DRONA CYBER SOLUTIONS

DRONA CYBER SOLUTIONS PVT LTD

ASYNCRAT & SCREENCONNECT: THE MECHANICS OF A SOPHISTICATED FREEWARE IMPERSONATION CAMPAIGN

A precise threat awareness report breaking down recent SEO poisoning and typosquatted delivery architectures. This document analyzes the hidden deployment parameters of specialized remote management trojans designed to systematically bypass enterprise endpoint controls.

PREPARED BY
Drona Cyber Solutions Pvt Ltd

DATE OF ISSUE
July 16, 2026

CLASSIFICATION MATRIX
HIGH: RED

THREAT INTELLIGENCE ADVISORY

Fake Freeware Installers Deploy ScreenConnect and AsyncRAT

Issued By: Drona Cyber Solutions Pvt Ltd

Intelligence Source: Drona Threat Intel

Target Sector: Global / Cross-Industry

Date: July 16, 2026

Severity Classification: HIGH

Executive Summary

Drona Threat Intel came across an article detailing a large-scale campaign where threat actors distribute the AsyncRAT remote access trojan by abusing the legitimate ScreenConnect remote management tool. The campaign targets a global audience across both individual and corporate computing environments.

The initial infection vector involves users downloading malicious archives from a network of over 90 spoofed websites that masquerade as official portals for popular freeware such as OBS Studio, DNS Jumper, and DS4Windows. These fraudulent sites are promoted through search engine optimization (SEO) techniques to rank highly in search engine results, maximizing user exposure and trust.

The downloaded archive contains a legitimate, signed Microsoft installer executable and a malicious DLL named `install.res.1033.dll`. When the user runs the installer, it leverages DLL sideloading to execute the malicious library, which covertly installs ScreenConnect in the background while the expected software installs. Once active, the threat actors use ScreenConnect to execute PowerShell and VBS scripts, disable local security controls, and ultimately deploy AsyncRAT via process hollowing into the legitimate `RegAsm.exe` process.

> **[CRITICAL RISK WARNING SYSTEM // CONSOLE_ALERT]**
>
> **Evasion Tactics Detected:** The threat architecture employs aggressive system security degradation mechanisms, including full system disk exclusions within Microsoft Defender and explicit User Account Control (UAC) prompt suppression via registry manipulation. This leaves the endpoint entirely vulnerable to subsequent covert actions, such as direct process hollowing and remote command orchestration.

Attack Chain & Distribution

The infrastructure of this campaign demonstrates a highly structured and multi-staged approach designed to maintain stealth while ensuring high victim conversion rates. The sequential delivery phases are detailed below:

- **Ingress via SEO Poisoning:** Threat actors establish an extensive infrastructure comprising over 90 typosquatted domains localized in up to 10 languages, mimicking popular software utility portals to lure victims.

- **Payload Archive Delivery:** Victims download a malicious ZIP archive containing a legitimate, signed Microsoft executable (e.g., `install.exe`) paired with a malicious library named `install.res.1033.dll`.
- **DLL Sideloading Execution:** When executed, the legitimate file sideloads the malicious DLL, which silently launches `msiexec.exe` to install a hidden ScreenConnect MSI package disguised as `vcredist_x64.dll` within the Assets folder.
- **Simultaneous Decoy Setup:** To avoid raising suspicion, the actual legitimate utility software setup wizard is displayed to the user concurrently.
- **Defense Evasion Orchestration:** The stealthily installed ScreenConnect agent executes a PowerShell script (`Fj5NmEsp9EuKrun.psl`) to modify registry values and create broad Microsoft Defender exclusions.
- **Process Hollowing Injection:** A series of VBScripts drops and extracts the final encrypted payload from `secret_bytes.txt`, decrypting it via a `0xA7` XOR key and injecting it directly into a suspended `RegAsm.exe` instance.
- **Persistent Lifecycle Access:** The malware creates a recurring scheduled task named `MasterPackager.Updater`, ensuring re-execution of the infection script every 2 minutes.

Technical Analysis of Core Capabilities

The campaign stands out due to its clever blending of social engineering, abuse of legitimate software, and sophisticated endpoint evasion techniques:

1. Exploitation of Trust Elements: By leveraging legitimate, signed Microsoft binaries for the sideloading trigger and using an authorized remote desktop tool (ScreenConnect), the actors bypass baseline application whitelisting and traditional behavior-based monitoring solutions.

2. Defense Control Degradation: The active PowerShell script explicitly targets the `ConsentPromptBehaviorAdmin` registry parameter to nullify User Account Control prompts. Furthermore, it creates broad exclusions across all local system disks, preventing Microsoft Defender from scanning the active components or the hollowed target processes.

3. Command and Control Infrastructure: The broader network infrastructure is divided into dedicated operational clusters. For example, one cluster uses `162.216.241[.]242` for initial landing pages and `198.23.185[.]81` for hosting malicious files, while another cluster located at `2.59.134[.]97` combines both functions to maintain robust operational continuity.

Strategic Recommendations

Organizations and individual administrators must proactively enforce the following mitigation matrix to protect infrastructure against this campaign:

Strategy Control	Actionable Requirement
TRAIN Users & Staff	Educate users to download software exclusively from official vendor websites and to be cautious of sponsored or top-ranking search engine results.
RESTRICT Execution Paths	Implement application control policies, such as AppLocker or Windows Defender Application Control, to restrict the execution of unauthorized software and MSI packages from untrusted locations.
AUDIT Persistence & Services	Continuously monitor for the anomalous creation of new services, particularly for remote administration tools like ScreenConnect, and for new scheduled tasks establishing persistence.
ENFORCE EDR & Heuristics	Utilize an Endpoint Detection and Response (EDR) solution to detect suspicious process chains, such as ScreenConnect spawning PowerShell or code injection into legitimate system processes like RegAsm.exe.
IMPLEMENT Network Egress Rules	Configure egress firewall rules to block outbound traffic to known malicious domains and IP addresses to disrupt command-and-control communications.
VALIDATE Software Signatures	Verify the authenticity and digital signatures of all software installers before execution, even if they appear to be legitimate.

Indicators of Compromise (IoCs)

The following technical indicators have been confirmed by Drona Threat Intel as part of this ongoing distribution campaign:

Indicator Value	Type	Context / Description
`mora1987.work[.]gd`	Domain	Malicious C2 Domain
`ds4windows[.]io`	Domain	Typosquatted Lure Domain
`ds4windows[.]net`	Domain	Typosquatted Lure Domain
`ds4windows[.]pro`	Domain	Typosquatted Lure Domain
`dnsjumper[.]app`	Domain	Typosquatted Lure Domain
`dns-jumper[.]com`	Domain	Typosquatted Lure Domain
`dnsjumper[.]pro`	Domain	Typosquatted Lure Domain
`studioobs[.]com`	Domain	Typosquatted Lure Domain
`studio-obs[.]net`	Domain	Typosquatted Lure Domain
`obs-studio[.]site`	Domain	Typosquatted Lure Domain
`servermanagemen[.]xyz`	Domain	Active Infrastructure C2

Indicator Value	Type	Context / Description
r[.]manage-server[.]xyz	Domain	Active Infrastructure C2
manageserver[.]xyz	Domain	Active Infrastructure C2
198[.]23[.]185[.]81	IPv4	Malicious File Hosting IP
185[.]254[.]97[.]249	IPv4	Malicious Infrastructure IP
45[.]145[.]41[.]205	IPv4	Malicious Infrastructure IP
B32810973132D11AFD61CCEE222BBB79	FileHash-MD5	Malicious DLL Payload Component
5B7E1FE55BD7B5EA54BD4ED1677E5A26	FileHash-MD5	Malicious DLL Payload Component
9A9CCD8B0E5D05F4EE776678024844DB	FileHash-MD5	Malicious DLL Payload Component

References

[1] Drona Threat Intel Campaign Repositories & Threat Feeds (Case Reference: Advisory-7787).

[2] External Intelligence Archive: https://securelist.com/tr/the-soc-files-screenconnect-campaign-with-asyncrat/120472/