These hackers have spent months hiding out in company networks undetected

By Danny Palmer

Published: 2020-09-29 · Archived: 2026-04-05 23:46:17 UTC

A cyber-espionage campaign is using new malware to infiltrate targets around the world including organisations in media, finance, construction and engineering.

Detailed by cybersecurity company Symantec, the attacks against organisations in the US, Japan, Taiwan and China are being conduced with the aim of stealing information and have been linked to an espionage group known as Palmerworm – aka BlackTech – which has a history of campaigns going back to 2013.

The addition of a US target to this campaign suggests the group is expanding campaigns to embrace a wider, more geographically diverse set of targets in their quest to steal information – although the full motivations remain unclear.

SEE: **Cybercrime and cyberwar: A spotter's guide to the groups that are out to get you**

In some cases, Palmerworm maintained a presence on compromised networks for a year or more, often with the aid of 'living-off-the-land' tactics that take advantage of legitimate software and tools, so as to not raise suspicion that something might be wrong – and also thus creating less evidence thath can be used to trace the origin of the attack.

Researchers haven't been able to determine how hackers gain access to the network in this latest round of Palmerworm attacks, but previous campaigns have deployed spear-phishing emails to compromise victims.

However, it's known that deployment of the malware uses custom loaders and network-reconnaissance tools similar to previous Palmerworm campaigns, leaving researchers "reasonably confident" it's the same group behind these attacks.

Palmerworm's malware also uses stolen code-signing certificates in the payloads in order to make them look more legitimate and more difficult for security software to detect. This tactic is also known to have been deployed by the group previously.

The trojan malware provides attackers with a secret backdoor into the network and that access is maintained with the use of several legitimate tools including PSExec and SNScan, which are exploited to move around the network undetected. Meanwhile, WinRar is used to compress files, making them easier for the attackers to extract from the network.

"The group is savvy enough to move with the times and follow the trend of using publicly available tools where they can in order to minimise the risk of discovery and attribution," said Dick O'Brien, principal on the threat

hunter team at Symantec. "Like many state sponsored attackers, they seem to be minimising the use of custom malware, deploying it only when necessary."

Organisations Symantec have identified as victims of Palmerworm include a media company and a finance company in Taiwan, a construction firm in China and a company in the US; in each case, attackers spent months secretly accessing the compromised networks. Shorter compromises of just a few days were detected on the networks of an electronics company in Taiwan and an engineering company in Japan.

SEE: Security Awareness and Training policy (TechRepublic Premium)

Symantec haven't attributed Palmerworm to any particular group, but Taiwanese officials have previously claimed that the attacks can be linked back to China. If that is the case, it suggests that Chinese hackers have targeted a Chinese company as part of the campaign – although researchers wouldn't be drawn on the potential implications of this.

However, what is certain is that whoever Palmerworm is working on behalf of, the group is unlikely to have ceased operations and will remain a threat.

"Give how recent some of the activity is, we consider them still active. The level of retooling we've seen, with four new pieces of custom malware, is significant and suggests a group with a busy agenda," said O'Brien.

While the nature of advanced hacking campaigns means they can be difficult to identify and defend against, organisations can go a long way to protecting themselves by having a clear view of their network and knowledge of what usual and unusual activity looks like – and blocking suspicious activity if necessary.

"Most espionage-type attacks are not a single event. They are a long chain of events where the attackers use one tool to perform one task, another tool to perform the next task, and then hop from one computer to another and so on," said O'Brien

"There are lots of steps the attacker has to take to get to where they want to go and do whatever they want to do. Each individual step is an opportunity for it to be detected, disrupted and even blocked. And what you'd hope is that, if they aren't detected during one step in that chain, they will be detected in the next," he added.

MORE ON CYBERSECURITY

- **Hackers are getting more hands-on with their attacks. That's not a good sign**
- **US charges Chinese hackers with 'unprecedented' attacks on gaming companies CNET**
- **Cyber-espionage warning: The most advanced hacking groups are getting more ambitious**
- **6 reasons hackers target businesses: Is your organization in the line of fire? TechRepublic**
- **Hacking and cyber espionage: The countries that are going to emerge as major threats in the 2020s**
