# Krebs on Security

In-depth security news and investigation

About the Author
Blog Advertising

09
Feb 12

Collaboration Fuels Rapid Growth of Citadel Trojan

Late last month I wrote about Citadel, an "open source" version of the **ZeuS Trojan** whose defining feature is a social networking platform where users can report and fix programming bugs, suggest and vote on new features, and generally guide future development of the botnet malware. Since then, I've been given a peek inside that community, and the view so far suggests that Citadel's collaborative approach is fueling rapid growth of this new malware strain.
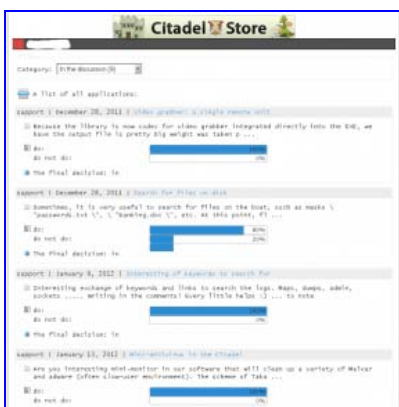

The CRM page shows democracy in action among Citadel botnet users.

A customer who bought a license to the Citadel Trojan extended an invitation to drop in on that community of hackers. Those who have purchased the software can interact with the developers and other buyers via comments submitted to the **Citadel Store**, a front-end interface that is made available after users successfully navigate through a two-step authentication process.

Upon logging into the Citadel Store, users see the main "customer resource management" page, which shows the latest breakdown of votes cast by all users regarding the desirability of proposed new features in the botnet code.

In the screen shot to the right, we can see democracy in action among miscreants: The image shows the outcome of voting on several newly proposed modules for Citadel, including a plugin that searches for specific files on the victim's PC, and a "mini-antivirus" program that can clean up a variety of malware, adware and other parasites already on the victim's computer that may prevent Citadel from operating cleanly or stealthily. Currently, there are nine separate modules that can be voted and commented on by the Citadel community.

1

Drilling down into the details page for each suggested botnet plugin reveals comments from various users about the suggested feature (screenshot below). Overall, users seem enthusiastic about most suggested new features, although several customers used the comments section to warn about potential pitfalls in implementing the proposed changes.
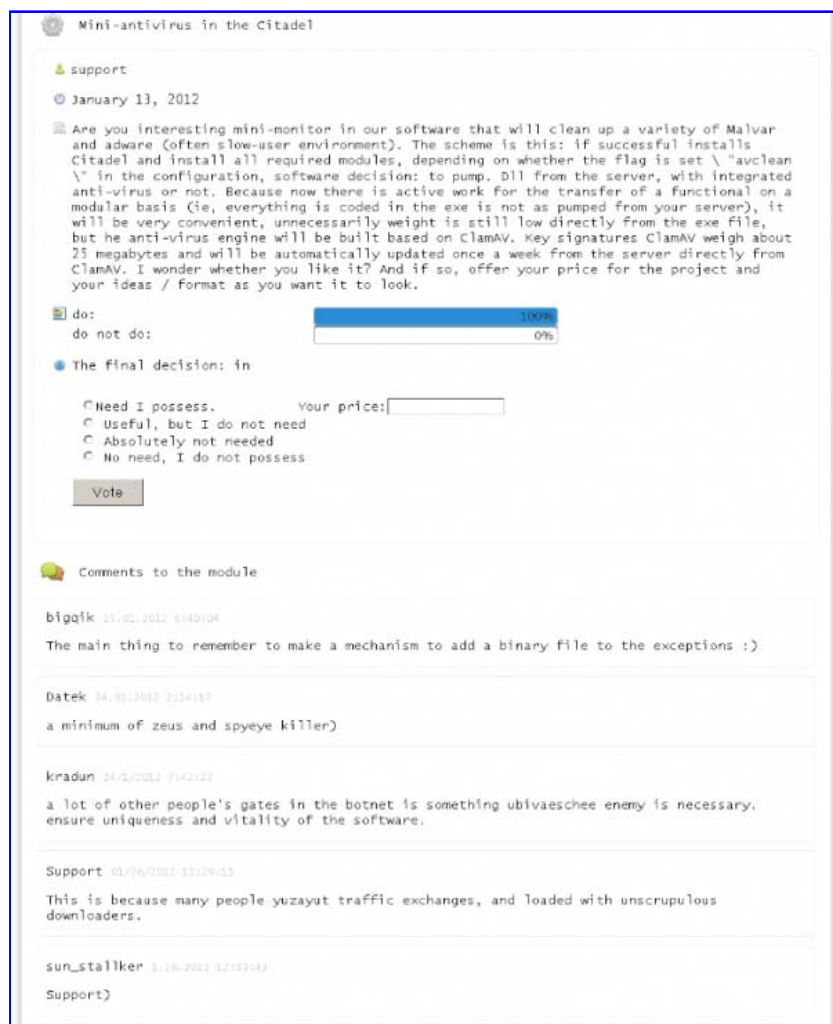
Citadel users discuss the merits of including a module to remove other parasites from host PCs.

The customer resource management page also reveals that although the principal authors of the Citadel Trojan treat this as their day job, they try their best to have a life on the weekends. A notice prominetly posted to the Citadel CRM homepage reads:

> *Please note regarding the Help Desk in the Jabber chat & CRM page*:
>
> Daily from 10.00 to 00.30
> **Sat, Sun – closed**, you can write us offline.
> All requests and questions will be processed on Monday.

The collegial atmosphere being cultivated by the Citadel authors appears to have hastened the malware's maturity, according to researchers at **Seculert**. In a blog post published Wednesday, researchers there said that they'd observed at least five new versions of Citadel since first spotting the malware on Dec. 17, 2011.

Seculert's **Aviv Raff** said that means the miscreants behind Citadel are pushing out a new version of the Trojan about once a week.

"The only similar Trojan who got close to this pace was the so called 'SpyZeus' Trojan," Raff said. "Others, including ZeuS itself, took between a month to several months to release a new version."

Tags: Aviv Raff, Citadel Store, Citadel Trojan, CRM, Seculert

2

This entry was posted on Thursday, February 9th, 2012 at 4:42 pm and is filed under A Little Sunshine, The Coming Storm, Web Fraud 2.0. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

12 comments

1. ❌ *nonameform*
   February 10, 2012 at 5:04 am

   It's obvious from the second screenshot that two comments were made by Russians. Since one of the posts in question is writen under nickname "Support" it seems to me that people behind Citadel are Russians. Both messages were probably translated into English with something like Google translate.

   "ubivaeschee" from Russian "ubivat'" (to kill).
   "yuzayut" is a barbarized version of English verb "to use".

   ○ ❌ *Christian*
      February 10, 2012 at 1:07 pm

      is google translate really that bad with russian? 😃
      german -> english got quite good with google translate.

      ■ ❌ *RCL*
         February 10, 2012 at 1:17 pm

         Russian is more irregular and complicated than German, that is putting aside that German and English are more closely related than Russian and English.

         From my experience, Google is very poor at translating from Russian, slightly better at translating to it.

2. ❌ *RCL*
   February 10, 2012 at 8:41 am

   What for do they need a video grabber?

   ○ *BrianKrebs*
      February 10, 2012 at 8:45 am

      Might be useful in watching to see whether the Web injections are working correctly on victim PCs when victims log into specific bank web sites.

      ■ ❌ *RCL*
         February 10, 2012 at 1:10 pm

         Aha, so that's for debugging… Makes sense 😃

3. ❌ *bt*
   February 11, 2012 at 1:01 pm

   not necesseraly "Russians", but definitely Russian speaking- that could be anybody from former Soviet Union's republic – Ukraine, Baltics, etc. and anywhere in the world. Could be your neighbour…

4. ❌ *Ed*
   February 11, 2012 at 2:18 pm

   Just wondering how much is this crimeware kit going for on the blackmarket?

   ○ *brian krebs*
      February 11, 2012 at 2:29 pm

      Ed – See the original story on this a few weeks back for the pricing info

      http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/

5. ❌ *curious observer*

3

February 12, 2012 at 12:14 pm

The malicious intent notwithstanding, this is an excellent business model. I really wish some above-the-ground software developers adopted this approach.

○   *William*
February 13, 2012 at 2:52 am

I know of one example: PowerArchiver, a full-featured compression/decompression program (similar to WinZip, but better in my opinion). The PowerArchiver developers have a page where users can propose and vote on improvements or new features.

○   *AlphaCentauri*
February 14, 2012 at 4:31 am

If you're a beta tester for any type of software, you get that kind of interface. And the smaller/hungrier the company, the more responsive. If you're beta testing for a one-person operation, you may see your comments implemented within a couple hours — very satisfying!

Advertisement

-

- **Recent Posts**

  - ○ NC Fuel Distributor Hit by $800,000 Cyberheist
  - ○ Krebs, KrebsOnSecurity, As Malware Memes
  - ○ Conversations with a Bulletproof Hoster
  - ○ Ragebooter: 'Legit' DDoS Service, or Fed Backdoor?
  - ○ Microsoft, Adobe Push Critical Security Updates
-

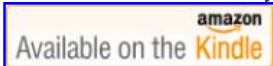- **Subscribe by email**

Your email:
Enter email address...

Subscribe   Unsubscribe

- **Made possible by Prolocation**

Prolocation: For all your hosting needs. Fast. Reliable. Powerful.

-

- **Click it!**

- **Sign Up for SANSFIRE 2013**

  Use "Krebs_5" for 5% off any class

- **Categories**

  - A Little Sunshine
  - All About Skimmers
  - How to Break Into Security
  - Latest Warnings
  - Other
  - Pharma Wars
  - Security Tools
  - Target: Small Businesses
  - The Coming Storm
  - Time to Patch
  - Web Fraud 2.0

- **All About ATM Skimmers**

  Click image for my skimmer series.

- **Archives**

  - May 2013
  - April 2013
  - March 2013
  - February 2013
  - January 2013
  - December 2012
  - November 2012
  - October 2012
  - September 2012
  - August 2012
  - July 2012
  - June 2012
  - May 2012
  - April 2012
  - March 2012
  - February 2012
  - January 2012
  - December 2011
  - November 2011
  - October 2011
  - September 2011
  - August 2011

- ## The Value of a Hacked PC

Badguy uses for your PC

- ## Tags

0day adobe adobe flash player adobe reader apple atm skimmer chrome chronopay cyberheist f-secure fbi firefox flash Glavmed gmail google Google Chrome Igor Gusev internet explorer java Mac mastercard mcafee microsoft money mules Mozilla opera Oracle pavel vrublevsky RSA Rustock Rx-Promotion safari secunia Spamit spyeye Symantec twitter Visa webmoney windows wired.com zero day zeus ZeuS Trojan

- ## Tools for a Safer PC

Tools for a Safer PC

- ## Blogroll

- ◦ Arbor Networks Blog
- ◦ Bleeping Computer
- ◦ CERIAS / Spaf
- ◦ Contagio Malware Dump
- ◦ Cyber Crime & Doing Time
- ◦ Cyveillance Blog
- ◦ DHS Daily Report

- ◦ [DSL Reports](#)
  - ◦ [ESET Threat Blog](#)
  - ◦ [F-Secure Blog](#)
  - ◦ [FireEye Malware Intel Lab](#)
  - ◦ [Fortinet Blog](#)
  - ◦ [Fox-IT International](#)
  - ◦ [GFI Labs](#)
  - ◦ [Google Online Security Blog](#)
  - ◦ [Graham Cluley, Sophos](#)
  - ◦ [Kaspersky Blog](#)
  - ◦ [Malware Domain List Forum](#)
  - ◦ [Malware Don't Need Coffee](#)
  - ◦ [Microsoft Malware Protection Center](#)
  - ◦ [Red Tape Chronicles](#)
  - ◦ [SANS Internet Storm Center](#)
  - ◦ [Schneier on Security](#)
  - ◦ [SecureWorks](#)
  - ◦ [Securing the Human](#)
  - ◦ [Securosis](#)
  - ◦ [StopBadware](#)
  - ◦ [Symantec Response Blog](#)
  - ◦ [TaoSecurity](#)
  - ◦ [TrendMicro Blog](#)
  - ◦ [Unmask Parasites Blog](#)
  - ◦ [US CERT](#)
  - ◦ [Websense](#)
  - ◦ [Wilders Security Forums](#)
  - ◦ [Wired.com's Threat Level](#)
  - ◦ [Xylitol](#)
-

The Pharma Wars

Spammers Duke it Out