Threat Actors Weaponize PDF Editor Trojan to Convert Devices into Proxies

By Aman Mishra

Published: 2025-08-21 · Archived: 2026-04-10 02:33:27 UTC

Researchers have discovered a complex campaign using trojanized software that uses authentic code-signing certificates to avoid detection and turn compromised machines into unintentional residential proxies, according to a recent threat intelligence notice from Expel Security.

The operation begins with files bearing the code-signing signature of “GLINT SOFTWARE SDN. BHD.,” a seemingly legitimate entity whose credentials have been abused to lend credibility to malicious payloads.

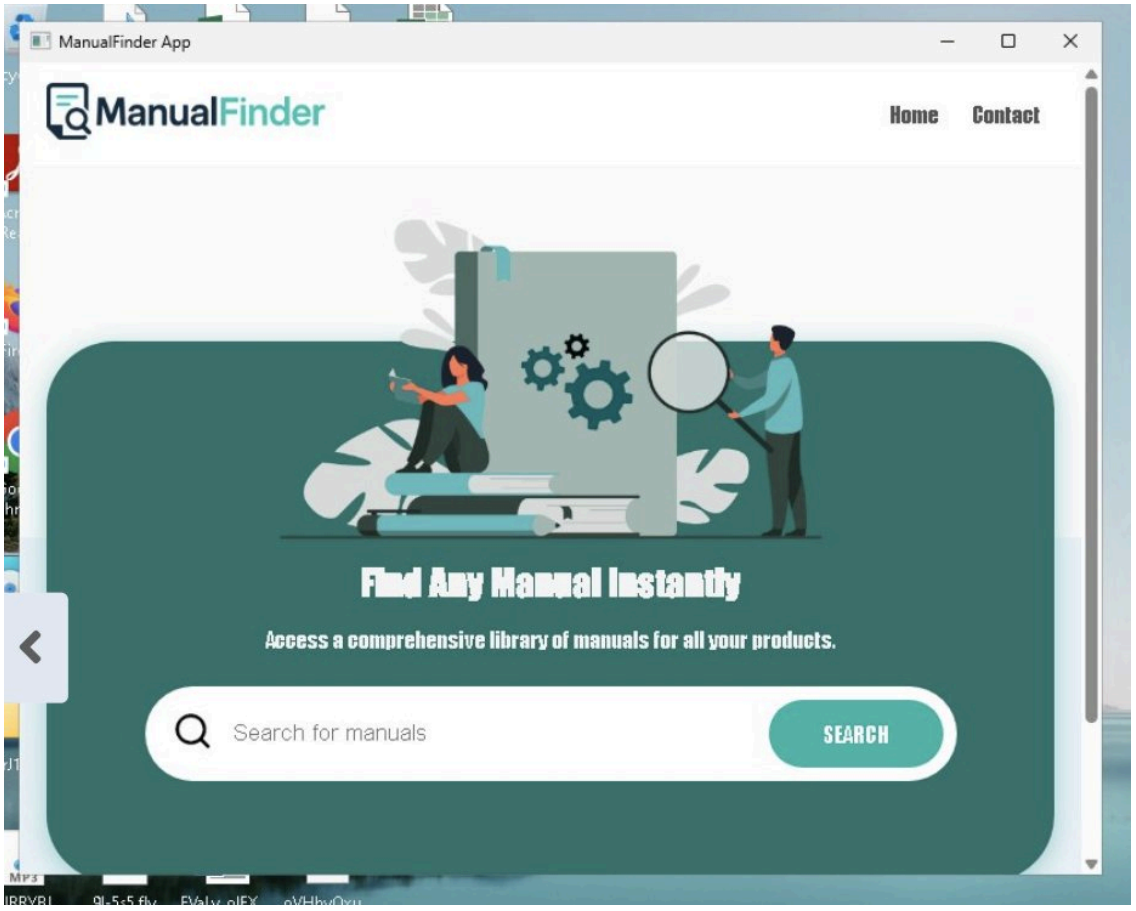
Malicious Code-Signing

Central to this scheme is a JavaScript dropper that facilitates the installation of a trojan dubbed “ManualFinder.”

This dropper is deployed through persistent mechanisms tied to the OneStart Browser, a known problematic application with a history of suspicious behavior.

The persistence is achieved via a scheduled task that executes the JavaScript file from the user’s temporary directory, ensuring the malware remains active across system reboots.

Once activated, the JavaScript establishes outbound connections to command-and-control (C2) domains such as mka3e8[.]com and y2iax5[.]com, from which it retrieves and installs the signed ManualFinder executable.



Manual Finder

This multi-stage infection chain highlights the attackers' focus on stealth and reliability, exploiting trusted certificates to bypass endpoint security controls and user scrutiny.

Dual-Function Malware

Further analysis reveals the insidious nature of the payloads involved. One of the signed files masquerades as a benign PDF editor but harbors trojan capabilities that covertly reconfigure the compromised device into a residential proxy node.

This transformation allows threat actors to route malicious traffic through the victim's IP address, effectively anonymizing their operations while potentially implicating the infected user in illicit activities.

The ManualFinder application, when executed in a controlled sandbox environment, presents itself as a legitimate utility designed to assist users in locating product manuals, complete with functional search features.

However, its deployment context raises alarms: it is involuntarily installed via the OneStart Browser, despite the associated website promoting it as a free tool without providing any direct download options.

This discrepancy suggests a deliberate strategy to distribute the malware through bundled or hijacked software channels, capitalizing on OneStart's established reputation for sketchy practices.

According to the report, Expel's investigation underscores how such dual-purpose malware blends utility with malice, complicating detection efforts as the benign facade can deceive both users and automated scanners.

The overall campaign reflects an evolving threat landscape where attackers weaponize everyday productivity tools, turning them into vectors for proxy networks that support activities like distributed denial-of-service attacks, data exfiltration, or anonymized cyber espionage.

The implications of this trojan are significant for cybersecurity professionals, as it demonstrates the abuse of code-signing infrastructure and the challenges in monitoring persistent, low-profile infections.

Organizations are advised to scrutinize software signatures, monitor scheduled tasks for anomalous JavaScript executions, and block known C2 domains to mitigate risks.

By converting devices into proxies, attackers not only expand their infrastructure but also expose victims to legal and reputational hazards, emphasizing the need for robust threat hunting and endpoint protection strategies.

Indicators of Compromise (IOCs)

Indicator Type	Description	Value
File Hash (MD5)	PDF Editor Trojan	d09b667391cb6f58585ead314ad9c599
File Hash (MD5)	ManualFinder Executable	1efaffcd54fd2df44ab55023154bec9b
File Hash (MD5)	OneStart Browser	27fb60fa0e002bdb628ecf23296884d3
Domain	Command-and-Control (C2)	mka3e8[.]com
Domain	Command-and-Control (C2)	y2iax5[.]com

[Aman Mishra]

Aman Mishra is a Security and privacy Reporter covering various data breach, cyber crime, malware, & vulnerability.
