New ESET research uncovers Gazer, the stealthy backdoor that spies on embassies

welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer/

August 30, 2017

Security researchers at ESET have released new research today into the activities of the notorious Turla cyberespionage group.

Graham Cluley
30 Aug 2017 - 02:53PM

Security researchers at ESET have released new research today into the activities of the notorious Turla cyberespionage group.

Security researchers at ESET have released new research today into the activities of the notorious Turla cyberespionage group, and specifically a previously undocumented backdoor that has been used to spy on consulates and embassies worldwide.

ESET's research team are the first in the world to document the advanced backdoor malware, which they have named "Gazer", despite evidence that it has been actively deployed in targeted attacks against governments and diplomats since at least 2016.

Gazer's success can be explained by the advanced methods it uses to spy on its intended targets, and its ability to remain persistent on infected devices, embedding itself out of sight on victim's computers in an attempt to steal information for a long period of time.

ESET researchers have discovered that Gazer has managed to infect a number of computers around the world, with the most victims being located in Europe. Curiously, ESET's examination of a variety of different espionage campaigns which used Gazer has identified that the main target appears to have been Southeastern Europe as well as countries in the former Soviet Union.

The attacks show all the hallmarks of past campaigns launched by the Turla hacking group, namely:

- Targeted organizations are embassies and ministries;
- Spearphishing delivers a first-stage backdoor such as Skipper;
- A second stealthier backdoor (Gazer in this instance, but past examples have included Carbon and Kazuar) is put in place;
- The second-stage backdoor receives encrypted instructions from the gang via C&C servers, using compromised, legitimate websites as a proxy.

> "ESET researchers have discovered that Gazer has managed to infect a number of computers around the world"

Another notable similarity between Gazer and past creations of the Turla cyberespionage group become obvious when the malware is analyzed. Gazer makes extra efforts to evade detection by changing strings within its code, randomizing markers, and wiping files securely.

In the most recent example of the Gazer backdoor malware found by ESET's research team, clear evidence was seen that someone had modified most of its strings, and inserted phrases related to video games throughout its code.

Gazer's creators appear to be video game fans.

Don't be fooled by the sense of humor that the Turla hacking group are showing here, falling foul of computer criminals is no laughing matter.

All organizations, whether governmental, diplomatic, law enforcement, or in traditional business, need to take today's sophisticated threats serious and adopt a layered defense to reduce the chances of a security breach.

Learn more about Gazer in ESET's research paper: Gazing at Gazer: "Turla's new second stage backdoor"

30 Aug 2017 - 02:53PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion