

This site uses cookies to offer you a complete experience. Find out more or close (x) this notification permanently.

BOOKMARK THIS SITE SEARCH Keywords GO DOWNLOAD BASKET YOUR ACCOUNT

SOFTPEDIA®

Updated one minute ago



autoevolution test drive: NISSAN Patrol

TODAY'S NEWS:

- HOME
- WINDOWS
- GAMES
- DRIVERS
- MAC
- LINUX
- SCRIPTS
- MOBILE
- HANDHELD
- NEWS

- NEWS CATEGORIES:
- Latest News
 - NEW! Oddiverse
 - Games
 - Microsoft
 - Science
 - Telecoms
 - Technology and Gadgets
 - Reviews
 - Apple
 - Linux
 - Life and Style
 - Webmaster
 - Security
 - Editorials
 - Interviews
 - Green

NEWS ARCHIVE >>
SOFTPEDIA REVIEWS >>
MEET THE EDITORS >>

I ♥ SOFTPEDIA

20k

Find us on Google+

Like 156k

Follow

- TRENDING TODAY
- Download UC Browser 8.8 for Java (Updated)
 - Download UC Browser 9.0 for Java (Test Version)
 - Syrian Electronic Army Hacks Sky News Apps In Google Play
 - Movie2K Blocked in the UK, Proxies Pop Up Hours Later
 - The 60-Second Microsoft Roundup: The Start Button Is Back, Users Don't Care About Metro
 - Download UC Browser 8.9 for Java
 - GeForce GTX 770 Tests Result in Benchmark Score List
 - UC Browser for Java 9.0 Now Available for Download
 - How to Access KickassTorrents and Other Censored Sites in the UK
 - KDE 4.11 Will Be a LTS Release, KDE 5.x to Get All the New Features

CHECK OUT THE MOBILE SITE AND GET OUR STORIES ON YOUR PHONE

Home > News > Security > Virus alerts

June 28th, 2012, 11:46 GMT · By [Eduard Kovacs](#)

Citadel Trojan Upgraded to Prevent Virtual Machine Analysis

Advance Persistent Threat

seculert.com/APT-Detection

Detect For Free. Immediate Results - Try Now!



AdChoices

SHARE: +1 5 Like 1 Send Tweet 39

Adjust text size: - +



S21sec experts notice two major improvements implemented by malware authors into the infamous Citadel. 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.

ENL3R3DC

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.

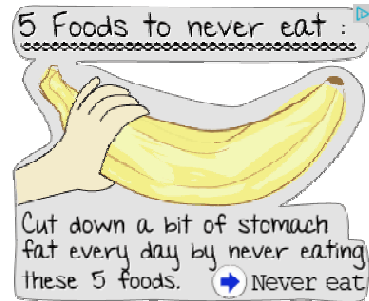
"While computing the stream cipher, in addition to the normal XOR operations of RC4, in each iteration the value is XORed with hash string's characters in a consecutive way," S21sec researchers Mikel Gastesi and Jozsef Gegeny explained.

"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."

Follow @EduardKovacs 2,959 followers

Add me on Google+

FILED UNDER: TROJAN CITADEL MALWARE



TRIAL.EVEONLINE.COM

Share your thoughts on this story...

3,666 hits · 1 comment

POST YOUR COMMENT

[Link to this article](#) · [Print article](#) · [Send to friend](#)

MUST-READ RELATED ARTICLES:



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



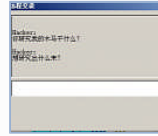
Trojan Causes Printers Worldwide to Print Until They Run Out of Paper



Fake BancorpSouth Emails Lure Users to Blackhole Exploit Kit



Old Trojan 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?

Copyright © 2001-2013 Softpedia. Contact/Tip us at news@softpedia.com

- WINDOWS
- GAMES
- DRIVERS
- MAC
- LINUX
- SCRIPTS
- MOBILE
- HANDHELD
- NEWS

[SUBMIT PROGRAM](#) | [ADVERTISE](#) | [GET HELP](#) | [SEND US FEEDBACK](#) | [RSS FEEDS](#) | [UPDATE YOUR SOFTWARE](#) | [ROMANIAN FORUM](#)

© 2001 - 2013 Softpedia. All rights reserved.
Softpedia® and the Softpedia® logo are registered trademarks of SoftNews NET SRL.

[Copyright Information](#) | [Privacy Policy](#) | [Terms of Use](#)