CTI Report – Trojanized PDF Editor Campaign (ManualFinder)

Executive Summary

A recent campaign is distributing trojanized PDF editor applications that deliver the malware ManualFinder. Once installed, affected endpoints may be converted into residential proxy nodes, enabling adversaries to obfuscate malicious traffic through victim networks. The campaign leverages legitimate-looking code signing certificates (notably issued to GLINT SOFTWARE SDN. BHD.) and malvertising funnels to gain user execution. Analysts assess this as a high-risk, commercially motivated operation with potential secondary impacts including credential theft and further payload delivery.

Threat Overview

- Threat Name: ManualFinder (delivered via fake PDF Editors)
- Threat Actor Motivation: Financially motivated, proxy-as-a-service ecosystem
- Distribution Method: Malvertising leading to fake “free PDF editor” download sites
- Malware Behavior:
  - Installs via MSI/EXE packages signed with stolen/abused certificates
  - Establishes persistence through scheduled tasks executing Node.js JavaScript
  - Contacts command-and-control (C2) infrastructure to download payloads
  - Masquerades as legitimate utility while enabling residential proxy services

Technical Details

- Persistence: Scheduled tasks calling node.exe to execute JavaScript from %TEMP%
- Evasion: Valid code signing certificate (GLINT SOFTWARE SDN. BHD., SSL.com EV cert)
- C2 Domains Observed: mka3e8[.]com, y2iax5[.]com, 5b7crp[.]com
- Sample Hashes:
  - ManualFinderApp.exe – SHA256: 71edb9f9f757616fe62a49f2d5b55441f91618904517337abd9d0725b07c2a51
  - ManualFinder-v2.0.196.msi – SHA256: ed797beb927738d68378cd718ea0dc74e605df0e66bd5670f557217720fb2871
  - PDFEditor-1.0.0.8.exe – SHA256: 9dc1b05b8fc53c84839164e82200c5d484b65eeba25b246777fa324869487140
- Infrastructure: Over 40+ malicious domains impersonating PDF utility services (e.g., fullpdf[.]com, pdfonestart[.]com)

Attribution & Origin

- Signing Entity: GLINT SOFTWARE SDN. BHD., registered in Malaysia
- Certificates issued by SSL.com in April 2025 (now revoked)
- Operation resembles commercially motivated proxy-botnet operators, not state-sponsored APT activity

Impact Assessment

- Risk Level: High
- Potential Impacts:
  - Endpoint hijacking into proxy networks
  - Credential and data exposure
  - Use of corporate IPs for malicious activity
  - Reputational and legal risk

Recommended Mitigations

1. Detection & Hunting:
   - Search for scheduled tasks invoking node.exe against %TEMP%*.js
   - Monitor network connections from node.exe or "PDFEditor" processes to listed C2 domains
   - Alert on binaries signed by GLINT SOFTWARE SDN. BHD.

2. Containment & Response:
   - Isolate and reimage infected systems
   - Block identified domains and hashes at firewall/EDR level
   - Rotate credentials on affected endpoints

3. Prevention:
   - Restrict user ability to install unapproved software
   - Block malvertising domains via DNS/web proxy
   - Implement strict application allowlists with code-signing reputation validation

Business Impact Summary

This campaign poses significant business risks beyond technical compromise:

- Brand & Reputation: If company IP addresses are abused as part of a proxy network, corporate reputation may suffer and relationships with partners or customers could be damaged.

- Legal & Compliance: Malicious activity routed through corporate systems could lead to regulatory scrutiny or liability, particularly under data protection and cybersecurity

frameworks.

- Operational Disruption: Reimaging and remediation across infected endpoints may cause downtime and loss of productivity.

- Financial Costs: Potential costs include incident response, regulatory fines, legal defense, and loss of business opportunities.

Recommendation: Executives should prioritize proactive detection, user awareness, and strict control of software installation to mitigate these risks.