DRONA CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

CRYSOME RAT: MULTI-STAGE ATTACK DELIVERS REMOTE ACCESS TROJAN VIA SPEAR-PHISHING CAMPAIGN

A comprehensive threat advisory detailing a sophisticated multi-stage campaign targeting logistics and transportation infrastructure. The attack leverages highly evasive living-off-the-land techniques, in-memory AMSI patching, and administrative privilege escalation to dismantle system defenses and install the CrySome Remote Access Trojan.

PREPARED BY
Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE
July 15, 2026

CLASSIFICATION MATRIX

HIGH: RED | MED | LOW

Advisory ID: DCS-TA-2026-7783
Issued By: Drona Cyber Solutions Pvt Ltd
Intelligence Source: Drona Threat Intel
Target Sector: Transportation & Logistics
Impacted Region: United States

SEVERITY CLASSIFICATION

HIGH RISK

EXECUTIVE SUMMARY

Drona Threat Intel came across an article detailing a multi-stage attack campaign that delivers the CrySome remote access trojan (RAT) [cite: 282]. The infection begins with a targeted spear-phishing email masquerading as a logistics rate confirmation, which directs the victim to a malicious website [cite: 283]. Upon downloading and executing an initial batch file, the attacker initiates a complex infection chain that leverages living-off-the-land techniques, including hidden PowerShell execution and in-memory AMSI patching [cite: 284].

The campaign escalates privileges using an ICMLuaUtil COM interface UAC bypass, and further evades defenses by deploying WinDefCtl, an open-source utility, to disable Microsoft Defender components [cite: 285]. Once the endpoint's defenses are weakened, the final payload, CrySome RAT, is installed [cite: 286]. This RAT establishes persistence via a scheduled task and provides the attacker with extensive capabilities, including hidden VNC, remote command execution, system reconnaissance, and credential theft from Chromium-based browsers [cite: 287].

[CRITICAL SYS_WARN: ENDPOINT_COMPROMISE]

Immediate Action Required: The CrySome RAT payload executes natively in the background while displaying a decoy PDF document to allay user suspicion [cite: 289]. It grants threat actors complete remote administration capabilities, persistent hidden VNC sessions, and the capability to systematically harvest and decrypt browser credentials and session cookies [cite: 290].

ATTACK CHAIN & DISTRIBUTION

The multi-stage infection process effectively blends social engineering, living-off-the-land techniques, and publicly available offensive security tools to bypass traditional controls [cite: 292]. The sequential execution flow progresses as follows [cite: 293]:

- **Initial Ingress Lure:** The attack commences with a targeted spear-phishing email from ***loadofferstender@gmail.com***, leading the victim to a malicious website ***signindat[.]com*** [cite: 294].
- **Script Execution Block:** The user downloads a malicious batch file, ***Rate_Confirmation_LD-2026-0847.bat***, which launches a hidden PowerShell process with ***-ExecutionPolicy Bypass*** parameters [cite: 295].
- **In-Memory AMSI Patch:** The script dynamically patches the ***AmsiScanBuffer*** function in memory to neutralize the Antimalware Scan Interface (AMSI) [cite: 296].
- **First-Stage Loader:** The batch file downloads ***ElevatorShellCode.exe***, saves it to the ***%TEMP%*** directory as ***es.exe***, and executes it in a hidden window [cite: 297].
- **Privilege Elevation Bypass:** The loader checks for administrative rights and executes a User Account Control (UAC) bypass leveraging the ***ICMLuaUtil*** COM interface [cite: 298].

- **Defense Impairment Injection:** The loader fetches ***stage.psl*** from the C2 infrastructure, executing it directly in memory using ***Invoke-Expression (IEX)*** [cite: 299]. This script adds explicit Microsoft Defender path/process exclusions for the ***%TEMP%*** folder and malicious targets [cite: 300].
- **Security Disabling Toolkit:** The open-source defensive evasion utility ***WinDefCtl*** is downloaded, masqueraded as ***%TEMP%\svchost.exe***, and executed with the ***kill*** argument [cite: 303]. It alters Image File Execution Options (IFEO) in an offline registry hive and loads a signed kernel driver, ***kvckiller.sys***, to fully terminate Microsoft Defender services [cite: 304].
- **Final Payload Delivery:** The final payload, ***patch.exe***, is saved as ***%TEMP%\patch_diag.exe*** and executed silently while a decoy PDF document is shown to the victim [cite: 305].

TECHNICAL ANALYSIS OF CORE CAPABILITIES

1. Defense Evasion and In-Memory Execution

The modular approach designed by the threat operators minimizes the signature footprint of individual components [cite: 308]. By chaining hidden PowerShell operations, in-memory AMSI manipulation, and volatile script executions via ***IEX***, the malware minimizes its disk footprint, complicating static file analysis and traditional signature detection [cite: 309].

2. Persistent Access Mechanism

Long-term access is reliably maintained via the automated establishment of a local Windows Scheduled Task named ***CrysomeLoader*** [cite: 311]. This task is configured to re-execute the primary client executable every 5 minutes from user-writable profiles [cite: 312]. Furthermore, the malware utilizes an internal ***AVKiller*** component to execute persistent ***Set-MpPreference*** scripts to ensure Microsoft Defender components remain disabled [cite: 313].

3. Browser Credential Harvesting

A dedicated information-stealing module explicitly targets local Chromium-based web browsers [cite: 315]. The module terminates active browser processes, drops an embedded recovery library named ***abe_decrypt.dll*** to disk, and injects it into the browser target [cite: 316]. The injected library extracts stored authentication credentials and active session cookies, outputting them into localized ***passwords.json*** and ***cookies.json*** structures for external exfiltration to the operator [cite: 317].

STRATEGIC RECOMMENDATIONS

Drona Threat Intel recommends implementing the following defense-in-depth mitigations to defend against these multi-stage techniques [cite: 319]:

MITIGATION CONTROL	ACTIONABLE SECURITY REQUIREMENT
PowerShell Monitoring	MONITOR for highly suspicious PowerShell arguments such as ***-ExecutionPolicy Bypass***, hidden windows, or dynamic in-memory execution patterns involving ***IEX*** [cite: 320].
Defender Protection	IMPLEMENT robust alerting rules for unauthorized modifications to Microsoft Defender parameters, including the deployment of ***Add-MpPreference*** or IFEO registry tampering [cite: 320].
Directory Restraints	

MITIGATION CONTROL	ACTIONABLE SECURITY REQUIREMENT
	AUDIT and investigate binary executions launched from user-writable structures like *%TEMP%*, particularly those masquerading as native system tasks like *svchost.exe* [cite: 320].
Persistence Detection	ENFORCE monitoring policies around the generation of new scheduled tasks executing binaries out of temporary or user profile directories [cite: 320].
Network Perimeter	BLOCK all known malicious domains, C2 servers, and IP addresses identified as part of this infrastructure at the firewall perimeter [cite: 323].
Security Awareness	TRAIN corporate personnel continuously on identifying targeted spear-phishing lures, specifically business-centric logistics rate confirmations [cite: 323].

INDICATORS OF COMPROMISE (IOCS)

The technical indicators linked to this campaign are maintained by Drona Threat Intel [cite: 325]. Network and endpoint security tools should be updated to block and detect these values [cite: 326]:

INDICATOR VALUE	TYPE	DESCRIPTION
`hxxps://signindat[.]com/ElevatorShellCode.exe`	`URL`	Malicious URL hosting first-stage loader [cite: 327]
`hxxps://signindat[.]com/update.exe`	`URL`	Malicious URL hosting WinDefCtl utility [cite: 327]
`hxxps://signindat[.]com/patch.exe`	`URL`	Malicious URL hosting CrySome RAT payload [cite: 327]
`hxxps://signindat[.]com/stage.psl`	`URL`	Malicious URL hosting stage 2 PowerShell script [cite: 327]
`signindat[.]com`	`Domain`	Malicious command and distribution domain [cite: 327]
`193[.]26[.]115[.]42:5555`	`IPv4:Port`	CrySome RAT Command & Control (C2) server [cite: 327]
`ec68666e8f0a3b9870d7177bab684c8dcfb8ca0bc7c8c484a71b2b33ea4e26f4`	`SHA-256`	Malicious File Hash [cite: 327]
`53f1da8a032115aa682749all4f4cfebcb5ef933400a89b4bbfa84f2057222ff`	`SHA-256`	Malicious File Hash [cite: 327]

Disclaimer & References: This document is compiled for proactive threat hunting and awareness purposes based on open-source intelligence and investigations credited to Drona Threat Intel. Reference URL: hxxps://www.levelblue.com/blogs/spiderlabs-blog/from-phishing-to-persistence-a-crysome-rat-infection-chain-analysis [cite: 328, 329].