INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 07:10 UTC

FishMonger Ports SprySOCKS to Windows: Kernel Drivers, Print Spooler Abuse, and Possible UEFI Persistence Signal Escalating Espionage Capability

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0491
Type	Threat Campaign
CVE ID	CVE-2023-24932
Severity	HIGH
CVSS Base Score	9.5
EPSS Score	0.1056 (95th percentile)
Affected Products	Windows (kernel driver subsystem, Print Spooler/svchost.exe); previously exploited N-days include Fortinet, GitLab, Microsoft Exchange Server, Progress Telerik UI, Zimbra
Published	2026-06-16T05:44:34
Discovery Source	Rss

Executive Summary

ESET has identified two new Windows variants of the SprySOCKS backdoor, attributed to FishMonger, a Chinese state-sponsored group also tracked as Earth Lusca and Aquatic Panda. The variants deploy kernel-mode rootkit capabilities and abuse the Windows Print Spooler service to achieve deep, persistent access on government and enterprise targets, with forensic evidence suggesting possible pre-OS (UEFI) persistence via a Secure Boot bypass vulnerability. Government agencies and enterprises running unpatched Windows systems, particularly those involved in foreign policy, defense, or critical infrastructure, face a high risk of long-term, undetected compromise.

Technical Analysis

FishMonger has deployed two undocumented Windows variants of SprySOCKS, a backdoor previously documented only on Linux. WIN_DRV loads a kernel-mode driver to hide network connections, processes, files, and registry keys, functioning as a rootkit. WIN_PLUS injects malicious code into svchost.exe by abusing the Windows Print Spooler service (T1055.001, T1543.003). Both variants represent a platform expansion from the Linux implant previously attributed to this actor. Active targeting between 2023 and 2024 focused on

government organizations in Honduras, Taiwan, Thailand, and Pakistan. Limited forensic evidence indicates possible UEFI bootkit deployment via CVE-2023-24932, a Windows Secure Boot bypass (CWE-693, CWE-284). The CVSS base score in source data is listed as 9.5; NVD's published base score for CVE-2023-24932 is 6.7 (per https://nvd.nist.gov/vuln/detail/cve-2023-24932). The higher figure appears to reflect contextual severity incorporating active exploitation; analysts should treat the base score as 6.7 and the effective risk as significantly elevated given campaign context. EPSS score is 0.106 at the 95th percentile, indicating high exploitation probability relative to the broader CVE population. The actor has previously exploited N-days in Fortinet, GitLab, Microsoft Exchange Server, Progress Telerik UI, and Zimbra for initial access (T1190). Additional relevant techniques include T1078 (Valid Accounts), T1547.001 and T1547.004 (Boot/Logon Autostart), T1542.003 (Bootkit), T1562.001 (Impair Defenses), T1027 (Obfuscated Files), T1071.001 (Web Protocols C2), and T1090.001 (Internal Proxy). CWE-506 (Embedded Malicious Code) applies to the driver and injected payload components.

Action Checklist

1. Step 1: Containment. Apply Microsoft's CVE-2023-24932 Secure Boot revocation updates immediately on all Windows systems. Microsoft has staged enforcement across multiple update phases; verify your systems have progressed to the enforcement phase per Microsoft's enterprise deployment guidance (https://support.microsoft.com/en-us/topic/enterprise-deployment-guidance-for-cve-2023-24932-88b8f034-20b7-4a45-80cb-c6049b0f9967). Prioritize internet-facing systems, VPN concentrators, and hosts with Print Spooler enabled. Disable the Print Spooler service on systems where it is not operationally required (NIST AC-6: Least Privilege; CIS 4.6).
2. Step 2: Detection. Hunt for unsigned or anomalously signed kernel drivers loaded at boot (review Windows Event Log, System channel, Event IDs 7045 and 219 for new service/driver installs). Audit svchost.exe instances for unusual parent processes or injected threads, baseline legitimate svchost child process trees and flag deviations. Check for Print Spooler service activity on non-print servers (Event ID 808, 316 in Microsoft-Windows-PrintService/Admin). Review UEFI/Secure Boot integrity via attestation logs or firmware integrity monitoring tools. Correlate against MITRE T1542.003 and T1543.003 hunting hypotheses. Apply NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs). Confirm these controls are active across all Windows endpoints and servers. MITRE D3FEND countermeasures D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are directly applicable.
3. Step 3: Eradication. Apply all phases of the CVE-2023-24932 remediation as documented by Microsoft. Review the boot manager revocation guidance at https://support.microsoft.com/en-us/topic/how-to-manage-the-windows-boot-manager-revocations-for-secure-boot-changes-associated-with-cve-2023-24932-41a975df-beb2-40c1-99a3-b3ff139f832d. On confirmed-compromised systems, treat the UEFI firmware as potentially modified, coordinate with hardware vendors for firmware integrity verification before returning systems to production. Remove unauthorized kernel drivers identified during detection. Revoke and rotate any credentials used on affected systems (MITRE D3FEND D3-CRO: Credential Rotation; D3-CH: Credential Hardening). Enforce least-privilege access to kernel driver installation paths (NIST AC-6; D3-UAP: User Account Permissions).
4. Step 4: Recovery. After patching, verify Secure Boot enforcement status via firmware settings and Windows attestation APIs. Confirm svchost.exe process trees have returned to known-good baselines. Re-enable Print Spooler only where operationally required, with enhanced monitoring. Validate audit log continuity, confirm no gaps exist in Windows Event Logs during the suspected compromise window (NIST AU-9: Protection of Audit Information; NIST AU-11: Audit Record Retention). Monitor for re-infection

indicators, including re-appearance of the driver service entries flagged in Step 2. Conduct a privilege account audit to confirm no persistence via valid accounts (NIST AC-2: Account Management; CIS 5.1: Establish and Maintain an Inventory of Accounts).

5. Step 5: Post-Incident. This campaign exposed several control gaps common in enterprise environments: (a) insufficient monitoring of kernel driver installations, addressable via NIST AU-2 (Event Logging) with explicit coverage of driver load events; (b) Print Spooler running on non-print servers despite years of documented abuse, addressable via CIS 4.6 (Securely Manage Enterprise Assets and Software) and NIST AC-6; (c) incomplete Secure Boot enforcement due to the staged rollout of CVE-2023-24932 mitigations, addressable by tracking patch phase completion rather than patch availability alone; (d) absence of UEFI firmware integrity monitoring on high-value targets. Review your vulnerability management process against CIS 7.1 and CIS 7.2 for N-day exposure timelines on the previously exploited products (Fortinet, GitLab, Exchange, Telerik UI, Zimbra). Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) as standing countermeasures on government-adjacent and critical infrastructure systems.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal, and (for government or regulated entities) the appropriate CISA or sector ISAC notification channel immediately if: memory forensics or firmware analysis confirms UEFI modification on any host (indicating pre-OS persistence that survives reimaging), if SprySOCKS C2 beaconing is detected from a host holding PII, PHI, CUI, or classified-adjacent data (triggering breach notification obligations), or if the scope of kernel driver deployment exceeds three hosts (indicating lateral movement beyond initial access and requiring enterprise-wide containment escalation).
Recovery Notes	After CVE-2023-24932 enforcement-phase patching and kernel driver removal, do not return any system to production until `Confirm-SecureBootUEFI` returns True AND a clean Autoruns scan (with VirusTotal integration) shows no unsigned or anomalous svchost-associated DLLs — both conditions must be satisfied, not either alone, because the SprySOCKS implant achieves persistence at two independent layers (UEFI/boot manager and user-space via Print Spooler). Monitor recovered systems for a minimum of 30 days post-remediation with Sysmon Event ID 6 (Driver Load) alerting enabled, given FishMonger's documented capability to re-establish access via the organization's externally-facing product set (Fortinet, GitLab, Exchange, Telerik UI, Zimbra) if those N-days remain unpatched. Any re-appearance of the specific driver service registry keys or Print Spooler provider DLL paths identified during the initial hunt should trigger immediate re-containment without waiting for confirmation.

Forensic Artifacts	Windows System Event Log — Event ID 7045 (new service installed) and 219 (kernel driver install failed signature validation): the SprySOCKS kernel driver registers as a Windows service at install time; these events record the driver binary path, service name, and account under which it was installed, providing the primary forensic trail for the rootkit's initial deployment on each host | HKLM\SYSTEM\CurrentControlSet\Services registry hive (offline export): FishMonger's kernel driver and any malicious Print Spooler provider DLL persist as service entries in this hive; an offline export before eradication captures the exact binary paths, load order group, and ImagePath values that identify the implant's installation footprint | Microsoft-Windows-PrintService/Admin and Operational event channels — Event IDs 808 and 316: these events are generated when SprySOCKS's Print Spooler-injected DLL component fails to load cleanly or when a rogue print provider is registered, making them a high-fidelity indicator of the Print Spooler abuse vector even on hosts where the kernel driver did not fully deploy | Full physical memory image (WinPmem or Magnet RAM Capture): SprySOCKS operates in kernel mode and hooks SSDT or DKOM structures to hide its process and driver entries from user-space tools; memory forensics with Volatility3 (using the `windows.driverscan` and `windows.modules` plugins) will surface rootkit components invisible to `tasklist`, `sc query`, and standard registry enumeration | UEFI/SPI flash dump (CHIPSEC or vendor firmware diagnostic tool): given ESET's assessment of possible pre-OS persistence, a firmware dump before any reflash or Secure Boot DBX update is the only forensic record of a potential UEFI implant; compare the PE image hashes of all DXE drivers in the dump against the vendor's published firmware release to identify unauthorized modules injected into the boot firmware

Per-Action IR Details

Step 1: Containment — Apply Microsoft's CVE-2023-24932 Secure Boot revocation updates immediately on all Windows systems. Microsoft has staged enforcement across multiple update phases; verify your systems have progressed to the enforcement phase per Microsoft's enterprise deployment guidance (https://support.microsoft.com/en-us/topic/enterprise-deployment-guidance-for-cve-2023-24932-88b8f034-20b7-4a45-80cb-c6049b0f9967). Prioritize internet-facing systems, VPN concentrators, and hosts with Print Spooler enabled. Disable the Print Spooler service on systems where it is not operationally required (NIST AC-6: Least Privilege; CIS 4.6).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: short-term containment actions taken to limit the spread and impact of a confirmed or suspected incident, including service disablement and patch application to reduce attacker footholds

Controls: NIST AC-6 (Least Privilege), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For teams without enterprise patch management, use a PowerShell one-liner to audit Secure Boot enforcement phase registry state across reachable hosts: `Invoke-Command -ComputerName (Get-Content hosts.txt) -ScriptBlock { Get-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\SecureBoot\State' }`. Enumerate Print Spooler status with: `Get-Service -Name Spooler -ComputerName (Get-Content hosts.txt) | Where-Object {$_.Status -eq 'Running'}`. Disable on non-print servers via: `Set-Service -Name Spooler -StartupType Disabled; Stop-Service -Name Spooler`. Document every host touched before changes are made.

Evidence: Before applying the CVE-2023-24932 revocation update or disabling Print Spooler on any host, capture volatile state that the update will invalidate or that process termination will destroy: (1) Run `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045 -or $_.Id -eq 219}` to snapshot all recently installed driver/service entries before the patch alters boot state. (2) Collect a full memory image using WinPmem or Magnet RAM Capture — FishMonger's SprySOCKS kernel-mode rootkit components and injected threads in svchost.exe will not survive a service stop or reboot. (3) Record active network connections with `Get-NetTCPConnection -State Established | Sort-Object RemoteAddress` before any network isolation, as SprySOCKS maintains a C2 channel that will drop on

isolation. (4) Export the current UEFI/Secure Boot variable state via `Confirm-SecureBootUEFI` and `Get-SecureBootPolicy` before the revocation update modifies the DBX (forbidden signatures) database. (5) Preserve the Windows Event Log System and Microsoft-Windows-PrintService/Admin channels (wevtutil epl System system.evtx; wevtutil epl Microsoft-Windows-PrintService/Admin printservice.evtx) before the Spooler service is stopped.

Step 2: Detection — Hunt for unsigned or anomalously signed kernel drivers loaded at boot (review Windows Event Log, System channel, Event IDs 7045 and 219 for new service/driver installs). Audit svchost.exe instances for unusual parent processes or injected threads — baseline legitimate svchost child process trees and flag deviations. Check for Print Spooler service activity on non-print servers (Event ID 808, 316 in Microsoft-Windows-PrintService/Admin). Review UEFI/Secure Boot integrity via attestation logs or firmware integrity monitoring tools. Correlate against MITRE T1542.003 and T1543.003 hunting hypotheses. Apply NIST AU-6 (Audit Record Review) and NIST SI-4 (no mapped control from provided reference — SI-4 is outside the provided control list; see note below). CIS 8.2 (Collect Audit Logs) must be confirmed active across all Windows endpoints and servers. Note: SI-4 (System Monitoring) is not included in the provided NIST control reference; if your organization's framework mapping includes it, apply accordingly — this advisory does not assert it from memory.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlating indicators across log sources to characterize the scope and mechanism of a suspected intrusion, including process-tree anomaly detection and driver integrity review specific to kernel-mode implants

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a configuration that enables Event ID 6 (Driver Load) with signature validation and Event ID 7 (Image Load) for svchost.exe. Use SwiftOnSecurity's Sysmon config as a baseline and add a rule to alert on any unsigned driver load (DriverLoaded where Signed=false). For process injection into svchost.exe, use Process Hacker (free) to inspect thread start addresses in svchost instances — any thread whose start address resolves outside a known DLL base is suspicious. Hunt Print Spooler abuse using: `Get-WinEvent -LogName 'Microsoft-Windows-PrintService/Admin' | Where-Object {$_.Id -eq 808 -or $_.Id -eq 316}`. For UEFI integrity without commercial tools, compare `bcdedit /enum firmware` output against a known-good baseline captured before suspected compromise.

Evidence: This is an analysis phase; however, evidence capture must precede any containment action triggered by findings. Specific artifacts to collect before acting on any positive indicator: (1) Sysmon Event ID 6 logs showing the loaded driver's ImageLoaded path, Hashes, and Signed/Signature status — SprySOCKS kernel drivers may use revoked or stolen code-signing certificates. (2) Export the HKLM\SYSTEM\CurrentControlSet\Services registry hive to preserve driver service registration entries that FishMonger's installer creates — `reg export HKLM\SYSTEM\CurrentControlSet\Services services_hive.reg`. (3) Collect Microsoft-Windows-PrintService/Admin and Operational channels in full — Event ID 808 (Print Spooler failed to load a plug-in) and 316 (Print Spooler failed to load a driver) are produced when the SprySOCKS DLL injected via Print Spooler encounters load errors, leaving a forensic trail even on partial deployment. (4) For svchost.exe injection analysis, collect a process memory dump of the suspicious svchost instance using ProcDump (`procdump -ma svchost_.dmp`) before any remediation kills the process. (5) Record output of `msinfo32 /nfo system.nfo` to capture loaded driver list and system firmware version before any patch modifies the boot environment.

Step 3: Eradication — Apply all phases of the CVE-2023-24932 remediation as documented by Microsoft. Review the boot manager revocation guidance at https://support.microsoft.com/en-us/topic/how-to-manage-the-windows-boot-manager-revocations-for-secure-boot-changes-associated-with-cve-2023-24932-41a975df-beb2-40c1-99a3-b3ff139f832d. On confirmed-compromised systems, treat the UEFI firmware as potentially modified — coordinate with hardware vendors for firmware integrity verification before returning systems to production. Remove unauthorized kernel drivers identified during detection. Revoke and rotate any

credentials used on affected systems (D3-CRO: Credential Rotation; D3-CH: Credential Hardening). Enforce least-privilege access to kernel driver installation paths (NIST AC-6; D3-UAP: User Account Permissions).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: removal of the threat from the environment, including deletion of malicious kernel-mode components, revocation of compromised credentials, and firmware integrity remediation on hosts where UEFI persistence is suspected

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: To remove an unauthorized kernel driver without EDR: (1) Boot to Windows Recovery Environment (WinRE) or a trusted live OS to delete the driver binary from %SystemRoot%\System32\drivers\ outside of the running OS, bypassing rootkit self-protection. (2) Delete the driver's service registry key from the offline hive using `regedit` mounted against the offline SYSTEM hive. (3) For credential rotation without a PAM tool, use Active Directory's `Set-ADAccountPassword` and `Disable-ADAccount` for all accounts that authenticated to the compromised host during the suspected window — pull this list from Security Event Log Event ID 4624 (logon) filtered by the compromise timeframe. (4) For UEFI firmware integrity verification without vendor tooling, use the UEFI shell `dmpstore` command or manufacturer diagnostic USB boot media to compare firmware measurements against published vendor checksums.

Evidence: Before removing any driver, rotating credentials, or touching firmware, the following volatile evidence must be preserved: (1) Full RAM image of the compromised host — SprySOCKS kernel components hook system calls and may only be fully visible in memory; WinPmem or Magnet RAM Capture must complete before any reboot or driver removal that will clear live state. (2) Export HKLM\SYSTEM\CurrentControlSet\Services for the specific driver service key FishMonger registered, and HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Print\Providers for any malicious Print Spooler provider DLL registered for persistence. (3) Copy the malicious driver binary from %SystemRoot%\System32\drivers\ (or the path from the Event ID 7045 entry) to an isolated forensic share before deletion — hash with SHA-256 for threat intelligence submission. (4) Collect Security Event Log Event IDs 4624, 4648, and 4672 (privileged logon) filtered to the compromise window to document every account whose credentials must be rotated. (5) If UEFI modification is suspected, use vendor firmware diagnostic tools or CHIPSEC (open-source) to dump the current SPI flash contents before any reflash — this is the only forensic record of a potential firmware implant.

Step 4: Recovery — After patching, verify Secure Boot enforcement status via firmware settings and Windows attestation APIs. Confirm svchost.exe process trees have returned to known-good baselines. Re-enable Print Spooler only where operationally required, with enhanced monitoring. Validate audit log continuity — confirm no gaps exist in Windows Event Logs during the suspected compromise window (NIST AU-9: Protection of Audit Information; NIST AU-11: Audit Record Retention). Monitor for re-infection indicators, including re-appearance of the driver service entries flagged in Step 2. Conduct a privilege account audit to confirm no persistence via valid accounts (NIST AC-2: Account Management; CIS 5.1: Establish and Maintain an Inventory of Accounts).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restoring systems to normal operation with verified integrity, confirming that Secure Boot enforcement is active, and monitoring for re-infection indicators specific to the FishMonger SprySOCKS implant

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Verify Secure Boot enforcement post-patch with: `Confirm-SecureBootUEFI` (should return True) and `Get-SecureBootPolicy` — if output shows policy GUIDs other than Microsoft's known enforcement GUIDs, escalate for firmware review. Validate svchost.exe process tree integrity using Autoruns (Sysinternals, free) — run with administrator privileges, go to the Services tab, and enable VirusTotal checking; any unsigned or low-prevalence svchost-associated DLL warrants investigation. For audit log continuity, check for gaps in the System and Security event logs using: `Get-WinEvent -LogName Security | Select-Object TimeCreated | Sort-Object TimeCreated` — any unexplained gap (log cleared event ID 1102, or timestamp jumps) during the suspected compromise window indicates

potential log tampering by the rootkit.

Evidence: Recovery validation is forward-looking, but gaps discovered here are forensic findings. Specifically: (1) Compare current `bcdedit /enum all` output against a known-good baseline to detect any residual unauthorized boot entries that survived patching — FishMonger's UEFI persistence mechanism, if deployed, may survive OS-level remediation. (2) Re-run `Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045 -or $_.Id -eq 219}` post-remediation and diff against the pre-remediation capture — any new or re-appearing driver install entry signals re-infection or persistence that eradication did not fully remove. (3) Review Security Event Log for Event ID 4720 (account created), 4728/4732/4756 (member added to privileged group), and 4698 (scheduled task created) from the full compromise window — FishMonger APT operators establish secondary persistence via valid accounts and scheduled tasks in parallel with kernel implants. (4) Validate that the CVE-2023-24932 DBX update is applied by checking the EFI forbidden signature database size has increased post-update using `Get-SecureBootUEFI -Name dbx`.

Step 5: Post-Incident — This campaign exposed several control gaps common in enterprise environments: (a) insufficient monitoring of kernel driver installations, addressable via NIST AU-2 (Event Logging) with explicit coverage of driver load events; (b) Print Spooler running on non-print servers despite years of documented abuse, addressable via CIS 4.6 (Securely Manage Enterprise Assets and Software) and NIST AC-6; (c) incomplete Secure Boot enforcement due to the staged rollout of CVE-2023-24932 mitigations, addressable by tracking patch phase completion rather than patch availability alone; (d) absence of UEFI firmware integrity monitoring on high-value targets. Review your vulnerability management process against CIS 7.1 and CIS 7.2 for N-day exposure timelines on the previously exploited products (Fortinet, GitLab, Exchange, Telerik UI, Zimbra). Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) as standing countermeasures on government-adjacent and critical infrastructure systems.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned review to close control gaps exposed by the FishMonger campaign, update detection logic for kernel-mode implants and Print Spooler abuse, and improve N-day response timelines for the product set FishMonger is known to exploit

Controls: NIST AU-2 (Event Logging), NIST AC-6 (Least Privilege), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a vulnerability management platform, build a simple N-day tracking spreadsheet that logs: product name, CVE, vendor advisory date, internal patch-applied date, and days-to-patch. Populate it retroactively for CVE-2023-24932 and the FishMonger-exploited product set (Fortinet, GitLab, Exchange, Telerik UI, Zimbra) to quantify your organization's actual N-day exposure window. For ongoing kernel driver monitoring without EDR, add a Sysmon Event ID 6 (Driver Load) Sigma rule to your log pipeline — a free community rule targeting unsigned driver loads is available in the SigmaHQ repository. Schedule a monthly `sc query type= driver` and hash-compare against a known-good baseline using PowerShell `Get-FileHash` to detect new or modified kernel drivers between hunts.

Evidence: Post-incident evidence collection focuses on gap documentation rather than volatile artifacts, but the following should be preserved for lessons-learned and potential regulatory reporting: (1) Retention of all raw Windows Event Logs (System, Security, Microsoft-Windows-PrintService/Admin) from the full compromise window per NIST AU-11 — minimum 1 year for most regulated environments, 3 years for federal. (2) Document the delta between Microsoft's CVE-2023-24932 advisory date (May 2023) and your organization's enforcement-phase completion date — this quantifies the Secure Boot exposure window and is a required input for any regulatory breach notification assessment. (3) Preserve the forensic images of compromised hosts (RAM and disk) for at least 90 days post-incident — FishMonger's UEFI persistence hypothesis may require vendor-assisted firmware analysis that cannot begin until the incident is fully scoped. (4) Catalog every host where Print Spooler was running but not required at the time of detection — this inventory directly informs the CIS 4.6 and AC-6 control gap remediation plan.

Detection Guidance

Focus detection on four areas. First, kernel driver installation: monitor Windows System Event Log for Event ID 7045 (new service installed) and Event ID 219 (driver load failure or unsigned driver) with alert thresholds on any driver not in your approved baseline. Cross-reference driver signing certificates against known-good inventories. Second, Print Spooler abuse and process injection: baseline all svchost.exe instances by parent process, loaded modules, and network connections. Alert on svchost.exe establishing outbound connections on non-standard ports or loading modules from user-writable paths. Monitor Microsoft-Windows-PrintService/Admin log for Event IDs 808 and 316 on non-print servers. Third, Secure Boot and UEFI integrity: review attestation health reports (Windows Health Attestation Service or equivalent EDR firmware telemetry) for Secure Boot policy changes or revocation bypass indicators consistent with CVE-2023-24932 exploitation. Fourth, C2 behavioral patterns: FishMonger has used internal proxy chaining (T1090.001) and standard web protocols for C2 (T1071.001), hunt for beaconing patterns from svchost.exe and anomalous HTTPS connections to low-reputation or newly registered domains. MITRE D3FEND countermeasures D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are directly applicable. No specific IOC values were included in the source data for this advisory; IOC enrichment should be sourced from the ESET research publication directly.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not available in source data`	No specific IOC hashes were included in the provided source material. Obtain IOCs directly from the ESET research publication on SprySOCKS Windows variants.	LOW

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1547.004** — Winlogon Helper DLL
- **T1564.001** — Hidden Files and Directories
- **T1083** — File and Directory Discovery
- **T1588.002** — Tool
- **T1574.002** — DLL Side-Loading
- **T1542.003** — Bootkit
- **T1105** — Ingress Tool Transfer
- **T1543.003** — Windows Service
- **T1055.001** — Dynamic-link Library Injection
- **T1562.001** — Disable or Modify Tools
- **T1053.005** — Scheduled Task

- **T1068** — Exploitation for Privilege Escalation
- **T1057** — Process Discovery
- **T1071.001** — Web Protocols
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1190** — Exploit Public-Facing Application
- **T1090.001** — Internal Proxy
- **T1082** — System Information Discovery
- **T1027** — Obfuscated Files or Information

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1547.004	Winlogon Helper DLL	Persistence
T1564.001	Hidden Files and Directories	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1588.002	Tool	Resource-Development
T1574.002	DLL Side-Loading	Persistence
T1542.003	Bootkit	Persistence
T1105	Ingress Tool Transfer	Command-And-Control
T1543.003	Windows Service	Persistence
T1055.001	Dynamic-link Library Injection	Defense-Evasion
T1562.001	Disable or Modify Tools	Defense-Evasion
T1053.005	Scheduled Task	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1057	Process Discovery	Discovery
T1071.001	Web Protocols	Command-And-Control
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1090.001	Internal Proxy	Command-And-Control
T1082	System Information Discovery	Discovery
T1027	Obfuscated Files or Information	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/china-linked-sprysocks-backdoor-e...	T3
How to manage the Windows Boot Manager revocations for Secure ...	https://support.microsoft.com/en-us/topic/how-to-manage-the-windows...	T1
Enterprise Deployment Guidance for CVE-2023-24932	https://support.microsoft.com/en-us/topic/enterprise-deployment-gui...	T1
Applying CVE-2023-24932 During OSD : r/SCCM - Reddit	https://www.reddit.com/r/SCCM/comments/1j3gf17/applying_cve20232493...	T3
CVE-2023-24932 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2023-24932	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-24932	T1

Generated 2026-06-17 07:10 UTC by TJS Security Command Center