Counter-Strike 1.6 features new Zero-Day, allowing malicious servers to hack gamers' computers

If you're a Counter-Strike player, be careful.

If you are a Counter-Strike player, be careful, because a recent study has shown that 39% of the game's currently active online servers are actually malicious servers, is set to hack computer gamers remotely.

Accordingly, a group of network security researchers at Dr. The Web has revealed that an attacker used malicious gaming servers to silently spread malicious code and take over the computer system of Counter-Strike gamers around the world by exploiting those zero-day vulnerabilities are hidden in the game client.

1. Scary data breaches in China: Information about the 'fertility' of more than 1.8 million women leaked

According to the researchers, Counter-Strike 1.6 - a popular game around the world for nearly two decades and still very popular at the moment, contains a lot of remote code execution vulnerabilities (RCE) has not been patched in its client software, allowing an attacker to execute arbitrary code on the gamer's computer as soon as the system connects to a malicious server without requiring any other interaction from the players.

Going into the investigation, security researchers have discovered that a Russian game server developer nicknamed 'Belonard' exploited these vulnerabilities in nature to promote these. Its illegal money-making activity and creates a botnet that includes many intrusive computer systems by infecting a custom Trojan.

1. Ransomware STOP started installing Trojans to steal victim passwords

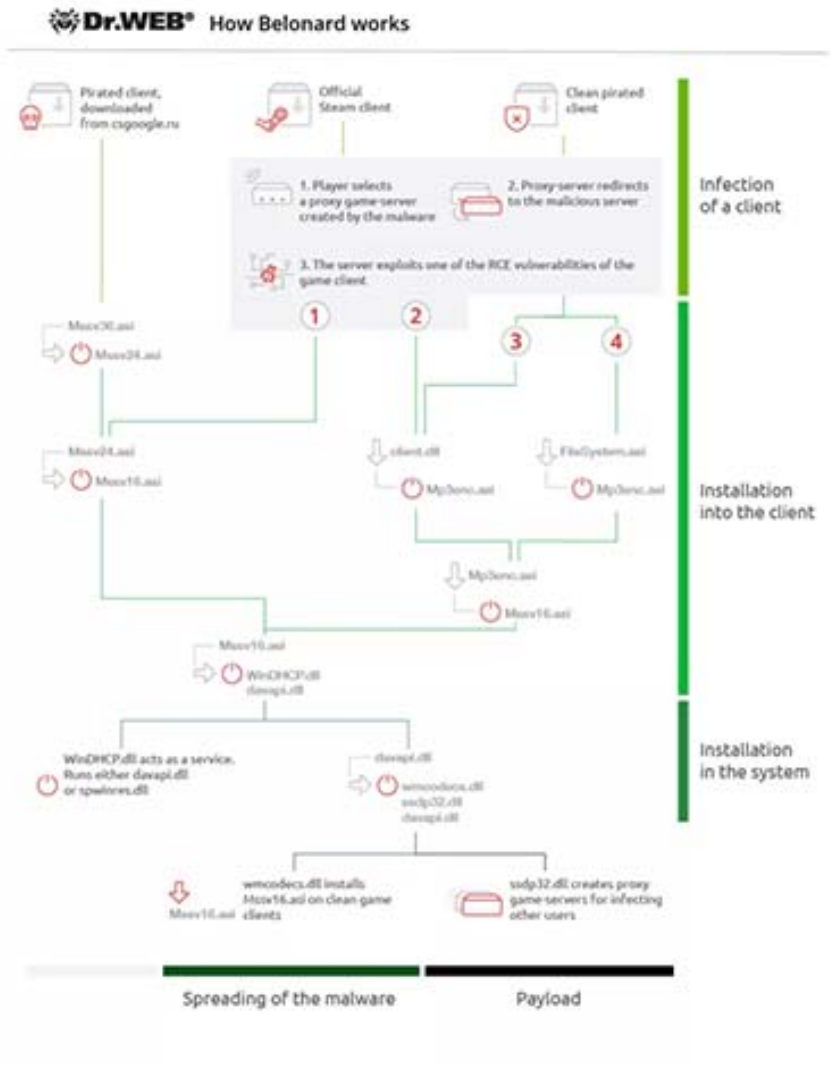
This custom trojan is named after the person who created it: Belonard, and is also designed with 'high durability', which replaces the list of game servers available in client applications. install on infected systems and create proxies to continue spreading Trojans.

"As a rule, proxy servers will usually display lower pings, so other players will see them at the top of the list. After selecting one of these servers, the player will be redirected to a malicious server and then their computer will be infected with Trojan.Belonard ', the Dr. Web team said in a report published last Wednesday.

Besides, the fake Russian server developer is also distributing a modified version of the game client through his website, and learned that the site has also been infected with the Belonard Trojan.

One of the 11 components of the Trojan will serve as a malicious client protection layer that "filters requests, files and commands received from other game servers and transfers data to changes." change (transferred to the client) for the Trojan developer server ".

Below is an attack sequence diagram showing how the Belonard Trojan works and infects gamers' computers:



1. KB4482887 update patched the Specter vulnerability, but it caused problems for some Windows 10 games

In addition, this malware also registered to create proxy game servers using API Steam and use encryption to store data on the system, as well as to contact the command and control server (command -and-control server) remotely.

"According to our analysis, out of 5,000 active servers and available on Steam clients, up to 1,951 systems were created by the Belonard Trojan, and this number accounts for 39% of the total number of servers. This game, a large-scale network can allow Trojan developers to promote other servers to make money, "the researchers said.

As soon as the research is completed, the team of Dr. The Web also reported vulnerabilities to Valve Corporation, the developer of the Counter-Strike 1.6 game.

In addition, Dr. researchers. The Web has also reported malicious domains used by malware developers to agencies responsible for managing website registration in Russia. The agency then suspended many domains in an attempt to remove this dangerous botnet.

Removing a few domains is a necessary action, but will generally not help prevent an attacker from setting up more malicious servers, unless the Counter-Strike developers do patch Remote code execution vulnerabilities are reported in this gaming software.