

SHADOW-EARTH-053 Uses Legacy Exchange Exploitation to Target Asia-Pacific Governments

 blog.polyswarm.io/shadow-earth-053-uses-legacy-exchange-exploitation-to-target-asia-pacific-governments

The Hivemind



Verticals Targeted: Government, Defense, Technology, Transportation, Critical Infrastructure

Regions Targeted: South Asia, Southeast Asia, East Asia

Related Families: ShadowPad, GODZILLA, NOODLERAT, IOX, GOST, Wstunnel, RingQ, VShell

Executive Summary

A newly identified China-aligned cyberespionage campaign tracked as SHADOW-EARTH-053 is targeting government agencies, defense-adjacent contractors, and critical infrastructure organizations across Asia through exploitation of unpatched Microsoft Exchange and IIS vulnerabilities. The operation relies heavily on legacy Exchange flaws, web shell persistence, ShadowPad malware deployment, credential theft, and covert tunneling infrastructure to maintain long-term access within victim environments. The campaign demonstrates

that older but still-exploitable enterprise infrastructure continues to provide reliable access opportunities for state-aligned espionage operators and reinforces the operational importance of proactive detection, behavioral monitoring, and layered telemetry visibility.

Key Takeaways

- SHADOW-EARTH-053 exploited legacy Microsoft Exchange vulnerabilities, including the ProxyLogon chain, to compromise government and critical infrastructure entities across Asia and at least one NATO member state.
- The threat actor deployed ShadowPad malware through DLL sideloading chains involving legitimate signed executables alongside GODZILLA web shells and multiple covert tunneling frameworks.
- Nearly half of observed victims were also targeted by the related intrusion cluster, known as SHADOW-EARTH-054, highlighting overlap in victimology, tooling, and operational ecosystems among China-aligned espionage actors.
- The campaign focused heavily on government ministries, Ministry of Defense contractors, transportation organizations, and strategic technology firms across South, Southeast, and East Asia.

Background

Trend Micro researchers identified a large-scale cyberespionage campaign attributed to the intrusion set referred to as SHADOW-EARTH-053, a China-aligned threat cluster targeting governments and strategic organizations throughout Asia. The operation demonstrates continued operational reliance on internet-facing Microsoft Exchange and IIS infrastructure as initial access vectors, despite the vulnerabilities involved being publicly disclosed and patched years earlier.

The campaign primarily leveraged the ProxyLogon exploit chain affecting Microsoft Exchange Server, including CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. Following successful exploitation, operators deployed GODZILLA web shells into Exchange and IIS directories to establish persistent remote access. The continued success of ProxyLogon exploitation underscores a broader issue affecting enterprise environments globally: internet-facing Exchange infrastructure remains a highly targeted enterprise attack surface for espionage-focused threat actors. While the vulnerabilities themselves are years old, many organizations continue operating legacy or poorly maintained Exchange environments due to operational constraints, delayed migration strategies, compatibility concerns, or limited security resources.

For espionage-focused operators such as SHADOW-EARTH-053, Exchange servers provide exceptionally valuable access. Successful compromise enables direct access to email communications, credential material, authentication flows, internal infrastructure mapping opportunities, and privileged administrative accounts. In many environments, Exchange servers also function as trusted internal systems with extensive connectivity to Active Directory and critical enterprise infrastructure, making them ideal pivot points for long-term intelligence collection operations.

Web Shell Persistence and Exchange Abuse

After initial exploitation, SHADOW-EARTH-053 established persistence using multiple ASPX and ASHX web shells. The use of Exchange OWA authentication paths remains a common tactic among Exchange-focused espionage actors because these directories already contain large volumes of legitimate ASPX content, making malicious files more difficult to identify during routine administrative review. Researchers also observed the use of an .ashx HTTP handler, representing a slight deviation from the more traditional .aspxweb shells often associated with earlier Chinese intrusion activity. This small adjustment may help evade simplistic detection logic focused specifically on ASPX file creation. In one observed intrusion, operators leveraged AnyDesk to deploy ShadowPad components, suggesting either previously obtained credentials, preexisting access, or secondary-stage operational expansion following initial compromise.

ShadowPad Deployment and DLL Sideloaded Operations

Once access was established, SHADOW-EARTH-053 deployed ShadowPad, a modular malware family historically associated with multiple China-aligned intrusion sets, including [APT41](#). The group relied heavily on DLL sideloading techniques involving signed legitimate executables. These chains allowed the attackers to abuse trusted applications to execute malicious DLL payloads while reducing the likelihood of detection.

Observed sideloading chains abused several legitimate binaries, including:

- GameHook.exe
- imecmnt.exe
- xReport.exe
- LUManager.EXE

These binaries loaded malicious DLLs. In observed sideloading chains, the malicious DLLs decrypted and launched ShadowPad payloads stored within the Windows Registry before deleting the payload after initial execution. This approach significantly complicates forensic recovery and reduces the likelihood of traditional file-based antivirus detection.

Researchers noted that the ShadowPad variant used by SHADOW-EARTH-053 lacked some of the advanced obfuscation and anti-analysis functionality observed in more modern variants deployed by other Chinese intrusion groups. This may suggest the operators only possess access to an older ShadowPad builder rather than the malware source code itself.

TosBtKbd.dll Loader and Registry-Staged Payloads

One of the more notable techniques observed during the campaign involved a Toshiba Bluetooth Stack sideloading chain using a renamed executable, CIATosBtKbd.exe, and a malicious DLL named TosBtKbd.dll. The loader retrieved shellcode from machine-specific registry keys located under:

```
HKEY_CURRENT_USER\Software\[ComputerName]
```

The malware then allocated executable memory using VirtualAlloc with PAGE_EXECUTE_READWRITE permissions before triggering shellcode execution through EnumDesktopsA callback injection. This technique allowed the malware to execute code indirectly through legitimate Windows API behavior rather than through overt execution functions that may be more heavily monitored by EDR solutions.

Persistence was achieved through a scheduled task named “M1onltor,” configured to execute every five minutes with elevated privileges. The use of registry-resident payload storage combined with callback execution reflects an emphasis on stealth, reduced forensic visibility, and defense evasion rather than large-scale destructive activity.

Reconnaissance, Credential Theft, and Active Directory Enumeration

Following compromise, SHADOW-EARTH-053 conducted extensive internal reconnaissance operations directly through compromised IIS worker processes. Observed activity included domain controller discovery, domain admin group enumeration, internal Exchange server discovery, LDAP enumeration, Active Directory exports using csvde.exe, PowerView-based user enumeration, and nslookup queries against internal Exchange systems.

Researchers also identified a lightweight custom binary named DomainMachines.exe used to enumerate hosts and scan common enterprise ports associated with SMB, RDP, WinRM, SQL services, Kerberos, and web infrastructure. Credential access operations relied heavily on well-established offensive tooling including Mimikatz, Evil-CreateDump, newdcsync, and Sharp-SMBExec.

Mimikatz execution occurred directly through rundll32.exe with sekurlsa::logonpasswords and lsadump::sam commands used for credential extraction and SAM database dumping. Notably, these tools were executed by w3wp.exe, directly tying credential theft activity to web-shell-

driven command execution through IIS worker processes. The group also leveraged Evil-CreateDump, likely a modified version of Microsoft's create-dump.exe utility, to dump LSASS memory for credential harvesting.

Tunneling Infrastructure and Covert Communications

SHADOW-EARTH-053 deployed multiple tunneling frameworks simultaneously within victim environments, demonstrating a layered approach to maintaining covert outbound communications. Observed tooling included IOX Proxy, GOST, Wstunnel, and multiple tunnel-core.exe variants. These tools established SOCKS5 proxies, HTTPS tunnels, and reverse communication channels to attacker infrastructure.

The use of multiple tunneling mechanisms against the same infrastructure suggests deliberate operational redundancy. Even if defenders detect and disrupt one tunnel, alternate communication channels may remain active, allowing operators to maintain persistence within compromised environments. Researchers also observed attackers disguising legitimate Windows binaries by renaming net.exe and powershell.exe using randomized .log filenames within ProgramData directories. This tactic attempts to evade simplistic security tooling that relies heavily on process-name-based detection rather than binary validation or behavioral analysis.

Lateral Movement and Exchange Infrastructure Expansion

SHADOW-EARTH-053 leveraged WMIC, Sharp-SMBExec, and custom RDP tooling for lateral movement across victim networks. One particularly notable technique involved propagating malicious web shells across additional internal Exchange servers by copying ASPX files directly through administrative SMB shares. This allowed the operators to rapidly expand access across Exchange infrastructure while minimizing the need for additional malware deployment or exploit activity.

Researchers also documented the use of Exchange management snap-ins and a custom "ExchangeExport" utility leveraging Exchange Web Services (EWS) APIs to export mailbox content belonging to high-profile individuals. In one instance, attackers created password-protected RAR archives containing PST mailbox data associated with executive personnel within targeted organizations. The operational focus on mailbox extraction strongly reinforces the espionage-oriented nature of the campaign.

Victimology

Victimology analysis revealed a strong concentration on government entities and defense-adjacent organizations across South, Southeast, and East Asia. Observed target countries

included Pakistan, Thailand, Malaysia, India, Myanmar, Sri Lanka, and Taiwan. Researchers also identified at least one victim organization within Poland, extending the campaign footprint into a NATO member state. Verticals targeted included government IT contractors, Ministry of Defense suppliers, transportation organizations, and technology consulting firms. Researchers also noted activity suggesting a possible defense-related supply chain intrusion scenario involving a technology customer connected to a Southeast Asian Ministry of Defense.

Operational Overlap

Nearly half of SHADOW-EARTH-053 victims were also targeted by the related intrusion cluster SHADOW-EARTH-054. Researchers identified overlap in:

- Initial access vectors
- Web shell deployment
- IOX Proxy usage
- Evil-CreateDump hashes
- Victim geography
- Operational infrastructure

However, investigators assessed that the overlap likely reflected independent exploitation of the same vulnerable infrastructure rather than coordinated operational activity between the groups. The researchers described this pattern as “Type A collaboration,” where separate intrusion sets exploit the same exposed environments using similar tradecraft and shared tooling ecosystems without necessarily operating together directly. This finding highlights the increasingly interconnected and overlapping nature of modern state-aligned cyber ecosystems, particularly among China-aligned operators sharing malware frameworks, infrastructure patterns, and operational tooling.

Analyst Commentary

SHADOW-EARTH-053 reinforces several long-standing realities about modern cyberespionage operations that defenders continue to struggle with operationally.

First, legacy Microsoft Exchange infrastructure remains a highly targeted enterprise attack surface for espionage-focused threat actors. The continued operational success of ProxyLogon exploitation years after disclosure demonstrates that patch publication alone does not meaningfully eliminate risk. Threat actors understand that many organizations, particularly government and critical infrastructure entities, operate complex environments where patch cycles are slow, fragmented, or operationally constrained. Those conditions

create long-tail exploitation opportunities that remain strategically valuable well beyond initial disclosure windows.

Second, the campaign suggests modern espionage operations increasingly prioritize operational resilience and stealth over highly customized malware development in every stage of the intrusion lifecycle. SHADOW-EARTH-053 relied on a combination of stealth-focused techniques such as registry-resident payload staging, callback execution, and DLL sideloading alongside openly available tunneling tools and publicly documented offensive utilities. This blended tradecraft approach allows operators to reduce development overhead while maintaining flexible and resilient post-compromise capabilities.

Third, the operational overlap between SHADOW-EARTH-053 and SHADOW-EARTH-054 highlights the growing complexity of attribution and intrusion clustering within China-aligned ecosystems. Shared malware families, overlapping infrastructure, reused operational tooling, and repeated exploitation of the same targets make strict attribution increasingly difficult. Defenders should avoid relying solely on actor-name-centric tracking and instead prioritize behavioral visibility, infrastructure telemetry, and operational tradecraft analysis.

From a defensive standpoint, this campaign further reinforces the importance of behavioral detection capabilities over signature-dependent approaches. Many of the techniques observed throughout the operation, including renamed binaries, DLL sideloading, web-shell-driven command execution through IIS worker processes, registry-staged payloads, and legitimate administrative tooling abuse, are specifically designed to blend into normal enterprise operations and bypass simplistic detection logic.

For organizations operating internet-facing infrastructure, particularly Exchange and IIS environments, visibility into process execution chains, outbound network communications, web shell deployment activity, and anomalous child processes spawned by w3wp.exe remains critical.

PolySwarm analysts assess that campaigns such as SHADOW-EARTH-053 further demonstrate why layered malware analysis and multi-engine behavioral visibility remain operationally important for modern enterprise defense. Threat actors increasingly rely on modified loaders, signed binaries, lightweight custom tooling, and low-prevalence malware variants specifically designed to reduce consensus detection rates across traditional security stacks.

PolySwarm's marketplace of specialized micro-engines provides multiple independent analysis perspectives on suspicious files and payloads, helping defenders identify emerging or low-consensus threats that may evade single-engine detection approaches. By aggregating results into a unified PolyScore alongside behavioral metadata, sandbox telemetry, and

malware family classifications, defenders can gain earlier visibility into suspicious artifacts associated with campaigns leveraging stealth-focused tradecraft such as ShadowPad sideloading chains and registry-resident payload delivery mechanisms.

As state-aligned intrusion sets continue targeting exposed enterprise infrastructure with persistent operational tradecraft, organizations should prioritize layered visibility, rapid patch management, proactive threat hunting, and behavioral telemetry analysis capable of identifying malicious activity, even when attackers abuse legitimate binaries and trusted enterprise applications.

IOCs

PolySwarm has multiple samples associated with this activity.

a65483b86847995a67de0fcb2a5487cd9c96361cb2e9dea8ab74005c8fef65ce
5bf35daaf26508fc136157818ead48cc5c7fa3a3e6273cde2c757673586a78a6
41f74c3fc32752b5c7b88e7a5723441cb827958bc21b647ffae469407f1ce99
f19a67b9c8805b335676f0fc17495839327f8135f791aa11d5d9adba2c83cc1c
0c63857269205f6505c259a56ea53b23b2bf7432aabb8647d59b321232ca7e36
97ea803792929f802388e9d0e75a3c79c28260d589bc2d87902c73c729ed6f9e
0eb72c1f1605d999488d903021d82a9ff4b937e6c1a1da50c55440f018e83ad9
884601e54fc2e6833167d33436b68e952020cdb99507b2807feec1bc086027c2
e12c2682a7949661fa99bf46723a1405c658d109411de3bf6cb04c57337cc020
23c2ebc8f9bac96b2fbbb9b00b457c48d65a9f66ec24fbfba339eeefd0539ad7
c935ded2729f0513672e261170d73d4e0e13a9b837f104d840c44a39b84c0d71
188c72b101cd8ad96ef971e8943bddb3acd9dc45fe1d8719217d171e600a29aa
9dda789b85fce6294f91a79b7271a93de36dfcef21fc680dc2bf4235141e47df

Don't have a PolySwarm account? Go [here](#) to sign up for a free Community plan or subscribe.

Contact us at hivemind@polyswarm.io | Check out our [blog](#) | [Subscribe](#) to our reports.

Topics: Threat Bulletin, APT41, ShadowPad, Cybersecurity, government targeting, CyberEspionage, ChinaAPT, ExchangeServer, ProxyLogon, ThreatIntelligence, ShadowEarth053