SECURITY ADVISORY

CYBER STASH

May, 2025

Fileless Remcos Remote Access Trojan

Context

In May 2025, a stealthy malware campaign was identified delivering a fileless variant of the Remcos Remote Access Trojan (RAT) via malicious Windows Shortcut (LNK) files and PowerShell-based execution chains. The campaign exemplifies how attackers are increasingly bypassing traditional security controls by leveraging native Windows tools like mshta.exe to execute payloads directly in memory — leaving minimal forensic traces.

Phishing emails, often themed around taxes, are used to lure victims into triggering the infection chain, ultimately granting attackers full remote access. This operation highlights a broader trend in cybercrime: the weaponisation of legitimate system components and fileless techniques to quietly establish persistent control, exfiltrate data, and evade detection. Remcos, once a commercial RAT, continues to evolve as a favoured tool in espionage, fraud, and credential theft — with this campaign marking a sharp escalation in its stealth and delivery.

These developments reinforce the need for a defence-in-depth strategy. Relying solely on a single security vendor — especially Microsoft Defender, which is deeply integrated into Windows and frequently targeted by attackers — leaves organisations exposed to blind spots. Combining complementary detection layers, including network, behavioural, and memory-based analysis, is essential to identify and disrupt modern threats that bypass conventional, signature-based defences.

Mitigation

Defending against the fileless Remcos Remote Access Trojan (RAT) demands a proactive, layered security approach.

Restrict LNK, HTA, and PowerShell Execution: Block .lnk and .hta files in email attachments and ZIP archives at the mail gateway. Restrict PowerShell to signed scripts only using Group Policy, and disable mshta.exe if not explicitly required by business functions.

Detect and Block Fileless Behaviours: Deploy EDR/XDR tools capable of detecting in-memory execution, especially abnormal PowerShell activity and use of CallWindowProc, VirtualAlloc, or CreateThread. Actively monitor for proxy execution via trusted binaries (LOLBins) like mshta.exe.

Technical Details

Remcos RAT is a 32-bit modular remote access trojan compiled in Visual Studio C++ 8. Although commercially distributed, it has long been repurposed by threat actors for espionage, credential theft, and full-system control. In this latest 2025 campaign, adversaries deploy a fileless variant that executes entirely in memory, bypassing disk-based detection by leveraging native Windows tools such as mshta.exe and PowerShell.

Key Enhancements & Tactics

- **Fileless Execution** (MITRE T1055 – Process Injection) A heavily obfuscated PowerShell script (24.ps1) uses custom shellcode to resolve API functions and inject Remcos into memory using VirtualAlloc, CallWindowProc, and similar techniques — leaving no artifacts on disk.

- **Living-off-the-Land Execution via mshta.exe** (MITRE T1218.007 – Signed Binary Proxy Execution: MSHTA) A malicious LNK file (new-tax311.lnk) embedded in a ZIP archive (new-tax311.zip) triggers mshta.exe to load a remote HTA application (xlab22.hta), initiating the attack chain from a trusted binary.

- **PowerShell Obfuscation and API Resolution** (MITRE T1059.001 – PowerShell) The 24.ps1 script is densely obfuscated, employing advanced techniques to walk the Process Environment Block (PEB) for dynamic API resolution and in-memory payload staging.

- **Command and Control** (MITRE T1071.001 – Web Protocols; T1573.002 – Encrypted Channels) The Remcos implant communicates with readysteaurants[.]com over TLS (port 2025). Encrypted configuration includes its name ("Remcos"), keylogger output (logs.dat), and a mutex identifier (Rmc-7SY4AX).

- **Persistence Mechanism** (MITRE T1547.001 – Registry Run Keys) The malware checks for its mutex to avoid reinfection and stores persistence data in the registry under Rmc-7SY4AX.

- **Anti-Analysis Techniques** (MITRE T1497 – Virtualization/Sandbox Evasion) Built-in checks detect sandboxed or virtualised environments, terminating execution when analysis indicators are found.

Remcos RAT Capabilities

- **Data Theft:** Keylogging, clipboard capture, screenshot exfiltration, and system fingerprinting.
- **Remote Access:** Full control over processes, files, services, registry, and UI elements.
- **Surveillance:** Microphone, webcam, and screen recording capabilities.
- **Payload Delivery:** Ability to download and execute secondary payloads from its C2 infrastructure.

Attack Chain Summary

- **Phishing Email**

T Tax-themed lure delivers a ZIP attachment containing new-tax311.lnk.

- **LNK Execution**

  On launch, the LNK invokes mshta.exe to fetch and run xlab22.hta from a remote server.

- **Payload Staging**

  The HTA downloads and executes:

  - 24.ps1: Obfuscated PowerShell loader for in-memory Remcos execution
  - 3.hta: Additional supporting HTA file
  - A decoy PDF to maintain user distraction and legitimacy

- **Post-Exploitation**

  Remcos installs persistence, establishes encrypted C2, and begins surveillance and data theft operations.

What Are HTA and LNK Files?

HTA Files (HTML Application): HTA files are Windows-based applications that use HTML and scripting languages like VBScript or JavaScript. When executed, they run with the same privileges as the user — making them powerful tools often abused by attackers to run arbitrary code under the guise of a trusted file type. Unlike standard HTML files, HTAs are not sandboxed by a browser, allowing direct interaction with the operating system.

LNK Files (Windows Shortcuts): LNK files are shortcut files commonly used in Windows to point to executables or scripts. Attackers weaponize LNK files by embedding commands that launch malicious payloads, often via trusted system binaries like mshta.exe or powershell.exe, enabling stealthy and user-triggered malware execution.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to Remcos RAT:

Tactic	Technique	ID	Details
Initial Access	Spearphishing Attachment	T1566.001	Tax-themed phishing email delivers ZIP with malicious .lnk shortcut.
Execution	PowerShell	T1059.001	Obfuscated 24.ps1 script loads shellcode and executes in memory.
Execution	Signed Binary Proxy Execution	T1218.007	mshta.exe runs remote xlab22.hta to begin payload delivery.
Persistence	Registry Run Keys	T1547.001	Stores persistence in Rmc-7SY4AX; checks mutex to avoid reinfection.
Defense Evasion	Process Injection	T1055	Uses shellcode and APIs (e.g.,
Defense Evasion	Obfuscated Scripts	T1027	PowerShell/VBScript obfuscation hides intent and avoids static detection.
Defense Evasion	Sandbox Evasion	T1497	Detects virtualisation tools and halts in analysis environments.
C2	Web Protocols	T1071.001	TLS C2 with readysteaurants[.]com over HTTPS (port 2025).
C2	Encrypted Channel	T1573.002	RCData-encrypted config; C2 traffic encrypted over TLS.
Collection	Data from Local System	T1005	Captures keystrokes, clipboard, metadata, and file info.
Collection	Screen Capture	T1113	Periodically captures user screen activity.
Collection	Audio Capture	T1123	Enables mic access for audio surveillance.

Cyber Threat Intelligence

The fileless Remcos RAT campaign uncovered in May 2025 represents a notable escalation in the tradecraft of commodity malware operators. While Remcos was originally developed as a legitimate remote administration tool, its adoption since 2016 by financially motivated cybercriminals and state-aligned threat actors has turned it into a core enabler of espionage, credential harvesting, financial fraud, and post-exploitation staging (e.g., delivery of Cobalt Strike, SystemBC).

Attribution & Adversary Profile

Although formal attribution remains unconfirmed, the tactics, techniques, and procedures (TTPs) used in this campaign closely resemble those employed by Malware-as-a-Service (MaaS) actors. The fileless execution chain, use of mshta.exe and PowerShell, obfuscated scripts, and encrypted TLS C2 traffic point to a highly skilled, developer-aware adversary focused on stealth, persistence, and evasion.

Notably, prior Remcos-based campaigns have been linked to groups like:

- **Gamaredon – a Russia-aligned APT** known for quick-deploy phishing lures and persistent access via commodity RATs.
- **Blind Eagle (APT-C-36) – a Latin American threat group** with a history of using tax-themed social engineering and commercial RATs to target public and private sector entities.

This campaign's tooling and tradecraft suggest a professionally operated Malware-as-a-Service (MaaS) affiliate, capable of adapting malware to avoid vendor-specific detection methods and sandbox environments.

Targeting & Victimology

The use of tax-themed phishing lures indicates a broad-based targeting strategy, timed to coincide with regional tax deadlines — a known social engineering window. This type of lure appeals across industries and geographies, likely aimed at small to mid-sized enterprises, professional service firms, and individuals in finance, accounting, or government roles. The ZIP archive and LNK file delivery format allows the adversary to bypass traditional email attachment filters, while the fileless execution chain helps avoid signature-based endpoint detection.

Motivations & Objectives

The primary motivation appears to be financial, given the toolset's capabilities:

- Credential theft
- Remote access to financial and operational systems
- Deployment of secondary payloads for ransomware or fraud
- Surveillance and data exfiltration for resale or extortion

The campaign reflects a growing convergence between cybercrime and advanced persistent threat (APT) methods, where commodity malware is being refined and operationalised for stealth, scale, and monetisation.

Yara Detection Rule

```
rule Fileless_Remcos_RAT_Generic_2025
{
  meta:
    description = "Detects generic artifacts of the May 2025 fileless Remcos RAT campaign"
    author = "CyberStash Threat Intelligence"
    date = "2025-05-23"
    threat_actor = "Possible MaaS affiliate"
    malware_family = "Remcos RAT"

  strings:
    // Known Remcos mutex or config keys
    $mutex = "Rmc-" nocase
    $config_file = "logs.dat" nocase
    $remcos_string = "Remcos" nocase

    // Obfuscated PowerShell indicators (common with shellcode loaders)
    $ps_virtualalloc = "VirtualAlloc"
    $ps_callwindowproc = "CallWindowProc"
    $ps_peb = "ProcessEnvironmentBlock"
    $ps_net_webclient = "New-Object Net.WebClient"
    $ps_iex = "iex"

    // HTA loader references (generic but relevant)
    $hta_mshta = "mshta.exe"
    $hta_script_tag = "<script>" ascii wide
    $hta_download_string = "DownloadString" ascii wide

    // C2 domain pattern keyword (can trigger across variants)
    $generic_c2 = "https://" ascii wide

  condition:
    // Must match multiple traits: obfuscated script + Remcos indicators or HTA behaviour
    (
      3 of ($ps_virtualalloc, $ps_callwindowproc, $ps_peb, $ps_net_webclient, $ps_iex) and
      1 of ($mutex, $remcos_string, $config_file)
    )
    or
    (
      $hta_mshta and 2 of ($hta_script_tag, $hta_download_string, $generic_c2)
    )
```

References

IOCs:

Type	IOC
SHA256	85dcc4bafccb5b9e255f75c2cd96fec1b4a5b30d09ae0d8eb571b312511d7df7
SHA256	ab8caac901b477c08934ec63978400eb369efb655114805ccba28c48272e5dad
SHA256	53589df3043939d10a049a56a1657ff05ccbf3ab536100e8d4c91d03d1010f6b
SHA256	3c35ec71596a34fc823394cb25c9715334cb8126c35d0491e08853d8db614921
URL	https://mytaxclientcopy[.]com/xlab22.hta
Domain	readysteaurants[.]com
IP Address	193.142.146[.]101
IP Address	162.254.39[.]129

Public Intelligence:

- https://blog.qualys.com/vulnerabilities-threat-research/2025/05/15/fileless-execution-powershell-based-shellcode-loader-executes-remcos-rat
- https://thehackernews.com/2025/05/fileless-remcos-rat-delivered-via-lnk.html
- https://www.broadcom.com/support/security-center/protection-bulletin/stealthy-shellcode-loader-executes-remcos-rat-in-fileless-attack-chain
- https://www.scworld.com/brief/updated-remcos-rat-deployed-in-fileless-intrusion