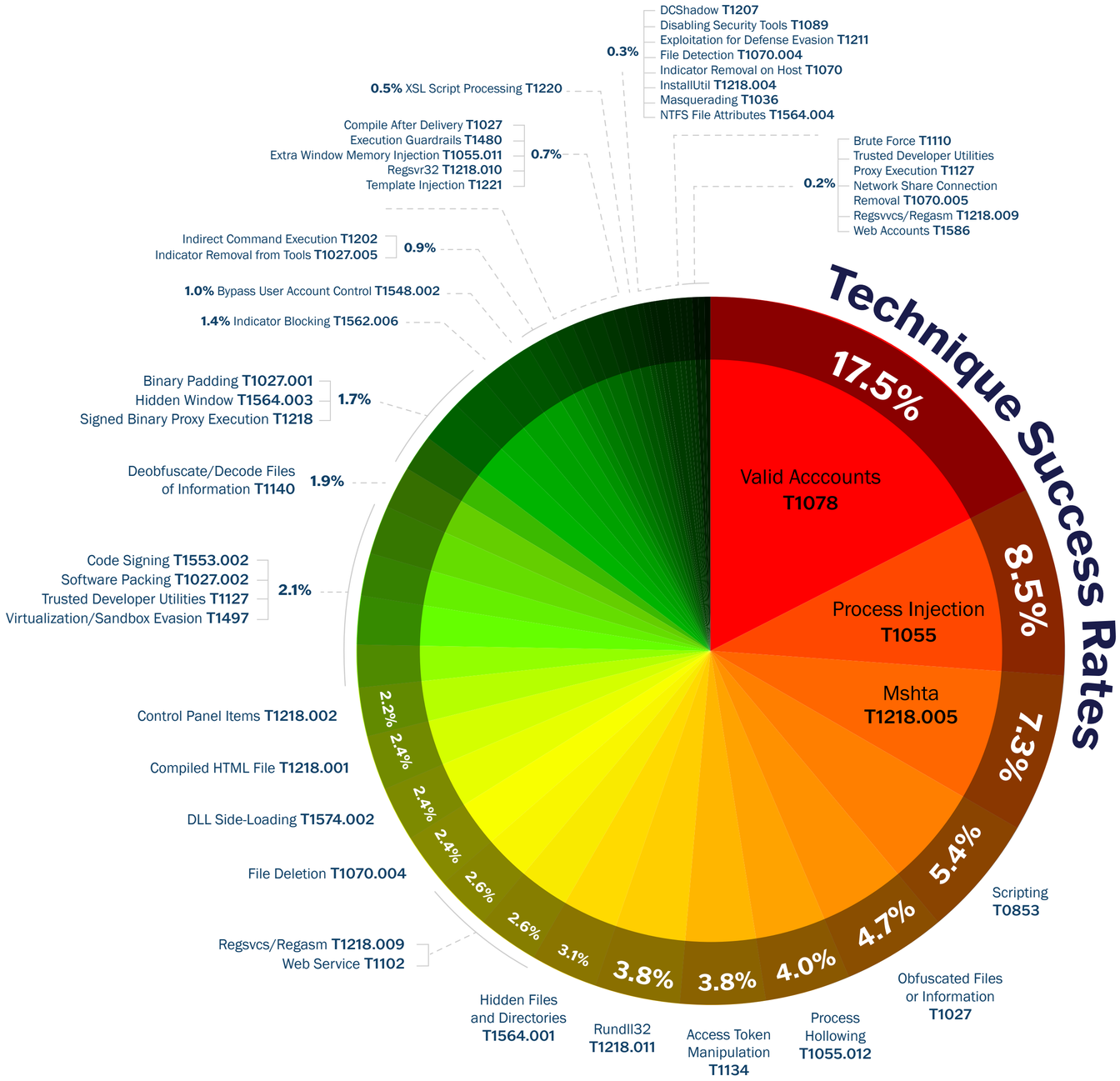
Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

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



FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

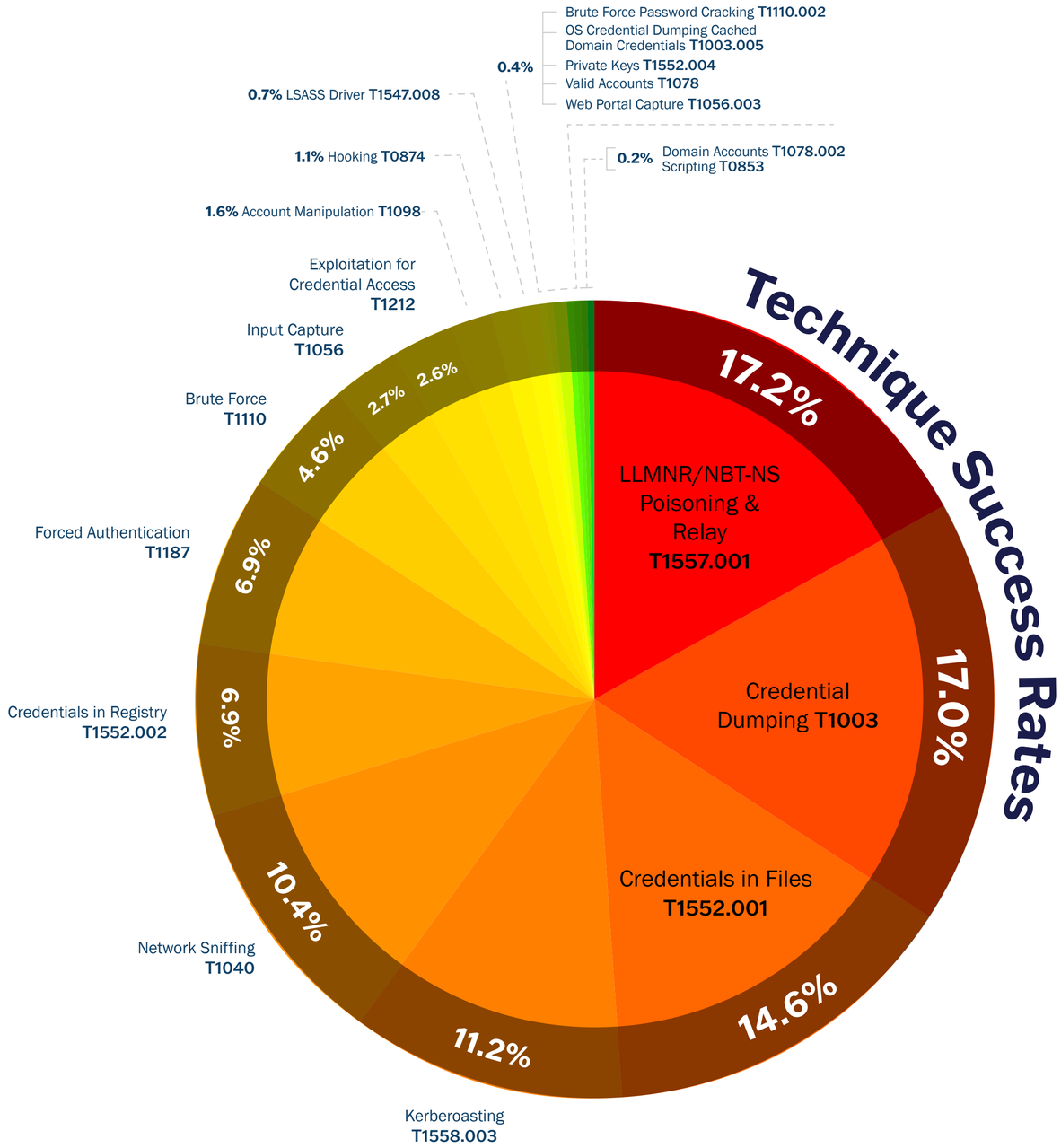
Credential Access

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. 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 Cyber Performance Goals (cisa.gov/cpg):

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



FY22 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.

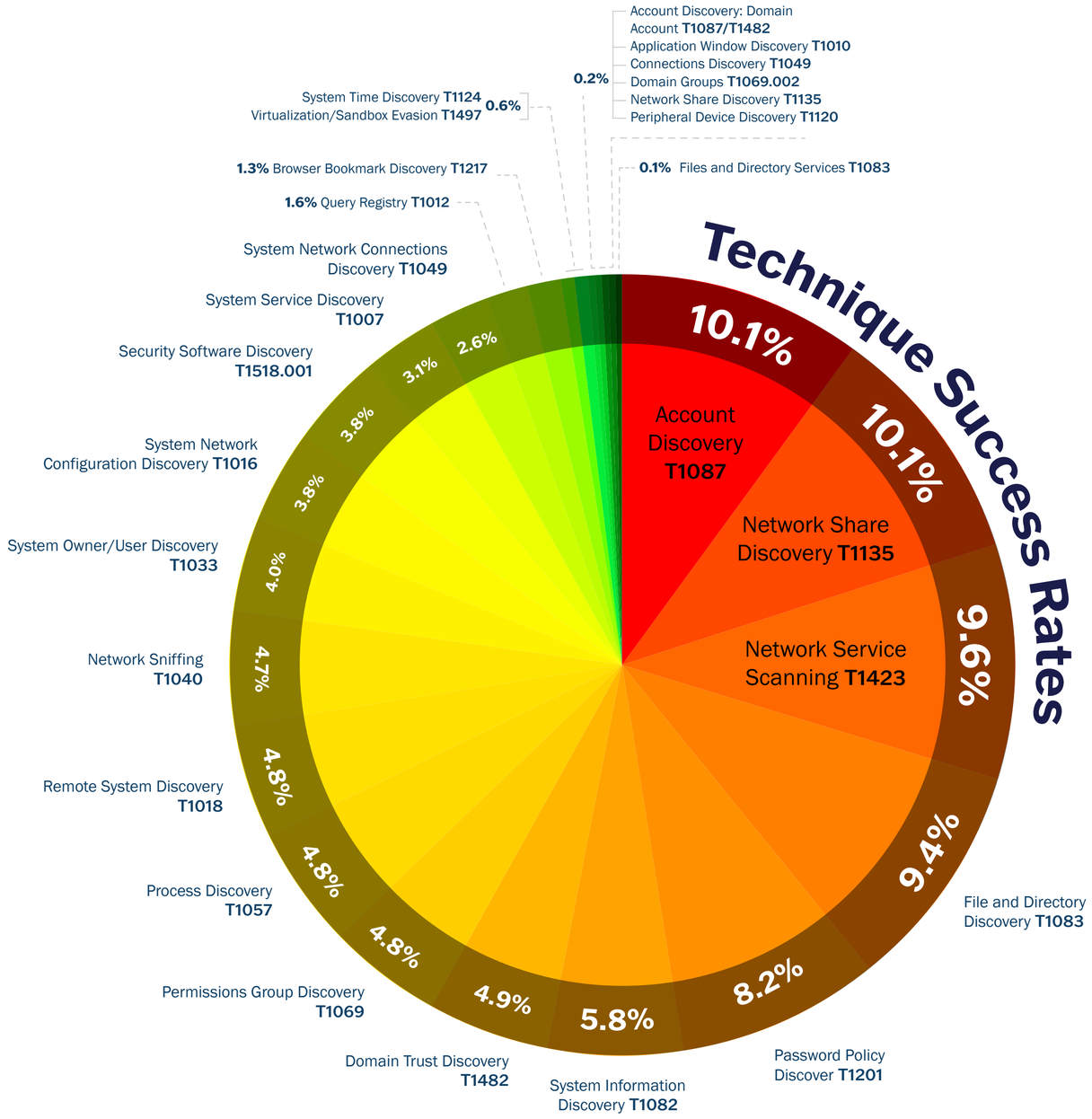
Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.F Network Segmentation

CPG 2.T Log Collection

CPG 3.A Detecting Relevant Threats and TTPs



FY22 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

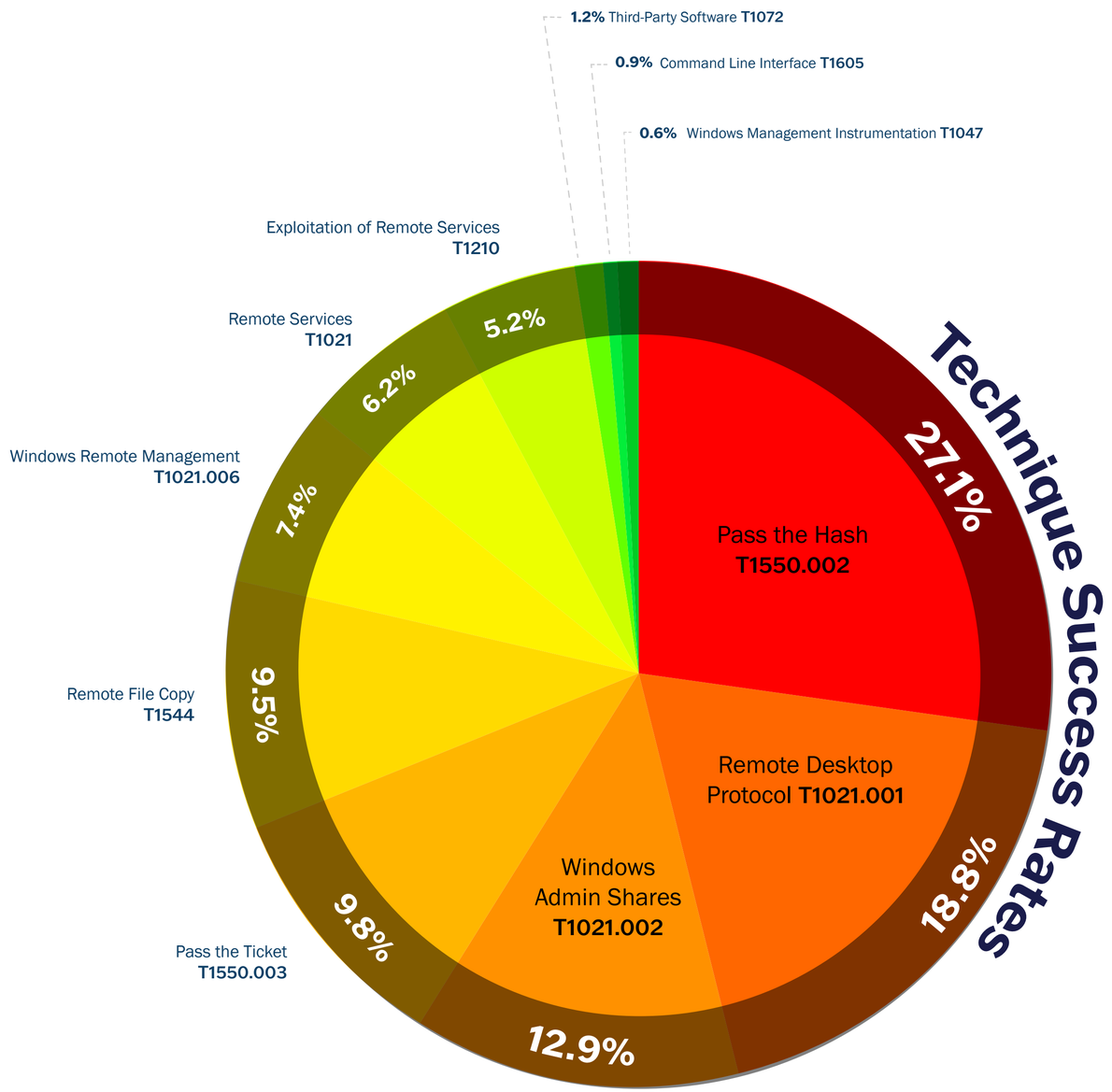
Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 2.C Unique Credentials

CPG 2.F Network Segmentation

CPG 2.H Phishing-Resistant Multifactor Authentication

CPG 2.T Log Collection



FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Collection

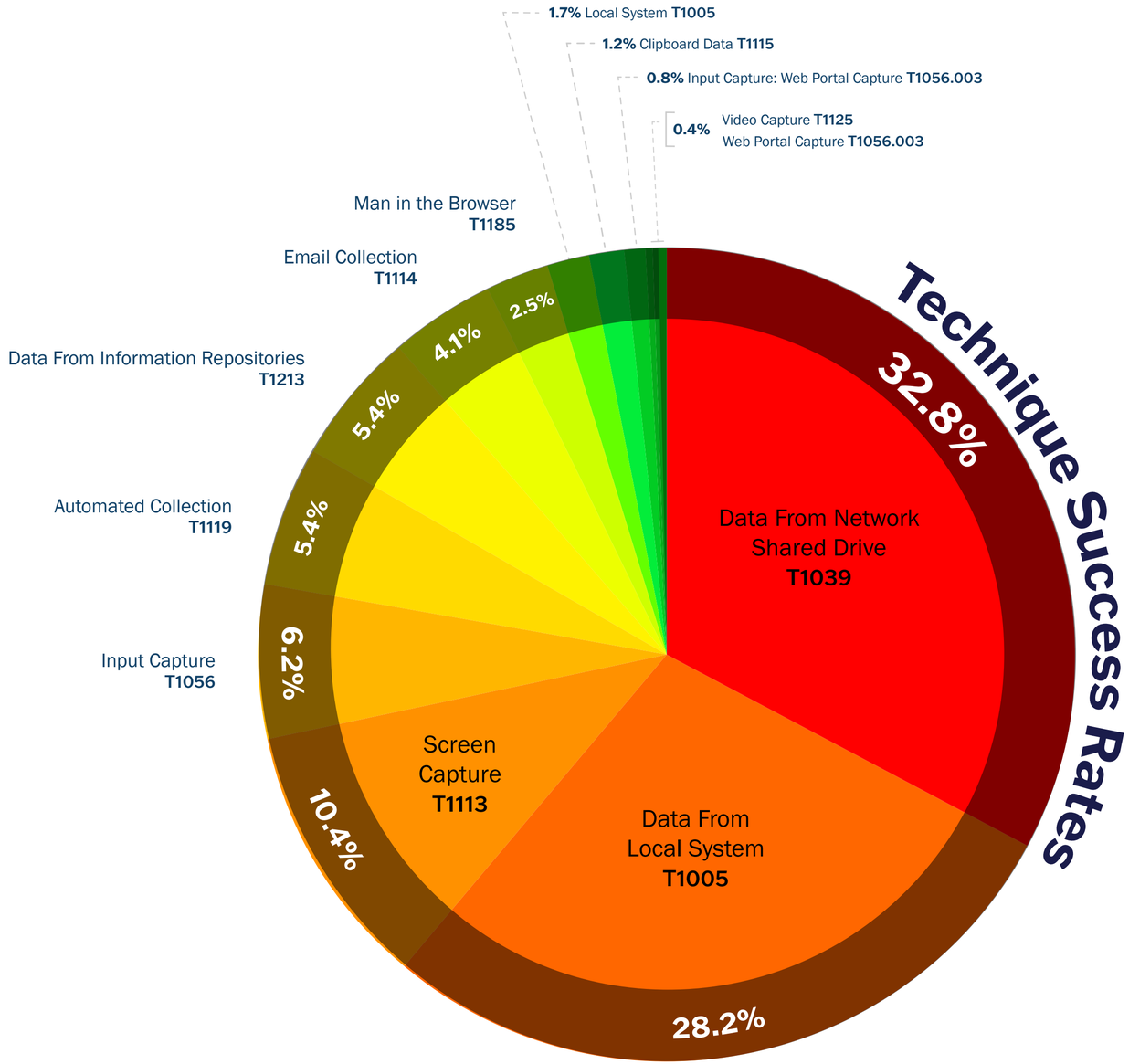
Threat actors use a variety of techniques to collect sensitive internal data, such as capturing screenshots and keyboard inputs. They often collect data by accessing shared drives.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 1.3 Log Collection

CPG 8.2 Detecting Relevant Threats and TTPs



FY22 RVA Results

MITRE ATT&CK™ TACTICS AND TECHNIQUES

Command and Control

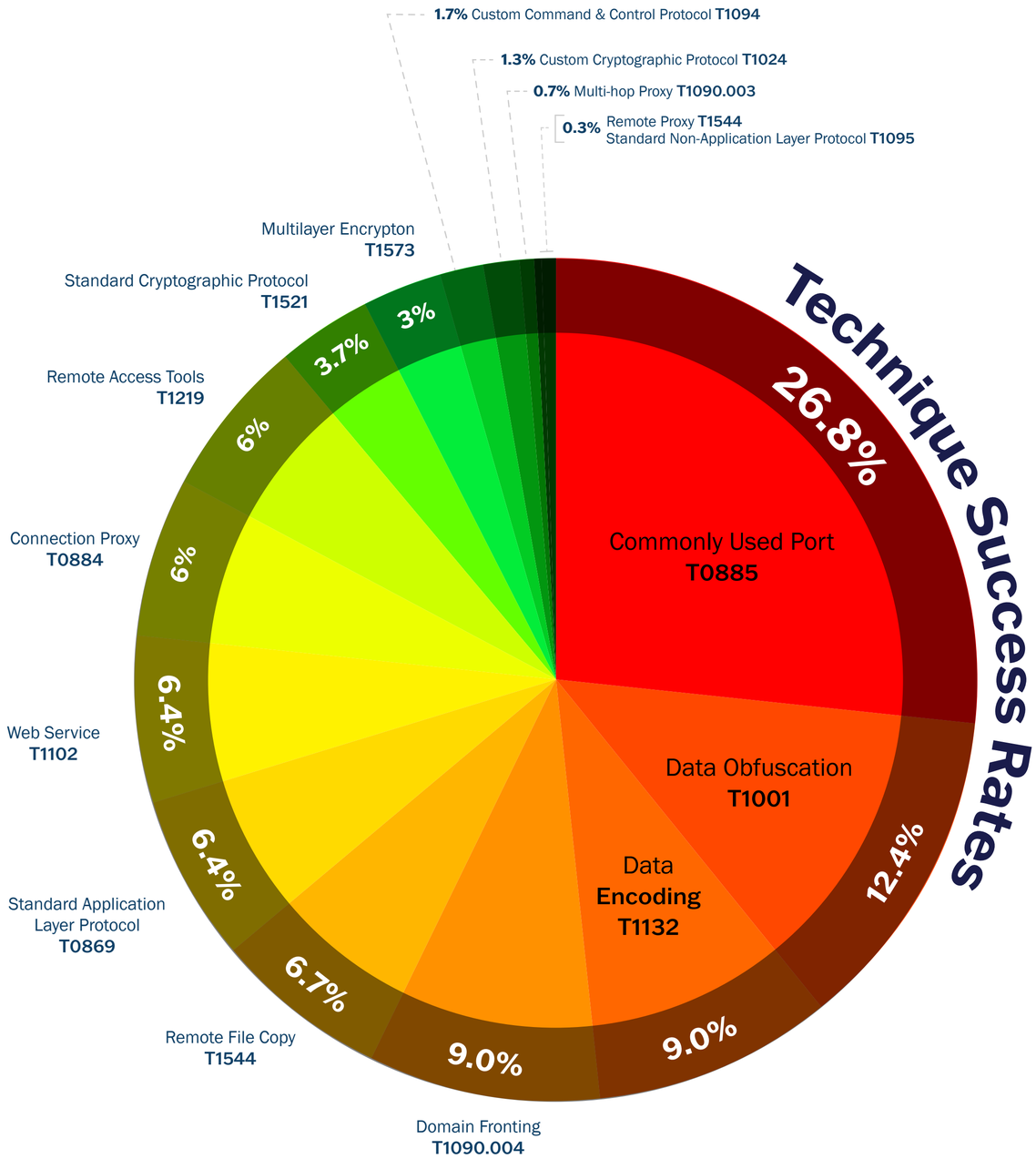
Threat actors use hidden communication channels between their remote servers and compromised systems within a targeted network to conduct internal activity without detection. Through backdoors or commonly used ports, threat actors can gain command and control of the compromised system.

Mitigations

Organizations can mitigate the risks associated with this technique by adhering to the following Cyber Performance Goals (cisa.gov/cpg):

CPG 3.1 Log Collection

CPG 8.2 Detecting Relevant Threats and TTPs



FY22 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 Cyber Performance Goals (cisa.gov/cpg):

CPG 2.T Log Collection

CPG 2.R System Backups

CPG 3.A Detecting Relevant Threats and TTPs