Palmerworm: Espionage Gang Targets the Media, Finance, and Other Sectors

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/palmerworm-blacktech-espionage-apt

The Threat Hunter Team at Symantec, a division of Broadcom (NASDAQ: AVGO), has uncovered a new espionage campaign carried out by the Palmerworm group (aka BlackTech) involving a brand new suite of custom malware, targeting organizations in Japan, Taiwan, the U.S., and China.

The attacks occurred in 2019 and continued into 2020, targeting organizations in the media, construction, engineering, electronics, and finance sectors. We observed the group using previously unseen malware in these attacks.

Palmerworm uses a combination of custom malware, dual use tools, and living-off-the-land tactics in this campaign. Palmerworm has been active since at least 2013, with the first activity seen in this campaign in August 2019.

Tactics, Tools, and Procedures

Palmerworm was observed using both dual-use tools and custom malware in these attacks.

Among the custom malware families we saw it use were:

- Backdoor.Consock
- Backdoor.Waship

- Backdoor.Dalwit
- Backdoor.Nomri

We have not observed the group using these malware families in previous attacks – they may be newly developed tools, or the evolution of older Palmerworm tools. Malware used by Palmerworm in the past has included:

- Backdoor.Kivars
- Backdoor.Pled

While the custom malware used by the group in this campaign is previously undocumented, other elements of the attack bear similarities to past Palmerworm campaigns, making us reasonably confident that it is the same group carrying out this campaign.

As well as the four backdoors mentioned, we also see the group using a custom loader and a network reconnaissance tool, which Symantec detects as Trojan Horse and Hacktool. The group also used several dual-use tools, including:

- **Putty** – can be leveraged by attackers for remote access, to exfiltrate data and send it back to attackers
- **PSExec** – is a legitimate Microsoft tool that can be exploited by malicious actors and used for lateral movement across victim networks
- **SNScan** – this tool can be used for network reconnaissance, to find other potential targets on victim networks
- **WinRAR** – is an archiving tool that can be used to compress files (potentially to make them easier to send back to attackers) and also to extract files from zipped folders

All these dual-use tools are commonly exploited by malicious actors like Palmerworm, with advanced persistent threat (APT) groups like this increasingly using living-off-the-land tactics, including the use of dual-use tools, in recent years. These tools provide attackers with a good degree of access to victim systems without the need to create complicated custom malware that can more easily be linked back to a specific group.

In this campaign, Palmerworm is also using stolen code-signing certificates to sign its payloads, which makes the payloads appear more legitimate and therefore more difficult for security software to detect. Palmerworm has been publicly documented using stolen code-signing certificates in previous attack campaigns.

We did not see what infection vector Palmerworm used to gain initial access to victim networks in this campaign, however, in the past the group has been documented as using spear-phishing emails to gain access to victim networks.

Victims

Symantec identified multiple victims in this campaign, in a number of industries, including media, construction, engineering, electronics, and finance. The media, electronics, and finance companies were all based in Taiwan, the engineering company was based in Japan, and the construction company in China. It is evident Palmerworm has a strong interest in companies in this region of East Asia.

We also observed Palmerworm activity on some victims in the U.S., however, we were unable to identify the sector of the companies targeted.

Palmerworm activity was first spotted in this campaign in August 2019, when activity was seen on the network of a Taiwanese media company and a construction company in China. The group remained active on the network of the media company for a year, with activity on some machines there seen as recently as August 2020.

Palmerworm also maintained a presence on the networks of a construction and a finance company for several months. However, it spent only a couple of days on the network of a Japanese engineering company in September 2019, and a couple of weeks on the network of an electronics company in March 2020. It spent approximately six months on one of the U.S.-based machines on which we observed activity.