Uroburos - highly complex espionage software with Russian roots

gdatasoftware.com/blog/2014/02/23968-uroburos-highly-complex-espionage-software-with-russian-roots

G Data Security experts have analyzed a very complex and sophisticated piece of malware, designed to steal confidential data. G Data refers to it as Uroburos, in correspondence with a string found in the malware's code and following an ancient symbol depicting a serpent or dragon eating its own tail.

In the course of today, this blog article is going to be updated. The G DATA SecurityLabs will publish a document with an in-depth analysis of the Uroburos malware!

What is Uroburos?

Uroburos is a rootkit, composed of two files, a driver and an encrypted virtual file system. The rootkit is able to take control of an infected machine, execute arbitrary commands and hide system activities. It can steal information (most notably: files) and it is also able to capture network traffic. Its modular structure allows extending it with new features easily, which makes it not only highly sophisticated but also highly flexible and dangerous. Uroburos' driver part is extremely complex and is designed to be very discrete and very difficult to identify.

Technical complexity suggests connections to intelligence agencies

The development of a framework like Uroburos is a huge investment. The development team behind this malware obviously comprises highly skilled computer experts, as you can infer from the structure and the advanced design of the rootkit. We believe that the team behind Uroburos has continued working on even more advanced variants, which are still to be discovered.

Uroburos is designed to work in peer-to-peer mode, meaning that infected machines communicate among each other, commanded by the remote attackers. By commanding one infected machine that has Internet connection, the malware is able to infect further machines within the network, even the ones without Internet connection. It can spy on each and every infected machine and manages to send the exfiltrated information back to the attackers, by relaying this exfiltrated data through infected machines to one machine with Internet connection. This malware behavior is typical for propagation in networks of huge companies or public authorities. The attackers expect that their target does have computers cut off from the Internet and uses this technique as a kind of workaround to achieve their goal.

Uroburos supports 32-bit and 64-bit Microsoft Windows systems. Due to the complexity of this malware and the supposed spying techniques used by it, we assume that this rootkit targets governments, research institutes, or/and big companies.

Relation to Russian attack against U.S. suspected

Due to many technical details (file name, encryption keys, behavior and more details mentioned in this report), we assume that the group behind Uroburos is the same group that performed a cyberattack against the United States of America in 2008 with a malware called Agent.BTZ. Uroburos checks for the presence of Agent.BTZ and remains inactive if it is installed. It appears that the authors of Uroburos speak Russian (the language appears in a sample), which corroborates the relation to Agent.BTZ. Furthermore, according to public newspaper articles, this fact, the usage of Russian, also applied for the authors of Agent.BTZ.

According to all indications we gathered from the malware analyses and the research, we are sure of the fact that attacks carried out with Uroburos are not targeting John Doe but high profile enterprises, nation states, intelligence agencies and similar targets.

Probably undiscovered for at least three years

The Uroburos rootkit is one of the most advanced rootkits we have ever analyzed in this environment. The oldest driver we identified was compiled in 2011, which means that the campaign remained undiscovered for at least three years.

Infection vector still unknown

At the current stage of the investigations it is unknown how Uroburos initially infiltrates high profile networks. Many infection vectors are conceivable. E.g. spear phishing, drive-by-infections, USB sticks, or social engineering attacks.