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

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

Symantec Enterprise Blogs
Threat Intelligence

Posted: 29 Sep, 20204 Min ReadThreat Intelligence
Translation: 日本語

Companies in Japan, Taiwan, U.S., and China among victims.

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.

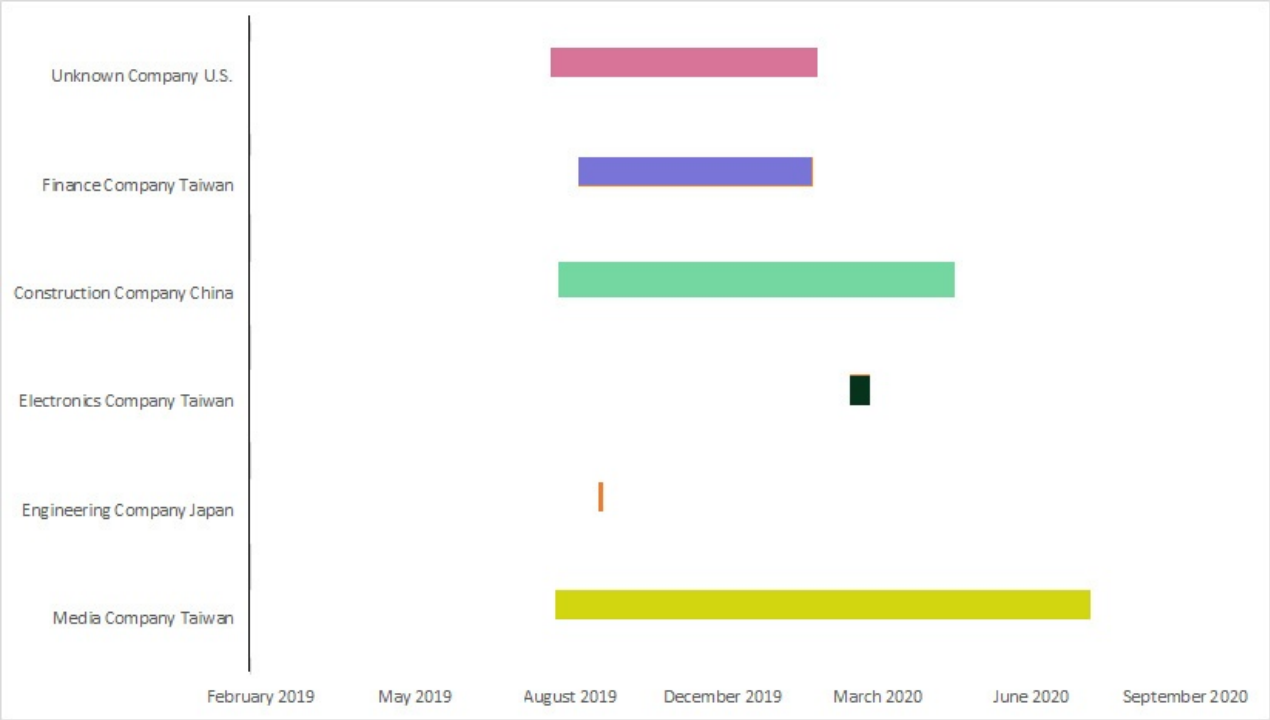

Figure. The amount of time Palmerworm spent on the networks of companies in the different sectors varied from a year to just a few days

The finance, media, and construction industries, then, appear to be of the biggest interest to Palmerworm in this campaign. There have been reports previously of Palmerworm targeting the media sector.

What do the attackers want?

While we cannot see what Palmerworm is exfiltrating from these victims, the group is considered an espionage group and its likely motivation is considered to be stealing information from targeted companies.

How do we know this is Palmerworm?

While the custom malware used in this attack is not malware we have seen used by Palmerworm before, some of the samples identified in this research are detected by other vendors as PLEAD, which is a known Palmerworm (aka Blacktech) malware family. We also saw the use of infrastructure that has previously been attributed to Palmerworm.

The group's use of dual-use tools has also been seen in previous campaigns identified as being carried out by Palmerworm, while the location of its victims is also typical of the geography targeted by Palmerworm in past campaigns. The group's use of stolen code-signing certificates has also been observed in previous Palmerworm attacks. These various factors make us reasonably confident we can attribute this activity to Palmerworm.

Symantec does not attribute Palmerworm's activity to any specific geography, however, Taiwanese officials have stated publicly that they believe Blacktech, which we track as Palmerworm, is backed by the Chinese government.

Conclusion

APT groups continue to be highly active in 2020, with their use of dual-use tools and living-off-the-land tactics making their activity ever harder to detect, and underlining the need for customers to have a comprehensive security solution in place that can detect this kind of activity.

Protection

The following protections are in place to protect customers against Palmerworm activity:

- Backdoor.Consock
- Backdoor.Waship
- Backdoor.Dalwit
- Backdoor.Nomri
- Backdoor.Kivars
- Backdoor.Pled
- Hacktool

- Trojan Horse

Indicators of Compromise

28ca0c218e14041b9f32a0b9a17d6ee5804e4ff52e9ef228a1f0f8b00ba24c11
3277e3f370319f667170fc7333fc5e081a0a87cb85b928219b3b3caf7f1e549c
35bd3c96abbf9e4da9f7a4433d72f90bfe230e3e897a7aaf6f3d54e9ff66a05a
485d5af4ad86e9241abd824df7b3f7d658b1b77c7dcc3c9b74bfe1ddc074c87d
4c05ee584530fd9622b9e3be555c9132fad961848ea215ecb0dd9430df7e4ed8
50ba9a2235b9b67e16e6bd26ae042a958d065eb2c5273f07eee20ec86c58a653
5818bfe75d73a92eb775fae3b876086a9e70e1e677b7c162b49fb8c1cc996788
5a35672f293f8f586fa9cfac0b09c2c52a85d4e8bc77b1ed4d7c16c58fe97a81
69d60562a8d69500e8cb47a48293894385743716e2214fd4e81682ab6ed1c46b
6d40c289a154142cdd5298e345bcea30b13f26b9eddfe2d9634e71e1fb935fbe
6f97022782d63c6cea53ad151c5b7e764e62533d8257e439033c0307437bfb2a
73799d67d32a2b5554c39330e81e7c8069feaa56520e22a7fd0a52e8857c510c
81a4b84700b5f4770b11a5fe30a8df42e5579fd622fd54143b3d2578df4b559d
884cefccd5b3c3a219a176c0c614834b5b6676abbac1d1c98f39624fccc71bf9
8cd6dfffc251f9571f7a82cca2eca09914c950f3b96aaaeaeaaeeac342f9b550
8da532ea294cc2c99e02ce8513a15b108a7c49bd90f7001ce6148955304733cb
9c436db49b27bed20b42157b50d8bdad414b12f01e2127718250565017a08d84
9e3ecda0f8e23116e1e8f2853cf07837dd5bc0e2e4a70d927b37cfe4f6e69431
a7f3b8afb963528b4821b6151d259cf05ae970bc4400b805f7713bd8a0902a42
aa51b69d05741144d139b422c3b90fdf6d7d5a36dd6c7090c226a0fc155ada34
b32ab70f3f441a775771d6c824d4526715460c0fd72a1dfdec8cd531aef5fabd
d4d5c73c40f50cdef1500fca8329bc8f3f05f6e2ffda9c8feb9be1dcca6ccd31
eed2ab9f2c09e47c7689204ad7f91e5aef3cb25a41ea524004a48bb7dc59f969
f11e2146b4b7da69112f4681daca0c5ec18917acc4cf4f78d8bff7ac0b53e15c
f21601686a2af1a312e0f99effa2c2755f872b693534dbe14f034fa23587ac0b

Indicators of Compromise
asiainfo.hpcloudnews.com
loop.microsoftmse.com
103.40.112.228
172.104.92.110
45.76.218.116
45.77.181.203

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.