STRIDE-MITRE ATT&CK ENTERPRISE

Drafted By: Art Rebultan

SPOOFING

Access Token Manipulation (T1134)
Command-Line Interface (T1059)
Credential Dumping (T1003)
Data Encrypted for Impact (T1486)
Execution through API (T1106)
Execution through Module Load (T1129)
Input Capture (T1056)
File and Directory Discovery (T1083)
LSASS Driver (T1177)
PowerShell (T1086)
Process Injection (T1055)
Rundll32 (T1085)
SID-History Injection (T1178)
Scheduled Task (T1053)
Scripting (T1064)
Signed Script Proxy Execution (T1216)
Spearphishing Attachment (T1193)
Startup Items (T1165)
User Execution (T1204)
Valid Accounts (T1078)

TAMPERING

Create Account (T1136)
Bootkit (T1067)
Data Destruction (T1485)
Data Encrypted for Impact (T1486)
Defacement (T1491)
Disk Content Wipe (T1488)
Disk Structure Wipe (T1487)
Obfuscated Files or Information (T1027)
Endpoint Denial of Service (T1499)
Exfiltration Over Alternative Protocol (T1048)
File Deletion (T1107)
Firmware Corruption (T1495)
Inhibit System Recovery (T1490)
Input Capture (T1056)
Network Denial of Service (T1498)
Resource Hijacking (T1496)
Runtime Data Manipulation (T1494)
Service Stop (T1489)
Screen Capture (T1113)
Service Execution (T1035)
Signed Script Proxy Execution (T1216)
Standard Cryptographic Protocol (T1032)
Standard Non-Application Layer Protocol (T1095)

REPUDIATION

Data Encrypted (T1022)
Obfuscated Files or Information (T1027)
Exfiltration Over Alternative Protocol (T1048)
Code Signing (T1116)
Create Account (T1136)
Service Execution (T1035)
Signed Script Proxy Execution (T1216)
Standard Cryptographic Protocol (T1032)
Trusted Relationship (T1199)

INFORMATION DISCLOSURE

Account Discovery (T1087)
Application Shimming (T1138)
BITS Jobs (T1197)
Clipboard (T1115)
Command-Line Interface (T1059)
Connection Proxy (T1090)
Credential Dumping (T1003)
Data Destruction (T1485)
Data Encrypted for Impact (T1486)
DLL Search Order Hijacking (T1038)
Data Compressed (T1002)
Data Encrypted (T1022)
Data from Information Repositories (T1213)
Data from Network Shared Drive (T1039)
Obfuscated Files or Information (T1027)
Deobfuscated/Decode Files or Information (T1140)
Exfiltration Over Alternative Protocol (T1048)
Exfiltration Over Command and Control Channel (T1041)
Exfiltration Over Physical Medium (T1052)
Exploit Public-Facing Application (T1190)
Network Service Scanning (T1046)
File Deletion (T1107)
File Permission Modification (T1222)
Indicator Removal on Host (T1070)
Indirect Command Execution (T1202)
Kernel Modules and Extensions (T1215)
Credential in Registry (T1214)
Exploitation for Privilege Escalation (T1068)
Rootkit (T1014)
Mshta (T1170)
Multi-hop Proxy (T1188)
Netsh Helper DLL (T1128)
Pass the Hash (T1075)
Process Discovery (T1057)
Remote Access Tools (T1219)
Remote File Copy (T1105)
Remote System Discovery (T1018)
Service Stop (T1489)
Scheduled Task (T1053)
Security Software Discovery (T1063)
Service Execution (T1035)
Signed Script Proxy Execution (T1216)
Standard Cryptographic Protocol (T1032)
Standard Non-Application Layer Protocol (T1095)
System Firmware (T1019)
System Information Discovery (T1082)
System Network Configuration Discovery (T1016)
System Network Connections Discovery (T1049)
System Service Discovery (T1007)

DENIAL OF SERVICE

Data Destruction (T1485)
Defacement (T1491)
Obfuscated Files or Information (T1027)
Endpoint Denial of Service (T1499)
Exfiltration Over Alternative Protocol (T1048)
Firmware Corruption (T1495)
Inhibit System Recovery (T1490)
Network Denial of Service (T1498)
Resource Hijacking (T1496)
Service Stop (T1489)
Scripting (T1064)
Service Execution (T1035)
Signed Script Proxy Execution (T1216)
Standard Cryptographic Protocol (T1032)
Uncommonly Used Port (T1065)

ELEVATION OF PRIVILEGE

Command-Line Interface (T1059)
Data Destruction (T1485)
Data Encrypted (T1022)
Obfuscated Files or Information (T1027)
Exfiltration Over Alternative Protocol (T1048)
File Deletion (T1107)
Kernel Modules and Extensions (T1215)
Code Signing (T1116)
Create Account (T1136)
Data Obfuscation (T1001)
Drive-by Compromise (T1189)
Rootkit (T1014)
Local Job Scheduling (T1168)
Modify Existing Service (T1031)
Screensaver (T1180)
Scripting (T1064)
Service Execution (T1035)
Signed Script Proxy Execution (T1216)
Standard Cryptographic Protocol (T1032)
Trusted Relationship (T1199)
Uncommonly Used Port (T1065)