simspace

# ATTACK CATALOG

2Q 2024

# 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 Attack Catalog appropriately.

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

# Table of Contents

# Index

# Index

# ALLANITE



Medium Complexity Estimated Attack Duration 11 MIN

**Targeted Industry or Sector:**
Critical Infrastructure, Energy

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Command and Control

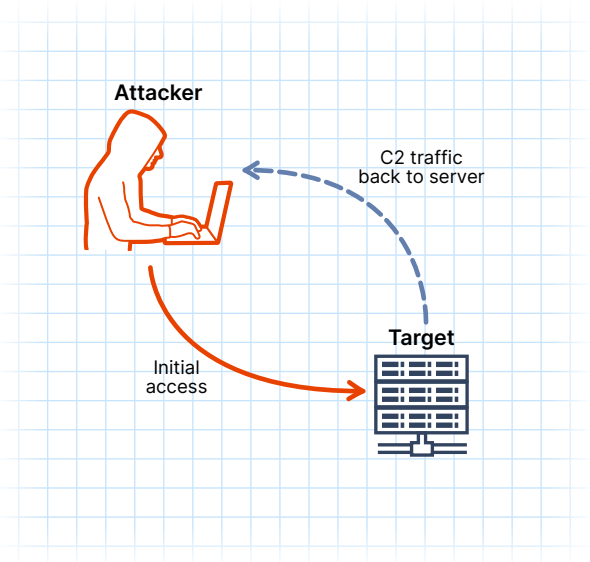
**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR

**Expected Outcomes:** Stop Attack, Remediate




**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The Russian cyber espionage group, ALLANITE, focuses on stealing information from industrial control systems (ICS) in the United States and the United Kingdom. After gaining access to a network via a watering hole or phishing attack, the threat group attempts to establish persistence in the ICS network for information-gathering purposes. There has been no indication that ALLANITE has attempted to disrupt or disturb the networks that it has exploited.

In this scenario, a C2 agent lands on a low-level victim and utilizes privileged credentials to add registry keys and create new hidden users with administrator-level permissions.

# APT3



High Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Aerospace, Defense, Government, Technology

**Targeted Environment:** IT

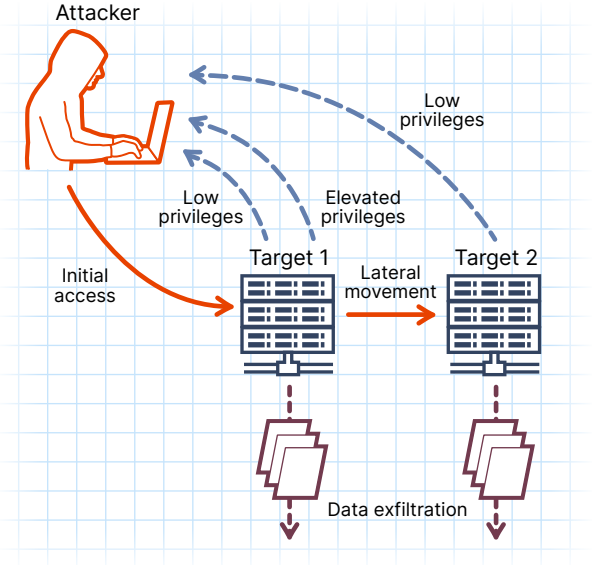
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Phishing, Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

After being discovered in 2010, the suspected Chinese threat group APT3 became infamous for attacking both US and UK targets in a variety of industries. In 2015, APT3 shifted its gaze to Hong Kong political organizations and used both zero-day and custom attack tools to disrupt operations. The US Department of Justice indicted three people affiliated with this group in 2017 on charges of computer hacking, theft of trade secrets, conspiracy, and identity theft.

In this scenario, a C2 agent lands on a low-level victim and collects a vast amount of data before elevating privileges. Several files are exfiltrated, persistence is obtained, and the automated attacker moves laterally to another victim. On the next victim, more data is staged and exfiltrated. The automated attacker then clears its tracks.

# APT19



Low Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Defense, Energy, Financial, Manufacturing, Technology, Telecommunications

**Targeted Environment:** IT

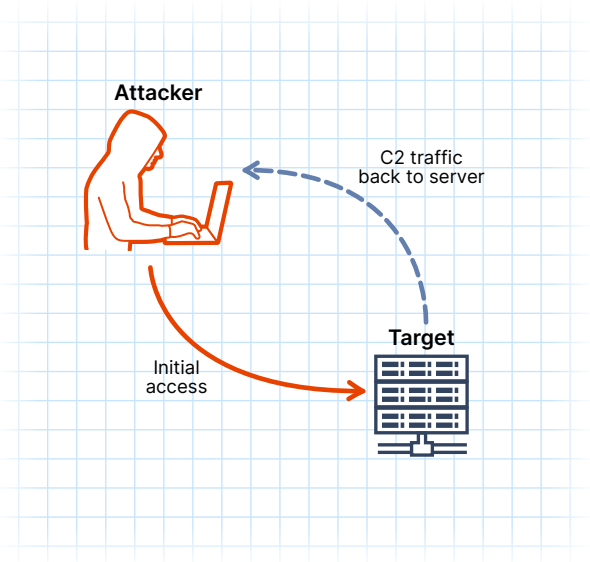
**Attack Tactics:**
- Initial Access
- Execution
- Privilege Escalation
- Defense Evasion
- Discovery
- Command and Control

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint

**Tools Sourced:** SIEM, EDR



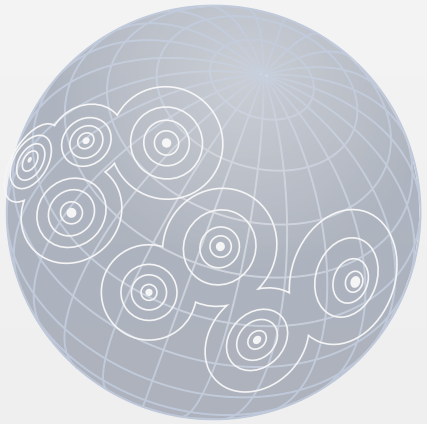

**Expected Outcomes:** Stop Attack, Remediate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The Chinese-based threat group, APT19, has actively targeted many industries with a variety of exploit types. Phishing emails, watering hole attacks, and even Cobalt Strike payloads have been employed to exploit victims. However, the group is less sophisticated than most other threat groups and is known to sometimes use off-the-shelf tools.

In this scenario, a C2 agent lands on a low-level victim and drops a malicious binary to disk after performing several discovery actions. The automated attacker takes advantage of two Windows LOLBins before exiting.



# APT29



Medium Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Academic, Government, Technology, Telecommunications

**Targeted Environment:** IT

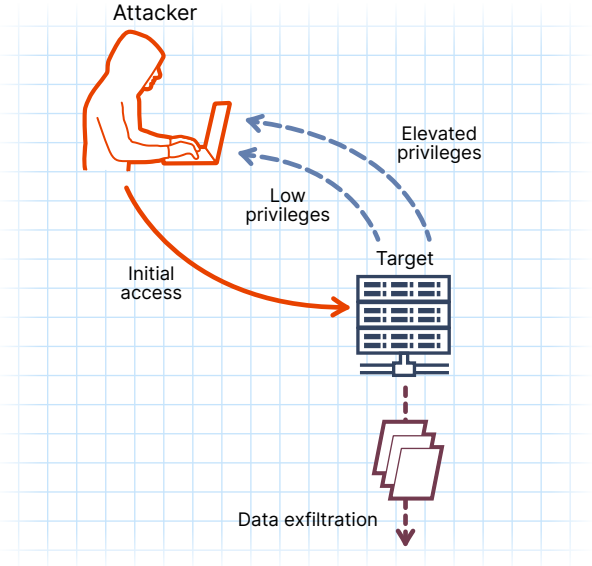
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** One Tier 4 target and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** EDR, IDPS



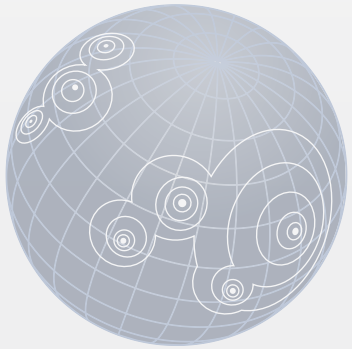

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Most likely associated with Russia's Foreign Intelligence Service (SVR), APT29 has targeted a variety of countries and industries since 2008. The threat group was responsible for attacking the Democratic National Committee, the governing body of the United States Democratic Party, beginning in 2015, and was behind the SolarWinds Orion Platform compromise in 2021, leading to the largest software supply chain breach ever recorded.

In this scenario, a C2 agent lands on a low-level victim and immediately performs a privilege escalation. After thwarting potential detection mechanisms, the automated attacker uncovers pertinent information about its host and subsequently collects, archives, and exfiltrates this data. The potential detection mechanisms are reinstated, and the automated attacker exits the victim.



# APT41



High Complexity Estimated Attack Duration 11 MIN

**Targeted Industry or Sector:** Healthcare, Telecommunications, Technology

**Targeted Environment:** IT

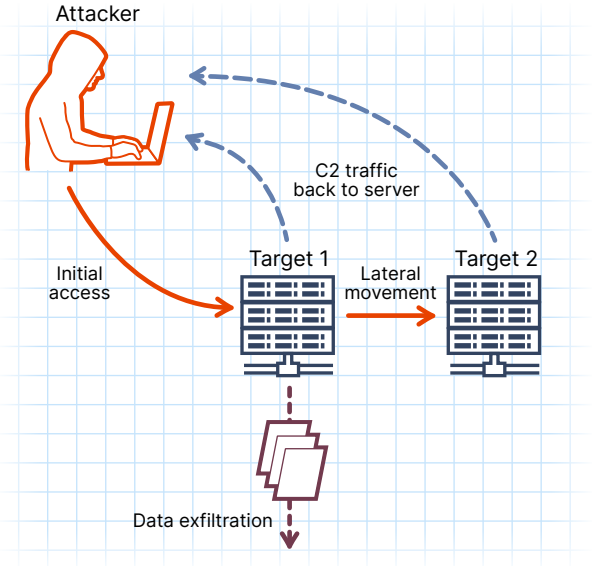
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



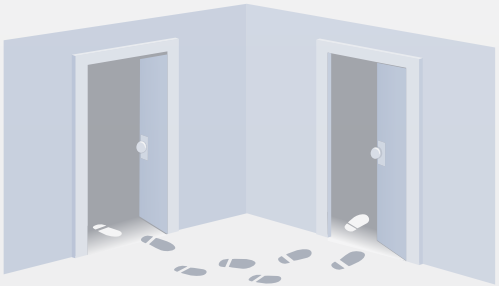

**Expected Outcomes:** Stop Attack, Contain and Mitigate, Remediate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The activity of APT41 is unique in the cybersecurity landscape because the group seems to carry out Chinese state-sponsored hacking activities in addition to financially-motivated attacks for personal gain. The group uses tools typically kept for exclusive use by the Chinese government for a variety of attacks. In September 2020, the US Department of Justice publicly released charges naming five people associated with this group for their role in hacking over 100 companies worldwide.

In this scenario, a C2 agent lands on a low-level victim and probes for host and network data. After the data is archived and exfiltrated, the automated attacker establishes persistence on the first victim and moves laterally to another victim. The automated attacker next clears the logs from the original victim, sets up a local administrator account on the victim for later use, and exits.



# Beaconer Deployment



Low Complexity

Estimated Attack Duration 5 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Discovery
- Command and Control

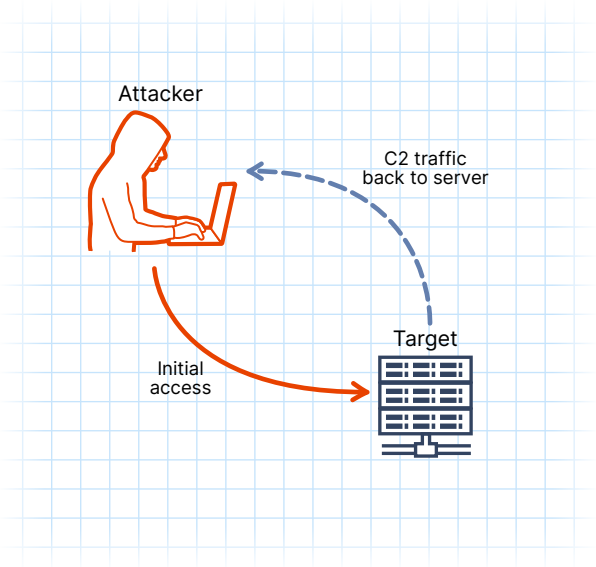
**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:**
One Tier 4 target and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** EDR, IDPS

**Expected Outcomes:** Stop Attack




**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim, gathers a large amount of information about the host and the domain, and quickly exits.

# BRONZE BUTLER



Extreme Complexity

Estimated Attack Duration **20** MIN

**Targeted Industry or Sector:**
Government, Manufacturing, Technology

**Targeted Environment:** IT

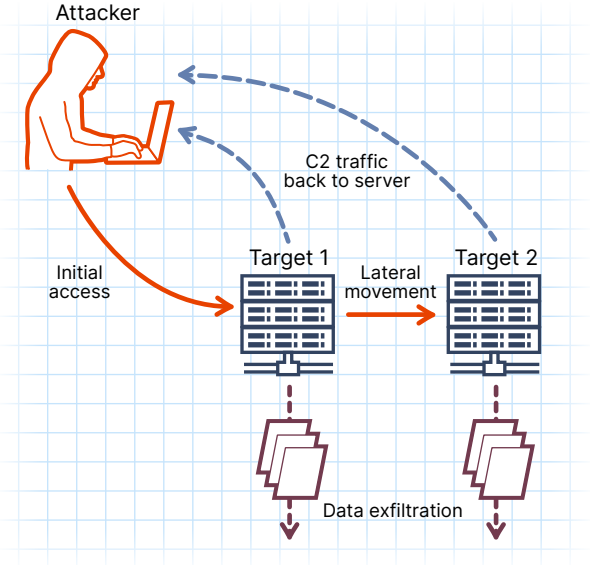
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



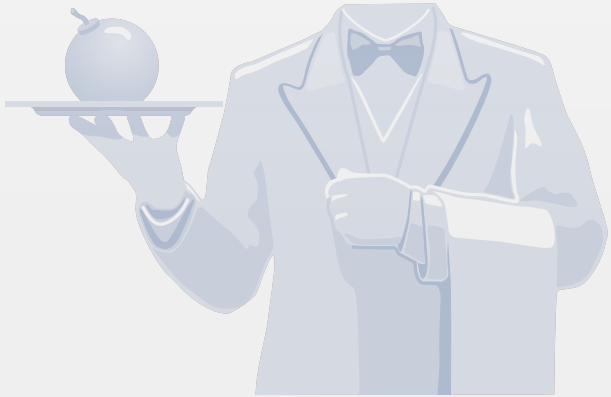

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

BRONZE BUTLER is intent on exfiltrating intellectual property and other confidential data from Japanese businesses. It strikes its victims with both zero-day exploits and custom malware. The group is believed to originate in China, but researchers have noticed that the attackers are likely fluent in Japanese based on the content of their spear phishing emails. Due to their mastery of cyber tradecraft and good operational security practices, BRONZE BUTLER has been able to stay inside of some corporate networks for up to five years.

In this scenario, a C2 agent lands on a low-level victim and performs basic discovery operations before archiving and exfiltrating data. The automated attacker covers its tracks and proceeds to move laterally to another victim where it performs similar steps before vanishing.



# Chimera



High Complexity

Estimated Attack Duration 32 MIN

**Targeted Industry or Sector:**
Aerospace, Technology

**Targeted Environment:** IT

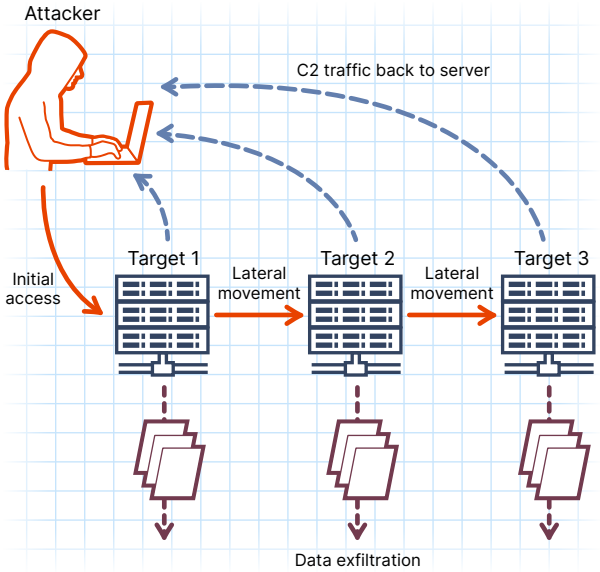
**Attack Tactics:**
- Reconnaissance
- Initial Access
- Execution
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Three Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, Application Logs, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Suspected to originate from China, the Chimera threat group is most known for its interest in disrupting the semiconductor industry in Taiwan. These operations most likely began in 2018. Chimera used a combination of custom tools and living-off-the-land binaries (LOLbins) to accomplish its tradecraft. The main motivation behind the attacks seems to be the theft of trade secrets from highly valuable semiconductor manufacturers.

In this scenario, a C2 agent lands on a low-level victim and performs extensive reconnaissance. After collecting and exfiltrating sensitive information, the automated attacker laterally moves to a second victim and repeats the process. The domain controller is targeted next, where sensitive information is collected and exfiltrated. Finally, forensic traces of its presence are removed, and the agent exits.

# Domain Controller Service Disruption and Exfiltration



High Complexity Estimated Attack Duration 5 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

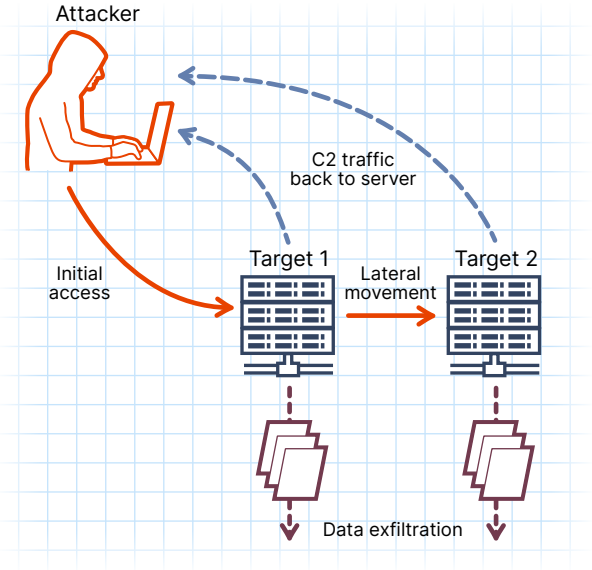
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



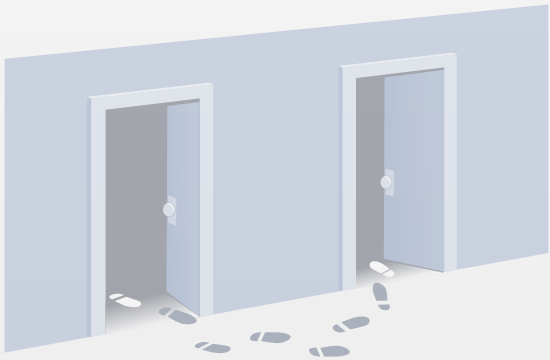

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and performs basic reconnaissance steps. After establishing persistence, host information is collected and exfiltrated. The automated attacker laterally moves to the domain controller and establishes persistence. After stopping a key service and exfiltrating more data, the automated attacker exits.



# Dragonfly



Medium Complexity

Estimated Attack Duration **38** MIN

**Targeted Industry or Sector:**
Critical Infrastructure,
Defense, Energy

**Targeted Environment:** IT

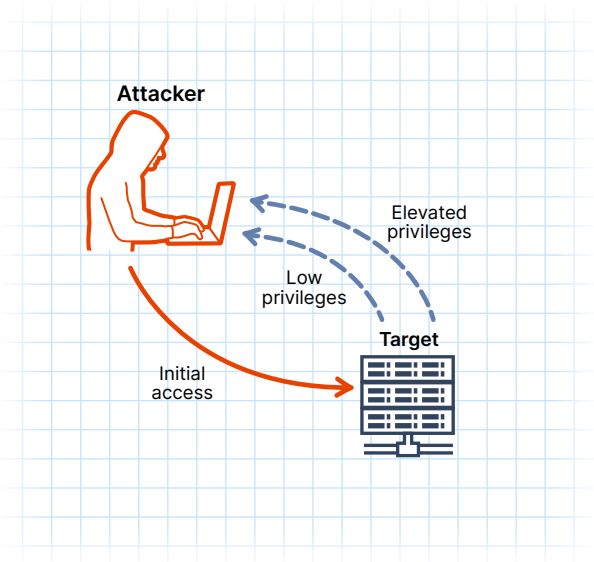
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Command and Control

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, Application Logs, System Logs

**Tools Sourced:** SIEM, EDR




**Expected Outcomes:** Stop Attack, Remediate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Since at least 2011, Dragonfly has been targeting the defense, aviation, and energy sectors in a variety of campaigns. The Russian cyber espionage group also focuses on companies that use industrial control systems (ICS), especially those involved in water and energy distribution. In March 2022, the United States Department of Justice offered a reward of up to $10 million in connection with apprehending four members of Dragonfly.

In this scenario, a C2 agent lands on a low-level victim and immediately elevates its privileges before performing numerous discovery commands on the local system. After modifying security settings and adding registry keys, the automated attacker creates new accounts, establishes persistence, and opens a backdoor for future access.

# GALLIUM



High Complexity

Estimated Attack Duration 17 MIN

**Targeted Industry or Sector:** Financial, Government, Telecommunications

**Targeted Environment:** IT

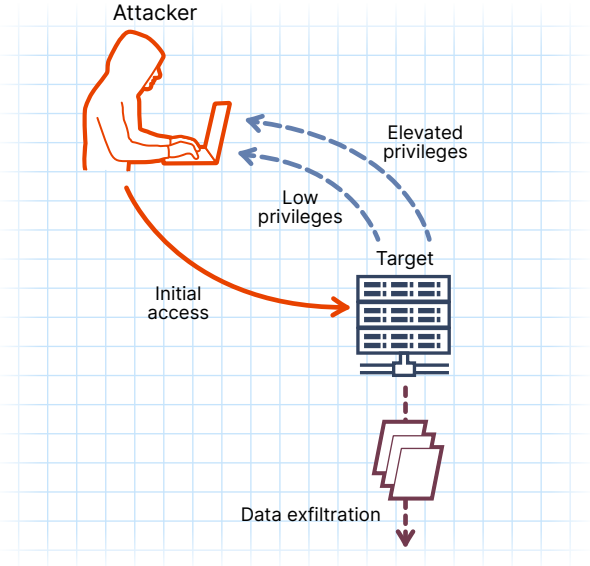
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** One Tier 4 target and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** EDR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

GALLIUM is likely a Chinese state actor, best known for targeting telecommunications groups around the world. The group typically targets vulnerable web servers, and, after gaining a foothold, drops web shells to maintain persistence. GALLIUM has been known to use a variety of off-the-shelf tools that have been modified to evade antimalware detection methods. These tools include Mimikatz, NBTScan, Netcat, PsExec, and even WinRAR.

In this scenario, a C2 agent lands on a low-level victim and immediately elevates its privileges. After discovering information about the host and archiving it on disk, the automated attacker exfiltrates its findings. Next, the attacker clears its tracks and vanishes.

# Hopi



Medium Complexity

Estimated Attack Duration 13 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Lateral Movement
- Command and Control

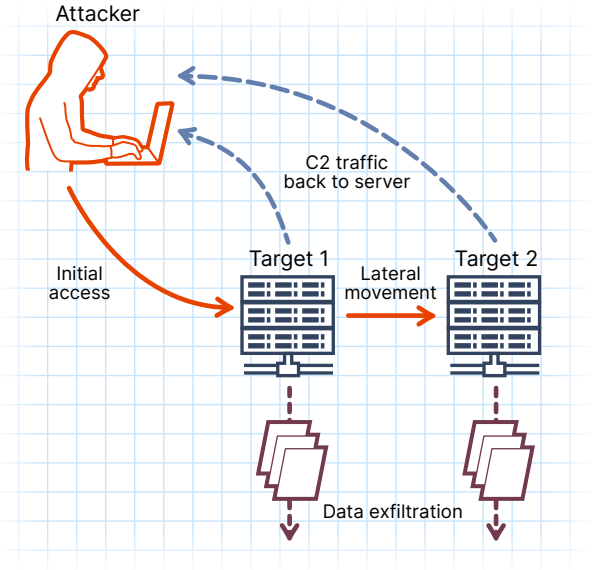
**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS

**Expected Outcomes:** Stop Attack, Contain and Mitigate




**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim, performs basic host reconnaissance, and exfiltrates data. The automated attacker laterally moves to another victim and repeats the same attack.

# Host-Based Artifact Dropper with Multiple File Exfiltration

▶ INDEX ▶ MITRE ATT&CK TTPs

High Complexity Estimated Attack Duration **39 MIN**

**Targeted Industry or Sector:** General

**Targeted Environment:** IT

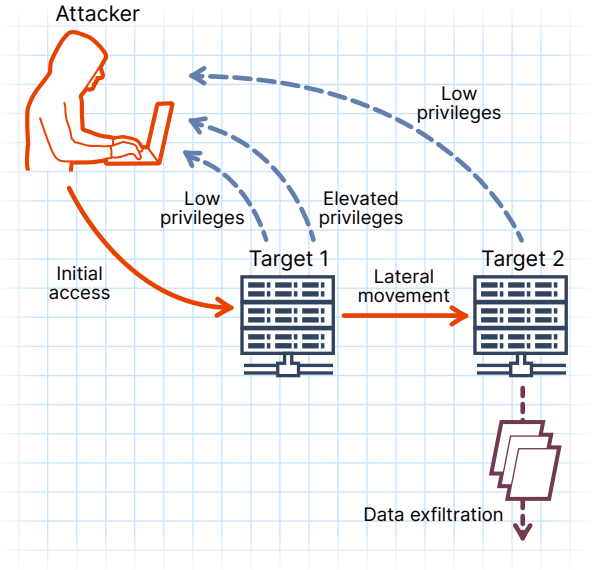
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and immediately elevates its privileges. After basic host reconnaissance and establishing persistence, the automated attacker moves laterally to another host. Data is collected and exfiltrated on both hosts. *Note: the automated attacker intentionally leaves behind a variety of artifacts for Blue Team detection and forensic analysis.*

# Initial Access VNC Recon



Low Complexity

Estimated Attack Duration **10 MIN**

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

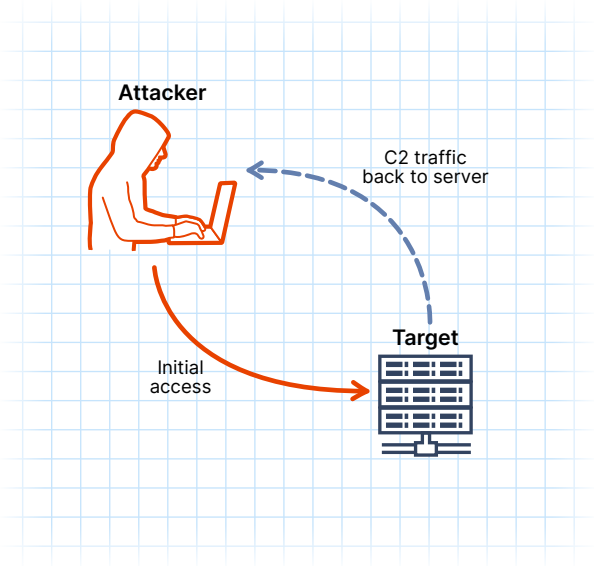
**Attack Tactics:**
- Initial Access
- Execution
- Defense Evasion
- Collection
- Command and Control

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, Application Logs, System Logs

**Tools Sourced:** SIEM, EDR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and drops remote access software. The automated attacker collects sensitive data from the unsuspecting target and quickly covers its tracks before exiting.

# Lazarus Group



Medium Complexity

Estimated Attack Duration 16 MIN

**Targeted Industry or Sector:** Critical Infrastructure, Defense, Energy, Financial, Government

**Targeted Environment:** IT

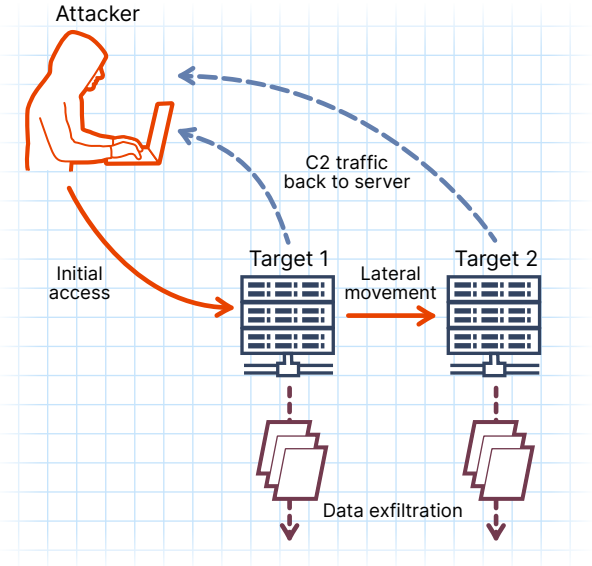
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, IDPS



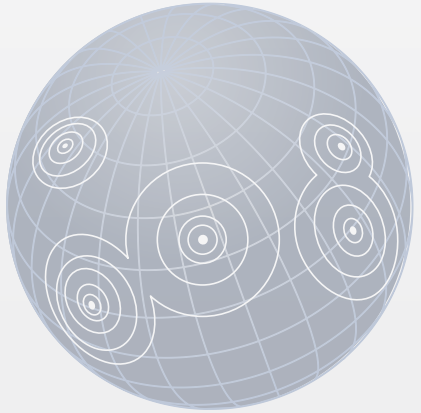

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The North Korean Lazarus Group has been active since at least 2009. It is best known for the attack on Sony Pictures in 2014 and the distribution of the crippling WannaCry ransomware in 2017. Lazarus Group has displayed technical acumen and a raw determination to wreak havoc around the world. Researchers believe the group is not only state-sponsored but also helps to bring in significant financial support for the North Korean government.

In this scenario, a C2 agent lands on a low-level victim and quickly collects and exfiltrates basic host intelligence. The automated attacker laterally moves to another victim, only to repeat the operation and subsequently exit.



# Leviathan – Variant 1



High Complexity Estimated Attack Duration 10 MIN

**Targeted Industry or Sector:** Academic, Aerospace, Defense, Government, Healthcare, Manufacturing, Transportation

**Targeted Environment:** IT

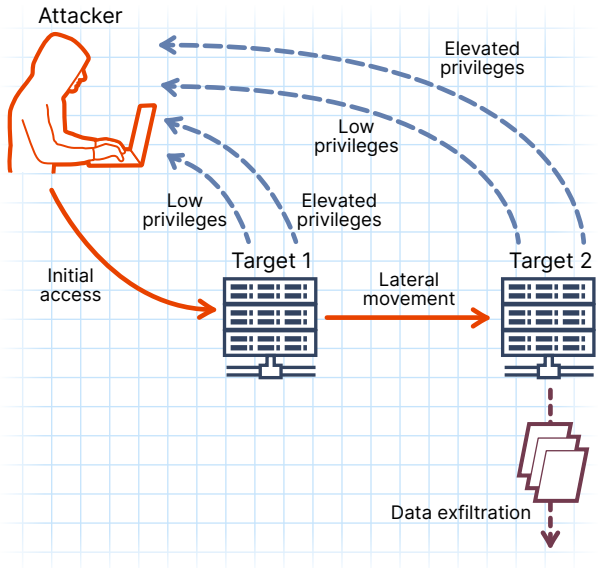
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Leviathan has been conclusively linked to a Chinese state security department and an affiliated front company. It has been active throughout the world in a variety of sectors since at least 2009. The group uses a plethora of attack types and has been particularly successful using phishing emails with malicious Microsoft Office macros. The US Department of Justice indicted four Leviathan group members in July 2021 for their malicious computer network activities.

In this scenario, a C2 agent lands on a low-level victim, immediately elevates its privileges, discovers network information, and establishes persistence. Quickly moving laterally to another host, the automated attacker performs another privilege escalation before establishing persistence and exfiltrating host data.

# Leviathan – Variant 2



Medium Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Academic, Aerospace, Defense, Government, Healthcare, Manufacturing, Transportation

**Targeted Environment:** IT

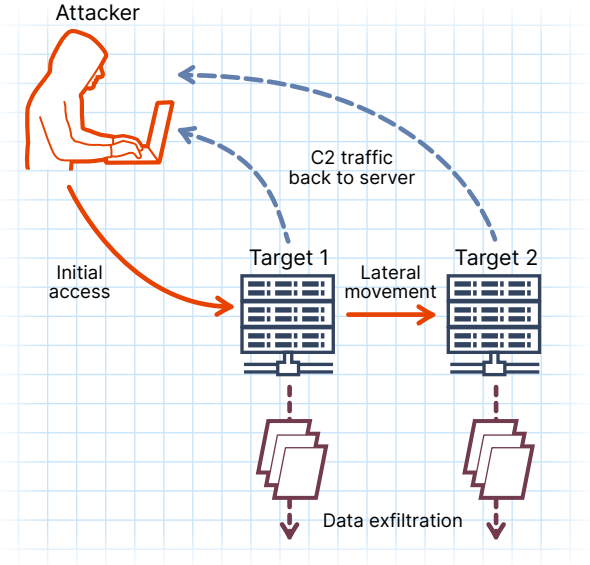
**Attack Tactics:**
- Initial Access
- Execution
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Leviathan has been conclusively linked to a Chinese state security department and an affiliated front company. It has been active throughout the world in a variety of sectors since at least 2009. The group uses a plethora of attack types and has been particularly successful using phishing emails with malicious Microsoft Office macros. The US Department of Justice indicted four Leviathan group members in July 2021 for their malicious computer network activities.

In this scenario, a C2 agent lands on a low-level victim and, after performing several discovery steps, proceeds to exfiltrate its findings. The automated attacker moves laterally to another victim host and performs more research. The data is exfiltrated to a web server, at which point the automated attacker exits the system.

# menuPass



Extreme Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:**
Aerospace, Defense, Energy, Financial, Government, Healthcare

**Targeted Environment:** IT

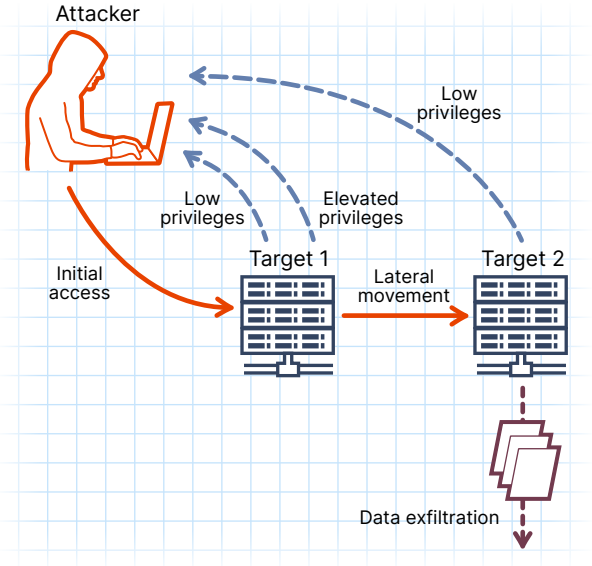
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



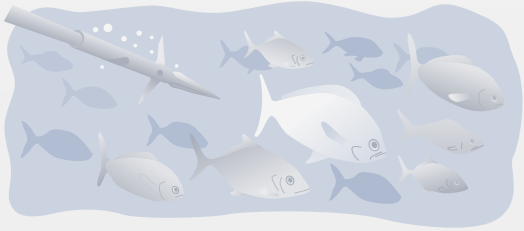

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The Chinese state-backed APT menuPass has primarily been concerned with espionage activities, and has been actively targeting a variety of sectors around the world since at least 2006. The group is known for developing sophisticated custom malware tools and deploying them after spear-phishing efforts have gained an initial foothold in an organization. menuPass has been known for targeting managed service providers (MSP) throughout the world and continues to steal intellectual property from both Japanese and Western entities.

In this scenario, a C2 agent lands on a low-level victim and immediately elevates its privileges. Before moving laterally to another victim, the automated attacker performs an extensive set of discovery operations. On the next host, data is collected and exfiltrated. The automated attacker clears its tracks and exits the system.



# Montezuma



High Complexity

Estimated Attack Duration 30 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

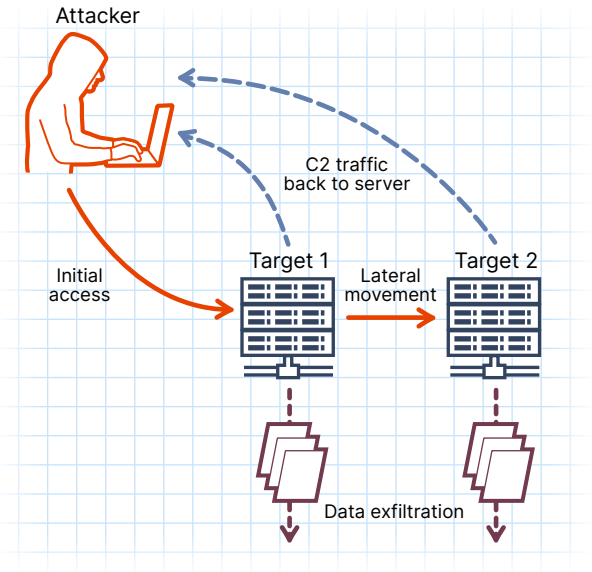
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and discovers a substantial amount of information about the host. After collecting and exfiltrating this data, the automated attacker moves laterally to another host and repeats the previous operations.

# Mustang Panda



Medium Complexity Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Government

**Targeted Environment:** IT

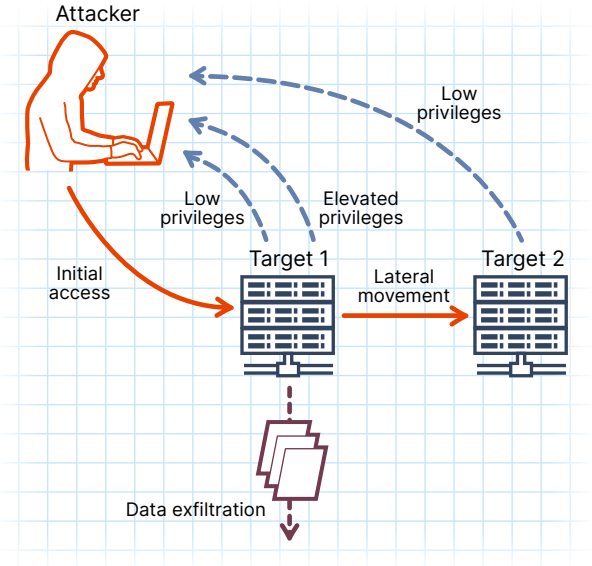
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Mustang Panda has its sights set on gathering intelligence from governments the world over. It continues to infiltrate private networks with specially crafted spear-phishing emails. The Chinese group has been actively tracked since 2017 and weaponizes vulnerabilities in various applications to gain a foothold and establish communications with its command infrastructure. With its combination of sophisticated social engineering and advanced malware development and deployment strategies, Mustang Panda is a formidable adversary for government networks worldwide.

In this scenario, a C2 agent lands on a low-level victim and immediately elevates its privileges. After acquiring knowledge of the host and network, the automated attacker collects and exfiltrates its findings. Moving onto another victim, communications with the C2 host are established before the automated attacker exits.

# OilRig



High Complexity Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:** Energy, Financial, Government, Telecommunications

**Targeted Environment:** IT

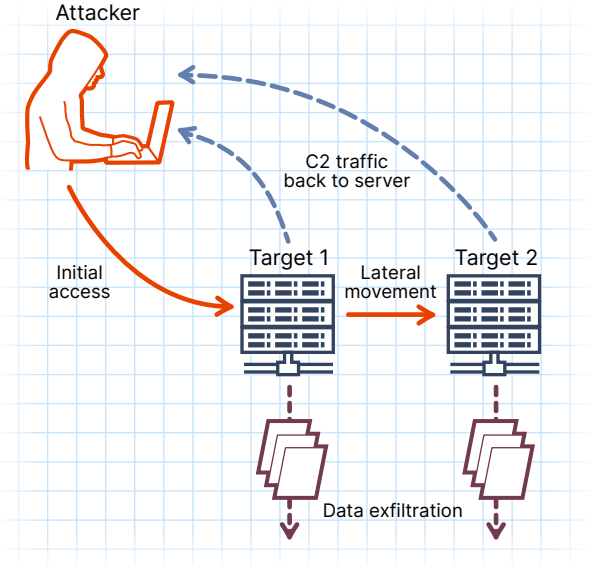
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Command and Control

**Attack Types:** Drive-By Compromise, Phishing

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



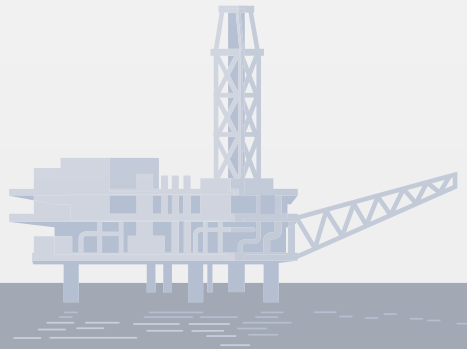

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The OilRig group is believed to hail from the Iranian government. It was first detected in 2012 during widespread attacks against Middle Eastern targets. When the group appeared, their apparent lack of sophistication was evident to researchers. Nevertheless, OilRig has greatly enhanced their tradecraft and was noted to be the first public threat group utilizing DNS-over-HTTPS (DoH) for exfiltrating data from its victims. OilRig continues to wreak havoc worldwide with a variety of custom tools and innovative techniques.

In this scenario, a C2 agent lands on a low-level victim and discovers information about the target. After exfiltrating data, the automated attacker moves laterally to another victim in the network. More information is gleaned by the automated attacker on the second host. After exfiltrating data and clearing its tracks, the automated attacker disappears.



# Operation Wocao



High Complexity

Estimated Attack Duration **30** MIN

**Targeted Industry or Sector:** Aerospace, Energy, Financial, Healthcare, Technology, Transportation

**Targeted Environment:** IT

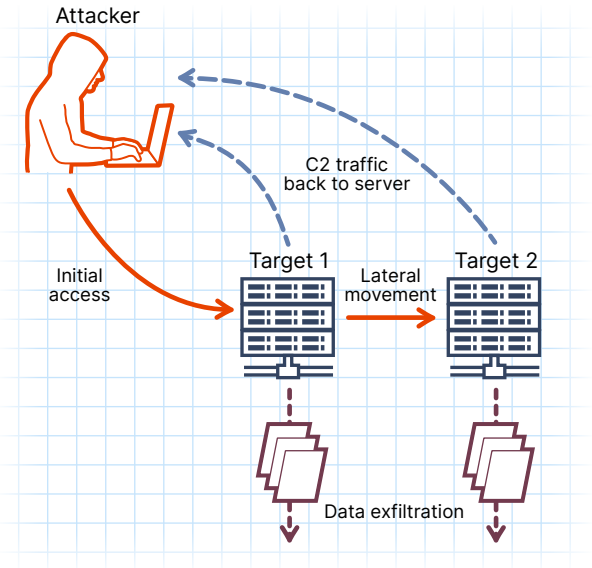
**Attack Tactics:**
- Initial Access
- Execution
- Defense Evasion
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The aim of the threat actors behind Operation Wocao is to conduct espionage against influential nations worldwide using simple tools and intelligent operational security to maintain a covert presence in victim networks. Operation Wocao is not itself a threat group although it was associated with the likely Chinese APT20. Instead, it was a campaign that operated from approximately 2017 to 2019. These hackers used web vulnerabilities to gain an initial foothold and then went directly for high-value targets with the aim of compromising credentials and setting up persistence. The campaign name originated from a Mandarin expletive entered by a frustrated operator after losing web shell access to a target.

In this scenario, a C2 agent lands on a low-level victim and queries its host for both system and domain information. Clearing its tracks, the automated attacker exfiltrates data and laterally moves to another victim. More information is discovered and exfiltrated. After clearing its tracks again, the automated attacker exits.

# Patchwork



Medium Complexity

Estimated Attack Duration **10 MIN**

**Targeted Industry or Sector:**
Government

**Targeted Environment:** IT

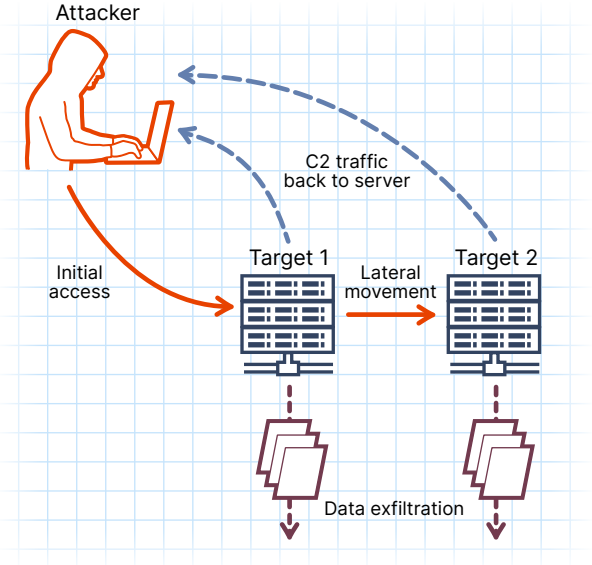
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS




**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Hailing from India since 2015, the Patchwork group is primarily focused on espionage efforts of foreign governments. Their tooling is wide in scope but typically not sophisticated because the group relies on publicly available applications and exploits. Nevertheless, Patchwork has grown to be a credible threat and continues to exfiltrate sensitive data using a variety of remote access trojans (RAT). In early 2022, the group humorously infected itself with a RAT, capturing keystrokes and screenshots of its own systems and virtual machines.

In this scenario, a C2 agent lands on a low-level victim and discovers a few key details concerning both system and network configuration. Data is exfiltrated, and the automated attacker moves laterally to another victim. After more discovery and exfiltration, the automated attacker exits the machine.

# Reconnaissance by an Insider Threat



Low Complexity

Estimated Attack Duration 3 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Defense Evasion
- Discovery
- Command and Control

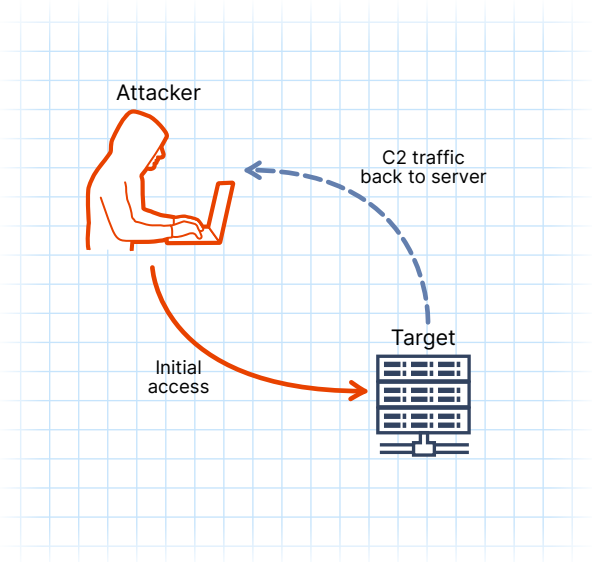
**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
One Tier 4 target and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** EDR, IDPS

**Expected Outcomes:** Stop Attack, Remediate




**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and simulates an insider threat, gathering a vast amount of both host and domain information before exiting.

# Tropic Trooper



Low Complexity

Estimated Attack Duration **11 MIN**

**Targeted Industry or Sector:** Government, Healthcare, Technology, Transportation

**Targeted Environment:** IT

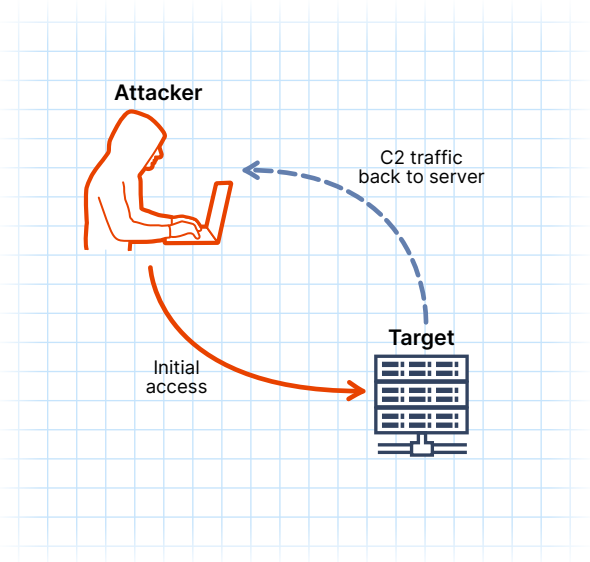
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Defense Evasion
- Discovery
- Command and Control

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:** Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, Application Logs, System Logs

**Tools Sourced:** SIEM, EDR




**Expected Outcomes:** Stop Attack, Remediate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This group appears to speak Chinese, but researchers are unable to pin down Tropic Trooper's affiliation. Tropic Trooper, now commonly referred to as "Earth Centaur", is known for its attacks on various industries located in Taiwan, the Philippines, and Hong Kong. The attackers seem to be adept at planting backdoors and focus on espionage activities, dumping credentials when possible and exfiltrating sensitive data.

In this scenario, a C2 agent lands on a low-level victim and quickly establishes persistence before dropping a custom toolkit. The automated attacker performs several discovery operations to uncover sensitive data.

# Turla



**Targeted Industry or Sector:**
Government

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Discovery
- Lateral Movement
- Command and Control
- Exfiltration

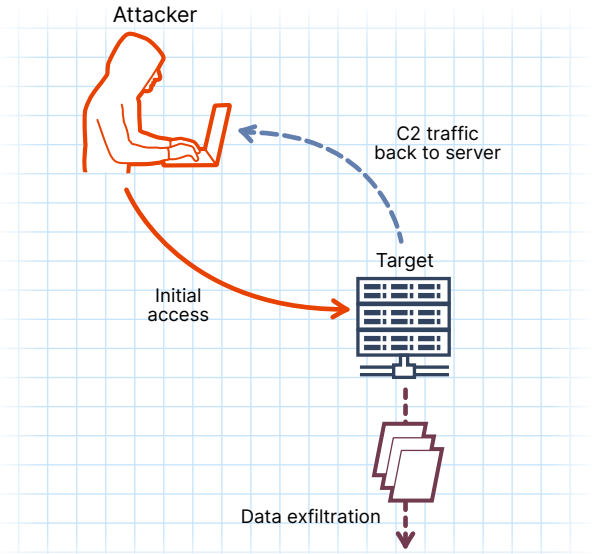
**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** EDR, IDPS

**Expected Outcomes:** Stop Attack, Contain and Mitigate

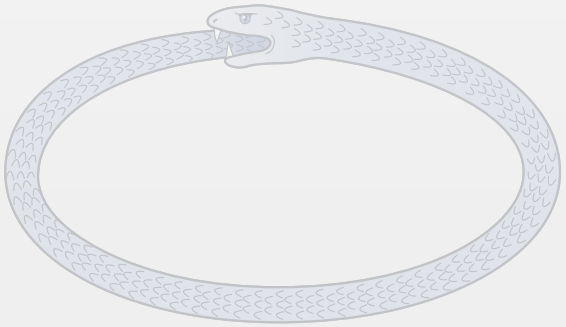



**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

The Russian APT Turla has leveraged sophisticated custom malware against at least 45 different countries. It has been active since 2004 and continues to defeat even the best defensive safeguards with its incredibly deft tradecraft. From using satellites for C2 operations to writing seemingly undetectable backdoors, the group dispatches its espionage efforts against a wide range of foreign sectors. While primarily focusing on Windows machines, Turla has also targeted both macOS and Linux in the quest for domain dominance.

In this scenario, a C2 agent lands on a low-level victim and launches a series of intricate discovery operations. Decoy activities mask the automated attacker's true intent while data is exfiltrated from the unsuspecting host.



# Ubiquitous Freedom



Medium Complexity Estimated Attack Duration 20 MIN

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

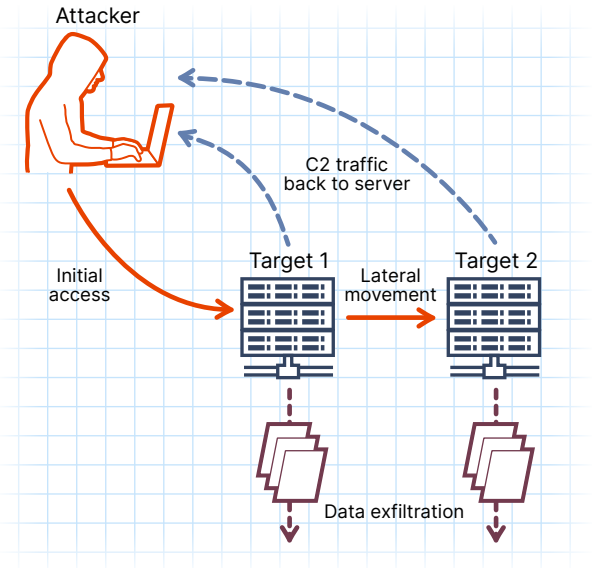
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS



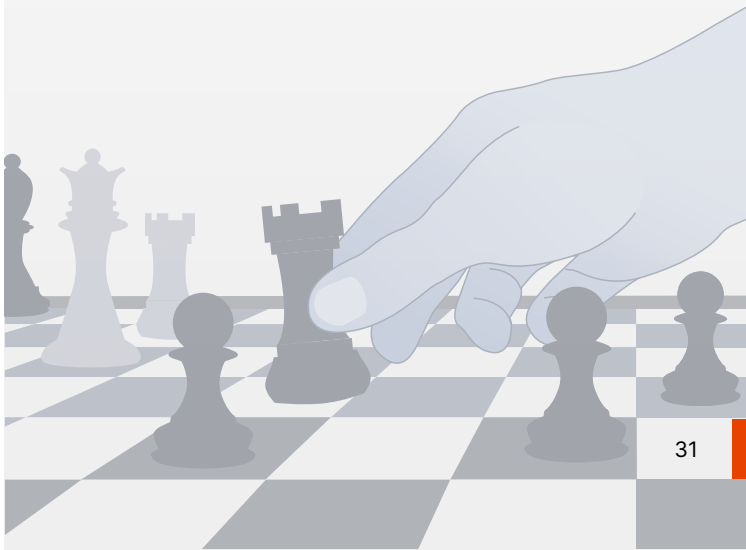

**Expected Outcomes:** Stop Attack, Contain and Mitigate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim and, after discovering a substantive amount of information, collects and exfiltrates its findings. Moving laterally to another host, the automated attacker again performs the same operations before exiting.



# Waning Spade



Low Complexity

Estimated Attack Duration **19 MIN**

**Targeted Industry or Sector:**
General

**Targeted Environment:** IT

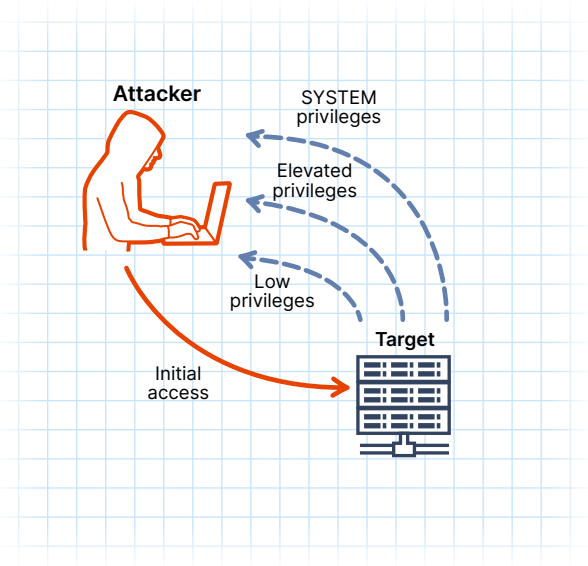
**Attack Tactics:**
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Discovery
- Command and Control

**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR




**Expected Outcomes:** Stop Attack, Remediate

**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

This is a SimSpace custom scenario and is not attributed to a specific threat actor.

In this scenario, a C2 agent lands on a low-level victim, performs basic discovery operations, and drops a tool to disk. Multiple privilege escalations allow for persistence as the SYSTEM user.

# Wizard Spider



Medium Complexity

Estimated Attack Duration 9 MIN

**Targeted Industry or Sector:**
Healthcare

**Targeted Environment:** IT

**Attack Tactics:**
- Initial Access
- Execution
- Privilege Escalation
- Discovery
- Lateral Movement
- Command and Control

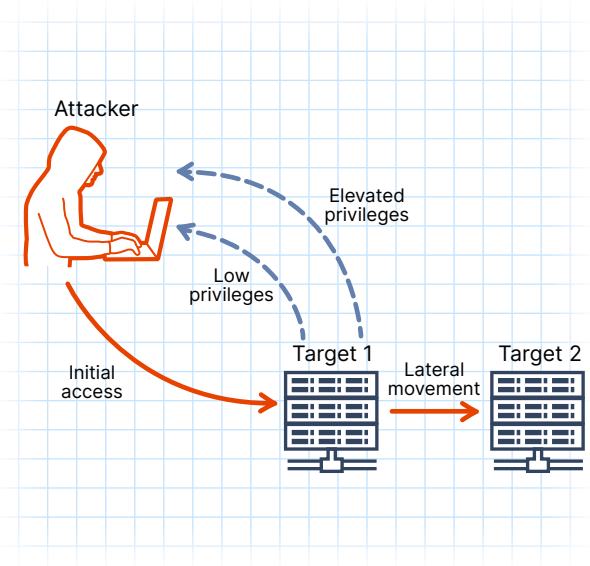
**Attack Types:** Drive-By Compromise

**Cyber Force Platform Prerequisites:**
Two Tier 4 targets and one Tier 1 domain controller, a mail relay

**Telemetry:** Network, Endpoint, System Logs

**Tools Sourced:** SIEM, EDR, SOAR, IDPS

**Expected Outcomes:** Stop Attack, Remediate




**Assume Breach?** Yes

**IOCs:** A list of available binaries, IP addresses, and domain names can be made available to White Cell/Control Cell operators

Wizard Spider, a highly profitable and financially motivated threat group, has most notably been associated with the Trickbot banking malware. The group is most likely responsible for the 2021 attack on the Health Service Executive (HSE) in Ireland which led to the shutdown of the entire health system nationwide. This was the largest cyberattack ever faced by the Irish government and the largest health services cyberattack in the world. Wizard Spider is suspected to originate in Russia and is linked to other well-known attack tools such as Ryuk, Conti, and BazarLoader.

In this scenario, a C2 agent lands on a low-level victim and probes for several key pieces of domain information. A privilege escalation reveals more domain intelligence. Finally, the agent moves laterally to another victim using living-off-the-land binaries (LOLbin).

# MITRE ATT&CK® TTPs

▶ INDEX

**ALLANITE** ▶ Attack Scenario

- Account Manipulation (T1098)
- Application Layer Protocol: Web Protocols (T1071.001)
- Create Account: Local Account (T1136.001)
- Create or Modify System Process: Windows Service (T1543.003)
- Drive-By Compromise (T1189)
- Hide Artifacts: Hidden Users (T1564.002)
- User Execution (T1024)
- Valid Accounts: Domain Accounts (T1078.002)

**APT3** ▶ Attack Scenario

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

**APT19** ▶ Attack Scenario

- Application Layer Protocol: Web Protocols (T1071.001)
- Drive-By Compromise (T1189)
- Ingress Tool Transfer (T1105)
- Signed Binary Proxy Execution: Rundll32 (T1218.011)
- System Information Discovery (T1082)
- User Execution (T1024)
- Valid Accounts: Domain Accounts (T1078.002)

# MITRE ATT&CK® TTPs

▶ INDEX

**APT29** ▶ Attack Scenario

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

**APT41** ▶ Attack Scenario

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

**Beaconer Deployment** ▶ Attack Scenario

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

**BRONZE BUTLER** ▶ Attack Scenario

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

**Chimera** ▶ Attack Scenario

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

**Domain Controller Service Disruption and Exfiltration** ▶ Attack Scenario

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

# MITRE ATT&CK® TTPs

▶ INDEX

**Dragonfly** ▶ Attack Scenario

- Account Discovery: Domain Account (T1087.002)
- Account Manipulation (T1098)
- Application Layer Protocol: Web Protocols (T1071.001)
- Create Account: Local Account (T1136.001)
- Create or Modify System Process: Windows Service (T1543.003)
- Drive-By Compromise (T1189)
- File and Directory Discovery (T1083)
- Impair Defenses: Disable or Modify System Firewall (T1562.004)
- Modify Registry (T1112)
- Network Share Discovery (T1135)
- Process Discovery (T1057)
- Software Discovery: Security Software Discovery (T1518.001)
- System Information Discovery (T1082)
- System Network Configuration Discovery (T1016)
- System Network Connections Discovery (T1049)
- System Owner/User Discovery (T1033)
- System Services: Service Execution (T1569.002)
- User Execution (T1024)
- Valid Accounts: Domain Accounts (T1078.002)

**GALLIUM** ▶ Attack Scenario

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

**Hopi** ▶ Attack Scenario

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

### Host-Based Artifact Dropper with Multiple File Exfiltration ▶ Attack Scenario

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

### Initial Access VNC Recon ▶ Attack Scenario

- Application Layer Protocol: Web Protocols (T1071.001)
- Deobfuscate/Decode Files or Information (T1140)
- Drive-By Compromise (T1189)
- Hide Artifacts (T1564)
- Indicator Removal on Host: File Deletion (T1070.004)
- Ingress Tool Transfer (T1105)
- Remote Access Software (T1219)
- Screen Capture (T1113)
- User Execution (T1024)

### Lazarus Group ▶ Attack Scenario

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

### Leviathan – Variant 1 ▶ Attack Scenario

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

### Leviathan – Variant 2 ▶ Attack Scenario

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

**menuPass** ▶ Attack Scenario

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

**Montezuma** ▶ Attack Scenario

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

**Mustang Panda** ▶ Attack Scenario

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

**OilRig** ▶ Attack Scenario

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

**Operation Wocao** ▶ Attack Scenario

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

**Patchwork** ▶ Attack Scenario

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

**Reconnaissance by an Insider Threat**
▶ Attack Scenario

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

**Tropic Trooper** ▶ Attack Scenario

- Application Layer Protocol: Web Protocols (T1071.001)
- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
- Deobfuscate/Decode Files or Information (T1140)
- Drive-By Compromise (T1189)
- File and Directory Discovery (T1083)
- Hide Artifacts: Hidden Files and Directories (T1564.001)
- Ingress Tool Transfer (T1105)
- Network Share Discovery (T1135)
- Process Discovery (T1057)
- Software Discovery (T1518)
- System Information Discovery (T1082)
- User Execution (T1024)

**Turla** ▶ Attack Scenario

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

# MITRE ATT&CK® TTPs

▶ INDEX

### Ubiquitous Freedom ▶ Attack Scenario

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

### Waning Spade ▶ Attack Scenario

- Application Layer Protocol: Web Protocols (T1071.001)
- BITS Jobs (T1197)
- Drive-By Compromise (T1189)
- Event Triggered Execution: Windows Management Instrumentation Event Subscription (T1546.003)
- Ingress Tool Transfer (T1105)
- Software Discovery (T1518)
- System Information Discovery (T1082)
- User Execution (T1024)
- Valid Accounts: Domain Accounts (T1078.002)

### Wizard Spider ▶ Attack Scenario

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



simspace.com info@simspace.com

SIMSPACE