The new Gazer - the back door targets the ministries and embassies around the world

Security researchers at ESET have discovered a new malware with the aim of consular offices, ministries and embassies around the world to track governments and diplomatic activities.

Security researchers at ESET have discovered a new malware with the aim of consular offices, ministries and embassies around the world to track governments and diplomatic activities.

Operating since 2016, this malware campaign uses a backdoor called Gazer, thought to be hacked by APT (persistent, intentional hacker) Turla, previously linked to Russian espionage. , proceed.

Gazer written in C ++ is a fake email intrusion door and hijack the target computer in two steps.

1. Malware dropped on the back door of Skipper, which was also related to Turla earlier.
2. Install elements of Gazer.

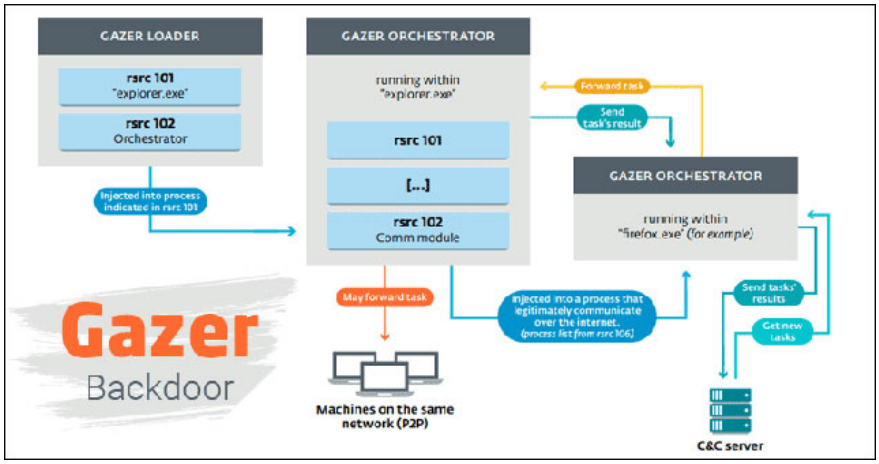

Diagram of operation principle of the Gazer rear door

In previous espionage campaigns, the Turla hack team used Carbon and Kazuar rear doors as malware in the second stage. According to research published by ESET (*https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf*), the following doors also have many similarities with Gazer.

The Gazer receives an encrypted command from a C&C server remotely and avoids being detected using a legitimate website that has been hacked into a proxy (these sites mostly use WordPress CMS). Instead of using Windows Crypto API, Gazer uses 3DES and RSA encryption libraries to encrypt data before sending it to C&C

server. This is the familiar tactic of the APT Turla group.

The Gazer used the technique of inserting code to take control of the computer and hide it for a long time to steal information. It is also possible to transfer the received command with a poisoned endpoint to another poisoned device in the system.

So far ESET researchers have discovered four variants of Gazer, mainly spying in Southeastern Europe and former Soviet political groups. Interestingly, previous versions of Gazer received Comodo authentication for Solid Loop Ltd, while the latest version had SSL authentication from Ultimate Computer Support Ltd.

According to the researchers, Gazer has been used to infect many computers around the world, mainly in Europe. Kaspersky Lab also released similar details about Gazer but called it the APT campaign 'Whitebear' (White Bear).*https://securelist.com/introducing-whitebear/81638/*