New Search

```
index=attack type=attack-pattern
| rename external_references{}.external_id as TID | rename x_mitre_data_sources{} as data_source
| eval technique = TID." ".name
| stats dc(technique) as techniques values(technique) as technique by data_source
| sort - techniques
```

All time

✓ 266 events (before 2/21/20 3:38:22.000 AM)   No Event Sampling

Statistics (59)

data_source	techniques	technique
Process monitoring	132	T1001 Data Obfuscation T1002 Data Compressed T1005 Data from Local System T1008 Fallback Channels T1010 Application Window Discovery T1011 Exfiltration Over Other Network Medium T1013 Port Monitors T1020 Automated Exfiltration T1022 Data Encrypted T1024 Custom Cryptographic Protocol T1025 Data from Removable Media T1026 Multiband Communication T1029 Scheduled Transfer T1030 Data Transfer Size Limits T1032 Standard Cryptographic Protocol T1035 Service Execution T1039 Data from Network Shared Drive T1041 Exfiltration Over Command and Control Channel T1043 Commonly Used Port T1047 Windows Management Instrumentation T1048 Exfiltration Over Alternative Protocol T1049 System Network Connections Discovery T1059 Command-Line Interface T1061 Graphical User Interface T1063 Security Software Discovery T1064 Scripting T1065 Uncommonly Used Port T1066 Indicator Removal from Tools T1068 Exploitation for Privilege Escalation T1071 Standard Application Layer Protocol T1072 Third-party Software T1074 Data Staged T1079 Multilayer Encryption T1083 File and Directory Discovery T1085 Rundll32

data_source	techniques	technique
		T1086 PowerShell
		T1088 Bypass User Account Control
		T1090 Connection Proxy
		T1093 Process Hollowing
		T1094 Custom Command and Control Protocol
		T1099 Timestomp
		T1103 AppInit DLLs
		T1105 Remote File Copy
		T1106 Execution through API
		T1108 Redundant Access
		T1109 Component Firmware
		T1111 Two-Factor Authentication Interception
		T1114 Email Collection
		T1117 Regsvr32
		T1118 InstallUtil
		T1121 Regsvcs/Regasm
		T1126 Network Share Connection Removal
		T1127 Trusted Developer Utilities
		T1128 Netsh Helper DLL
		T1129 Execution through Module Load
		T1132 Data Encoding
		T1136 Create Account
		T1137 Office Application Startup
		T1138 Application Shimming
		T1139 Bash History
		T1140 Deobfuscate/Decode Files or Information
		T1142 Keychain
		T1143 Hidden Window
		T1148 HISTCONTROL
		T1149 LC_MAIN Hijacking
		T1150 Plist Modification
		T1152 Launchctl
		T1153 Source
		T1154 Trap
		T1155 AppleScript
		T1156 .bash_profile and .bashrc
		T1158 Hidden Files and Directories
		T1159 Launch Agent
		T1160 Launch Daemon
		T1161 LC_LOAD_DYLIB Addition
		T1163 Rc.common
		T1165 Startup Items
		T1166 Setuid and Setgid
		T1167 Securityd Memory
		T1168 Local Job Scheduling
		T1170 Mshta
		T1173 Dynamic Data Exchange
		T1174 Password Filter DLL
		T1175 Component Object Model and Distributed COM
		T1176 Browser Extensions
		T1177 LSASS Driver

data_source	techniques	technique
		T1179 Hooking T1180 Screensaver T1181 Extra Window Memory Injection T1182 AppCert DLLs T1183 Image File Execution Options Injection T1185 Man in the Browser T1186 Process Doppelgänging T1191 CMSTP T1196 Control Panel Items T1198 SIP and Trust Provider Hijacking T1201 Password Policy Discovery T1202 Indirect Command Execution T1203 Exploitation for Client Execution T1204 User Execution T1209 Time Providers T1210 Exploitation of Remote Services T1211 Exploitation for Defense Evasion T1212 Exploitation for Credential Access T1214 Credentials in Registry T1215 Kernel Modules and Extensions T1216 Signed Script Proxy Execution T1217 Browser Bookmark Discovery T1218 Signed Binary Proxy Execution T1219 Remote Access Tools T1220 XSL Script Processing T1222 File and Directory Permissions Modification T1223 Compiled HTML File T1480 Execution Guardrails T1482 Domain Trust Discovery T1485 Data Destruction T1486 Data Encrypted for Impact T1488 Disk Content Wipe T1489 Service Stop T1490 Inhibit System Recovery T1494 Runtime Data Manipulation T1496 Resource Hijacking T1497 Virtualization/Sandbox Evasion T1500 Compile After Delivery T1501 Systemd Service T1502 Parent PID Spoofing T1503 Credentials from Web Browsers T1504 PowerShell Profile T1514 Elevated Execution with Prompt T1518 Software Discovery T1529 System Shutdown/Reboot T1531 Account Access Removal
File monitoring	75	T1002 Data Compressed T1005 Data from Local System T1013 Port Monitors T1020 Automated Exfiltration

data_source	techniques	technique
		T1022 Data Encrypted
		T1025 Data from Removable Media
		T1039 Data from Network Shared Drive
		T1052 Exfiltration Over Physical Medium
		T1061 Graphical User Interface
		T1063 Security Software Discovery
		T1064 Scripting
		T1072 Third-party Software
		T1074 Data Staged
		T1083 File and Directory Discovery
		T1085 Rundll32
		T1086 PowerShell
		T1091 Replication Through Removable Media
		T1092 Communication Through Removable Media
		T1096 NTFS File Attributes
		T1099 Timestomp
		T1105 Remote File Copy
		T1107 File Deletion
		T1108 Redundant Access
		T1114 Email Collection
		T1119 Automated Collection
		T1129 Execution through Module Load
		T1137 Office Application Startup
		T1139 Bash History
		T1140 Deobfuscate/Decode Files or Information
		T1143 Hidden Window
		T1144 Gatekeeper Bypass
		T1145 Private Keys
		T1146 Clear Command History
		T1147 Hidden Users
		T1148 HISTCONTROL
		T1150 Plist Modification
		T1152 Launchctl
		T1153 Source
		T1154 Trap
		T1156 .bash_profile and .bashrc
		T1158 Hidden Files and Directories
		T1159 Launch Agent
		T1160 Launch Daemon
		T1161 LC_LOAD_DYLIB Addition
		T1163 Rc.common
		T1164 Re-opened Applications
		T1165 Startup Items
		T1166 Setuid and Setgid
		T1168 Local Job Scheduling
		T1169 Sudo
		T1177 LSASS Driver
		T1180 Screensaver
		T1187 Forced Authentication
		T1202 Indirect Command Execution
		T1206 Sudo Caching

data_source	techniques	technique
		T1209 Time Providers T1210 Exploitation of Remote Services T1211 Exploitation for Defense Evasion T1217 Browser Bookmark Discovery T1222 File and Directory Permissions Modification T1223 Compiled HTML File T1485 Data Destruction T1486 Data Encrypted for Impact T1492 Stored Data Manipulation T1494 Runtime Data Manipulation T1500 Compile After Delivery T1501 Systemd Service T1503 Credentials from Web Browsers T1504 PowerShell Profile T1505 Server Software Component T1514 Elevated Execution with Prompt T1518 Software Discovery T1519 Emond T1534 Internal Spearphishing T1539 Steal Web Session Cookie
Process command-line parameters	71	T1002 Data Compressed T1005 Data from Local System T1010 Application Window Discovery T1022 Data Encrypted T1025 Data from Removable Media T1035 Service Execution T1039 Data from Network Shared Drive T1047 Windows Management Instrumentation T1049 System Network Connections Discovery T1059 Command-Line Interface T1061 Graphical User Interface T1063 Security Software Discovery T1064 Scripting T1066 Indicator Removal from Tools T1074 Data Staged T1083 File and Directory Discovery T1085 Rundll32 T1086 PowerShell T1088 Bypass User Account Control T1096 NTFS File Attributes T1099 Timestomp T1107 File Deletion T1117 Regsvr32 T1118 InstallUtil T1119 Automated Collection T1121 Regsvcs/Regasm T1126 Network Share Connection Removal T1136 Create Account T1137 Office Application Startup T1138 Application Shimming

data_source	techniques	technique
		T1139 Bash History
		T1140 Deobfuscate/Decode Files or Information
		T1143 Hidden Window
		T1144 Gatekeeper Bypass
		T1150 Plist Modification
		T1152 Launchctl
		T1153 Source
		T1154 Trap
		T1155 AppleScript
		T1156 .bash_profile and .bashrc
		T1158 Hidden Files and Directories
		T1161 LC_LOAD_DYLIB Addition
		T1166 Setuid and Setgid
		T1170 Mshta
		T1180 Screensaver
		T1191 CMSTP
		T1196 Control Panel Items
		T1201 Password Policy Discovery
		T1202 Indirect Command Execution
		T1204 User Execution
		T1206 Sudo Caching
		T1214 Credentials in Registry
		T1215 Kernel Modules and Extensions
		T1216 Signed Script Proxy Execution
		T1217 Browser Bookmark Discovery
		T1218 Signed Binary Proxy Execution
		T1220 XSL Script Processing
		T1222 File and Directory Permissions Modification
		T1223 Compiled HTML File
		T1482 Domain Trust Discovery
		T1485 Data Destruction
		T1486 Data Encrypted for Impact
		T1488 Disk Content Wipe
		T1489 Service Stop
		T1490 Inhibit System Recovery
		T1497 Virtualization/Sandbox Evasion
		T1500 Compile After Delivery
		T1501 Systemd Service
		T1518 Software Discovery
		T1529 System Shutdown/Reboot
		T1531 Account Access Removal

data_source	techniques	technique
API monitoring	33	T1006 File System Logical Offsets T1010 Application Window Discovery T1013 Port Monitors T1067 Bootkit T1093 Process Hollowing T1096 NTFS File Attributes T1098 Account Manipulation T1106 Execution through API T1109 Component Firmware T1111 Two-Factor Authentication Interception T1129 Execution through Module Load T1155 AppleScript T1173 Dynamic Data Exchange T1175 Component Object Model and Distributed COM T1177 LSASS Driver T1178 SID-History Injection T1179 Hooking T1181 Extra Window Memory Injection T1185 Man in the Browser T1186 Process Doppelgänging T1196 Control Panel Items T1197 BITS Jobs T1198 SIP and Trust Provider Hijacking T1207 DCShadow T1209 Time Providers T1217 Browser Bookmark Discovery T1482 Domain Trust Discovery T1489 Service Stop T1502 Parent PID Spoofing T1503 Credentials from Web Browsers T1514 Elevated Execution with Prompt T1519 Emond T1539 Steal Web Session Cookie

data_source	techniques	technique
Packet capture	33	T1001 Data Obfuscation T1008 Fallback Channels T1024 Custom Cryptographic Protocol T1026 Multiband Communication T1030 Data Transfer Size Limits T1032 Standard Cryptographic Protocol T1043 Commonly Used Port T1048 Exfiltration Over Alternative Protocol T1071 Standard Application Layer Protocol T1079 Multilayer Encryption T1090 Connection Proxy T1094 Custom Command and Control Protocol T1095 Standard Non-Application Layer Protocol T1098 Account Manipulation T1102 Web Service T1104 Multi-Stage Channels T1105 Remote File Copy T1108 Redundant Access T1126 Network Share Connection Removal T1132 Data Encoding T1171 LLMNR/NBT-NS Poisoning and Relay T1172 Domain Fronting T1175 Component Object Model and Distributed COM T1176 Browser Extensions T1185 Man in the Browser T1189 Drive-by Compromise T1190 Exploit Public-Facing Application T1197 BITS Jobs T1205 Port Knocking T1207 DCShadow T1483 Domain Generation Algorithms T1491 Defacement T1493 Transmitted Data Manipulation

data_source	techniques	technique
Process use of network	32	T1001 Data Obfuscation
		T1008 Fallback Channels
		T1020 Automated Exfiltration
		T1024 Custom Cryptographic Protocol
		T1026 Multiband Communication
		T1029 Scheduled Transfer
		T1030 Data Transfer Size Limits
		T1032 Standard Cryptographic Protocol
		T1043 Commonly Used Port
		T1048 Exfiltration Over Alternative Protocol
		T1065 Uncommonly Used Port
		T1066 Indicator Removal from Tools
		T1071 Standard Application Layer Protocol
		T1072 Third-party Software
		T1079 Multilayer Encryption
		T1090 Connection Proxy
		T1094 Custom Command and Control Protocol
		T1095 Standard Non-Application Layer Protocol
		T1104 Multi-Stage Channels
		T1105 Remote File Copy
		T1108 Redundant Access
		T1114 Email Collection
		T1132 Data Encoding
		T1156 .bash_profile and .bashrc
		T1176 Browser Extensions
		T1187 Forced Authentication
		T1189 Drive-by Compromise
		T1191 CMSTP
		T1219 Remote Access Tools
		T1220 XSL Script Processing
		T1483 Domain Generation Algorithms
		T1496 Resource Hijacking

data_source	techniques	technique
Windows Registry	24	T1013 Port Monitors
		T1035 Service Execution
		T1072 Third-party Software
		T1086 PowerShell
		T1101 Security Support Provider
		T1103 AppInit DLLs
		T1117 Regsvr32
		T1122 Component Object Model Hijacking
		T1128 Netsh Helper DLL
		T1131 Authentication Package
		T1137 Office Application Startup
		T1138 Application Shimming
		T1171 LLMNR/NBT-NS Poisoning and Relay
		T1173 Dynamic Data Exchange
		T1174 Password Filter DLL
		T1175 Component Object Model and Distributed COM
		T1180 Screensaver
		T1182 AppCert DLLs
		T1183 Image File Execution Options Injection
		T1196 Control Panel Items
		T1198 SIP and Trust Provider Hijacking
		T1214 Credentials in Registry
		T1489 Service Stop
		T1490 Inhibit System Recovery
Netflow/Enclave netflow	22	T1008 Fallback Channels
		T1024 Custom Cryptographic Protocol
		T1026 Multiband Communication
		T1029 Scheduled Transfer
		T1030 Data Transfer Size Limits
		T1032 Standard Cryptographic Protocol
		T1043 Commonly Used Port
		T1047 Windows Management Instrumentation
		T1048 Exfiltration Over Alternative Protocol
		T1065 Uncommonly Used Port
		T1071 Standard Application Layer Protocol
		T1090 Connection Proxy
		T1094 Custom Command and Control Protocol
		T1095 Standard Non-Application Layer Protocol
		T1102 Web Service
		T1104 Multi-Stage Channels
		T1105 Remote File Copy
		T1171 LLMNR/NBT-NS Poisoning and Relay
		T1188 Multi-hop Proxy
		T1205 Port Knocking
		T1483 Domain Generation Algorithms
		T1498 Network Denial of Service

data_source	techniques	technique
Windows event logs	21	T1098 Account Manipulation T1136 Create Account T1143 Hidden Window T1171 LLMNR/NBT-NS Poisoning and Relay T1173 Dynamic Data Exchange T1175 Component Object Model and Distributed COM T1178 SID-History Injection T1179 Hooking T1183 Image File Execution Options Injection T1191 CMSTP T1196 Control Panel Items T1197 BITS Jobs T1198 SIP and Trust Provider Hijacking T1202 Indirect Command Execution T1208 Kerberoasting T1222 File and Directory Permissions Modification T1484 Group Policy Modification T1490 Inhibit System Recovery T1502 Parent PID Spoofing T1529 System Shutdown/Reboot T1531 Account Access Removal
Authentication logs	20	T1047 Windows Management Instrumentation T1088 Bypass User Account Control T1098 Account Manipulation T1108 Redundant Access T1114 Email Collection T1126 Network Share Connection Removal T1136 Create Account T1146 Clear Command History T1147 Hidden Users T1148 HISTCONTROL T1175 Component Object Model and Distributed COM T1178 SID-History Injection T1184 SSH Hijacking T1185 Man in the Browser T1199 Trusted Relationship T1207 DCShadow T1212 Exploitation for Credential Access T1213 Data from Information Repositories T1506 Web Session Cookie T1522 Cloud Instance Metadata API

data_source	techniques	technique
Network protocol analysis	17	T1001 Data Obfuscation
		T1048 Exfiltration Over Alternative Protocol
		T1094 Custom Command and Control Protocol
		T1095 Standard Non-Application Layer Protocol
		T1102 Web Service
		T1104 Multi-Stage Channels
		T1105 Remote File Copy
		T1108 Redundant Access
		T1132 Data Encoding
		T1176 Browser Extensions
		T1187 Forced Authentication
		T1188 Multi-hop Proxy
		T1207 DCShadow
		T1219 Remote Access Tools
		T1493 Transmitted Data Manipulation
		T1496 Resource Hijacking
		T1498 Network Denial of Service
DLL monitoring	16	T1013 Port Monitors
		T1086 PowerShell
		T1101 Security Support Provider
		T1122 Component Object Model Hijacking
		T1128 Netsh Helper DLL
		T1129 Execution through Module Load
		T1131 Authentication Package
		T1173 Dynamic Data Exchange
		T1174 Password Filter DLL
		T1175 Component Object Model and Distributed COM
		T1177 LSASS Driver
		T1179 Hooking
		T1196 Control Panel Items
		T1198 SIP and Trust Provider Hijacking
		T1209 Time Providers
		T1220 XSL Script Processing
Azure activity logs	14	T1108 Redundant Access
		T1136 Create Account
		T1190 Exploit Public-Facing Application
		T1199 Trusted Relationship
		T1213 Data from Information Repositories
		T1496 Resource Hijacking
		T1522 Cloud Instance Metadata API
		T1526 Cloud Service Discovery
		T1528 Steal Application Access Token
		T1530 Data from Cloud Storage Object
		T1535 Unused/Unsupported Cloud Regions
		T1536 Revert Cloud Instance
		T1537 Transfer Data to Cloud Account
		T1538 Cloud Service Dashboard

data_source	techniques	technique
Binary file metadata	14	T1002 Data Compressed
		T1022 Data Encrypted
		T1061 Graphical User Interface
		T1066 Indicator Removal from Tools
		T1072 Third-party Software
		T1085 Rundll32
		T1107 File Deletion
		T1108 Redundant Access
		T1116 Code Signing
		T1149 LC_MAIN Hijacking
		T1161 LC_LOAD_DYLIB Addition
		T1179 Hooking
		T1196 Control Panel Items
		T1209 Time Providers
AWS CloudTrail logs	13	T1108 Redundant Access
		T1136 Create Account
		T1190 Exploit Public-Facing Application
		T1199 Trusted Relationship
		T1213 Data from Information Repositories
		T1496 Resource Hijacking
		T1522 Cloud Instance Metadata API
		T1526 Cloud Service Discovery
		T1530 Data from Cloud Storage Object
		T1535 Unused/Unsupported Cloud Regions
		T1536 Revert Cloud Instance
		T1537 Transfer Data to Cloud Account
		T1538 Cloud Service Dashboard
Loaded DLLs	12	T1086 PowerShell
		T1101 Security Support Provider
		T1103 AppInit DLLs
		T1117 Regsvr32
		T1122 Component Object Model Hijacking
		T1131 Authentication Package
		T1138 Application Shimming
		T1177 LSASS Driver
		T1179 Hooking
		T1182 AppCert DLLs
		T1198 SIP and Trust Provider Hijacking
		T1209 Time Providers

data_source	techniques	technique
Stackdriver logs	11	T1108 Redundant Access T1190 Exploit Public-Facing Application T1199 Trusted Relationship T1213 Data from Information Repositories T1496 Resource Hijacking T1526 Cloud Service Discovery T1530 Data from Cloud Storage Object T1535 Unused/Unsupported Cloud Regions T1536 Revert Cloud Instance T1537 Transfer Data to Cloud Account T1538 Cloud Service Dashboard
Application logs	7	T1068 Exploitation for Privilege Escalation T1190 Exploit Public-Facing Application T1198 SIP and Trust Provider Hijacking T1199 Trusted Relationship T1213 Data from Information Repositories T1492 Stored Data Manipulation T1505 Server Software Component
Malware reverse engineering	7	T1008 Fallback Channels T1024 Custom Cryptographic Protocol T1026 Multiband Communication T1032 Standard Cryptographic Protocol T1071 Standard Application Layer Protocol T1079 Multilayer Encryption T1149 LC_MAIN Hijacking
System calls	7	T1088 Bypass User Account Control T1138 Application Shimming T1142 Keychain T1155 AppleScript T1176 Browser Extensions T1203 Exploitation for Client Execution T1215 Kernel Modules and Extensions