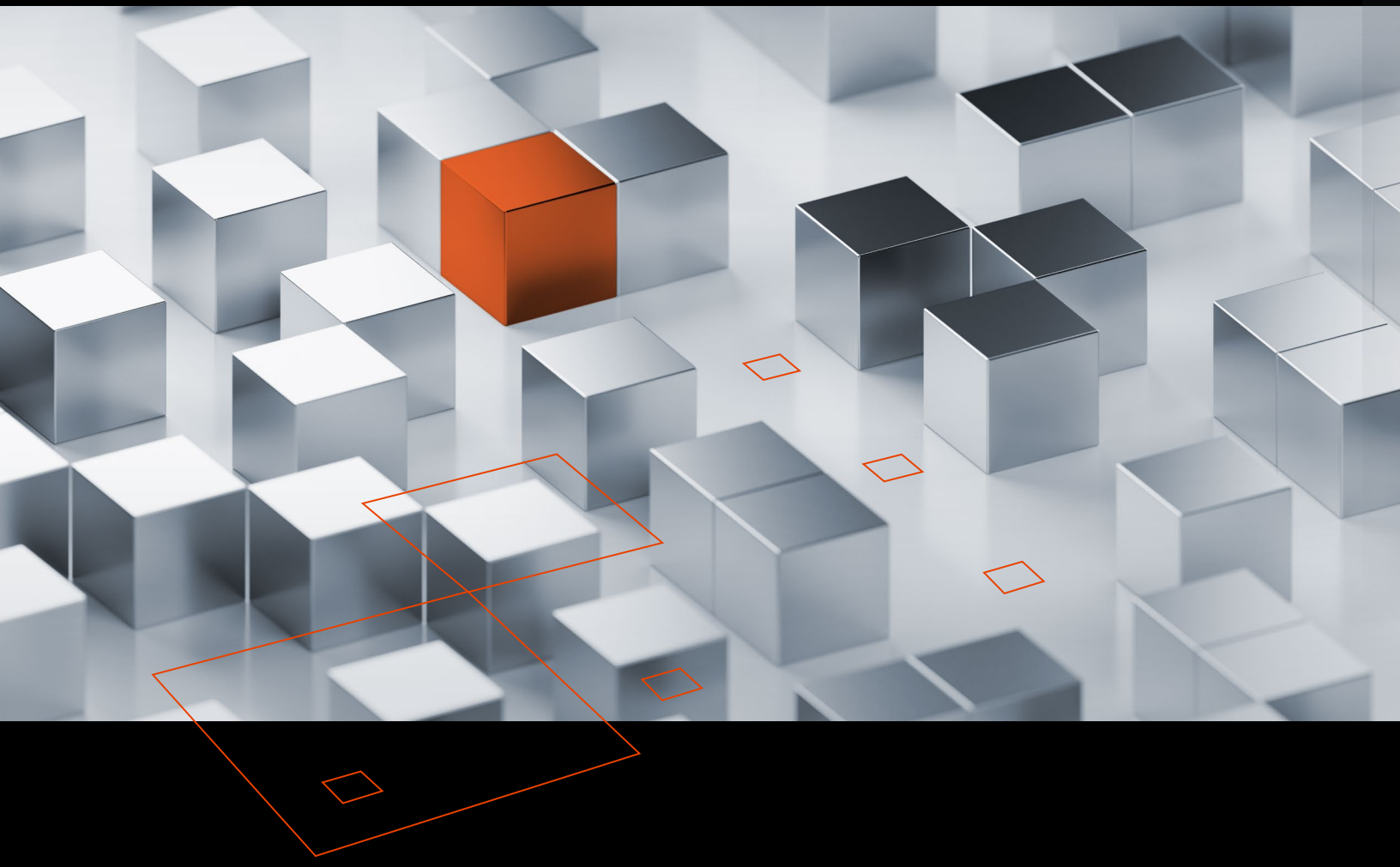
2Q 2022

SIMSPACE

ATTACK CATALOG

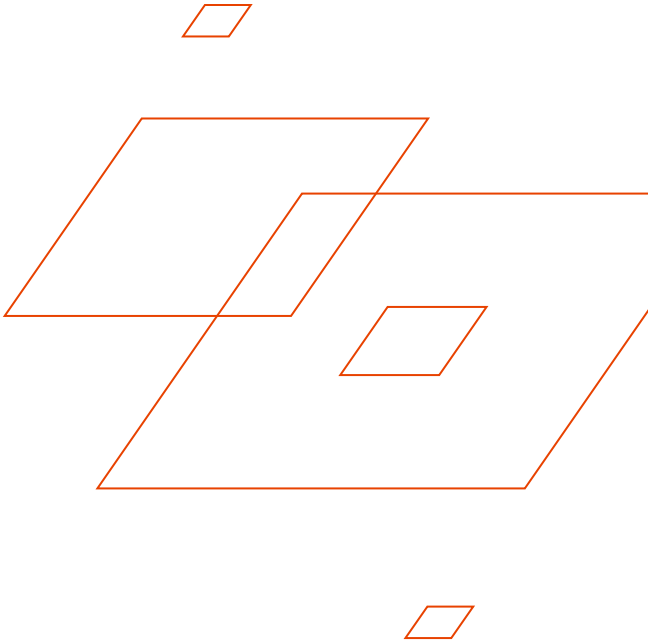


Disclaimer

While this catalog is designed to provide the audience with as accurate and up-to-date information as possible on tradecraft, methodologies, technologies, vulnerabilities, and exploits, the information provided is based upon the information available at time of publishing. Should new and updated information become available, SimSpace will update its Content Catalog appropriately.

All content available in this catalog is approved for worldwide distribution and usage.

Table of Contents



Index

■ New Q2 2022

Title	Difficulty	Duration (Min)	Availability
APT Chimera (China)	Intermediate	32	Available
APT Patchwork (India)	Intermediate	10	Available
■ APT3 Inspired Scenario	Intermediate	9	Available
■ APT29-Solorigate (Russia)	Intermediate	9	Available
APT32-Cobalt Kitty (Vietnam)	Intermediate	—	4Q22
APT34 OilRig (Iran)	Intermediate	9	Available
APT38: Lazarus (North Korea)	Intermediate	16	Available
APT39 (Iran)	Intermediate	—	3Q22
■ APT41 (China)	Intermediate	11	Available
■ Beaconer Deployment	Intermediate	5	Available
Bronze Butler (China)	Intermediate	20	Available
■ Domain Controller Service Disruption and Exfiltration	Intermediate	5	Available
Dragonfly 2.0 (Russia)	Intermediate	—	3Q22
■ GALLIUM (China)	Intermediate	17	Available
Honeybee	Intermediate	—	3Q22
Hopi	Intermediate	13	Available
■ Host-Based Artifact Dropper w/ Multiple File Exfil	Intermediate	39	Available
Kimsuky (North Korea)	Intermediate	—	3Q22
Leviathan (China)	Intermediate	10	Available
■ Leviathan Inspired Scenario	Intermediate	9	Available
menuPass (China)	Intermediate	—	3Q22
■ menuPass Inspired Scenario	Intermediate	9	Available
Montezuma	Intermediate	30	Available
■ Mustang Panda (China)	Intermediate	9	Available
Operation Wocao (China)	Intermediate	30	Available
Ransomware	Intermediate	7	Available
■ Reconnaissance by an Insider Threat	Intermediate	3	Available
Threat Group-3390 (China)	Intermediate	—	4Q22
Tropic Trooper (China)	Intermediate	—	4Q22
■ Turla (Russia)	Intermediate	17	Available
Ubiquitous Freedom	Intermediate	20	Available
■ Wizard Spider (Russia)	Intermediate	9	Available

Current Scenarios

APT Chimera (China)

Intermediate

Publisher: SimSpace

32 minutes

Description

An automated attack meant to emulate an APT actor with the common names Chimera and CyCraft. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Service Discovery (T1007)
- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Indicator Removal On Host: Clear Windows Event Logs (T1070.001)
- Indicator Removal On Host: File Deletion (T1070.004)
- Indicator Removal On Host: Timestomp (T1070.006)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Account Discovery: Local Account (T1087.001)
- Account Discovery: Domain Account (T1087.002)
- Email Collection: Local Email Collection (T1114.001)
- System Time Discovery (T1124)
- Network Share Discovery (T1135)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Browser Bookmark Discovery (T1217)
- Domain Trust Discovery (T1482)
- Exfiltration Over Web Service (T1567)

APT Patchwork (India)

Intermediate

Publisher: SimSpace

10 minutes

Description

Inspired by Patchwork group. An automated attack meant to emulate an APT actor with the common name Patchwork (named after the threat actor using code copy/pasted from various online forms, similar to a patchwork quilt). Attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

APT3 Inspired Scenario

Intermediate

Publisher: SimSpace

9 minutes

Description

Inspired by an advanced persistent threat (APT) actor with the common names APT3, Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, and TG-0110. Implements a series of tactics, techniques, and procedures typically used by the threat actor commonly described as APT3. Infiltrates via a phishing link, moves laterally via a remote scheduled task, and exfiltrates data from that lateral host.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- Remote Services (T1021)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Indicator Removal On Host (T1070)
- Application Layer Protocol: Web Protocols (T1071.001)
- Data Staged: Local Data Staging (T1074.001)
- Valid Accounts: Local Accounts (T1078)
- Taint Shared Content (T1080)
- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Account Manipulation (T1098)
- Create Account: Local Account (T1136)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

APT29-Solorigate (Russia)

Intermediate

Publisher: SimSpace

9 minutes

Description

Inspired by APT29. An automated attack meant to emulate an APT actor with the common names Solorigate, SUNBURST, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, and APT29. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Service Discovery (T1007)
- System Network Configuration Discovery (T1016)
- Process Discovery (T1057)
- Application Layer Protocol: Web Protocols (T1071.001)
- Valid Accounts: Local Accounts (T1078)
- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Automated Collection (T1119)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Archive Collected Data: Archive Via Utility (T1560.001)
- Impair Defenses: Disable Windows Event Logging (T1562.002)
- Impair Defenses: Disable Or Modify System Firewall (T1562.004)
- Exfiltration Over Web Service (T1567)

APT34 OilRig (Iran)

Intermediate

Publisher: SimSpace

9 minutes

Description

An automated attack meant to emulate an APT actor with the common names OilRig, APT34, and Helix Kitten. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Indicator Removal On Host (T1070)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

APT38: Lazarus (North Korea)

Intermediate

Publisher: SimSpace

16 minutes

Description

Inspired by APT38. Implements an automated attack meant to emulate an APT actor with operations known as Lazarus Group. Attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- System Time Discovery (T1124)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

APT41 (China)

Intermediate

Publisher: SimSpace

11 minutes

Description

Inspired by APT41. An automated attack meant to emulate an APT actor with the common names WICKED PANDA and APT41. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Windows Management Instrumentation (T1047)
- Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Obfuscated Non C2 Protocol (T1048.003)
- System Network Connections Discovery (T1049)
- Indicator Removal On Host: Clear Windows Event Logs (T1070.001)
- Indicator Removal On Host: File Deletion (T1070.004)
- Application Layer Protocol: Web Protocols (T1071.001)
- Account Manipulation (T1098)
- Network Share Discovery (T1135)
- Create Account: Local Account (T1136)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Create Or Modify System Process: Windows Service (T1543.003)
- Archive Collected Data: Archive Via Utility (T1560.001)
- Exfiltration Over Web Service (T1567)
- System Services: Service Execution (T1569.002)

Beaconer Deployment

Intermediate

Publisher: SimSpace

5 minutes

Description

Gains access to a host via a spearphishing link. Opens a bypass session on that host, collects information, and deploys a beaconer.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Phishing: Spearphishing Link (T1566.002)

Bronze Butler (China)

Intermediate

Publisher: SimSpace

20 minutes

Description

Implements an automated attack meant to emulate an APT actor with the common names Bronze Butler, Tick, Nian, and StalkerPanda. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- Scheduled Task/Job (T1053)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Indicator Removal On Host: File Deletion (T1070.004)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- File And Directory Discovery (T1083)
- Account Discovery: Domain Account (T1087.002)
- Screen Capture (T1113)
- System Time Discovery (T1124)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Archive Collected Data: Archive Via Utility (T1560.001)
- Exfiltration Over Web Service (T1567)

Domain Controller Service Disruption and Exfiltration

Intermediate

Publisher: SimSpace

5 minutes

Description

Gains initial access in the network via a phishing email link. It utilizes the domain administrator credentials on the initial access host, and then uses those with schtasks-based lateral movement techniques to move laterally from the initial access host to the Domain Controller (DC). The scenario exfiltrates data from both the initial access and lateral host victims. It also disrupts the availability of the infrastructure by killing a 'critical' process on the DC.

Attack Intent Domain Controller Service Disruption and Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Windows Management Instrumentation (T1047)
- System Network Connections Discovery (T1049)
- Application Layer Protocol: Web Protocols (T1071.001)
- Account Discovery: Domain Account (T1087.002)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Service Stop (T1489)
- Boot Or Logon Autostart Execution: Registry Run Keys Startup Folder (T1547.001)
- Archive Collected Data: Archive Via Utility (T1560.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

GALLIUM (China)

Intermediate

Publisher: SimSpace

17 minutes

Description

An automated attack meant to emulate an APT actor with the common names Operation Soft Cell and GALLIUM. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Data From Local System (T1005)
- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Indicator Removal On Host: File Deletion (T1070.004)
- Application Layer Protocol: Web Protocols (T1071.001)
- Valid Accounts: Local Accounts (T1078)
- System Information Discovery (T1082)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Archive Collected Data (T1560)
- Exfiltration Over Web Service (T1567)

Hopi

Intermediate

Publisher: SimSpace

13 minutes

Description

An automated attack that is unique and not attributed to a specific threat actor. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Exfiltration Over Web Service (T1567)

Host-Based Artifact Dropper w/ Multiple File Exfil

Intermediate

Publisher: SimSpace

39 minutes

Description

Attempts to gain access to a lateral host, potentially on a different subnet. Achieves persistence on the initial access host in two ways and the lateral host in one way. Exfiltrates data from the lateral host through two different channels and intentionally leaves behind a variety of artifacts for Blue Team detection and forensic analysis.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Remote System Discovery (T1018)
- Remote Services (T1021)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Scheduled Task/Job (T1053)
- Scheduled Task/Job: Scheduled Task (T1053.005)
- Application Layer Protocol: Web Protocols (T1071.001)
- Data Staged: Local Data Staging (T1074.001)
- Valid Accounts: Local Accounts (T1078)
- Taint Shared Content (T1080)
- Account Discovery: Domain Account (T1087.002)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Boot Or Logon Autostart Execution: Registry Run Keys Startup Folder (T1547.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

Leviathan (China)

Intermediate

Publisher: SimSpace

10 minutes

Description

An automated attack meant to emulate an APT actor with common names Leviathan, Kryptonite Panda, and Gadolinium. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Owner User Discovery (T1033)
- Process Discovery (T1057)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Internal Spearphishing (T1534)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

Leviathan Inspired Scenario

Intermediate

Publisher: SimSpace

9 minutes

Description

Inspired by an advanced persistent threat (APT) actor with the common names APT40, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, Leviathan, and TEMP.Periscope. Implements a series of tactics, techniques, and procedures typically used by the threat actor commonly described as Leviathan. The actor infiltrates via a phishing link, moves laterally via a remote scheduled task, and exfiltrates data from that lateral host via a shared drive.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- Scheduled Task/Job (T1053)
- Scheduled Task/Job: Scheduled Task (T1053.005)
- Application Layer Protocol: Web Protocols (T1071.001)
- Valid Accounts: Local Accounts (T1078)
- Taint Shared Content (T1080)
- Create Account: Local Account (T1136)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

menuPass Inspired Scenario

Intermediate

Publisher: SimSpace

9 minutes

Description

Inspired by an advanced persistent threat (APT) actor with the common names menuPass, Cicada, POTASSIUM, Stone Panda, Red Apollo, CVNX, APT10, and HOGFISH. Implements a series of tactics, techniques, and procedures typically used by the threat actor commonly known as APT10. The actor infiltrates via a phishing link, moves laterally, and exfiltrates data from that lateral host.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- System Network Connections Discovery (T1049)
- Scheduled Task/Job (T1053)
- Scheduled Task/Job: Scheduled Task (T1053.005)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Indicator Removal On Host: File Deletion (T1070.004)
- Application Layer Protocol: Web Protocols (T1071.001)
- Data Staged: Local Data Staging (T1074.001)
- Valid Accounts: Local Accounts (T1078)
- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Phishing: Spearphishing Link (T1566.002)
- Exfiltration Over Web Service (T1567)

Montezuma

Intermediate

Publisher: SimSpace

30 minutes

Description

An automated attack that is unique and not attributed to a specific threat actor. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- Remote Services: Smb Windows Admin Shares (T1021.002)
- Scheduled Transfer (T1029)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Application Layer Protocol: Web Protocols (T1071.001)
- Data Staged (T1074)
- Data Staged: Local Data Staging (T1074.001)
- System Information Discovery (T1082)
- Clipboard Data (T1115)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Archive Collected Data (T1560)
- Exfiltration Over Web Service (T1567)

Mustang Panda (China)

Intermediate

Publisher: SimSpace

9 minutes

Description

An automated attack meant to emulate an APT actor with the common names TA416, RedDelta, BRONZE PRESIDENT, and Mustang Panda. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Network Connections Discovery (T1049)
- Scheduled Task/Job (T1053)
- Process Discovery (T1057)
- Application Layer Protocol: Web Protocols (T1071.001)
- Data Staged: Local Data Staging (T1074.001)
- Valid Accounts: Local Accounts (T1078)
- System Information Discovery (T1082)
- File And Directory Discovery (T1083)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery (T1518)
- Exfiltration Over Web Service (T1567)

Operation Wocao (China)

Intermediate

Publisher: SimSpace

30 minutes

Description

Implements an automated attack meant to emulate an APT actor with the common name Operation Wocao. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Service Discovery (T1007)
- Query Registry (T1012)
- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- Remote Services: Smb Windows Admin Shares (T1021.002)
- Windows Management Instrumentation (T1047)
- System Network Connections Discovery (T1049)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Indicator Removal On Host: Clear Windows Event Logs (T1070.001)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- File And Directory Discovery (T1083)
- Account Discovery: Domain Account (T1087.002)
- System Time Discovery (T1124)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Impair Defenses: Disable Or Modify System Firewall (T1562.004)
- Exfiltration Over Web Service (T1567)

Ransomware

Intermediate

Publisher: SimSpace

7 minutes

Description

Searches for a target computer with valuable files. Deploys persistence, downloads ransomware, and executes ransomware on a specific file. Uses initial access, discovery, persistence, lateral movements, and command line.

Attack Intent Ransomware

Execution Sequential

MITRE Tactics and Sub-techniques

- Data from Local System (T1005)
- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: SMB/Windows Admin Shares (T1021.002)
- Obfuscated Files or Information (T1027)
- Obfuscated Files or Information: Binary Padding (T1027.001)
- Process Discovery (T1057)
- Command and Scripting Interpreter (T1059)
- Data Staged (T1074)
- Ingress Tool Transfer Technique (T1105)
- Brute Force (T1110)
- Brute Force: Password Cracking (T1110.002)
- User Execution (T1204)
- User Execution: Malicious File (T1204.002)
- Data Encrypted for Impact (T1486)
- Impair Defenses (T1562)
- Impair Defenses: Disable or Modify Tools (T1562.001)
- Impair Defenses: Disable Windows Event Logging (T1562.002)
- Hide Artifacts (T1564)
- Hide Artifacts: Hidden Files and Directories (T1564.001)
- Phishing (T1566)
- Phishing: Spearphishing Attachment (T1566.001)
- Lateral Tool Transfer (T1570)

Reconnaissance by an Insider Threat

Intermediate

Publisher: SimSpace

3 minutes

Description

Emulates an insider threat model with a valid user already on the system. The malicious user opens a reverse shell session on the initial host, and then uses it to enumerate information about the host and the network it resides on.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Service Discovery (T1007)
- Application Window Discovery (T1010)
- Query Registry (T1012)
- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- System Network Connections Discovery (T1049)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Account Discovery: Domain Account (T1087.002)
- Peripheral Device Discovery (T1120)
- System Time Discovery (T1124)
- Network Share Discovery (T1135)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Virtualization Sandbox Evasion (T1497)

Turla (Russia)

Intermediate

Publisher: SimSpace

17 minutes

Description

An automated attack meant to emulate an APT actor with the common names Turla, Group 88, Belugasturgeon, Waterbug, WhiteBear, VENOMOUS BEAR, Snake, and Krypton. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- System Service Discovery (T1007)
- Query Registry (T1012)
- System Network Configuration Discovery (T1016)
- Remote System Discovery (T1018)
- Remote Services: Net Use (T1021)
- System Network Connections Discovery (T1049)
- Process Discovery (T1057)
- Permission Groups Discovery: Local Groups (T1069.001)
- Permission Groups Discovery: Domain Groups (T1069.002)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Peripheral Device Discovery (T1120)
- System Time Discovery (T1124)
- Drive By Compromise (T1189)
- Password Policy Discovery (T1201)
- User Execution (T1204)
- Software Discovery: Security Software Discovery (T1518.001)
- Exfiltration Over Web Service (T1567)

Ubiquitous Freedom

Intermediate

Publisher: SimSpace

20 minutes

Description

An automated attack that is unique and not attributed to a specific threat actor. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols. This scenario includes common discovery and lateral movement techniques, along with VM detection via LoLbin commands.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Application Window Discovery (T1010)
- System Network Configuration Discovery (T1016)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- System Owner User Discovery (T1033)
- Scheduled Task/Job (T1053)
- Application Layer Protocol: Web Protocols (T1071.001)
- System Information Discovery (T1082)
- Email Collection: Email Forwarding Rule (T1114.003)
- Peripheral Device Discovery (T1120)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Virtualization Sandbox Evasion: System Checks (T1497.001)
- Virtualization Sandbox Evasion: User Activity Based Checks (T1497.002)
- Virtualization Sandbox Evasion: Time Based Evasion (T1497.003)
- Exfiltration Over Web Service (T1567)

Wizard Spider (Russia)

Intermediate

Publisher: SimSpace

9 minutes

Description

An automated attack meant to emulate an APT actor with the common names UNC1878, TEMP.MixMaster, Grim Spider, and Wizard Spider. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

MITRE Tactics and Sub-techniques

- Remote System Discovery (T1018)
- Remote Services (T1021)
- Remote Services: Net Use (T1021)
- Windows Management Instrumentation (T1047)
- Application Layer Protocol: Web Protocols (T1071.001)
- Valid Accounts: Domain Accounts (T1078)
- Account Discovery: Domain Account (T1087.002)
- System Time Discovery (T1124)
- Drive By Compromise (T1189)
- User Execution (T1204)
- Domain Trust Discovery (T1482)

Upcoming Scenarios

APT32-Cobalt Kitty (Vietnam) **(Available 4Q22)**

Intermediate

Publisher: SimSpace

Description

Inspired by APT32. An automated attack meant to emulate an APT actor with the common names SeaLotus, OceanLotus, APT-C-00, APT32, and Operation Cobalt Kitty. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

APT39 (Iran) **(Available 3Q22)**

Intermediate

Publisher: SimSpace

Description

Inspired by APT39. An automated attack meant to emulate an APT actor with the common names REMIX KITTEN, ITG07, Chafer, and APT39. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

Dragonfly 2.0 (Russia) **(Available 3Q22)**

Intermediate

Publisher: SimSpace

Description

An automated attack meant to emulate an APT actor with the common names IRON LIBERTY, DYMALLOY, Berserk Bear, and Dragonfly 2.0. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

Honeybee **(Available 3Q22)** Intermediate

Publisher: SimSpace

Description

An automated attack meant to emulate an APT actor with the common name Honeybee. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

Kimsuky (North Korea) **(Available 3Q22)** Intermediate

Publisher: SimSpace

Description

An automated attack meant to emulate an APT actor with the common names STOLEN PENCIL, Thallium, Black Banshee, Velvet Chollima, and Kimsuky. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

menuPass (China) **(Available 3Q22)** Intermediate

Publisher: SimSpace

Description

Inspired by APT10. An automated attack meant to emulate an APT actor with the common names Cicada, POTASSIUM, Stone Panda, APT10, Red Apollo, CVNX, HOGFISH. and menuPass. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

Threat Group-3390 (China) **(Available 4Q22)**

Intermediate

Publisher: SimSpace

Description

An automated attack meant to emulate an APT with the common names TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse, and Threat Group-3390. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential

Tropic Trooper (China) **(Available 4Q22)**

Intermediate

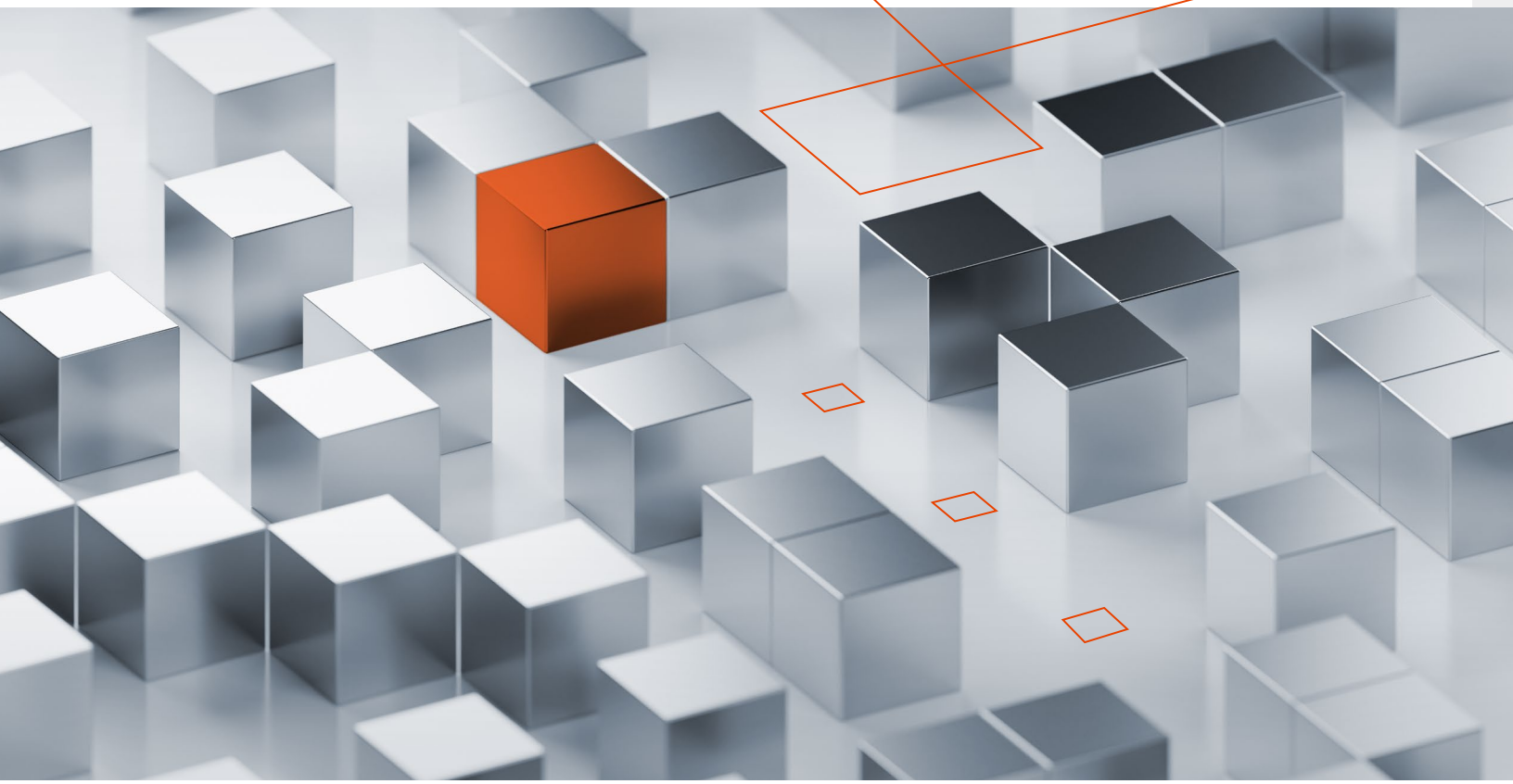
Publisher: SimSpace

Description

An automated attack meant to emulate an APT actor with the common names Pirate Panda, KeyBoy, and Tropic Trooper. The attack attempts to exfiltrate victim's data through C2 channels and alternative protocols.

Attack Intent Data Exfiltration

Execution Sequential



SimSpace.com
info@simspace.com
+1.617.237.6223

SIMSPACE

052022