

Inside Shadow-Earth-053: A China-Aligned Cyberespionage Campaign Against Government and Defense Sectors in Asia

By Daniel Lunghi, Lucas Silva Apr 30, 2026 Read time: 14 min (3781 words)

Published: 2026-04-30 · Archived: 2026-05-14 02:00:22 UTC

Table 1. Legitimate executables vulnerable to DLL sideloading abused by SHADOW-EARTH-053

SHADOW-EARTH-053 uses a legitimate Toshiba Bluetooth Stack executable, renamed to *CIATosBtKbd.exe*, to sideload a malicious DLL (*TosBtKbd.dll*). This loader employs a multistage evasion technique by retrieving its payload from the Windows Registry rather than embedding it within the binary. Upon execution, the loader calls *GetComputerNameA* to identify the host and access a machine-specific registry key at *HKEY_CURRENT_USER\Software\[ComputerName]*. From here, it retrieves a binary value named *scode*, which contains the shellcode payload.

The malware then allocates memory using *VirtualAlloc* (configured with *PAGE_EXECUTE_READWRITE* permissions) and executes the shellcode via callback injection. By passing the shellcode's address as a callback parameter to the legitimate Windows API function *EnumDesktopsA*, the malware tricks the operating system into executing the malicious code during standard desktop enumeration. This method avoids direct execution calls that often trigger security monitoring systems. Persistence was achieved via a Scheduled Task named *M1onltor*, configured to run the sideloaded binary every five minutes with the highest privileges. Note that the specific shellcode payload could not be retrieved for analysis.

In several attacks, an executable named *mdync.exe* was deployed on the victim's network. Although the file could not be retrieved for static analysis, endpoint telemetry reveals that the executable established beaconing connections to 141[.]164[.]46[.]77. We observed that this tool was dropped by the side-loaded DLL *TosBtKbd.dll*.

We observed the group leveraging the [IOX](#) proxy by creating local accounts and setting the *LocalAccountTokenFilterPolicy* value to 1. This configuration grants full administrative privileges to remote connections from all local administrators (and not just the built-in RID 500 account), enabling lateral movement via Pass-the-Hash.

Beyond IOX, we observed SHADOW-EARTH-053 deploying multiple tunneling tools within a single environment, suggesting a layered approach to maintaining covert communication channels. These include:

- GOST (GO Simple Tunnel): An open-source tunnel written in Go, GOST was used to establish SOCKS5 proxies and WebSocket-based tunnels to external infrastructure. The attacker configured both local SOCKS5 listeners and relay-based reverse tunnels to the IP address 96[.]9[.]125[.]227.
- Wstunnel: Another open-source tunneling tool deployed as *wt.exe*, Wstunnel was configured to tunnel SOCKS5 traffic over HTTPS to the same command-and-control (C&C) IP address.

We also saw the threat actor rename a tool from *tunnel-core.exe* to *code.exe* and pass a single parameter (*client.toml*) to it. We observed communications to the IP address 96[.]19[.]125[.]227 on port 8067, however the tool itself was not available for further inspection.

The deployment of multiple tunneling tools to the same C&C address suggests operational redundancy, ensuring persistent outbound connectivity even if individual tools are detected and blocked. All tools were staged in C:\Users\Public, consistent with the group's known preference for publicly writable staging directories.

In mid-December 2025, SHADOW-EARTH-053 retrieved one ShadowPad sample from the IP address 194[.]38[.]111[.]3 listening on port 1790. Sandbox telemetry showed Linux samples being retrieved from the same IP and port in early December. These samples were [NOODLERAT](#) ELF files, a malware family that is shared among multiple groups performing espionage or cybercrime, and which we have extensively [covered](#) in previous blog entries.

The NOODLERAT samples used the domain check[.]office365-update[.]com as C&C, which was registered on November 19, 2025. This domain name matches registration patterns found for other recent domain names belonging to SHADOW-EARTH-053. For these reasons, and following our [threat attribution framework news-cybercrime-and-digital-threats](#), we attribute these samples to SHADOW-EARTH-053 with low confidence. These samples were also observed by [multiple vendors](#) as part of the active exploitation of [CVE-2025-55182](#) (React2Shell).

RingQ

In one targeted environment, we detected a sample of RingQ, which is an open-source tool of Chinese origin available on GitHub that is designed to pack malicious binaries in order to evade detection by security solutions.

The intrusion set also uses domain names that impersonate products, security solution companies, or are related to the DNS protocol, likely to make them appear legitimate.

We also observed the group renaming legitimate Windows system binaries to evade process-based detection. In one incident, *net.exe* was copied to C:\ProgramData with randomized filenames using a *\$(RANDOM).log* naming pattern (e.g., *\$D5PLAA1.log*, *\$9XF5WLD.log*). PowerShell binaries were similarly disguised (e.g., *\$C06KCQ2.log*, *\$VMB9AIT.log*, *\$6T8BLJP.log*). This technique targets security solutions that rely on process name matching rather than binary hash verification.

SHADOW-EARTH-053 uses Windows Management Instrumentation Command-line (WMIC) for lateral movement, installing backdoors and tools onto additional hosts. We also observed the group deploying a suspected custom remote desktop protocol (RDP) launcher (under the name *smss.exe*) and a C# implementation of SMBExec known as [Sharp-SMBExec](#).

In one environment, the group propagated web shells to additional internal Exchange servers by copying them over administrative shares (e.g., *copy charcode.aspx \\[IP]\c\$\inetpub\wwwroot\aspnet_client\system_web*). This technique allows rapid expansion across the Exchange infrastructure without deploying additional tooling, leveraging existing administrative credentials and the compromised web shell as an execution platform.

The group collects credentials that can be used to further its objectives, notably through the use of the [Evil-CreateDump](#) tool. The tool appears to be based on Microsoft's [create-dump.exe](#) utility, likely modified to target LSASS process memory for credential extraction.

Mimikatz was executed directly via *rundll32.exe* with command-line arguments for credential extraction (*sekurlsa::logonpasswords*) and local SAM database dumping (*lsadump::sam*). These commands were spawned by the IIS worker process (*w3wp.exe*), confirming execution through a web shell.

Additionally, we observed the group dropping and executing a binary called *newdcsync*, which, based on the command line and filename, was likely used for DCSync attacks.

We observed the attacker deploying the RAR executable, and in one instance, we saw the creation of a password-protected RAR archive containing messages (a PST file) from an executive in the targeted company.

In one specific case, SHADOW-EARTH-053 used its access to the victim's Exchange server to install a snap-in for Exchange management. The process revealed an iterative approach: initial attempts to enumerate mailboxes via Get-Mailbox failed, prompting the attacker to explicitly load the snap-in (*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.SnapIn*) and bypass execution policy. Subsequent iterations refined the technique further, switching from Get-Mailbox to Get-User for a broader scope, and adding fields such as *userAccountControl* and *AccountDisabled* to identify active high-value accounts. This progression from noisy initial attempts to more refined, stealthier commands was observed within a single session.

Additionally, the threat actor used a custom "ExchangeExport" tool to export the mailbox content of high-profile users via the Exchange Web Services (EWS) API. Microsoft observed similar activity by [Silk Typhoon](#) (Hafnium). Unfortunately, the tool could not be retrieved for further analysis.

Victimology

Our investigation indicates that this campaign has a distinct geographic focus, primarily targeting governmental entities, mostly in Asia. Most observed targets were concentrated in South, East, and Southeast Asia, particularly:

- Pakistan
- Thailand
- Malaysia
- India
- Myanmar
- Sri Lanka
- Taiwan

Note that despite focusing on Asia, the threat actor's footprint extended beyond this region, with at least one target in Poland. This distribution suggests a strategic interest in Asian geopolitical entities, while the global targets may indicate opportunistic exploitation or a broadening of the group's scope.

Beyond the government sector, SHADOW-EARTH-053 also targeted the technology industry. In at least two countries, we observed the group focusing on IT consulting firms holding government contracts, particularly those that listed the Ministry of Defense as one of their customers.

Finally, we found limited number of victims within the transportation industry in Southeast Asia.

Overlaps

Our investigation revealed that multiple targets were compromised up to 8 months before the deployment of ShadowPad, using identical entry points. In these earlier instances, the attackers gained access via vulnerable IIS or Microsoft Exchange servers and subsequently deployed web shells to maintain persistence.

Three possible scenarios may explain the relationship between the groups:

- **Independent exploitation:** SHADOW-EARTH-053 independently exploited these servers by leveraging the same vulnerabilities previously used by SHADOW-EARTH-054. This scenario matches the "Type A" collaboration from our Premier Pass-as-a-Service model [published](#) last year. This involves the deployment of backdoors through web shells, exploitation of vulnerable public facing servers, and similar initial access techniques. In such cases, any observed coordination between intrusion sets is likely incidental rather than intentional.
- **Asset repurposing:** SHADOW-EARTH-053 simply repurposed the web shells left behind from the earlier intrusion by SHADOW-EARTH-054.
- **Same group:** SHADOW-EARTH-053 and SHADOW-EARTH-054 are a single group using multiple TTPs.

In three recent cases, a malicious loader family attributed to SHADOW-EARTH-054 was detected in organizations previously targeted by SHADOW-EARTH-054 and later by SHADOW-EARTH-053. The same vulnerabilities were exploited again to deliver this loader, with no apparent connection to previously deployed malware. This pattern reinforces our assessment of a Type A collaboration — independent exploitation of the same vulnerabilities, with no evidence of operational coordination between the two intrusion sets. It also renders the third scenario unlikely, as targeting an already-compromised organization using a different malware toolkit would be operationally inconsistent.

In addition to the similarities in initial breach vectors, we identified significant overlap in **post-exploitation capabilities**. Both groups utilized an identical toolkit, leveraging a mix of custom-developed malware and utilities:

- Evil-CreateDump
- IOX Proxy

Notably, our analysis confirmed that these artifacts shared **identical file hashes**, indicating the use of the exact same binaries rather than just similar software.

Notably, the following activity sequence was observed at the same endpoints:

1. Compromise with SHADOW-EARTH-054 malware (late 2024/early 2025).
2. Deployment of ShadowPad implants by SHADOW-EARTH-053 (mid-2025).
3. Re-exploitation by SHADOW-EARTH-054 (early 2026).

The following image shows the timeline of events:

Notably, nearly half of the targets of SHADOW-EARTH-053 were also targeted by SHADOW-EARTH-054, primarily in Malaysia, Sri Lanka, and Myanmar. We also identified targets unique to SHADOW-EARTH-054 in Malaysia, Brazil, and Taiwan, operating in similar industries to those targeted by SHADOW-EARTH-053, plus a telecommunications equipment reseller.

Although both groups exhibit significant overlaps in victimology and TTPs, we have chosen to categorize them into two distinct temporary intrusion sets based on the details outlined above.

Attribution and motivation

The deployment of malware families (most notably ShadowPad) is strongly associated with China-aligned intrusion sets. Both the selected targets and operational timing also align closely with geopolitical events and strategic interests in the region.

During the investigation, we quickly found that two different groups were operating in similar environments. Regarding SHADOW-EARTH-053, we found no strong overlap with any known publicly reported group. Meanwhile, for SHADOW-EARTH-054, we found multiple malware loaders that we could not attribute, and a [VShell sample](#) that communicates with 209[.]141[.]40[.]254.

This malware family used to be open source and is known for being used by multiple intrusion sets. We also noticed the threat actor issuing a “ping” command to zimbra-beta[.]info. Both the IP address and the domain name are listed in a report on [CL-STA-0049](#), an intrusion set that primarily uses the SQUIDDOOR malware (which we call VARGEIT).

The infection vector used by CL-STA-0049 matches what we observed, however none of the other TTPs match, and we found no traces of VARGEIT. Therefore, we chose to use the temporary name SHADOW-EARTH-054.

We know of two other intrusion sets using VARGEIT: [Earth Alux](#) and [REF7707](#), where the malware is called [FinalDraft](#). Again, none of the TTPs from the related reports match the activity we observed from SHADOW-EARTH-054.

The intrusion set’s ultimate objective remains unclear; the sensitive nature of the targets suggests that this activity is likely related to cyberespionage against foreign countries and intellectual property theft. We also found one instance where SHADOW-EARTH-054 tried to reach the webmail of a Ministry of Defense in Southeast Asia from the environment of a technology customer, suggesting a possible supply chain attack scenario.

Risk management guidance

The primary entry vector used in this campaign were vulnerabilities in internet-facing IIS applications. Organizations should prioritize applying the latest security updates and cumulative patches to Microsoft Exchange and any web applications hosted on IIS. In scenarios where immediate patching is not feasible, we strongly recommend deploying Intrusion Prevention Systems (IPS) or Web Application Firewalls (WAF) with rulesets specifically tuned to block exploit attempts against these known CVEs (Virtual Patching).

To counter the deployment of web shells, administrators should implement strict File Integrity Monitoring (FIM) on critical web directories (e.g., C:\inetpub\wwwroot or Exchange Client Access paths). Alerts should be

configured for the creation or modification of executable server-side scripts (such as *.aspx*, *.ashx*, or *.jsp*) in these directories. Affected paths should also be scanned for unreferenced or suspicious files, with particular attention to files with mismatched timestamps or high entropy (indicating obfuscated code).

Organizations can also reduce the attack surface by hardening IIS configurations:

- **Restrict permissions:** Organizations should ensure that the IIS worker process (*w3wp.exe*) runs with the lowest possible privileges and does not have administrative rights or the ability to write to arbitrary directories.
- **Disable unused features:** IT and security teams should remove unnecessary IIS modules and handlers that are not required for business operations.
- **Application whitelisting:** Enterprises should enforce policies that prevent the IIS process from launching unauthorized binaries or script interpreters.

The presence of a web shell often leads to anomalous process execution. Security teams should monitor Endpoint Detection and Response (EDR) telemetry for:

- **Suspicious child processes:** Organizations should set up alerts for when the IIS worker process spawns command shells (e.g., *cmd.exe*, *powershell.exe*) or reconnaissance tools (e.g., *whoami.exe*, *net.exe*). This is a high-fidelity indicator of remote code execution.
- **Anomalous network traffic:** Security teams should monitor for unexpected outbound connections initiated by the web server, which may indicate C&C communication.
- **Organizations should also monitor and restrict access to directories commonly used as staging grounds, including C:\ProgramData, C:\Users\Public, C:\PerfLogs, and C:\Windows\Temp.** These locations are frequently exploited by threat actors to drop and execute payloads without requiring immediate administrative privileges, and their broad write permissions make them easy to overlook during routine inspection.

Conclusion

SHADOW-EARTH-053 represents a persistent and methodical China-aligned threat actor operating across Asia and beyond. By exploiting long-known but still-unpatched vulnerabilities in internet-facing Exchange and IIS servers, the group has successfully compromised government ministries, defense-adjacent contractors, and transportation organizations across at least eight countries, demonstrating that N-day vulnerabilities remain a viable and effective entry point even years after their disclosure.

The relationship between SHADOW-EARTH-053 and SHADOW-EARTH-054 adds a further layer of complexity to the threat landscape. While the two intrusion sets share tooling, initial access methods, and victim overlap, the available evidence points to independent exploitation of the same vulnerabilities rather than coordinated operation. This pattern underscores the scale and persistence of state-sponsored espionage activity targeting Asian government and critical infrastructure sectors.

Organizations operating internet-facing Microsoft Exchange or IIS infrastructure, particularly in the affected regions, should treat this campaign as a strong signal to audit patch levels, review web shell detection capabilities,

and scrutinize outbound traffic from web servers. The indicators of compromise and threat hunting queries provided in this report offer a practical starting point for identifying potential exposure.

Proactive security with TrendAI Vision One™

[TrendAI Vision One™one-platform](#) platform is the industry-leading AI cybersecurity platform that centralizes cyber risk exposure management, security operations, and robust layered protection.

[one-platform](#) TrendAI Vision One™ Threat Intelligence Hub

[TrendAI Vision One™ Threat Intelligence Hubproducts](#) provides the latest insights on emerging threats and threat actors, exclusive strategic reports from TrendAI™ Research, and TrendAI Vision One™ Threat Intelligence Feed in the TrendAI Vision One™ platform. This research was first reported to Threat Intelligence Hub subscribers in February 2026.

Emerging Threats: [SHADOW-EARTH-053 and SHADOW-EARTH-054: Overlapping Cyberespionage Groups Targeting Government Entities in Asia](#)

Threat Actors: [SHADOW-EARTH-053](#)

[SHADOW-EARTH-053 and SHADOW-EARTH-054: Overlapping Cyberespionage Groups Targeting Government Entities in Asia](#)

Hunting Queries

TrendAI Vision One™ customers can use the Search App to match or hunt the malicious indicators mentioned in this blog post with data in their environment.

Possible Webshell: eventSubId: 101 AND objectFilePath: (*.aspx OR *.ashx OR *.jsp) AND processFilePath: *\\w3wp.exe

More hunting queries are available for TrendAI Vision One™ with [Threat Intelligence Hubproducts](#) entitlement enabled.

Indicators of Compromise (IoCs)

The IoCs for the threats discussed in this entry can be found [here](#).

Source: https://www.trendmicro.com/en_us/research/26/d/inside-shadow-earth-053.html