June 28th, 2012, 11:46 GMT · By Eduard Kovacs

Citadel Trojan Upgraded to Prevent Virtual Machine Analysis

S21sec experts notice two major improvements implemented by malware authors into the infamous Citadel Trojan. Its encryption algorithm is changed, but it has also been fitted with a mechanism that detects if it's executed inside a virtual machine or a sandbox.

The enhancements have already been seen in the wild, but they've also been advertised on a Russian underground forum.

The anti-emulator function is described as being able to protect the botnet against those who might want to perform reverse engineering on them (like those *meddling* security researchers).

Basically, when the malware is executed, it checks to see if it's run inside applications such as CWSandbox, VMware, or Virtualbox.

If it detects their presence, it doesn't remove itself and it doesn't stop from working. Instead, it begins to operate in a *sneaky* manner.

The Trojan creates a fake domain name and attempts to connect to it. This strategy should fool the researchers into believing that the (C&C) command and control server cannot be reached and that the bot is dead.

By closing all the processes related to VMware, such as *vmwareuser.exe* and *vmwaretray.exe*, experts forced the malware to begin working normally and connect to the real C&C server.

This is not the only change brought to Citadel. Experts have found that the RC4 is slightly different compared to previous versions, an internal hash being added to the algorithm.

"While computing the stream cipher, in addition to the normal XOR operations of RC4, in each iteration the value is XORed with hash string's characters in a consecutive way," S21sec researchers Mikel Gastesi and Jozsef Gegeny explained.

"The change in the RC4 algorithm affects also how the Trojan communicates with its control panel, due to the same algorithm is used to encrypt network traffic. Therefore the new control panel won't be able to handle connections coming from older versions of the bot."

FILED UNDER: TROJAN | CITADEL | MALWARE


London Olympics-Themed Spam: Prize Notifications, Awards and Visa Lotteries


Trojan Causes Printers Worldwide to Print Until They Run Out of Paper

Fake BancorpSouth Emails Lure Users to Blackhole Exploit Kit


Old Tojan Spreads as Photo on ICQ


Experts Confronted by Malware Developer While Researching Diablo III Keylogger

READER COMMENTS:

Comment #1 by: **Bo** on 25 Jul 2012, 09:40 UTC

reply to this comment

how do I get rid of this Citadel trojan?