CERT-EU

Memo

02/07/2019 - TLP:WHITE

# Western technology firms targeted by Chinese threat actors

Reference: Memo [190702-1] Date: 02/07/2019 - Version: 1.1
Keywords: technology, espionage, China, Europe, United States, supply chain compromise, cloud services, 5G
Sources: publicly available information

## Key Points

- Chinese hackers breached the networks of several technology firms, globally, from 2010 to 2017.
- The attacks were reportedly conducted by first penetrating the cloud computing service of Hewlett Packard Enterprise.
- Technology companies racing against Chinese firms appear to have been priority targets.

## Summary

On June 26, Reuters reported that hackers affiliated to the Chinese Ministry of State Security had breached the networks of several technology firms, globally, from 2010 to 2017, in a campaign dubbed "Cloud Hopper". The campaign ensnared at least six more major technology firms, touching five of the world's 10 biggest tech service providers, and including:

| Target | Country | Sector |
|---|---|---|
| Hewlett Packard Enterprise | US | IT |
| IBM | US | IT |
| Fujitsu | Japan | IT |
| Tata Consultancy Services | India | IT |
| NTT Data | Japan | IT |
| Dimension Data | US | IT |
| Vale | Brazil | Mining |
| Syngenta | Swiss | Biotech |

| Target | Country | Sector |
|---|---|---|
| Computer Science Corp. | US | IT |
| DXE Technology | US | IT |
| Ericsson | Sweden | Telecoms |
| Sabre | US | Travel booking |
| Huntington Ingalls Indust. | US | Nuclear submarines |
| Valmet | Finland | IT, automation, energy |
| SKF | Sweden | Manufacturing |

The attacks were reportedly conducted by first penetrating the cloud computing service of Hewlett Packard Enterprise (HPE), thereafter using it to launch attacks on additional customers to steal large amounts of data. According to people involved in the investigations, the attacker tactics can be summarised as follows.

1. Infiltrate the cloud service provider, usually via spear phishing email designed to trick employees into downloading malware or giving away their passwords.
2. Once inside, map out the environment, establish footholds and find the target: the system administrator who controls the company "jump servers" which act as a bridge to client networks.
3. After passing through the "jump server," map out the victim network and identify commercially sensitive data.
4. Encrypt and exfiltrate the data, either directly from the client victim or back through the service provider.

## Comments

The Cloud Hopper campaign was the subject of a US indictment in December that accused two Chinese nationals of identity theft and fraud. Several cyber-security firms believe that these two hackers belong to a threat group dubbed APT10 (aka Stone Panda). CERT-EU has recently reported on investigations of APT10 activities (see Memo-s [181223], [190319], [190626]). Additional companies that likely became victims of APT10 include Norway's Visma, Japan's Keidanren, and France's Airbus (supply chain). In most cases, APT10 used cloud services targeting combined with supply chain compromise as the main tactics.

The victimology of APT10 campaigns shows how technology companies racing against Chinese firm have become priority targets. The Ericsson's case is illustrative as the company has been racing against China's Huawei Technologies to build infrastructure for 5G networks.

In the case of the former Swiss biotech firm Syngenta, it is important to mention that this firm was taken over by state-owned Chinese chemicals conglomerate ChemChina in 2017, during the same period as the HPE investigation into Chinese attacks on its network.

The targeting of a major US travel agency is also particularly interesting. With such a compromise, China was able to track where corporate executives or US government officials were traveling. That would open the door to in-person approaches, physical surveillance or attempts at installing digital tracking tools on their devices.

This report comes in the wake of other major cyber-espionage operations in the technology sector.

| Campaigns | Threat actor | Victims | Sectors | Time |
|---|---|---|---|---|
| Cloud Hopper | China – APT10 | See above | IT, Telecoms | 2010-2017 |
| Soft Cell | China – possibly AP10 | 10 cellular providers from Africa, Middle East, Europe | Telecoms providers (mobile phones) | 2017-Present |