ATTACKIQ®

THREAT REPORT

The Evolution of RomCom

From Backdoor to Cyberwar

Francis Guibernau
Senior Adversary Research Engineer

Table of Contents

Executive Summary

RomCom isn't a genre... It's a weapon. More specifically, it is a commodity malware operated as a polyvalent payload leveraged in state-aligned geopolitical espionage and financially motivated operations. Since its emergence, RomCom has demonstrated progressive adaptability, evolving through five distinct iterations, each introducing increased sophistication, modularity, and functionality.

What began with a report from the United Kingdom's National Cyber Security Centre (NCSC) quickly unraveled into a sprawling investigation. A reference to a downloader known as Damascened Peacock served as the cornerstone of the puzzle that led AttackIQ's Adversary Research Team (ART) to correlate 25 fragmented sources, spanning five years of threat activity.

As a result, we reconstructed the operational footprint of its operator, an eponymous criminal adversary whose operations are consistently aligned with the geopolitical interests of the Russian Federation, as demonstrated by sustained targeting of Ukraine and NATO-aligned nations.

Over time, both the operator and its payload have demonstrated operational overlaps and collaborative connections with other prominent cybercriminal entities. These connections suggest a shared or coordinated infrastructure and highlight the growing convergence between political espionage and financially driven extortion operations.

These connections, along with the behaviors exhibited by RomCom and its associated activities, are now emulated in seven newly released adversary emulations—AttackIQ's largest emulation release to date. These emulations are designed to help organizations validate their security controls, assess detection coverage, and strengthen their defensive posture against this sophisticated and evolving threat.

Key Findings

- **RomCom isn't a genre...** It's a weapon. While initially focused on Ukraine and NATO-aligned nations, RomCom-associated activities have expanded to include targets in the Government, Defense, and Humanitarian sectors.
- **Polyvalent and evolving threat.** RomCom has demonstrated progressive adaptability, evolving through five distinct iterations, each introducing increased sophistication, modularity, and functionality.
- **Overlapping connections with Ransomware groups.** Evidence shows tight integration between RomCom deployments and the use of Cuba, Industrial Spy, and Underground ransomware in double-extortion operations.

RomCom Remote Access Trojan (RAT)

RomCom is a Remote Access Trojan (RAT) family that has been active since at least May 2022. Primarily known for acquiring persistence and execution through Component Object Model (COM) Hijacking, a technique that abuses the Windows COM infrastructure by redirecting legitimate system processes to load malicious payloads, it has undergone multiple evolutionary stages, resulting in five distinct versions, each demonstrating increasing sophistication, modularity, and capabilities:

- **RomCom 1.0 (May 2022):** The initial variant performs environment reconnaissance by collecting system and user information, enumerating disks, files, installed applications, and running processes. Once completed, the information is exfiltrated to a hardcoded Command and Control (C2) server using the WinHTTP API. Additionally, it captures screenshots and supports self-deletion upon receiving a specific command.
- **RomCom 2.0 (June 2022):** An enhanced version of the original, which introduced significant enhancements over its predecessor, reflecting a more mature and stealthier toolset. It is optimized for espionage operations and long-term persistence, featuring improved data exfiltration techniques.
- **RomCom 3.0 (February 2023):** Architecturally modular, this version is structured into three modular components: a Loader, a Worker Module, and a Network Handler. Typically deployed via modified MSI or EXE installers, it represents a substantial leap in flexibility and functionality by introducing support for the execution of 42 distinct commands, although some are slight variations of each other.
- **RomCom 4.0 (August 2023):** This variant, also known as PEAPOD, maintains the three-component architecture, which is loaded entirely from memory, with the worker module stored within the registry. Communications leverage a Microsoft Edge 1.0 User-Agent and enforce TLS 1.2. Notably, it replaces localhost socket-based Inter-Process Communication (IPC) with named pipes, increasing stealth.
- **RomCom 5.0 (September 2024):** This variant, also known as SnipBot and SingleCamper, builds upon RomCom 3.0 but incorporates techniques observed in RomCom 4.0. It introduces support for new commands and evasion techniques.

RomCom RAT is delivered through a variety of Stagers, including downloaders, droppers, and loaders, typically embedded in trojanized versions of legitimate software. These are distributed through fake installers masquerading as popular applications, enabling the operator to bypass traditional security controls and gain initial access.

It is operated by the eponymous Russian adversary RomCom, also known as UAT-5647 and Storm-0978, an adaptive and increasingly sophisticated multi-motivational threat that has been active since at least 2022.

This adversary closely monitors geopolitical developments surrounding the war in Ukraine, leveraging these dynamics to conduct credential harvesting and data exfiltration activities presumably in support of Russian intelligence objectives. Its targeting has included government entities, political figures, and military personnel in Ukraine, Poland, and other NATO-aligned countries, as well as humanitarian and healthcare organizations assisting Ukrainian refugees. Additionally, RomCom has infiltrated organizations across the Defense, Finance, Telecommunications, and Technology sectors, particularly those with direct or indirect involvement in the Ukrainian conflict.

Beyond its geopolitical activities, RomCom also engages in opportunistic ransomware and extortion-focused operations. Initially, the adversary **leveraged** the Industrial Spy ransomware to conduct financially motivated activities in parallel with its espionage efforts. However, beginning in **July 2023**, RomCom transitioned to deploying Underground ransomware, a strain **regarded** as the successor to Industrial Spy due to substantial code overlap, suggesting a deliberate rebranding effort.

Industrial Spy refers both to a ransomware group and strain that **emerged** in April 2022, initially operating as a data extortion marketplace where criminals could acquire stolen information from compromised organizations. It was promoted through payload downloaders disguised as software cracks and adware, which dropped README.txt files advertising the platform.

Over time, Industrial Spy evolved into a full-fledged ransomware operation. Before introducing its proprietary strain in May 2022, the adversary briefly experimented with Cuba ransomware.

Cuba is a ransomware strain that **emerged** in December 2019 and gained notoriety in November 2021, following an **advisory** issued by the Federal Bureau of Investigation (FBI) outlining Indicators of Compromise (IOCs) associated with its activities. Since its emergence, it has **undergone** extensive refinement of its Tactics, Techniques, and Procedures (TTPs) to improve efficiency and effectiveness, evolving into a prevalent high-impact threat.

It is **operated** by the financially motivated adversary Tropical Scorpius, also known as Void Rabisu and UNC2596. Despite its name, Cuba ransomware appears to originate from Russia, as evidenced by its behavior of terminating execution on systems configured with Russian language settings or keyboard layouts.

Notably, in **May 2022**, a ransomware **sample** was identified appending the .cuba extension and dropping ransom notes referencing Cuba's Dedicated Leak Site (DLS), although the associated TOX ID and contact email pointed to Industrial Spy infrastructure, suggesting operational collaboration between both adversaries.

In October 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) **issued** an alert highlighting RomCom's presence in Ukraine. Victims were lured through phishing emails impersonating the Ukrainian Armed Forces, which redirected them to download a malicious executable responsible for decoding and executing the RAT. Despite the absence of a Cuba ransomware deployment, researchers consider the activity consistent with Tropical Scorpius operations.

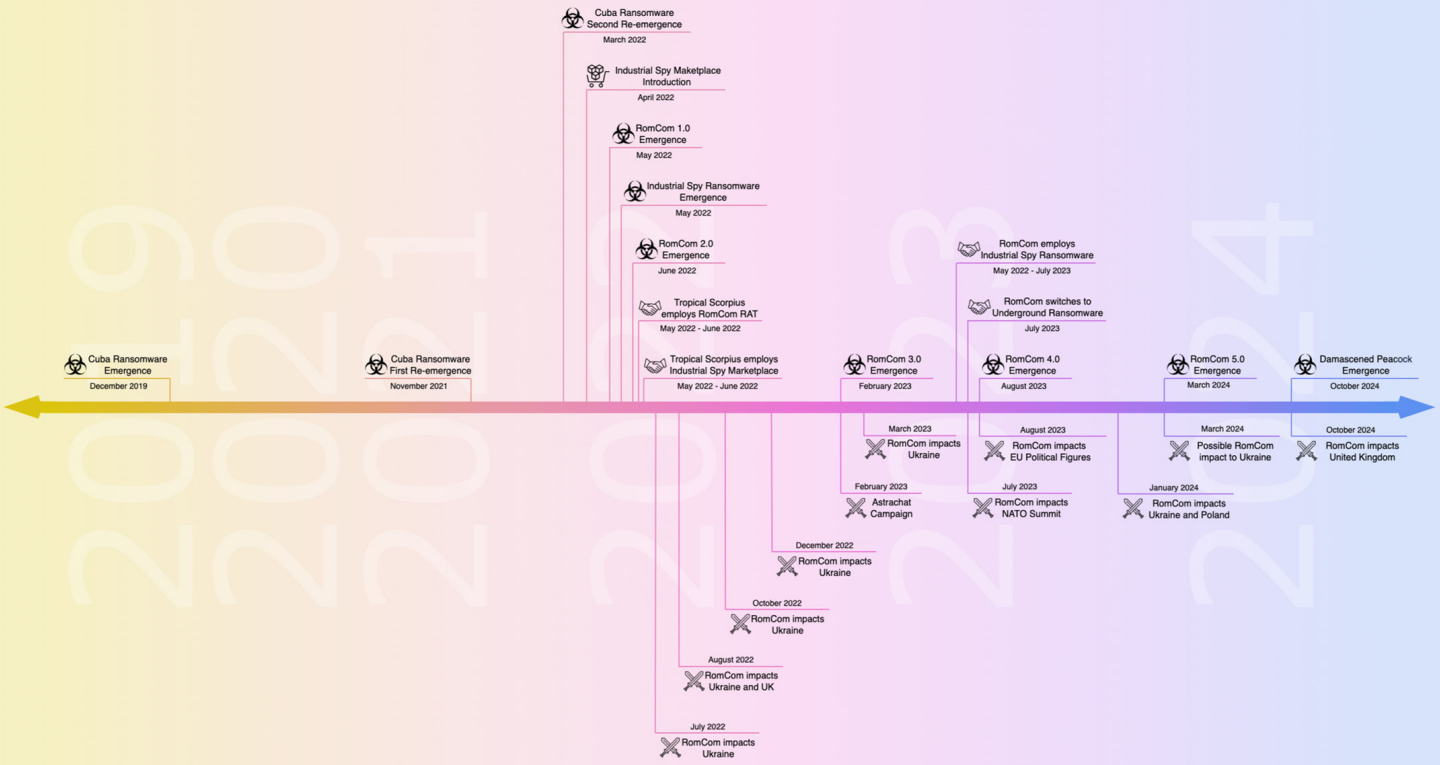
Tropical Scorpius has also been linked to Industrial Spy through multiple operational overlaps. According to Palo Alto Networks, in **May 2022**, exfiltrated data from Cuba-related activities was subsequently listed on the Industrial Spy marketplace. While the reasons behind Tropical Scorpius' decision to leverage the Industrial Spy marketplace instead of their own DLS remain unclear, researchers suspect that there is more involvement between the two groups than originally thought.

This connection was further corroborated in December 2022, when the Cybersecurity and Infrastructure Security Agency (CISA) **reported**, based on third-party intelligence, that a healthcare organization was compromised by suspected Cuba ransomware operators who leveraged the RomCom RAT and later deployed Industrial Spy ransomware.

RomCom was initially developed as an eCrime commodity malware, engineered to facilitate the deployment and persistence of malicious payloads, enabling its integration into prominent and extortion-focused ransomware operations. Early overlaps with ransomware strains, particularly Industrial Spy and its successor Underground, highlighted its dual role as both a Remote Access Trojan (RAT) and a facilitator of high-impact ransomware activity, combining commercial commodity with financially motivated objectives.

The Adversary Research Team (ART) at AttackIQ assesses that RomCom transitioned from a purely profit-driven commodity to become a utility leveraged in nation-state operations. This evolution became evident as RomCom was increasingly employed in campaigns aligned with Russia's strategic and political interests, particularly in the context of the war in Ukraine. Targeting against government institutions, military personnel, humanitarian organizations, and NATO-aligned entities demonstrates RomCom's operational shift toward an instrument of statecraft, supporting Russian intelligence objectives while retaining its eCrime versatility.

Timeline of Events



ATTACKIQ

Entity Relationships

2024-09

RomCom TTPs

RomCom is a Remote Access Trojan (RAT) family that has been active since at least May 2022. Primarily known for acquiring persistence and execution through Component Object Model (COM) Hijacking, a technique that abuses the Windows COM infrastructure by redirecting legitimate system processes to load malicious payloads, it has undergone multiple evolutionary stages, resulting in five distinct versions, each demonstrating increasing sophistication, modularity, and espionage capabilities.

RomCom RAT is delivered through a variety of Stagers, including downloaders, droppers, and loaders, typically embedded in trojanized versions of legitimate software. These are distributed through fake installers masquerading as popular applications, enabling the operator to bypass traditional security controls and gain initial access.

This emulation encompasses the payload samples and all observed post-compromise Tactics, Techniques, and Procedures (TTPs) exhibited by RomCom RAT and its supporting stagers with the intent of providing customers with the opportunity to detect and/or prevent a compromise in progress.

1. Access Vectors: Initial Access Payloads

Consists of first-stage components that were employed as infection vectors. It includes payloads delivered as Compressed Archives (ZIP), Executables (EXE), and Microsoft Installers (MSI).

> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related initial access payload samples.

2. Stagers: Downloader, Loader, and Dropper Components

Consists of intermediary components employed to facilitate the transition between initial access payloads and last-stage implants. These stagers are responsible for retrieving and deploying subsequent payloads, primarily through COM hijacking.

> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related stager samples.

3. Stagers: TTPs

Consists of the post-compromise behaviors exhibited by stager components during RomCom-associated activity since its inception.

Access Token Manipulation (T1134): This scenario enables the `SeDebugPrivilege` privilege for the current process using the `AdjustTokenPrivilege` Windows API.

Virtualization/Sandbox Evasion (T1497): This scenario will execute the `IsDebuggerPresent` Windows API to detect the presence of a debugger attached to the current process.

System Information Discovery (T1082): This scenario executes the native `systeminfo` command to retrieve all the Windows system information.

System Information Discovery (T1082): This scenario executes `NtQuerySystemInformation` API with the `SystemModuleInformation` argument to enumerate system modules.

Query Registry (T1012): This scenario queries the `MachineGUID` value located within the `HKLM\SOFTWARE\Microsoft\Cryptography` registry key, which contains the unique identifier of the system.

System Location Discovery (T1614): This scenario executes the `GetUserDefaultLCID` Windows API to retrieve the user default locale ID from the system.

System Location Discovery (T1614): This scenario executes the `GetLocaleInfoW` Windows API to retrieve the user's default country locale code from the system.

Process Discovery (T1057): This scenario uses Windows API to receive a list of running processes by calling `CreateToolhelp32Snapshot` and iterating through each process object with `Process32FirstW` and `Process32NextW`.

Windows Management Instrumentation (WMI) (T1047): This scenario obtains process information by executing the `Win32_Process` WMI command.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

4. RomCom RAT: Associated Payloads and Components

Consists of the final-stage payloads and modular components associated with RomCom RAT across multiple versions. These include standalone payloads as well as architecturally modular implants.

Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related stager samples.

5. RomCom RAT 1.0: TTPs

Consists of the post-compromise behaviors exhibited by the RomCom 1.0 variant during activities conducted since its inception in May 2022.

Native API (T1106): This scenario executes the `CreateProcessA` Windows API call to create a new process for a given executable payload.

Native API (T1106): This scenario executes the `LoadLibrary` Windows API call to execute a staged executable file to load a custom Dynamic-Link Library (DLL).

System Binary Proxy Execution: Rundll32 (T1218.011): This scenario executes an export function from an AttackIQ Dynamic-Link Library (DLL) using the `RunDll32` Windows utility.

Access Token Manipulation: Parent PID Spoofing (T1134.004): This scenario executes the `CreateProcess` Windows API, which allows the caller to specify a parent process for the newly created one. By doing so, it enables the spawned process to appear as though it were created by a legitimate Microsoft process.

Process Discovery (T1057): This scenario uses the Window's built-in `tasklist` command to discover running processes.

System Information Discovery (T1082): This scenario executes the `GetLogicalDrives` Windows API call to retrieve the currently available disk drives.

System Information Discovery (T1082): This scenario executes the `GetDriveTypeA` Windows API call to retrieve information regarding the system's physical drives.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through HTTP POST requests.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through ICMP Echo requests.

6. RomCom RAT 2.0: TTPs

Consists of the post-compromise behaviors exhibited by the RomCom 2.0 variant during activities conducted since its inception in June 2022.

System Binary Proxy Execution: Rundll32 (T1218.011): This scenario executes an export function from an AttackIQ Dynamic-Link Library (DLL) using the `RunDll32` Windows utility.

Access Token Manipulation: Parent PID Spoofing (T1134.004): This scenario executes the `CreateProcess` Windows API, which allows the caller to specify a parent process for the newly created one. By doing so, it enables the spawned process to appear as though it were created by a legitimate Microsoft process.

Virtualization/Sandbox Evasion (T1497): This scenario will execute the `IsDebuggerPresent` Windows API to detect the presence of a debugger attached to the current process.

Query Registry (T1012): This scenario queries the `MachineGUID` value located within the `HKLM\SOFTWARE\Microsoft\Cryptography` registry key, which contains the unique identifier of the system.

System Location Discovery (T1614): This scenario executes the `GetUserDefaultLCID` Windows API to retrieve the user default locale ID from the system.

System Location Discovery (T1614): This scenario executes the `GetLocaleInfoW` Windows API to retrieve the user's default country locale code from the system.

Process Discovery (T1057): This scenario uses Windows API to receive a list of running processes by calling `CreateToolhelp32Snapshot` and iterating through each process object with `Process32FirstW` and `Process32NextW`.

Software Discovery (T1518): This scenario queries the registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall`, which contains entries for all the software installed on the system.

System Information Discovery (T1082): This scenario executes the `GetLogicalDrives` Windows API call to retrieve the currently available disk drives.

System Information Discovery (T1082): This scenario executes the `GetDriveTypeW` Windows API call to retrieve information regarding the system's physical drives.

6. RomCom RAT 2.0: TTPs

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through HTTP POST requests.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through ICMP Echo requests.

7. RomCom RAT 3.0: TTPs

Consists of the post-compromise behaviors exhibited by the RomCom 3.0 variant during activities conducted since its inception in February 2023.

System Binary Proxy Execution: Rundll32 (T1218.011): This scenario executes an export function from an AttackIQ Dynamic-Link Library (DLL) using the `RunDll32` Windows utility.

Virtualization/Sandbox Evasion (T1497): This scenario will execute the `IsDebuggerPresent` Windows API to detect the presence of a debugger attached to the current process.

System Location Discovery (T1614): This scenario executes the `GetOEMCP` Windows API to retrieve the current Original Equipment Manufacturer (OEM) code page identifier for the operating system.

System Location Discovery (T1614): This scenario executes the `GetACP` Windows API to retrieve the current Windows ANSI code page identifier for the operating system.

Process Discovery (T1057): This scenario uses Windows API to receive a list of running processes by calling `CreateToolhelp32Snapshot` and iterating through each process object with `Process32FirstW` and `Process32NextW`.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

Domain Trust Discovery (T1482): This scenario calls the native `nltest` utility with the `/trusted_domains` option to retrieve a list of trusted Active Directory domains associated with this host.

8. RomCom RAT 5.0: TTPs

Consists of the post-compromise behaviors exhibited by the RomCom 5.0 variant during activities conducted since its inception in September 2024.

System Binary Proxy Execution: Rundll32 (**T1218.011**): This scenario executes an export function from an AttackIQ Dynamic-Link Library (DLL) using the `RunDll32` Windows utility.

System Information Discovery (T1082): This scenario executes the native `systeminfo` command to retrieve all the Windows system information.

System Network Configuration Discovery (T1016): This scenario executes the native Window's command `ipconfig /all` to obtain the host's IP information.

File and Directory Discovery (T1083): This scenario executes the native `dir` command to enumerate files of interest on the system.

Domain Trust Discovery (T1482): This scenario calls the native `nltest` utility with the `/trusted_domains` option to retrieve a list of trusted Active Directory domains associated with this host.

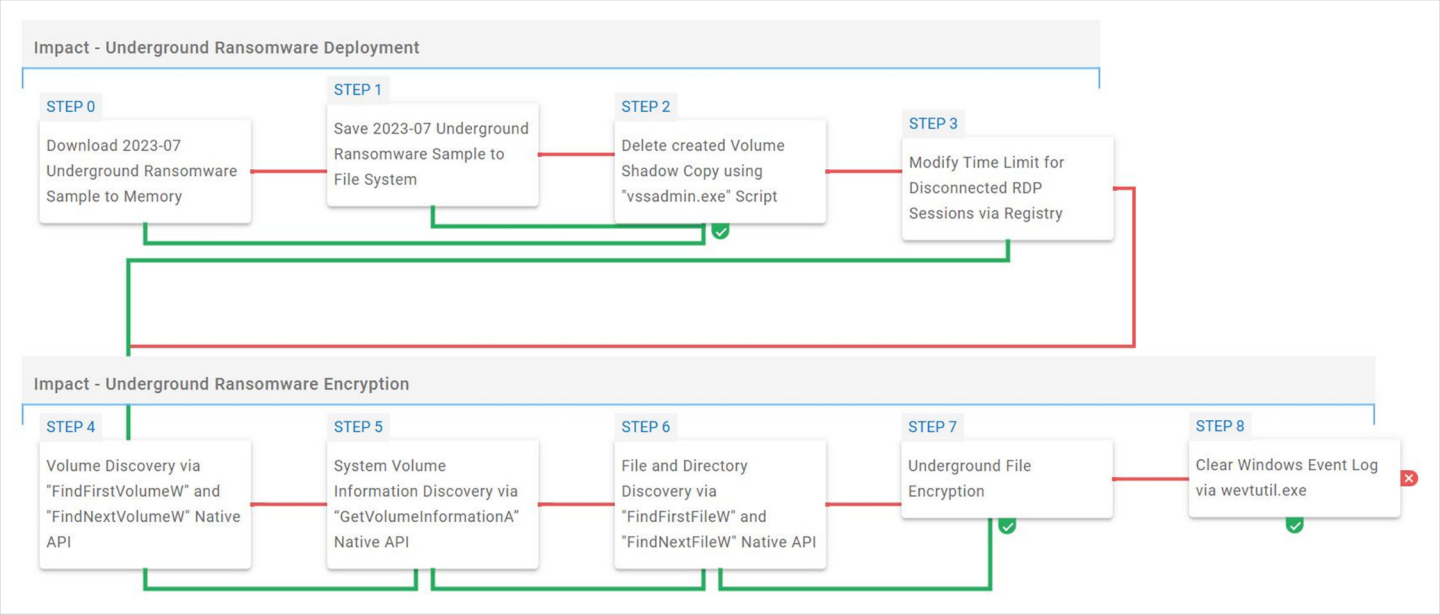
Application Layer Protocol: Web Protocols (T1071.001): This scenario communicates over the Hypertext Transfer Protocol (HTTP) protocol on port 443, intentionally bypassing Secure Sockets Layer (SSL).

Continued on next page.

2023-08

Underground Ransomware TTPs

Underground is a ransomware strain that has been active since at least 2023 and is regarded as the successor to Industrial Spy due to substantial code overlap, suggesting a deliberate rebranding effort. Since July 2023, Underground has been employed by the RomCom adversary, also known as UAT-5647 and Storm-0978.

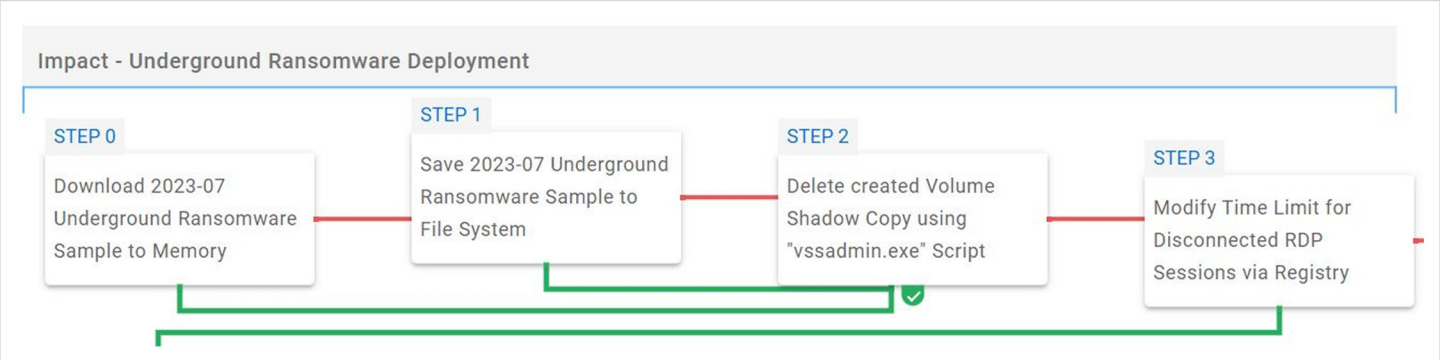


Following deployment, Underground deletes shadow copies, configures Remote Desktop and Terminal Server sessions to persist for up to 14 days after disconnection, terminates targeted services, and clears all Windows Event Logs. It then encrypts files using the 3DES algorithm, with both the encryption key and Initialization Vector (IV) secured through RSA encryption. Upon completing the encryption routine, Underground deletes itself, demonstrating its interest in impeding recovery, masking its activity, and hindering forensic analysis.

This emulation replicates the sequence of behaviors associated with the deployment of Underground ransomware on a compromised system with the intent of providing customers with the opportunity to detect and/or prevent a compromise in progress.

Impact - Underground Ransomware Deployment

This stage begins with the deployment of the Underground ransomware, which, once operational, deletes Volume Shadow Copies via `vssadmin.exe`. Next, it modifies the timeout for disconnected RDP sessions by altering the `MaxDisconnectionTime` value under the `Terminal Services` registry key.



Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known Underground ransomware samples.

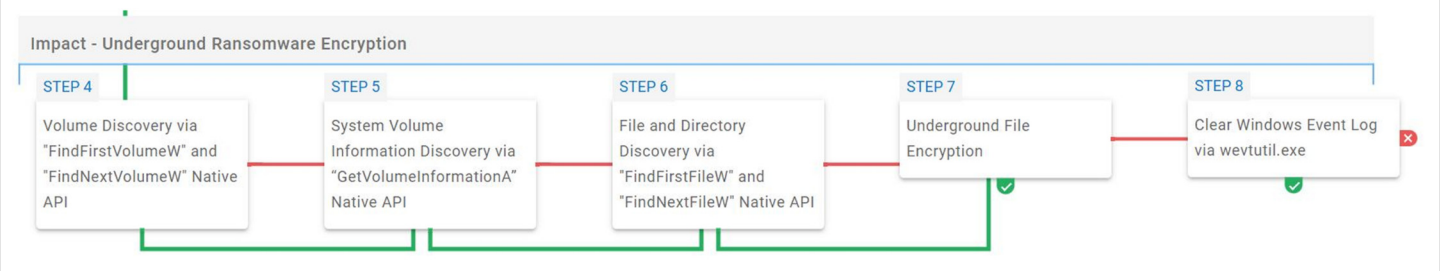
Inhibit System Recovery (T1490): This scenario executes the `vssadmin.exe` Windows utility to delete a Volume Shadow Copy created by the emulation.

Modify Registry (T1112): This scenario modifies the time limit for disconnected Remote Desktop Protocol (RDP) sessions by altering the `MaxDisconnectionTime` value under the `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services` registry key.

Continued on next page.

Impact - Underground Ransomware Encryption

This stage begins with the discovery of available volumes by invoking the `FindFirstVolumeW` and `FindNextVolumeW` APIs, followed by the retrieval of additional metadata via the `GetVolumeInformationA` API. The identified volumes are then recursively traversed using the `FindFirstFileW` and `FindNextFileW` APIs to locate files of interest, which are subsequently encrypted using a combination of 3DES and RSA-1024. Finally, Windows Event Logs are cleared using `wevtutil.exe`, hindering forensic analysis efforts.



System Information Discovery (T1082): This scenario executes the `FindFirstVolumeW` and `FindNextVolumeW` Windows API calls to iterate through the available volumes of the system.

System Information Discovery (T1082): This scenario executes the `GetVolumeInformationA` Windows API function to retrieve volume information.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

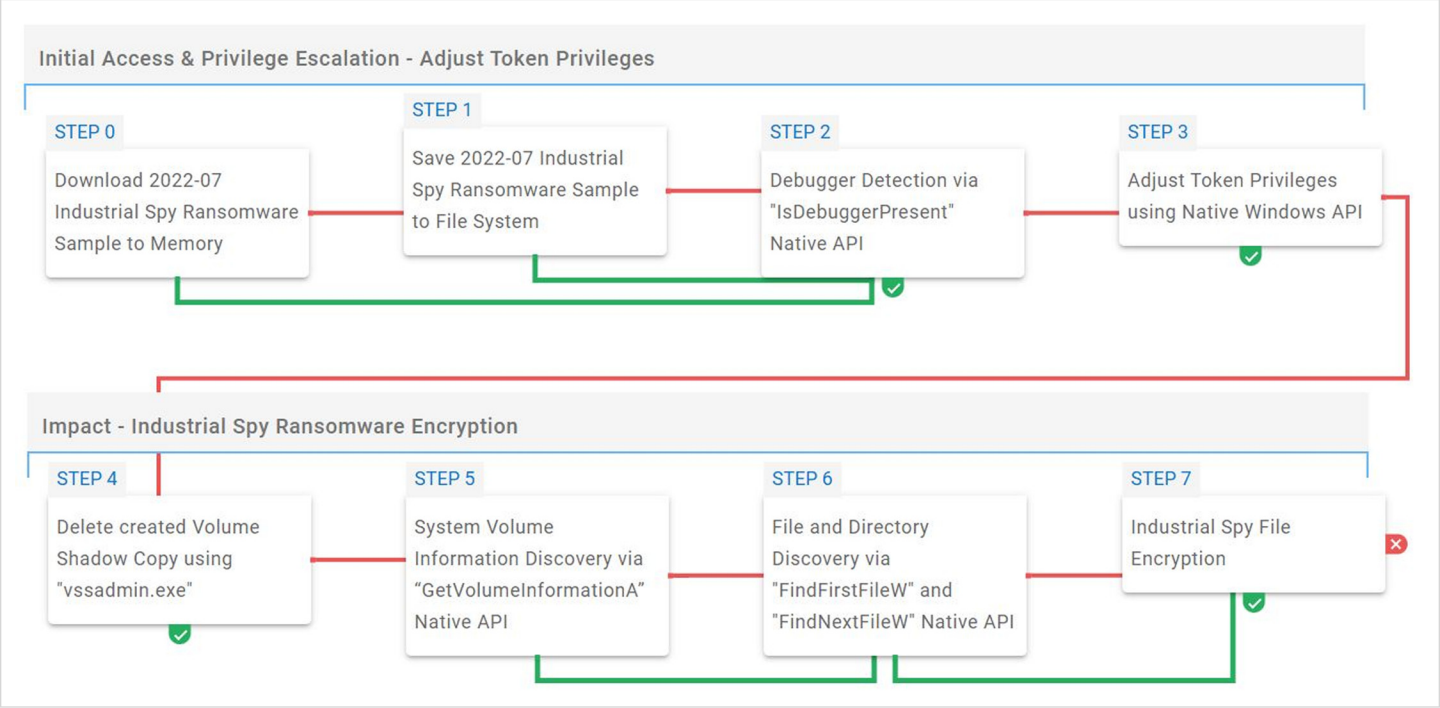
Data Encrypted for Impact (T1486): This scenario simulates the file encryption routine used by common ransomware families. Files matching an extension list are identified and encrypted in place using the same encryption algorithms employed by Underground ransomware.

Continued on next page.

2022-08

Industrial Spy Ransomware TTPs

Industrial Spy refers to both a ransomware group and a strain that **emerged** in April 2022, initially operating as a data extortion marketplace where criminals could acquire stolen information from compromised organizations. It was promoted through payload downloaders disguised as software cracks and adware, which dropped README.txt files advertising the platform. Over time, Industrial Spy evolved into a full-fledged ransomware operation. Before introducing its proprietary strain in May 2022, the adversary briefly experimented with Cuba ransomware.

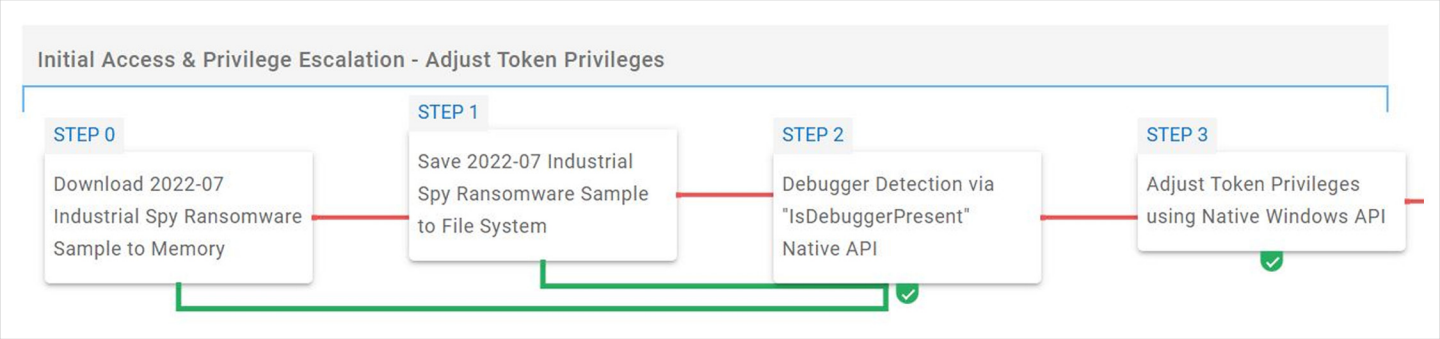


Despite its functionality, Industrial Spy lacked many modern features such as anti-analysis or obfuscation capabilities. Its operations combine data exfiltration with file encryption to conduct double extortion attacks. While some activities involve only data exfiltration and ransom demands, others include file encryption using a combination of 3DES and RSA encryption algorithms.

This emulation replicates the sequence of behaviors associated with the deployment of Industrial Spy ransomware on a compromised system with the intent of providing customers with the opportunity to detect and/or prevent a compromise in progress.

Initial Access & Privilege Escalation - Adjust Token Privileges

This stage begins with the deployment of the Industrial Spy ransomware, which, once operational, attempts to detect the presence of a debugger by invoking the `IsDebuggerPresent` Windows API. If no debugger is detected, it proceeds to call the `AdjustTokenPrivileges` API to enable the `SeBackupPrivilege`, elevating its ability to access files regardless of access control restrictions.



Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known Industrial Spy ransomware samples.

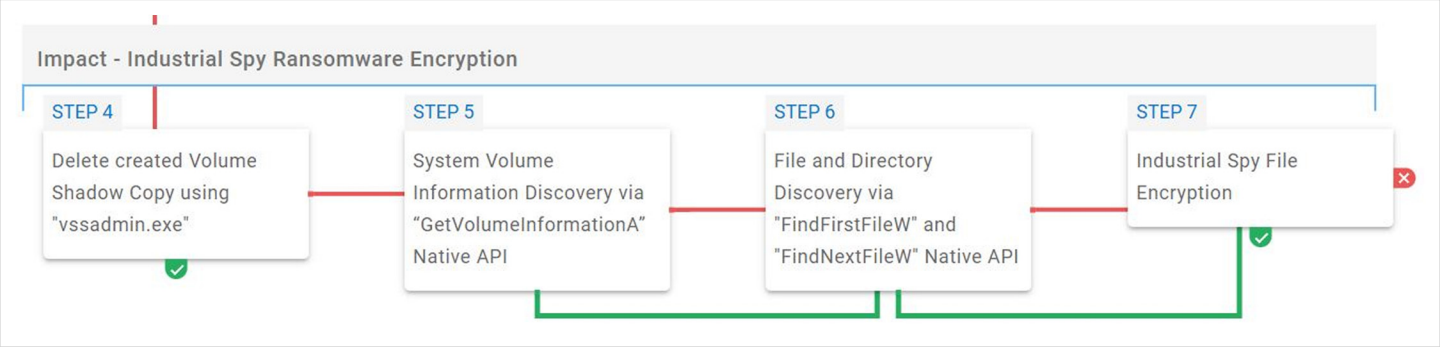
Virtualization/Sandbox Evasion (T1497): This scenario will execute the `IsDebuggerPresent` Windows API to detect the presence of a debugger attached to the current process.

Access Token Manipulation (T1134): This scenario enables the `SeBackupPrivilege` privilege for the current process using the `AdjustTokenPrivilege` Windows API.

Continued on next page.

Impact - Industrial Spy Ransomware Encryption

This stage begins with the deletion of Volume Shadow Copies via vssadmin.exe to hinder recovery efforts. It then retrieves information about available volumes using `GetVolumeInformationA`, recursively traversing them via the `FindFirstFileW` and `FindNextFileW` APIs to locate files of interest. Subsequently, the located files are encrypted using a combination of 3DES and RSA-1024.



Inhibit System Recovery (T1490): This scenario executes the `vssadmin.exe` Windows utility to delete a Volume Shadow Copy created by the emulation.

System Information Discovery (T1082): This scenario executes the `GetVolumeInformationA` Windows API function to retrieve volume information.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

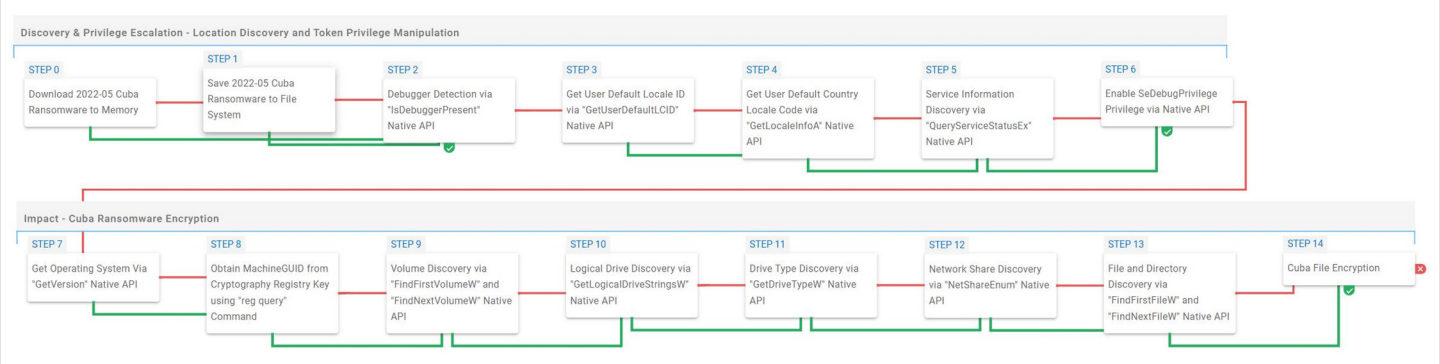
Data Encrypted for Impact (T1486): This scenario simulates the file encryption routine used by common ransomware families. Files matching an extension list are identified and encrypted in place using the same encryption algorithms employed by Industrial Spy ransomware.

Continued on next page.

2023-09

Cuba Ransomware TTPs

Cuba is a ransomware strain that emerged in December 2019, which gained notoriety in November 2021, following an advisory issued by the Federal Bureau of Investigation (FBI) outlining Indicators of Compromise (IOCs) associated with its activities. Since its emergence, it has undergone extensive refinement of its Tactics, Techniques, and Procedures (TTPs) to improve efficiency and effectiveness, evolving into a prevalent high-impact threat.



It is operated by the financially motivated adversary Tropical Scorpius, also known as Void Rabisu and UNC2596. Despite its name, Cuba ransomware appears to originate from Russia, as evidenced by its behavior of terminating execution on systems configured with Russian language settings or keyboard layouts.

Throughout 2022, Cuba was linked to numerous high-profile incidents, particularly targeting government institutions across Europe. In September, the government of Montenegro disclosed an incident during which sensitive information, including financial documents, correspondence, account details, balance sheets, and tax documents, was exfiltrated. The following month, the Ukrainian Computer Emergency Response Team (CERT-UA) issued an alert highlighting RomCom's presence in Ukraine. Despite the absence of Cuba ransomware deployment, researchers consider the activity consistent with Tropical Scorpius operations.

Cuba has historically been distributed via the Hancitor loader, commonly delivered through malicious email attachments. Its operators have also exploited Microsoft Exchange vulnerabilities, specifically ProxyShell and ProxyLogon, as initial access vectors. In addition, they have abused an Avast driver vulnerability as part of their antivirus-disabling routine.

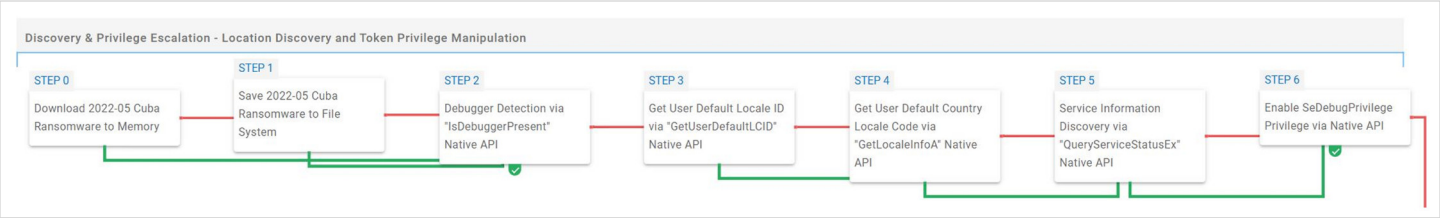
The ransomware's post-compromise toolkit is extensive, incorporating native Windows utilities such as Remote Desktop Protocol (RDP), Server Message Block (SMB), and PsExec, as well as offensive frameworks like Cobalt Strike for Lateral Movement and Command and Control, and Mimikatz for credential harvesting.

Related operations follow a double extortion model, combining data encryption with data theft, alongside a Dedicated Leak Site (DLS) that exposes organizations that have allegedly been compromised. This leak site features both a public section listing breached organizations and a restricted, paid section where exfiltrated data is sold to third parties.

This emulation replicates the sequence of behaviors associated with the deployment of Cuba ransomware on a compromised system with the intent of providing customers with the opportunity to detect and/or prevent a compromise in progress.

Discovery & Privilege Escalation - Location Discovery and Token Privilege Manipulation

This stage begins with the deployment of Cuba ransomware, which, once operational, attempts to detect the presence of a debugger by invoking the `IsDebuggerPresent` API. It then retrieves locale information using the `GetUserDefaultLCID` and `GetLocaleInfoA` APIs. Subsequently, it gathers details about active services via `QueryServiceStatusEx` and invokes `AdjustTokenPrivileges` to enable the `SeDebugPrivilege`, granting broader access to protected processes.



Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known Cuba ransomware samples.

Virtualization/Sandbox Evasion (T1497): This scenario will execute the `IsDebuggerPresent` Windows API to detect the presence of a debugger attached to the current process.

System Location Discovery (T1614): This scenario executes the `GetUserDefaultLCID` Windows API to retrieve the user default locale ID from the system.

Discovery & Privilege Escalation - Location Discovery and Token Privilege Manipulation

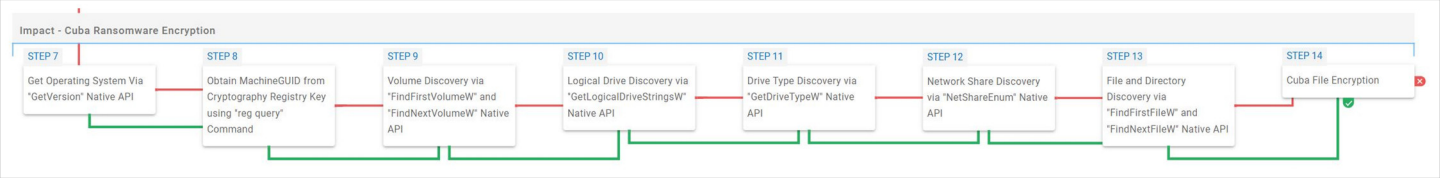
System Location Discovery (T1614): This scenario executes the `GetLocaleInfoA` Windows API to retrieve the user's default country locale code from the system.

System Service Discovery (T1007): This scenario executes the `QueryServiceStatusEx` and `EnumDependentServices` Windows API calls to retrieve information pertaining to a given service.

Access Token Manipulation (T1134): This scenario enables the `SeDebugPrivilege` privilege for the current process using the `AdjustTokenPrivilege` Windows API.

Impact - Cuba Ransomware Encryption

This stage begins with system information gathering by invoking the `GetVersion` API and the retrieval of the Machine Globally Unique Identifier (GUID). It then enumerates available volumes via the `FindFirstVolumeW` and `FindNextVolumeW` APIs, followed by collecting drive information using `GetLogicalDriveStringsW` and `GetDriveTypeW`.



Subsequently, it conducts network share discovery through `NetShareEnum` and recursively traverses the file system by invoking the `FindFirstFileW` and `FindNextFileW` APIs to locate files of interest, which are ultimately encrypted using a combination of Salsa20 and RSA-1024.

System Information Discovery (T1082): This scenario executes the `GetVersion` Windows API call to retrieve information regarding the operating system version.

Query Registry (T1012): This scenario queries the `MachineGUID` value located within the `HKLM\SOFTWARE\Microsoft\Cryptography` registry key, which contains the unique identifier of the system.

System Information Discovery (T1082): This scenario executes the `FindFirstVolumeW` and `FindNextVolumeW` Windows API calls to iterate through the available volumes of the system.

Impact - Cuba Ransomware Encryption

System Information Discovery (T1082): This scenario executes the `GetLogicalDriveStringsW` Windows API call to retrieve information regarding the system's physical drives.

System Information Discovery (T1082): This scenario executes the `GetDriveTypeW` Windows API call to retrieve information regarding the system's physical drives.

Network Share Discovery (T1135): This scenario executes the `NetShareEnum` Windows native API call to enumerate network shares from the local computer.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

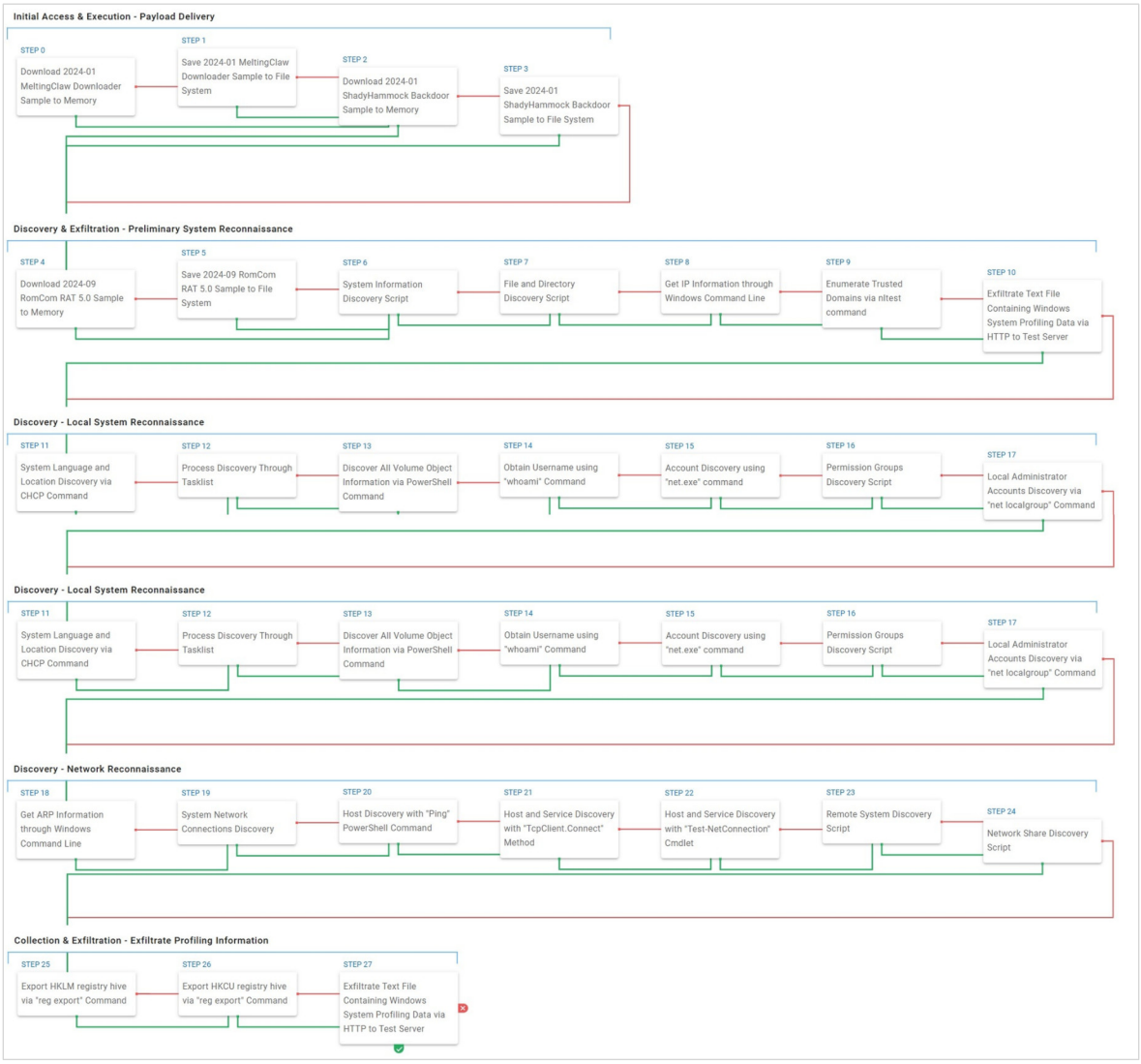
Data Encrypted for Impact (T1486): This scenario simulates the file encryption routine used by common ransomware families. Files matching an extension list are identified and encrypted in place using the same encryption algorithms employed by Cuba ransomware.

Continued on next page.

2024-09

RomCom – From MeltingClaw Downloader via ShadyHammock Backdoor to Deployment

On October 17, 2024, Cisco Talos **disclosed** a surge of activity beginning in late 2023, targeting Ukrainian government institutions and unidentified entities in Poland. The activity was attributed to the Russian adversary RomCom, also tracked as UAT-5647 and Storm-0978, an adaptive and increasingly sophisticated, multi-motivational threat that has been active since at least 2022.



During these activities, Talos identified two distinct intrusion chains, each leveraging different payloads to accomplish their objectives. Analysis indicated that the adversary was expanding its arsenal, developing a diverse set of components written in multiple languages, including Go, C++, Rust, and Lua, designed for cross-platform compatibility.

One of the activities featured a previously undocumented variant of RomCom RAT, designated by Talos as *SingleCamper*. This strain was confirmed to be the same as the one identified by Palo Alto Networks in **September 2024**, where it was referred to as *SnipBot*. While primarily derived from RomCom 3.0, it incorporates techniques observed in its successor, RomCom 4.0. Owing to this hybrid architecture and enhanced capabilities, the malware has been classified as RomCom 5.0.

This activity began with a spearphishing email delivering *config-pdf.dll* (fa400cb70d13cb329d05877b8fe73ed5), a C++-based downloader identified as *MeltingClaw*. Its primary purpose is to retrieve and deploy a second-stage payload, *libapi.dll* (498c620d80651de26da8f3b850f3045a), a C++-based backdoor known as *ShadyHammock*. The backdoor is executed through Component Object Model (COM) Hijacking, specifically abusing the `Sync Registration` interface, identified by its Globally Unique Identifier (GUID), to establish persistence and ensure execution.

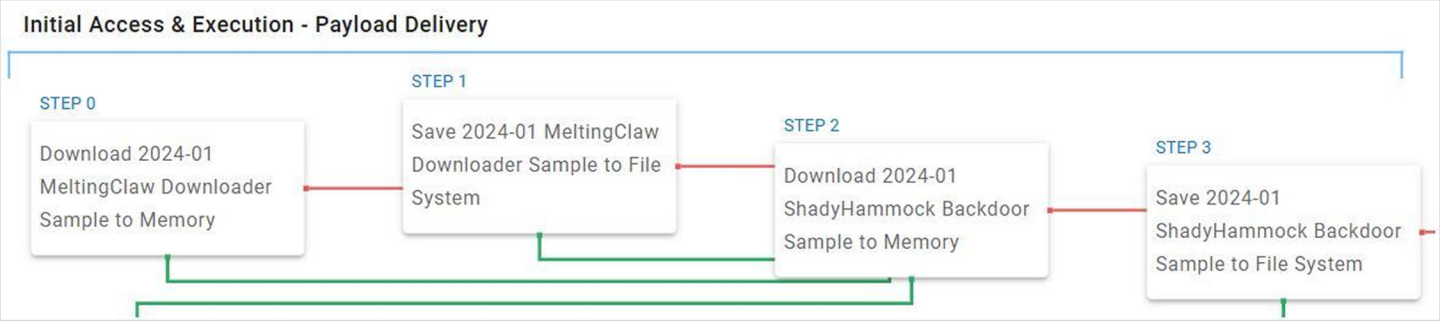
In addition to deploying the backdoor, *MeltingClaw* downloads and stores supplementary payloads within the `HKCU\Software\AppDataSoft\Software\` registry key. This key typically contains three encoded values: two representing additional next-stage payloads and one containing configuration information. The binary content from these entries is retrieved, decoded into Dynamic-Link Libraries (DLLs), and traversed to identify their export functions for in-memory execution.

Subsequently, ShadyHammock loads and executes these payloads via explorer.exe, one of which is RomCom 5.0. The backdoor also binds to a local port on 127.0.0.1, establishing a loopback-only communication channel that enables interaction between ShadyHammock and RomCom without exposing the connection externally.

Once deployed, *RomCom* establishes a connection to its Command and Control (C2) server over port 443 (HTTPS), transmitting preliminary system registration information. It then executes a series of reconnaissance commands issued by the C2 server, returning their output. Based on the collected information, the adversary determines whether the compromised system warrants further post-compromise activities, which encompass multiple **MITRE ATT&CK Tactics** and are primarily conducted through a reverse shell established by the payload.

Initial Access & Execution - Payload Delivery and Deployment

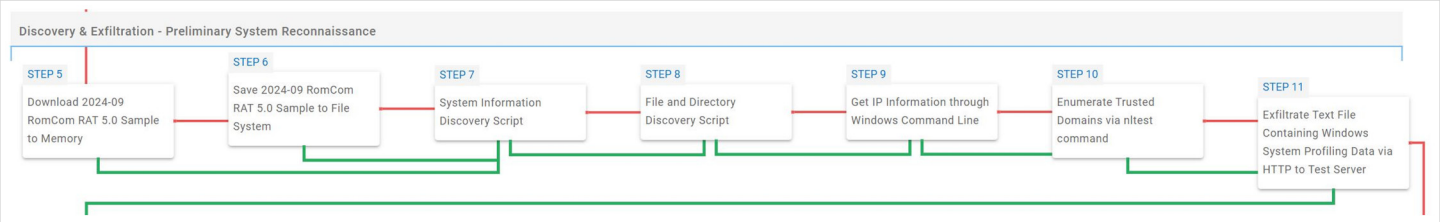
This stage begins with the deployment of *MeltingClaw*, a C++-based downloader employed to deliver *ShadyHammock*, a C++-based backdoor which is deployed through Component Object Model (COM) Hijacking.



> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

Discovery & Exfiltration - Preliminary System Reconnaissance

This stage begins with the deployment of *RomCom RAT 5.0*, also referred to as *SnipBot* or *SingleCamper*. Once operational, it executes a series of preliminary reconnaissance commands to gather general system information, filesystem structure, network configuration, and enumerate trusted domains. Subsequently, it transmits the collected data to the Command and Control (C2) server as part of the initial system registration process.



Discovery & Exfiltration - Preliminary System Reconnaissance

Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

System Information Discovery (T1082): This scenario executes the native `systeminfo` command to retrieve all the Windows system information.

File and Directory Discovery (T1083): This scenario executes the native `dir` command to enumerate files of interest on the system.

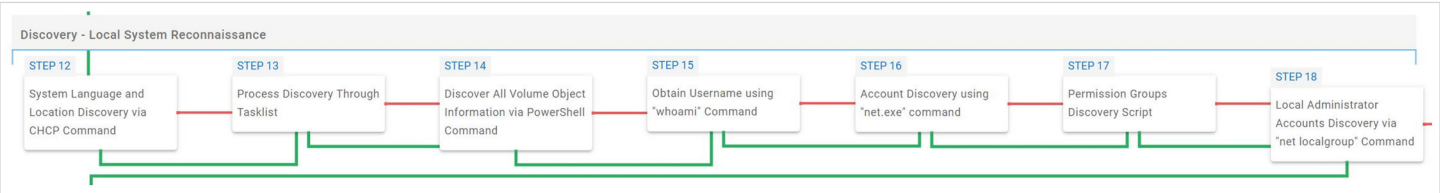
System Network Configuration Discovery (T1016): This scenario executes the native Window's command `ipconfig /all` to obtain the host's IP information.

Domain Trust Discovery (T1482): This scenario calls the native `nltest` utility with the `/trusted_domains` option to retrieve a list of trusted Active Directory domains associated with this host.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through HTTP POST requests.

Discovery - Local System Reconnaissance

This stage focuses on local system reconnaissance through the execution of discovery-oriented commands issued by the Command and Control (C2) server. These are designed to collect general system information, including language and location settings, running processes, available storage volumes, active account username, existing user accounts, and both local and domain permission groups.



System Language Discovery (T1614.001): This scenario executes the `chcp` command to collect information on the active console code page of the system.

Process Discovery (T1057): This scenario uses the Window's built-in `tasklist` command to discover running processes.

Discovery - Local System Reconnaissance

System Information Discovery (T1082): This scenario executes the `Get-Volume` PowerShell cmdlet to retrieve all volume objects of the system.

System Owner/User Discovery (T1033): This scenario executes the `whoami` command to retrieve the username of the running user account.

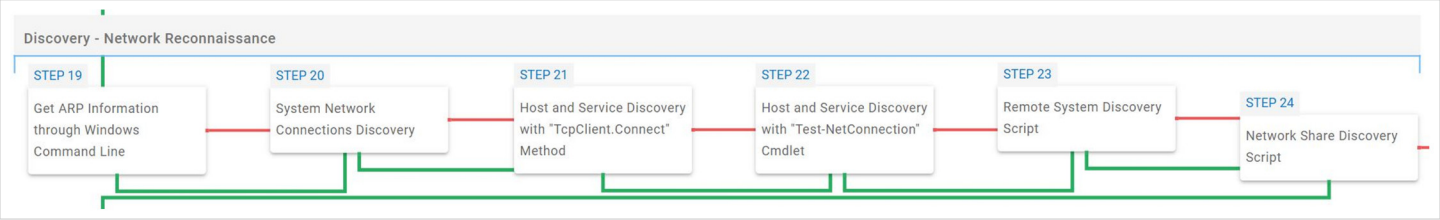
Account Discovery (T1087): This scenario executes the `net user` command to retrieve a list of available accounts on the system.

Permission Groups Discovery: Local Groups (T1069.001): This scenario executes the `net localgroup administrators` command to enumerate a set of users with administration privileges.

Permission Groups Discovery: Domain Groups (T1069.002): This scenario executes the `net group /domain` command to enumerate domain permission groups.

Discovery - Network Reconnaissance

This stage focuses on network reconnaissance through the execution of discovery-oriented commands issued by the Command and Control (C2) server. These are intended to collect information related to the Address Resolution Protocol (ARP) table, adjacent and connected systems, along with their available services, and available network shares.



System Network Configuration Discovery (T1016): This scenario executes the `arp -a` command to obtain the system's Address Resolution Protocol (ARP) information.

System Network Connections Discovery (T1049): This scenario executes the `netstat` native Windows command line tool to collect active connections and any listening services running on the host.

Network Service Discovery (T1046): This scenario leverages, through a PowerShell script, the `TcpClient.Connect` .Net Class to perform network system and service discovery.

Discovery - Network Reconnaissance

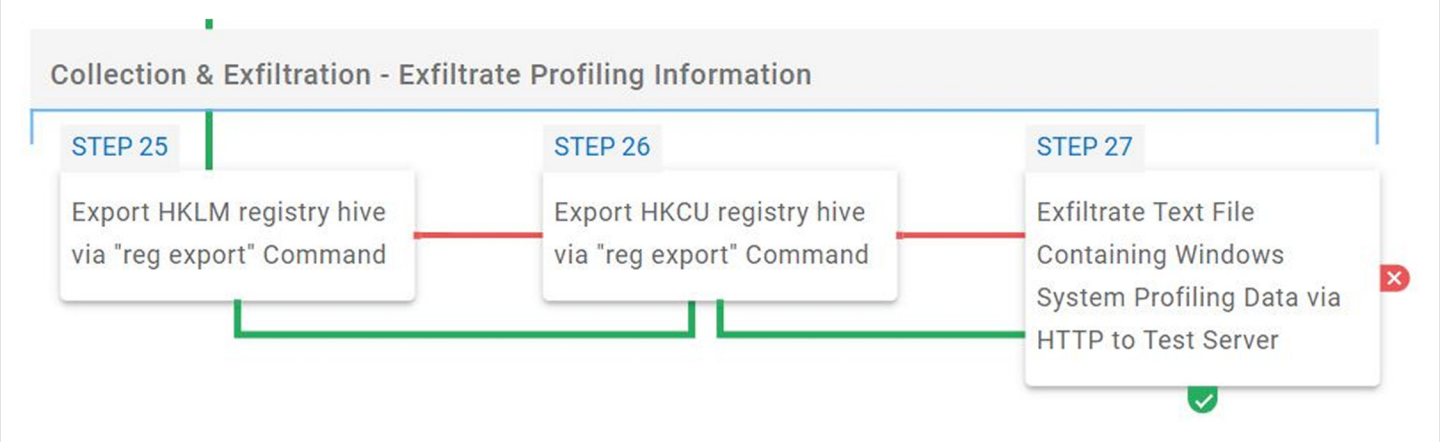
Network Service Discovery (T1046): This scenario leverages, through a PowerShell script, the `Test-NetConnection` cmdlet to perform network system and service discovery.

Remote System Discovery (T1018): This scenario executes the `net view` command to enumerate remotely accessible systems available on the network.

Network Share Discovery (T1135): This scenario executes the `net share` utility to enumerate all of the local mapped network shares.

Collection & Exfiltration - Exfiltrate Profiling Information

This stage begins with the dumping of the `HKEY_LOCAL_MACHINE` and `HKEY_CURRENT_USER` registry hives. It then proceeds to compress the collected data using PowerShell's Compress-Archive cmdlet, which is employed to perform data staging in preparation for exfiltration via HTTP POST requests.



Query Registry (T1012): This scenario dumps the `HKEY_LOCAL_MACHINE` registry hive through the `reg export` command.

Query Registry (T1012): This scenario dumps the `HKEY_CURRENT_USER` registry hive through the `reg export` command.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated, compressed text file, created through the `Compress-Archive` PowerShell cmdlet, containing the output from a series of discovery commands through HTTP POST requests.

2024-09

RomCom - From Spearphishing Link to Signed Downloader to Deployment

On September 23, 2024, Palo Alto Networks **disclosed** the identification of a previously undocumented RomCom-associated payload designated *SnipBot*, in reference to the mutex SnipMutex established when executed. This strain is primarily derived from RomCom 3.0 but incorporates techniques observed in its successor, RomCom 4.0. Owing to this hybrid architecture and enhanced capabilities, the malware has been classified as RomCom 5.0.

This activity began with a spearphishing email containing a link redirecting to temp.sh, a legitimate file-sharing service leveraged to host the initial RomCom 5.0 **Downloader**, which masquerades as a Portable Document Format (PDF) document.

The **Downloader**, titled *Attachment_Medical report.exe* (c0e499402acb6c302228b4a7923d5db6), is signed with a presumably stolen or spoofed digital certificate issued to CC Byg og Udlejning ApS, a Denmark-based real estate company.

Upon execution, the **Initial Downloader** performs two simple yet effective sandbox evasion techniques. First, it verifies the original filename by hashing the process name and comparing it against a hardcoded value. Next, it inspects the HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs registry key to ensure it contains at least 100 entries, indicating a genuine, user-driven environment.

Once the environment is deemed safe, the **Initial Downloader** proceeds to retrieve and execute in memory a Dynamic-Link Library (DLL) named *config-pdf.dll* (ea1900f26e23465deef32201a2e75192). This component serves as a **Secondary Downloader** and is responsible for orchestrating the subsequent stages of the intrusion.

Next, the **Secondary Downloader** issues the command get_update_manager2 to the Command and Control (C2) server to retrieve the RomCom **Loader**, *keyprov.dll* (0fe12e3cc81bfc5ce0fb2f8f653648a8).

The **Loader** is deployed using the Component Object Model (COM) hijacking technique, which involves modifying the registry value associated with a specific Class ID (CLSID) to register the payload as the thumbnail cache library within the current user's registry hive. As a result, any process invoking that CLSID loads the RomCom Loader instead. One such process is explorer.exe, which is forcibly restarted by the **Downloader** to guarantee that the **Loader** is executed.

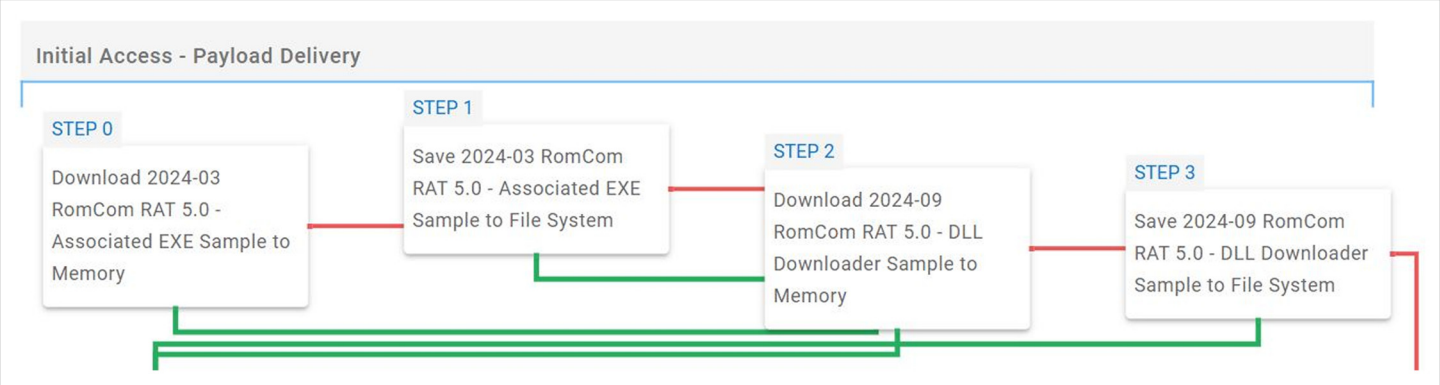
Simultaneously, *config-pdf.dll* downloads the encrypted SnipBot payload, single.dll (3e3727e236ca26c88e2d86984d2e05ce), and stores it within the registry under HKCU\SOFTWARE\AppDataSoft\Software as a binary value named trem1.

Once the Loader is injected into explorer.exe, it decrypts and executes the payload directly from the registry. In addition, it establishes a TCP network listener on port 1342 to receive incoming commands.

Once operational, RomCom 5.0 supports a total of 27 commands. For its initial C2 beacon, single.dll transmits a string composed of several host-specific attributes, including the computer and domain name, MAC address, Windows build number, and whether the system is running a Windows Server edition.

Initial Access - Payload Delivery

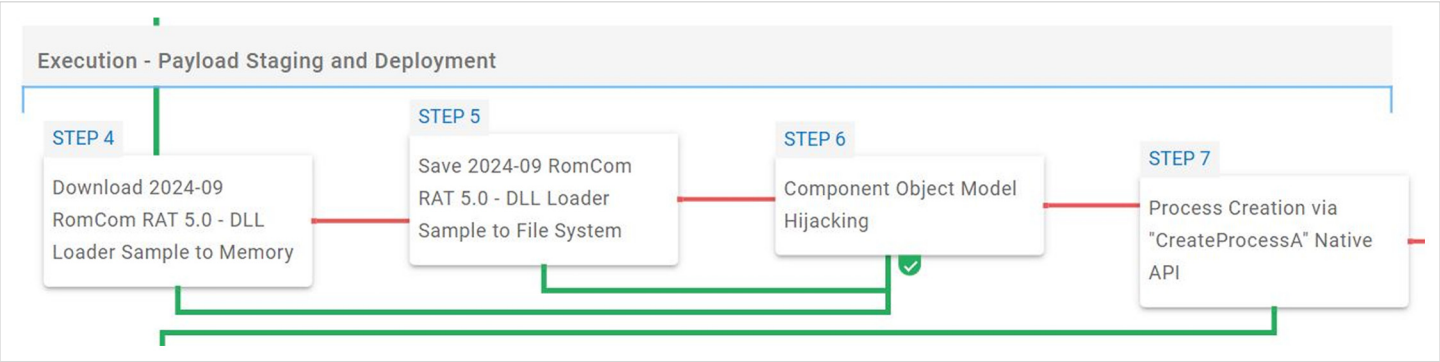
This stage begins with the deployment of an executable (EXE) that functions as a downloader of a Dynamic-Link Library (DLL) named *config-pdf.dll*, which acts as a secondary downloader for the next stage payload.



> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

Execution - Payload Staging and Deployment

This stage begins with the deployment of a Dynamic-Link Library (DLL) loader called keyprov.dll, which is deployed through Component Object Model (COM) Hijacking. Once operational, it is capable of executing files through the `CreateProcess` Windows API.



> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

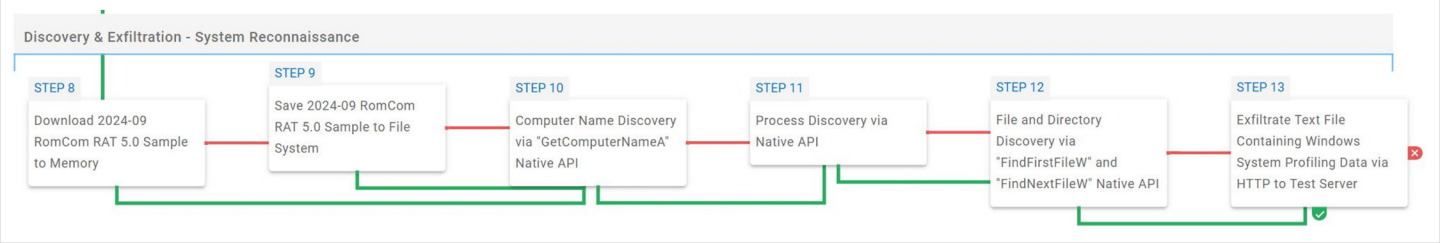
Execution - Payload Staging and Deployment

Component Object Model Hijacking (T1546.015): This scenario performs Component Object Model (COM) Hijacking by assigning a specified Dynamic-Link Library (DLL) to a targeted COM Instance. It then executes a process that utilizes the hijacked instance, ensuring the DLL is loaded and executed.

Native API (T1106): This scenario executes the `CreateProcessA` Windows API call to create a new process for a given executable payload.

Discovery & Exfiltration - System Reconnaissance

This stage begins with the deployment of *RomCom RAT 5.0*, also referred to as *SnipBot* or *SingleCamper*. Once operational, it executes a series of preliminary reconnaissance commands to collect general system information, including the computer's name, running processes, and the structure and contents of the file system. Finally, the collected data is exfiltrated via HTTP POST requests.



Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

System Information Discovery (T1082): This scenario will execute the `GetComputerNameA` Windows API call to retrieve a NetBIOS associated with the local computer.

Process Discovery (T1057): This scenario uses Windows API to receive a list of running processes by calling `CreateToolhelp32Snapshot` and iterating through each process object with `Process32FirstW` and `Process32NextW`.

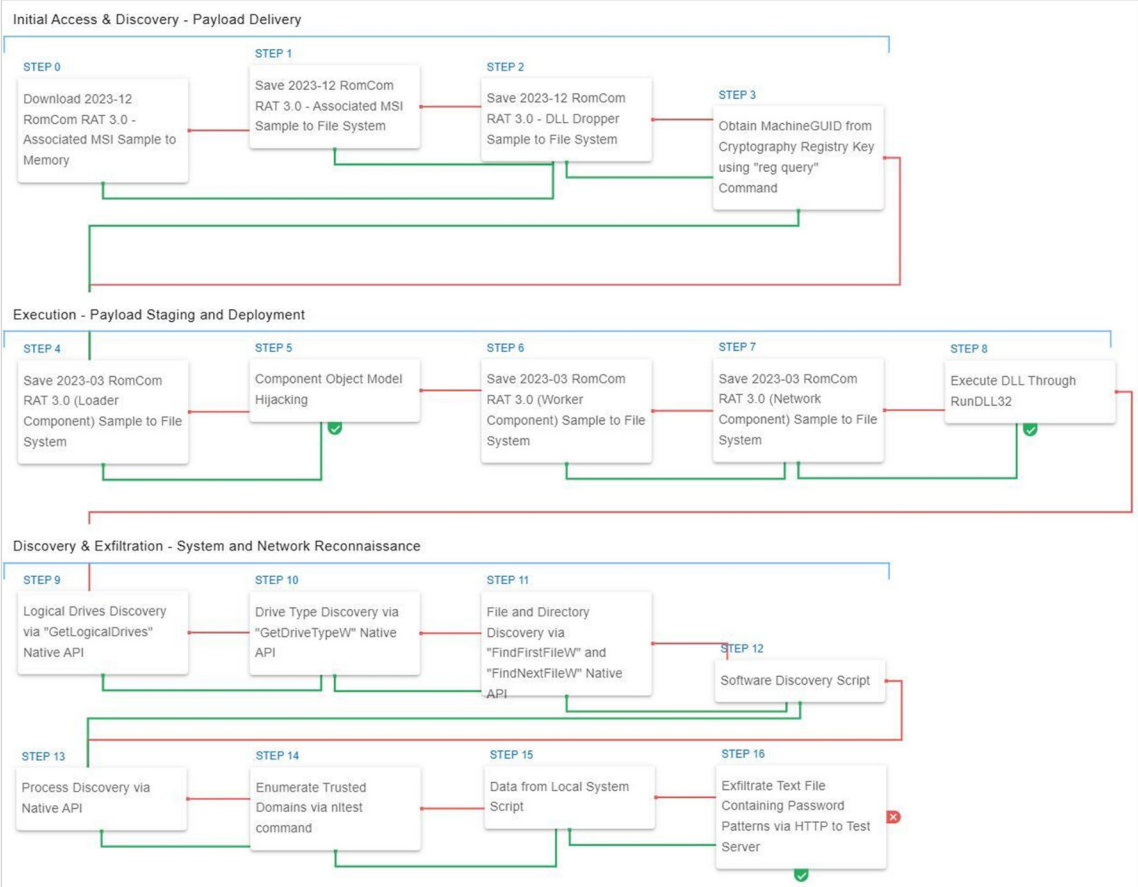
File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and FindNextFileW Windows API calls to perform the enumeration of the file system.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of Windows system profiling data by transmitting a pre-generated text file containing the output from a series of discovery commands through HTTP POST requests.

2023-02

RomCom - The AstraChat Campaign

On May 30, 2023, Trend Micro reported the identification of RomCom-associated payloads deployed in activities targeting objectives in Eastern Europe during February 2023. The campaign leveraged RomCom 3.0 components embedded within the software installation package of AstraChat, an enterprise XMPP-based messaging application.



The activity began with the deployment of *astrachat.msi* (3fb0d18c06a2f0f58f53dbf81a49fd1b), a Microsoft Installer (MSI) archive containing legitimate AstraChat files. However, it also includes a malicious Dynamic-Link Library (DLL) file, *InstallA.dll* (096c2f8467f23c1aa7c6ca3d3540c785), which is responsible for dropping three VMProtect'ed DLLs into the %PUBLIC%\Libraries directory:

- **Loader Component:** prxyms3231462335.dll (29db4fd1c8ddd001a04f511ab8fa3af1)
- **Worker Component:** winipfile3231462335.dll0 (5356fc8e2ab9403dde8651f4da2ce56b)
- **Network Component:** netid3231462335.dll0 (941962c7d370324dffefacc3feb6f320)

The numeric string embedded in the filenames is derived from the Machine Globally Unique Identifier (GUID) obtained from the Windows Registry.

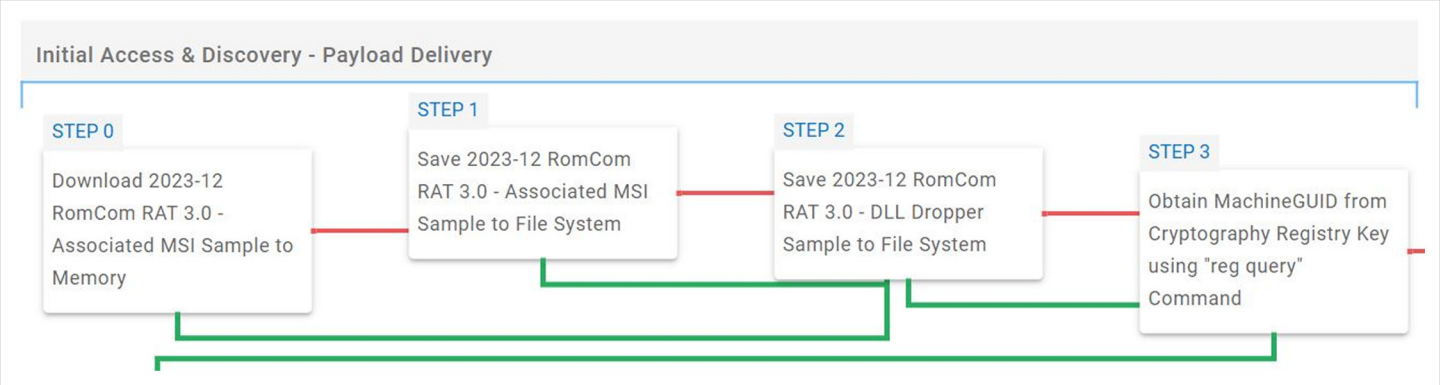
Next, *InstallA.dll* performs a Component Object Model (COM) hijacking technique, which involves modifying the registry value associated with a specific Class ID (CLSID) so that any process invoking it loads the RomCom **Loader** instead. One such process is explorer.exe, which is forcibly restarted by the **Dropper** to ensure that the **Loader** is executed.

Once operational, the **Loader** leverages rundll32.exe to execute both the **Worker** (*winipfile3231462335.dll0*) and Network (*netid3231462335.dll0*) components.

Once active, RomCom communicates through HTTP POST requests made by the **Network** component, interpreting commands received in response. RomCom 3.0 supports a total of 42 commands, several of which are minor variations of one another.

Initial Access & Discovery - Payload Delivery

This stage begins with the deployment of a Microsoft Installer (MSI) archive, which contains legitimate files associated with AstraChat, an enterprise XMPP-based messaging application.

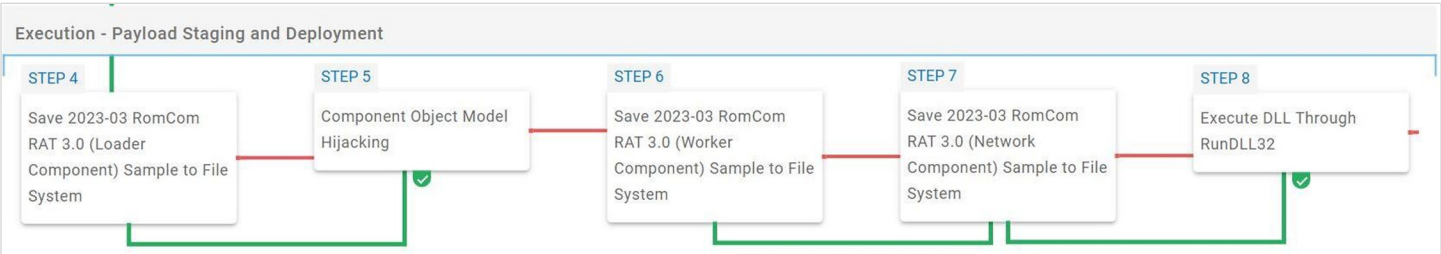


Upon execution, the MSI drops a Dynamic-Link Library (DLL) named *InstallA.dll,* which once loaded retrieves the machine's Globally Unique Identifier (GUID) from the Windows Registry.

> **Ingress Tool Transfer (T1105):** These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.
>
> **Query Registry (T1012):** This scenario queries the `MachineGUID` value located within the `HKLM\SOFTWARE\Microsoft\Cryptography` registry key which contains the unique identifier of the system.

Execution - Payload Staging and Deployment

This stage begins with the deployment of RomCom 3.0, an architecturally modular version of the Remote Access Trojan (RAT), consisting of a Loader Component, a Worker Module, and a Network Handler.



The loader is executed through Component Object Model (COM) hijacking, which subsequently deploys both the Worker Module and the Network Handler using RunDLL32.

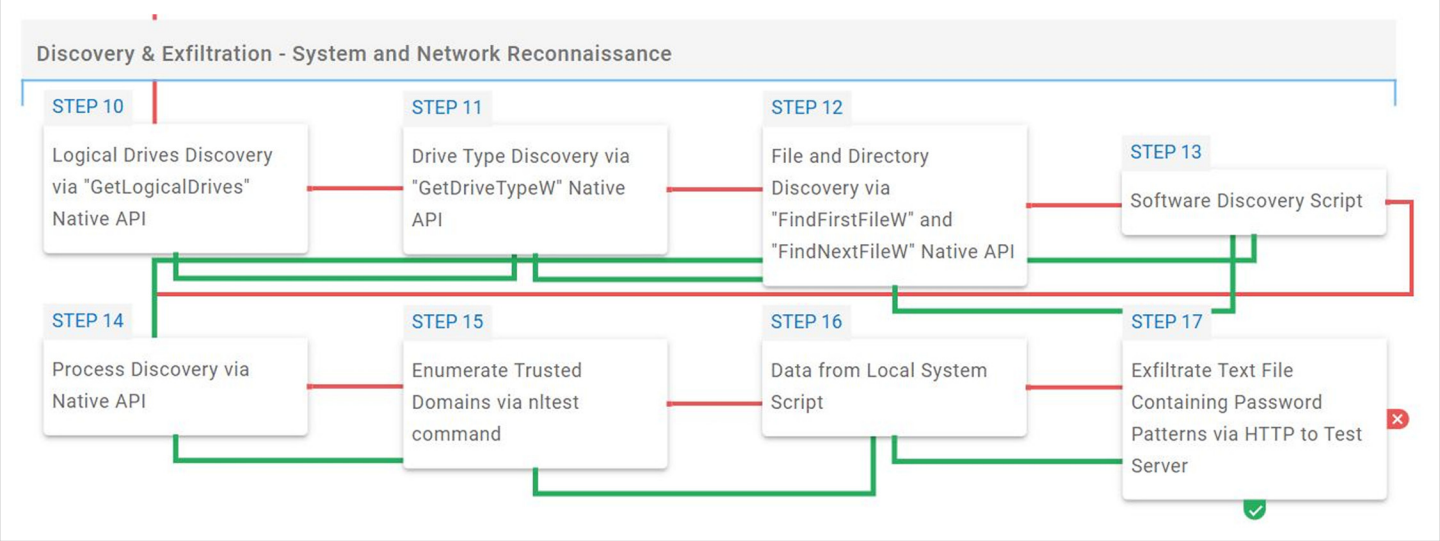
Ingress Tool Transfer (T1105): These scenarios involve downloading specific files into memory and saving them to disk, in independent scenarios, to evaluate the effectiveness of network and endpoint controls in preventing the delivery of known RomCom-related samples.

Component Object Model Hijacking (T1546.015): This scenario performs Component Object Model (COM) Hijacking by assigning a specified Dynamic-Link Library (DLL) to a targeted COM Instance. It then executes a process that utilizes the hijacked instance, ensuring the DLL is loaded and executed.

System Binary Proxy Execution: Rundll32 (T1218.011): This scenario executes an export function from an AttackIQ Dynamic-Link Library (DLL) using the `RunDll32` Windows utility.

Discovery & Exfiltration - System and Network Reconnaissance

This stage focuses on system and network reconnaissance by enumerating system drives, filesystem structure, installed software, active processes, and trusted domains.



Once enumeration is complete, it proceeds to collect files of interest from the system and concludes with the exfiltration of pre-generated sensitive files via HTTP POST requests.

System Information Discovery (T1082): This scenario executes the `GetLogicalDrives` Windows API call to retrieve the currently available disk drives.

System Information Discovery (T1082): This scenario executes the `GetDriveTypeW` Windows API call to retrieve information regarding the system's physical drives.

File and Directory Discovery (T1083): This scenario executes the `FindFirstFileW` and `FindNextFileW` Windows API calls to perform the enumeration of the file system.

Software Discovery (T1518): This scenario queries the registry key `HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall`, which contains entries for all the software installed on the system.

Process Discovery (T1057): This scenario uses Windows API to receive a list of running processes by calling `CreateToolhelp32Snapshot` and iterating through each process object with `Process32FirstW` and `Process32NextW`.

Discovery & Exfiltration - System and Network Reconnaissance

Domain Trust Discovery (T1482): This scenario calls the native `nltest` utility with the `/trusted_domains` option to retrieve a list of trusted Active Directory domains associated with this host.

Data from Local System (T1005): This scenario performs bulk collection of specific file types from the system, staging them locally in preparation for exfiltration.

Exfiltration Over C2 Channel (T1041): This scenario simulates the exfiltration of sensitive data by transmitting a text file with password patterns through HTTP POST requests.

Continued on next page.

Conclusion

This investigation into the RomCom malware family underscores what's possible when the cybersecurity community works in parallel, building on one another's insights, even when those connections aren't immediately obvious. Drawing from more than two dozen publicly available sources, this research connects years of fragmented findings to reveal a larger operational picture: RomCom is not just a persistent backdoor, but the nucleus of an evolving malware ecosystem used in both espionage and financially motivated attacks.

RomCom's trajectory—from a relatively unsophisticated backdoor in 2022 to a modular, stealth-oriented tool linked to espionage and ransomware operations in 2024—demonstrates the need for defenders to move beyond static IOCs and engage with threats at the behavioral level. The emulations released alongside this report are designed to enable exactly that. By emulating the tactics, techniques, and procedures used by RomCom and its affiliates, security teams can proactively test and strengthen their defenses in real-world conditions.

This report would not have been possible without the openness of the threat intelligence community and the researchers who published samples, shared behavioral indicators, and documented sightings, even when attribution was evolving. Their work laid the foundation for our investigation and reinforced a critical truth: security is a collective effort. When practitioners connect the dots across time, geographies, and threat categories, we move closer to understanding and ultimately mitigating the adversaries we face.

Francis Guibernau

Senior Adversary Research Engineer

Francis Guibernau is a Senior Adversary Research Engineer and member of the Adversary Research Team (ART) at AttackIQ. Francis conducts in-depth threat research and analysis to design and create highly sophisticated and realistic adversary emulations. He also coordinates the Cyber Threat Intelligence (CTI) project, which focuses on researching, analyzing, tracking, and documenting adversaries, malware families, and cybersecurity incidents. Francis has extensive experience in adversary intelligence, encompassing both Nation-State and eCrime threats, as well as in vulnerability assessment and management, having previously worked at Deloitte and BNP Paribas.

ATTACKIQ®

U.S. Headquarters
171 Main Street
Suite 656
Los Altos, CA 94022
+1 (888) 588-9116
info@attackiq.com

About AttackIQ

AttackIQ, the leading provider of Adversarial Exposure Validation (AEV) solutions, is trusted by top organizations worldwide to validate security controls in real time. By emulating real-world adversary behavior, AttackIQ closes the gap between knowing about a vulnerability and understanding its true risk. AttackIQ's AEV platform aligns with the Continuous Threat Exposure Management (CTEM) framework, enabling a structured, risk-based approach to ongoing security assessment and improvement.

The company is committed to supporting its MSSP partners with a Flexible Preactive Partner Program that provides turn-key solutions, empowering them to elevate client security. AttackIQ is passionate about giving back to the cybersecurity community through its free award-winning AttackIQ Academy and founding research partnership with MITRE Center for Threat-Informed Defense.