Krebs on Security

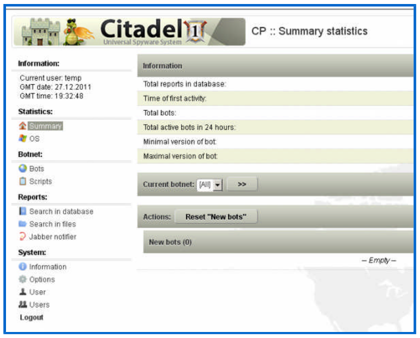
In-depth security news and investigation

About the Author
Blog Advertising

23
Jan 12

‘Citadel’ Trojan Touts Trouble-Ticket System

Underground hacker forums are full of complaints from users angry that a developer of some popular banking Trojan or bot program has stopped supporting his product, stranding buyers with buggy botnets. Now, the proprietors of a new **ZeuS Trojan** variant are marketing their malware as a social network that lets customers file bug reports, suggest and vote on new features in upcoming versions, and track trouble tickets that can be worked on by the developers and fellow users alike.



Current user: temp
GMT date: 27.12.2011
GMT time: 19:32:48

Information

Total reports in database:
Time of first activity:
Total bots:
Total active bots in 24 hours:
Minimal version of bot:
Maximal version of bot:

Current botnet: [All]

Actions:

New bots (0)

– Empty –

A screenshot of the Citadel botnet panel.

The ZeuS offshoot, dubbed **Citadel** and advertised on several members-only hacker forums, is another software-as-a-service malware development. Its target audience? Those frustrated with virus writers who decide that coding their next creation is more lucrative and interesting than supporting current clients.

“Its no secret that the products in our field — without support from the developers — result in a piece of junk on your hard drive. Therefore, the product should be improved according to the wishes of our customers,” Citadel’s developers claim in an online posting. “One problem is that you have probably experienced developers who ignore your instant messages, because there are many customers but there is only one developer.”

In the following excerpt, taken from a full description of Citadel’s innovations, the developers of this malware strain describe its defining feature as a social networking platform for malware users that is made available through a Web-based portal created by the malware itself.

“We have created for you a special system — call it the social network for our customers. Citadel CRM Store allows you to take part in product development in the following ways:

- Report bugs and other errors in software. All tickets are looked at by technical support you will receive a timely response to your questions. No more trying to reach the author via ICQ or Jabber.

-Each client has the right to create an unlimited number of applications within the system. Requests can contain suggestions on a new module or improvements of existing module. Such requests can be public or private.

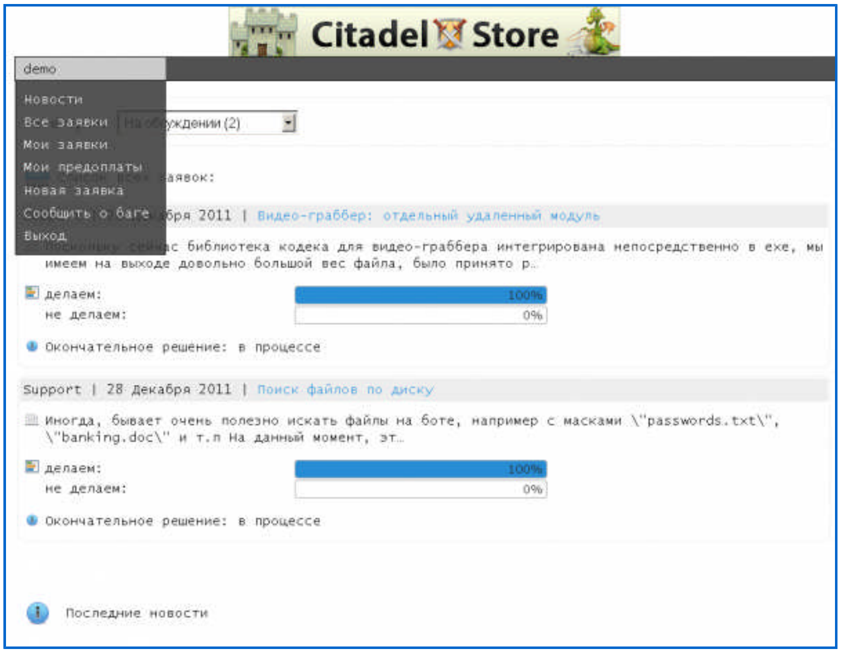
-Each client has a right to vote on new ideas suggested by other members and offer his/her price for development of the enhancement/module. The decision is made by the developers on whether to go forward with certain enhancement or new module depending on the voting results.

-Each client has the right to comment on any application and talk to any member. Now it is going to be interesting for you to find partners and like-minded people and also to take active parts in discussions with the developers.

- You can see all stages of module development, if it is approved other members. We update the status and time to completion.

- You may pay a deposit, if module is approved (50%). After the deposit is paid by the members, the project starts moving forward, so that the money is paid directly to coders and there will be no laziness or inaction. Everything is clear: every stage of development is thoroughly shown.

-Easy jabber [instant message] notification of new member or developer comments, or the availability of new custom applications.



заявок:

бря 2011 | Видео-граббер: отдельный удаленный модуль

с библиотека кодека для видео-граббера интегрирована непосредственно в exe, мы имеем на выходе довольно большой вес файла, было принято р..

делаем: 100%
не делаем: 0%

Окончательное решение: в процессе

Support | 28 декабря 2011 | Поиск файлов по диску

Иногда, бывает очень полезно искать файлы на боте, например с масками \"passwords.txt\", \"banking.doc\" и т.п На данный момент, эт..

делаем: 100%
не делаем: 0%

Окончательное решение: в процессе

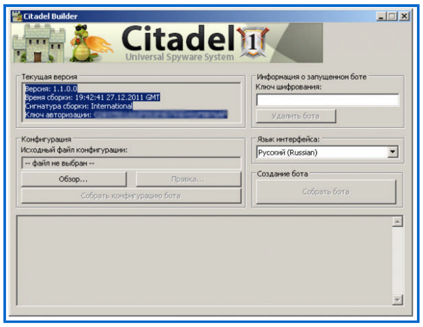
Последние новости

The Citadel store lets users file and track bug reports, and request and vote on new features.

Citadel may be the first notable progeny of ZeuS since the ZeuS source code was leaked online last year. The authors claim that it includes a number of bug fixes for the most recent ZeuS version, including full support for grabbing credentials from victims using **Google Chrome**. Also bundled with this update is a component that can record and transmit videos of the victim’s screen activity.

The basic Citadel package — a bot builder and botnet administration panel — retails for $2,399 + a $125 monthly “rent,” but some of its most innovative features are sold as a la carte add-ons. Among those is a $395 software module that allows botmasters to sign up for a service which automatically updates the bot malware to evade the last antivirus signatures. The updates are deployed via a separate Jabber instant message bot, and each update costs an extra $15.

Citadel also boasts a feature that hints at its creator’s location(s). According to the authors, if the malware detects that the victim’s machine is using a Russian or Ukrainian keyboard, it will shut itself down. This feature is almost certainly a hedge to keep the developers out of trouble: Authorities in those regions are far less likely to pursue the Trojan’s creators if there are no local victims.



Версия: 1.1.0.0
Время сборки: 19:42:41 27.12.2011 GMT
Сигнатура сборки: International
Ключ авторизации: [redacted]

-- файл не выбран --

Русский (Russian)

The Citadel bot builder.

It will be interesting to see if these malware developers hold true to their word. The growth of a more real-time, user-driven and crowdsourced malicious software market would be a truly disturbing innovation. For now, the miscreants behind Citadel appear upbeat about their chances of ushering in such a reality.

“It’s very interesting for us to work with our clients,” they wrote in an online forum posting. “A lot of authors write in forums that they ‘support the product,’ but at the end the updates only come out once every three months or the author disappears forever. Problem is in author’s motivation. You support us, we support you. It is easy.”

Tags: Citadel CRM, Citadel Store, Citadel Trojan, Google Chrome, ICQ, Jabber, ZeuS Trojan

This entry was posted on Monday, January 23rd, 2012 at 12:12 am and is filed under A Little Sunshine, Latest Warnings, 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.

7 comments

1. *prairie_sailor*
   January 23, 2012 at 6:05 pm

   It seems to me that the best way to combat this is for software writers (i.e. Adobe Reader/Flash/Shockwave/AIR and Oracle Java) need to make their updates more automatic with less user interaction (ala Google Chrome) They also need to up their time for the default check for updates – once a day at least instead of once per week or month.

   On kind of a sidways note – has any one seen a recentl explination why the 64-bit version of Java for windows does not have an auto updater yet? I am seeing this installed more and more by OEMs and with no auto-updater since its release in late 2008 no auto-updater means that ther are alot of unsafe machines out there.

2. *Daniel*
   January 23, 2012 at 10:55 pm

   My problem with approach is that it makes the already ignorant user (which is most users) even more dependent on the major software vendors. I’m reminded of the old saying that the only thing it takes for evil to flourish is for good people to run to those in authority. In some ways I fear the omnipotent reach Google/Java more than I do these guys.

   There has to be a better solution than an ever escalating arms race between various groups of brainiacs. At a certain point all the members of the intellectual oligarchy look alike.

   - *prairie_sailor*
     January 24, 2012 at 4:40 pm

     Unfortunately most end users don’t know what to do when the update boxes for Flash/Java etc pop up so they tend to ignore them. The end result – horribly out of date software with easily exploitable vulnerabilities. The only other solution I see in the end is to start requiring a licence to use a computer (kind of like a driver’s licence) – like that’s going to happen any time soon.

3. *John*
   January 24, 2012 at 4:57 pm

   CP means child porn

4. *ZoomZoom*
   January 25, 2012 at 2:56 pm

   Someone break this down for me, please. We have developers that actively tout their latest and greatest malware versions, offer support, and charge one time and/or maintenance fees for the software and/or support.

   It looks like this would require registering domains and setting up payment systems, which, with some effort, could be tied to a real, living and breathing human being with a birth certificate and a government-issued ID of some sort…not just a witty handle on a forum somewhere.

   With the amount of Customer Identification Program (CIP) required by US banks (and I am assuming similar laws in foreign countries), the banks WILL have identifying information on these individuals, even if they are IDing them only as a signitory or beneficial owner on an account that’s receiving payments for the malware.

   Or maybe I am ignorant and overly optimistic…?

- *helly*
  February 1, 2012 at 6:43 pm

  Sadly it generally doesn’t work out that these guys can be easily caught by the methods you mention. They tend not to funnel their money directly through US banks for one thing. There are also cash services like Liberty Reserve or Web Money that make these type of transactions even more difficult to trace.

  In addition there are also escrow services out there that these guys can use to ensure their transactions are safe.

  And finally even if you do track one of these guys down, getting local law enforcement to prosecute can be extremely challenging. These guys tend not to operate in countries where law enforcement is on the ball with this stuff.

  There is a whole slew of other challenges I’m glossing over, but hopefully that provides you a bit more insight into how these guys do that stuff.

5. *roflem*
   February 14, 2012 at 2:45 pm

   I wonder what CIS means when they say :
   “Our software does not work on Russian-language systems. If a Russian or Ukrainian layout is detected, the bot terminates.

   This is done to prevent installs on CIS systems. You may disagree, but that’s taboo for us.”

   ??????

- 🔍

- ## Recent Posts

  - Reports: Liberty Reserve Founder Arrested, Site Shuttered
  - Skype Beta Plugs IP Resolver Privacy Leak
  - NC Fuel Distributor Hit by $800,000 Cyberheist
  - Krebs, KrebsOnSecurity, As Malware Memes
  - Conversations with a Bulletproof Hoster

-

- ## Subscribe by email

  Your email:
  Enter email address...

  Subscribe Unsubscribe

- ## Made possible by Prolocation

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

- amazon Available on the Kindle

- ## Click it!

  Donate

- ## 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

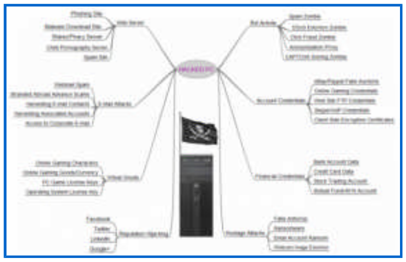
  Click image for my skimmer series.

- ## 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
- July 2011
- June 2011
- May 2011
- April 2011
- March 2011
- February 2011
- January 2011
- December 2010
- November 2010
- October 2010
- September 2010
- August 2010
- July 2010
- June 2010
- May 2010
- April 2010
- March 2010
- February 2010
- January 2010
- December 2009

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 Liberty Reserve Mac mastercard mcafee microsoft money mules 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

Powered by WordPress. Privacy Policy