CERT-EU

Memo

25/07/2019 - TLP:WHITE

# Extended use of the likely Chinese Winnti malware

Reference: Memo [190725-1] – Version: 1.0
Keywords: China, Germany, cyber-espionage, cybercrime, industry, political
Sources: publicly available information

## Key Points

- According to media, the Winnti malware has been used for cyber espionage purposes against German industries.
- Initially, the malware was likely developed by cyber-criminals, then repurposed and shared with other actors.

## Summary

On July 23, German public broadcasters BR and NDR reported[1] that the likely Chinese Winnti malware has infected at least six DAX[2] corporations. According to BR, a high-ranking German official said the actors behind Winnti continue to be highly active. For their investigation, BR and NDR interviewed more than 30 people: company staff, IT security experts, government officials, and representatives of security authorities. The goal of the attackers was to collect information on the organisational charts of their targets, cooperating departments, IT systems of business units, and trade secrets. Investigations showed that the hackers were, however, implementing poor operational security (OPSEC) practices. For example, they wrote the names of the companies they wanted to spy on directly into their malware.

Initially, the collective behind Winnti was motivated by financial gain and the gaming sector was especially targeted. For example, by 2011, one of their victims was Gameforge, a company that offers so-called freemium games: while playing the games is free, it is possible to buy virtual items/money with real money. The Winnti hackers were able to directly access Gameforge's databases and modify accounts to become 'virtually' richer.

Then, by 2014, the Winnti malware code was no longer limited to game developers. According to Costin Raiu from Kaspersky, 'Nine years ago, things were much more clear-cut. There was a single team, which developed and used Winnti. It now looks like there is at least a second group that also uses Winnti.' According to BR, the second group's job is mainly industrial espionage. For example, BR says they found evidence that, in 2014, the Winnti hackers broke into the networks of Henkel, a manufacturer of many industrial products, including adhesives for industrial applications. Interestingly, in 2019, two French adhesives manufacturers, Covesto and Bostik, were reportedly infected by Winnti.

The Winnti malware has also reportedly infected political targets (Hong Kong, Tibet). Hackers have also used Winnti for the collection of large sets of personal data from Marriott and Lion Air customers. According to BR findings, victims of Winnti malware include the following:

| Sector | Targets | Likely motive |
|---|---|---|
| Gaming | Gameforge, Valve | Financial gain |
| Software | Teamviewer | Industrial espionage |
| Technology | Siemens, Sumitomo, Thyssenkrupp | |
| Pharma | Bayer, Roche | |
| Chemical | BASF, Covestro, Shin-Etsu | |
| Government | Hong Kong | Political espionage |
| Government (via Telecom) | Possibly the 'Central Tibetan Administration' via a telecom provider | |
| Hotels | Marriott | Personal data collection |
| Airline | Lion Air | |

## Comments

The case of Winnti is an excellent illustration of a malware initially developed for cybercriminal purposes and which has since been repurposed for cyber-espionage. Although it is not exactly known how it has been shared, it is highly likely that several hacking groups have used this malware. This tactic indeed offers an excellent means of anonymising operations and making attribution difficult. This also gives one plausible explanation for the poor OPSEC practises observed from Winnti users. Although it is likely that some Winnti attacks are state-sponsored and support Chinese government objectives, we cannot rule out that other, non-Chinese, hackers have also used the malware.

In an attempt to distinguish cybercriminal and cyber-espionage activities, industry reporting has given several different names to group(s) using Winnti such as Winnti group, Wicked Spider, Wicked Panda, APT17, APT22, Barium, Axiom, Deputy Dog, Dogfish, ShadowHammer, and Blackfly.

[1] https://web.br.de/interaktiv/winnti/english/
[2] https://en.wikipedia.org/wiki/DAX