Backdoor.Daxin

Threat: **Advanced Persistent Threat**

Author: **Jeffrey Farnan** Date Originally Published: **March 31th, 2022**

1. SUMMARY

- Backdoor.Daxin malware is an advanced persistent threat found by the Symantec Threat Hunter team in November 2021. They said it's the most advanced piece of malware coming from China linked actors exhibiting technical complexity previously unseen. It uses an unusual communication system that enables remote attackers to use multiple infected machines on a network as hops to disguise traffic. The malware is specifically tailored for use against well-defended networks and has been used against several types of targets, including military organizations, government agencies, critical infrastructure operators, and others.

2. MALWARE FAMILY

- **Type** = APT.
- **Sub-type** = Rootkit / Backdoor / Espionage Tool.

- Backdoor.Daxin malware is an advanced persistent threat (APT) which uses sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time. It disguises itself as a malicious Windows kernel driver to gain access to the system. The primary function of Daxin malware is a backdoor, to communicate with the attackers and to allow for further malicious software to be installed. This backdoor appears to be used in a long-running espionage campaign against select governments and other critical infrastructure targets.

3. MALWARE CHARATERISTICS

- **Suspected country of origin** = China.
- **First seen date/period** = In China: 2013. Western countries: November: 2021.
- **Still active** = Yes.
- **Last submitted sample as of writing this article** = February, 2022.

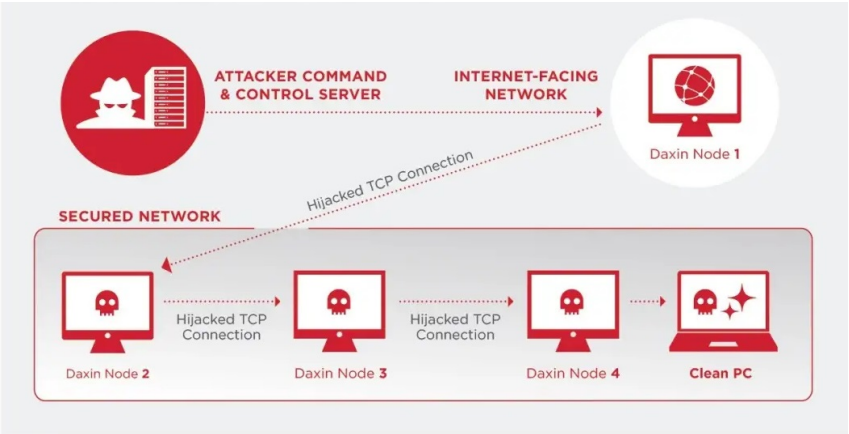
4. MALWARE HISTORY

Backdoor.Daxin seems to have many of the capabilities and command-and-control features which are reminiscent of Regin, an advanced espionage tool believed to been develop by the RSA for spying on other countries. Although western security researchers only recently discovered Daxin it may have been circulating in China for some time, since around 2013 and may have been in continuous development. There have been attacks on Chinese IT companies in the past few years:

- In November 2019 an attack which made use of Daxin against an unnamed IT company, they also used a backdoor tool called Owlproxy.
- In May 2020 Daxin and Owlproxy were discovered on a single computer in another tech company.
- In July 2020 a failed attack was made against a military target involving two attempts to install a suspicious driver making it similar behaviour to Daxin.

5. MALWARE DESCRIPTION

- Backdoor.Daxin is developed with the goal of cyberespionage with a level of technical complexity previously unseen from these threat actors before. Daxin comes in the form of a Windows kernel driver which is a rare format for malware nowadays. The malware allows the attacker to perform various communications and data-gathering operations on the infected computer.
- **Backdoor:** Daxin is a backdoor that allows the attacker to perform operations such as reading and writing arbitrary files and can also start arbitrary processes and interact with them.
- **Communication:** Daxin's capabilities suggest the attackers invested significant effort into developing communication techniques that can blend in unseen with normal network traffic on the target's network. It does this by not starting its own network services but abusing any legitimate services already running on the infected computers.
    - **Stealth:** It communicates without been noticed, by hijacking TCP / IP sessions. It does this by monitoring traffic, searching for certain patterns and disconnecting the original recipient. This method allows Daxin to avoid strict firewall rules by hijacking legitimate traffic, and it also minimizes the chance that security teams notice any network anomalies.



    - Daxin can also encapsulate raw network packets in such a way that any response packets sent are forwarded to the attacker, allowing them to communicate with legitimate services on the infected machine's network.

- Daxin has the ability to make hops across multiple infected nodes with just a single command. Hopping around a compromised network is typical, but not with a single action, most attackers get from node to node one command at a time.

6. POTENTIAL CUSTOMER DEFENSE

The people who are controlling Backdoor.Daxin are highly skilled hackers who are hacking into high value targets with well-defended networks. Governments and large organisations such as telecommunications, transportation and manufacturing sectors can defend against this type of attack by the following these security measures:

- All security products should be kept updated and security patches need to be applied on all end devices.
- Ensure care is taken when downloading any documents that it comes from a legitimate source.
- Ensure Endpoint protection and Antivirus and Anti Malware should be configured and with hardening on all end nodes.
- Web proxy should be implemented.
- NextGen Firewalls should be implemented with firmware and malicious signature detection.
- Configure Outbound and Inbound rules on web and application server and ports need to be filtered via a firewall.
- Data-Loss Prevention (DLP) needs to be implemented on end devices.
- Implement of Web Application firewall (WAF) with strong security policies.

Research Sources:

- https://duo.com/decipher/china-linked-group-using-new-daxin-backdoor
- https://www.securityweek.com/symantec-super-stealthy-daxin-backdoor-linked-chinese-threat-actor
- https://usa.kaspersky.com/resource-center/threats/regin-platform-malware
- https://cybersrcc.com/2022/03/04/daxin-malware-new-espionage-backdoor/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/daxin-backdoor-espionage