Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 264

ACG-CSB 090622264

Reference Number ACG-CSB 090622264

Understanding the Risk of Daxin Malware

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as **"Restricted"** pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

Daxin is a backdoor malware that allows its controller to install further malicious software, has network tunneling capabilities, can relay communications across infected nodes, is able to hijack legitimate Transmission Control Protocol (TCP)/Internet Protocol (IP) connections and is otherwise an incredibly complex piece of code. It allows the attacker to perform various operations on the infected computer such as reading and writing arbitrary files.

Daxin malware is a highly sophisticated rootkit backdoor with complex, stealthy command and control (C2) functionality that enabled remote actors to communicate with secured devices not connected directly to the internet. Daxin appears to be optimized for use against hardened targets, allowing the actors to deeply burrow into targeted networks and exfiltrate data without raising suspicions.

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. Specifically, the malware avoids starting its own network services. Instead, it can abuse any legitimate services already running on the infected computers.

Among the unusual aspects of Daxin, besides generating no suspicious network traffic to remain unseen, the malware can be both the initiator and the target of a key exchange. The ability to relay commands across a network of infected computers within the attacked organization, creating a multi-node communications channel that permits recurring access to the compromised computers for extended periods of time. 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.

Daxin comes in the form of a Windows kernel driver, it excels at using a single external command to jump from one breached system to another within the network. To remain unnoticed, Daxin does not open any new network services or attempt communications

that could seem suspicious. Instead, it hijacks legitimate TCP/IP services, while listening for specific traffic patterns that it can recognize as a valid command and it implements advanced communications functionality, which both provides a high degree of stealth and permits the attackers to communicate with infected computers on highly secured networks, where direct internet connectivity is not available. It may also lower the risk of discovery by Security Operations Center (SOC) analyst monitoring for network anomalies.

Daxin is a backdoor implant that provides the attackers with the ability to conduct various intrusive actions on the infected devices. However, the apparent goal of the attackers is data-gathering. The chosen targets are carefully selected from a range of different industries and sectors, including telecommunications, transportation, and manufacturing. Government organizations also have been targeted with Daxin.

Daxin has one of the most complex features observed in China-linked malware campaigns. There is an immediate need to adopt a dynamic approach to security, along with continuous assessment and updates in existing security measures. Organizations are suggested to make use of Indicator of Compromise (IOCs) that may help in the detection of malicious activity.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow these tips to avoid being a victim of Daxin Malware attack:

- Use strong passwords and secure two-factor authentication;
- Implement email security and spam protection;
- Implement edge micro-segmentation;
- Activate and manage your alerts;
- Install anti-virus and anti-spyware software; and
- Limit application privileges.

For additional information, please refer to the following websites:

- https://www.techrepublic.com/article/daxin-a-chinese-linked-malware-that-is-dangerous-and-nearly-impossible-to-detect/
- https://www.cisa.gov/uscert/ncas/current-activity/2022/02/28/broadcom-software-discloses-apt-actors-deploying-daxin-malware
- https://thehackernews.com/2022/03/china-linked-daxin-malware-targeted.html

POINT OF CONTACT

Please contact **PMAJ JUN-JUN S DAGURO,** Police Community Relations Officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 723-0401 local 7483 for any inquiries related to this CYBER SECURITY BULLETIN.