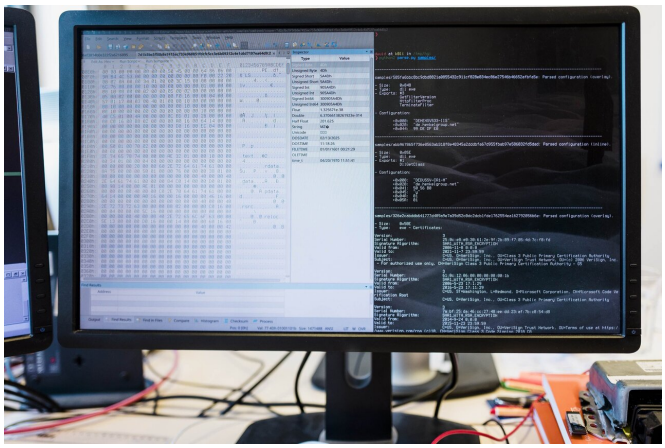
Hacking group Winnti has targeted several industrial enterprises

24 July 2019



Binary code – visible on the left – is more or less unreadable to humans. Part of the Bochum researchers' work is translating it into understandable language. Credit: RUB, Kramer

Together with an investigative team at Bayerischer Rundfunk (BR) and Norddeutscher Rundfunk (NDR), researchers at Ruhr-Universität Bochum have unearthed how the hacking group Winnti, also known as APT10, commits its attacks on German and international companies that have been their victims so far. Winnti has supposedly been operating from China for at least 10 years, spying on enterprises worldwide. In Germany, attacks on corporations Thyssen-Krupp and Bayer have come to light.

Following analyses conducted by the team headed by Professor Thorsten Holz at Horst Görtz Institute for IT Security in Bochum, at least a dozen companies have been impacted by Winnti software, among them six DAX corporations. The main targets are enterprises from the chemical industry and the semiconductor, pharmaceutical and telecommunication industries and manufacturers of video games. The media reported about the investigation results on 24 July 2019.

Modular malware

The BR and NDR news agency consulted Thorsten Holz and his Ph.D. student Moritz Contag as co-researchers. They are experts in software analysis, specifically in binary code analysis. They wanted to find out the workings of Winnti espionage in detail.

"Today, there are three generations of Winnti software," explains Thorsten Holz, a speaker at the Casa Cluster of Excellence (Cyber-Security in the Age of Large-Scale Adversaries). "The software is based on a modular structure. The group can use any modules to assemble malware specifically for the respective purpose and tailored to the victim company." For example, the construction kit may contain a module that hides the software on one of the servers at the targeted enterprise, one module that collects information in the company's intranet, and a module that establishes an outside communication channel.

Control server for malware partially integrated in the intranet

The software's binary code includes a configuration file that contains options for controlling the malware. Binary code can be run directly by the processor, but it is more or less unreadable to humans. The IT experts from Bochum translated the code into legible language and demonstrated that the files contained, for example, information on which server controlled the malware and where the malware was located in the victim's system.

The hacking group often used external servers to control the malware, but sometimes compromised intranet servers were used for this purpose, too. "Interestingly enough, the configuration files also include hints of which companies or organisations have been attacked," explains Thorsten Holz. "Presumably, this helps the group organise their attacks."

The analysed malware files were extracted from the Virustotal database. Any user can use this service to upload files and have them checked by 50 virus scanners. All uploaded files are saved in a database.

After analysing different versions of the malware, Moritz Contag used his findings to analyse several hundred configuration files. He also successfully extracted certificates used by the attackers to more fully conceal their malware.

The investigative journalists contacted 14 enterprises in order to warn them of a possible malware infection. Some of the targeted companies admitted that they'd been a victim of an attack; several analyses are still ongoing. The Winnti group has not only targeted companies, but also the Hong Kong government. The media thus suspect that Winnti may not only be engaged in industrial, but also in political espionage.

Malware infection is often conducted via phishing emails. If a user clicks on a link or opens an attachment in such an email, Winnti software installs itself on the system. The attackers then use that system for further attacks within the intranet. The software can hide unnoticed on an infected server until it is activated by a signal from the control server. Subsequently, the program communicates with the control server via an encrypted channel, for example, by sending specific data from the intranet to the attackers.

"Our analysis has also shown that the Winnti software frequently remains dormant for weeks or months; then it becomes active for a day or perhaps a week, before switching off again," Thorsten Holz says.

Attacks on Linux systems detected

Winnti software aims at infecting Windows systems. However, there is now also a version for Linux, discovered in March 2019. "We studied this malware version, too," says Thorsten Holz. "It works pretty much like Winnti."

Provided by Ruhr-Universitaet-Bochum