

# Daxin Returns: Stealthy Malware Resurfaces in Taiwan Alongside a New Backdoor

By About the Author

Archived: 2026-07-17 02:01:42 UTC

## Key findings

- Backdoor.Daxin, the China-linked kernel-mode rootkit that Symantec first uncovered and exposed in 2022, is still operational. It was found running on a compromised host in Taiwan in 2026, more than four years after it was first uncovered.
- On the same machine, the Symantec Threat Hunter Team discovered a previously unknown backdoor, Backdoor.Stupig, whose novel tradecraft may link it to the Daxin operation, though no code-level connection has been confirmed.
- Stupig uses a technique not documented in any known malware family. A Trojanized keyboard-layout DLL loaded by winlogon.exe lets an attacker run commands as System directly from the Windows logon screen, before anyone signs in and without raising a logon audit event.
- Both samples carry compile timestamps from early 2013, but the host was not reporting telemetry until May 2026. Combined with the actor's known pattern of long-term, stealthy persistence, this suggests the intrusion may have gone undetected on the network for 13 years.
- The victim was a Taiwan-based subsidiary of a multinational high-tech manufacturer.

## Overview

More than four years after Symantec first uncovered Backdoor.Daxin, the malware has resurfaced. Symantec's Threat Hunter Team uncovered Daxin in active use on a compromised host in Taiwan in May 2026, long after the tool was last found.

Alongside it, our researchers found a previously undocumented backdoor (Backdoor.Stupig) that uses a technically distinctive approach to persistence and pre-authentication code execution. No code-level relationship between the two tools has been established. However, their co-deployment on the same host, complementary functions, and similarities in development practices suggest a link. The two samples also carry compile timestamps a few weeks apart in early 2013. While such timestamps can be edited, it is more likely that both samples were created within a short window of one another, which would be consistent with their use by the same actor.

## Background: Backdoor.Daxin

Daxin is a Windows kernel-mode driver backdoor that Symantec first [uncovered and publicly documented in early 2022](#), though samples have been traced as far back as 2013. At the time, Symantec assessed Daxin as the most advanced piece of malware it had seen used by a China-linked actor. Its defining characteristic is its approach to

command and control. Rather than establishing its own outbound connections, the driver monitors incoming TCP traffic for specific patterns and hijacks existing legitimate connections to carry encrypted command-and-control (C&C) traffic. This made Daxin exceptionally difficult to identify with conventional network monitoring. The malware also supported multi-hop communications through chains of infected hosts, allowing operators to reach systems on isolated network segments. Symantec attributed Daxin to a China-linked espionage group that conducted long-running espionage campaigns against select governments and other targets of strategic interest to China.

## 2026 activity

The recent malicious activity was uncovered in May 2026. The compromised host had no telemetry on record before May 12, 2026, indicating that it had not been reporting data previously. As a result, both samples could have been present on the host, or elsewhere on the network, for a considerable period before they became visible. The age of the tools, which carry compile timestamps dating to 2013, suggest the compromise may have been underway for years before it came to light.

The most likely initial access vector was an outdated version of the Digiwin single sign-on portal, which was still using Java Development Kit (JDK) 1.5 and 1.6 installations dating from 2009 to 2011. Both JDK versions are long past end-of-life, reaching that status in 2009 and 2013 respectively.

Two tools were identified:

- **Backdoor.Daxin** (srt64.sys): A kernel-mode driver installed in %SystemRoot%\System32\drivers. The driver was digitally signed, which would help it pass Windows driver-signature checks. The backdoor was identical to the one documented in our 2022 report, and its compile and signing timestamps date to January 2013.
- **Backdoor.Stupig** (a.dll / kbdus1.dll): A previously unknown backdoor, documented below. It was deployed in the Windows directory as a.dll. It was later detected in the System32 directory, renamed kbdus1.dll. Its compile timestamp dates to February 2013.

## Operational security adjustment?

The reappearance of Stupig, renamed from a.dll to kbdus1.dll, in the system directory, appears to have been triggered by the first detection event on a.dll on May 28, 2026. On June 1, the renamed malware (kbdus1.dll) was detected in the System32 directory. The new filename was constructed to closely resemble the legitimate Windows keyboard-layout library kbdus.dll, which provides U.S. English keyboard input and resides in the same directory. Placing the file there under a name that differed by a single appended character was designed to pass casual visual inspection and evade filename-based detection controls.

When the renamed version of Stupig was placed in the System32 directory remains unknown. The attackers may have installed it after the first version (a.dll) was detected on May 28, although no evidence of this was found. Alternatively, the attackers may have installed it as a redundant backdoor at the time of the original infection and it only became active after the primary backdoor was detected and removed.

## Backdoor.Stupig

Backdoor.Stupig is a DLL backdoor that achieves persistence by registering as a keyboard-layout provider, causing win32k.sys to load it into winlogon.exe at system startup. The DLL returns a valid KBDTABLES pointer so the keyboard layout functions normally, giving nothing away to any process or administrator inspecting the loaded module. This persistence mechanism is related to the Winlogon Helper DLL technique described in MITRE ATT&CK T1547.004 but uses a different registry loading path, one not previously documented in known malware families.

Once running inside winlogon.exe, the backdoor monitors the Windows logon screen for usernames beginning with the string: stupig. When such a username is entered, any string following the prefix is executed as SYSTEM on the secure desktop (Winsta0\Winlogon). If nothing follows the prefix, a command prompt running as SYSTEM is spawned directly on the logon screen. The real LsaLogonUser is then called unchanged, causing the system to return a standard failed-logon response. No audit event anomaly is generated beyond a failed logon entry for an unusual username.

The malware also installed inline hooks on SspiCli!LsaLogonUser and Advapi32!CredUnprotectA via VirtualProtect, ZwAllocateVirtualMemory and memcpy, enabling credential interception within the winlogon.exe process. A call to LoadLibraryA("msyun.dll") referenced a companion payload that was not present in the artifacts recovered during this investigation.

Stupig has not been identified in any prior public reporting and did not match any known malware family in similarity analysis. While we did not identify a specific connection between the Daxin driver and Stupig in our analysis, there is evidence to suggest that the two pieces of malware were created by the same group. In addition to the compilation timestamps dating from 2013, both shared similarities in development practices, suggesting that Stupig's author was familiar with Daxin's source code.

## Targeting

The victim was a Taiwan-based subsidiary of a multinational high-tech manufacturer. While previous victims of Daxin were governments, the common thread is that all targets appear to be of strategic interest to China. Our 2022 investigation documented use of the tool against government, telecommunications, transportation, and manufacturing targets. Taiwan's advanced manufacturing base has been the focus of sustained Chinese intrusion activity across multiple reported campaigns.

## Significance

Daxin stands out for tradecraft most actors never attempt. Instead of calling out to a command-and-control server, it hijacks legitimate inbound network traffic, making its communications very hard to detect, and it can relay commands across chains of infected machines to reach systems with no direct internet access. Finding it active in 2026 indicates the operation behind it never went away; it went quiet. Because the Daxin actor is known for maintaining long-term, stealthy persistence in targeted networks, and because this host only became visible in May 2026, it is plausible that the actor had maintained access to this network for a very long period, potentially more than a decade.

If linked to the same actor, the Stupig backdoor adds a further capability. By hiding inside the Windows logon process and registering as a keyboard-layout provider, Stupig gives operators SYSTEM-level command execution and credential theft before a user signs in, an access method most defenders are not aware of nor watching for. Whether the same operators deployed both tools cannot be confirmed, but their functions are complementary.

## Protection

For the latest protection updates, please visit the [Symantec Protection Bulletin](#).

Symantec products detect the activity described in this blog using the following definitions:

- Backdoor.Daxin
- Backdoor.Stupig

## Indicators of Compromise

### File indicators

49c827cf48efb122a9d6fd87b426482b7496ccd4a2dbca31ebbf6b2b80c98530 – srt64.sys (Backdoor.Daxin)

5bb5cffda4647940919a185df37aab2aef71ca3010a6c1d05bdcc8bc8fb3af3f – a.dll / kbdus1.dll (Backdoor.Stupig)

---

Source: <https://www.security.com/threat-intelligence/daxin-returns-stupig>