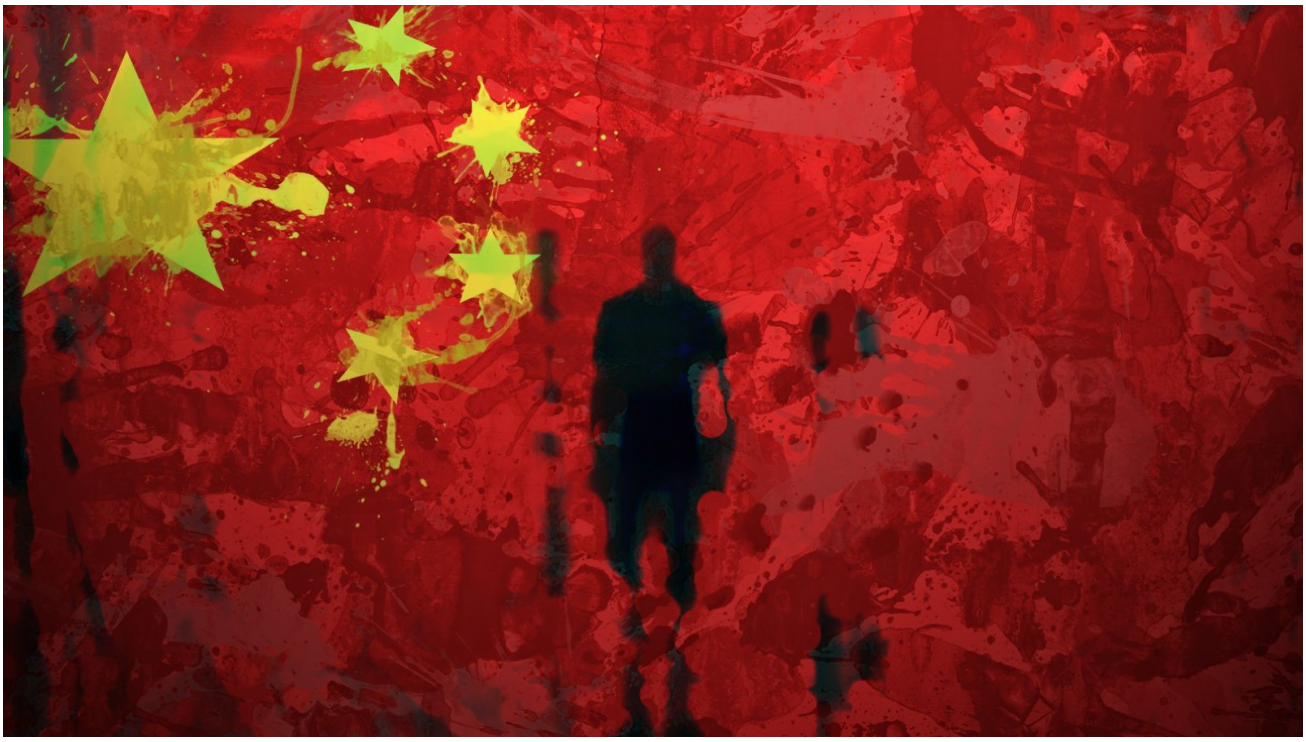
Chinese cyberspies target govts with their ‘most advanced’ backdoor

bleepingcomputer.com/news/security/chinese-cyberspies-target-govts-with-their-most-advanced-backdoor/

Bill Toulas

By
Bill Toulas

- February 28, 2022
- 02:32 PM
- 0



Security researchers have discovered Daxin, a China-linked stealthy backdoor specifically designed for deployment in hardened corporate networks that feature advanced threat detection capabilities.

According to a technical report published by Symantec's Threat Hunter team today, Daxin is one of the most advanced backdoors ever seen deployed by Chinese actors.

One point of differentiation in Daxin is its form, which is a Windows kernel driver, an atypical choice in the malware landscape. Its stealthiness comes from its advanced communication features, which mix its data exchange with regular internet traffic.

"Daxin is, without doubt, the most advanced piece of malware Symantec researchers have seen used by a China-linked actor," Symantec said in a new report.

"Considering its capabilities and the nature of its deployed attacks, Daxin appears to be optimized for use against hardened targets, allowing the attackers to burrow deep into a target’s network and exfiltrate data without raising suspicions."

Hiding in legitimate network traffic

Backdoors provide threat actors with remote access to a compromised computer system, allowing them to steal data, execute commands, or download and install further malware.

Because these tools are typically used to steal information from protected networks or further compromise a device, they need to involve some form of data transfer encryption or obfuscation to evade raising alarms on network traffic monitoring tools.

Daxin does this by monitoring network traffic on a device for specific patterns. Once these patterns are detected, it will hijack the legitimate TCP connection and use it to communicate with the command and control server.

By hijacking TCP communications, the Daxin malware can hide malicious communication in what is perceived as legitimate traffic and thus remain undetected.

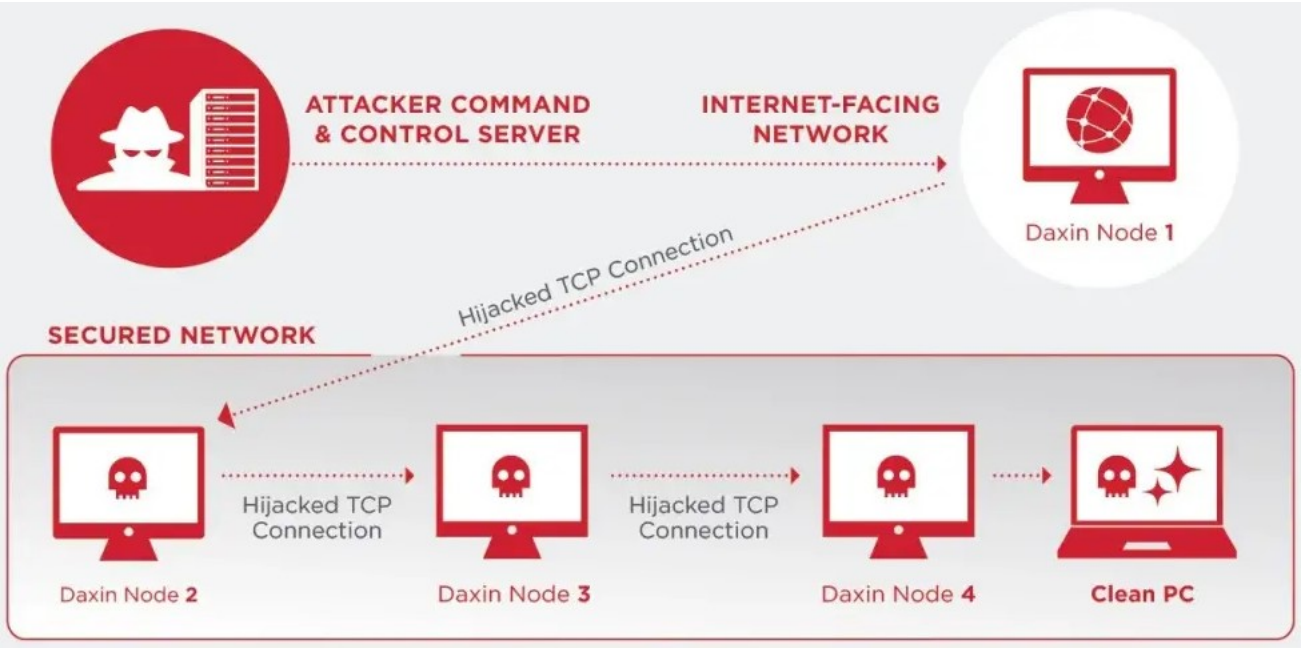
"Daxin's use of hijacked TCP connections affords a high degree of stealth to its communications and helps to establish connectivity on networks with strict firewall rules. It may also lower the risk of discovery by SOC analysts monitoring for network anomalies," explains the report by Symantec.

This essentially opens an encrypted communication channel for transmitting or stealing data, all done through a seemingly innocuous TCP tunnel.

"Daxin's built-in functionality can be augmented by deploying additional components on the infected computer. Daxin provides a dedicated communication mechanism for such components by implementing a device named \\.\Tcp4," further explained Symantec.

"The malicious components can open this device to register themselves for communication. Each of the components can associate a 32-bit service identifier with the opened \\.\Tcp4 handle. The remote attacker is then able to communicate with selected components by specifying a matching service identified when sending messages of a certain type."

Daxin also stands out due to its capability to establish intricate communication pathways across multiple infected computers at once, using a single command to a set of nodes.



Daxin establishing communication channels on compromised networks *(Symantec)*

This allows the threat actors to quickly re-establish connections and encrypted communication channels in well-guarded networks.

At the same time, while the nodes are active and serve as relay points, the chances of the malicious traffic being marked as suspicious are kept at a minimum.

Chinese cyber-espionage

Symantec's threat analysts have found evidence linking Daxin to the Chinese state-backed hacking group Slug (aka Owlproxy).

Reportedly, the particular backdoor has been actively used in attacks since at least November 2019, while researchers spotted signs of its deployment again in May 2020 and July 2020.

The most recent attacks involving Daxin were observed in November 2021, targeting telecommunication, transportation, and manufacturing companies.

It's worth noting that Symantec claims the malware was first sampled back in 2013, already featuring the advanced detection-avoidance techniques that we see in today's version.

However, no attacks that involved Daxin were observed until later, even though it's likely that the stealthy hackers simply remained undetected until 2019.

Related Articles:

BPFDoor: Stealthy Linux malware bypasses firewalls for remote access

Chinese hackers abuse VLC Media Player to launch malware loader

Backdoor baked into premium school management plugin for WordPress

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

- Backdoor
- China
- Daxin
- Malware

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: