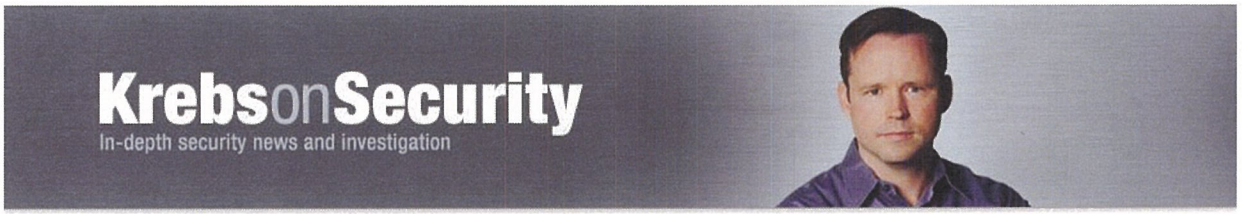
EXHIBIT 9

Krebs on Security

In-depth security news and investigation



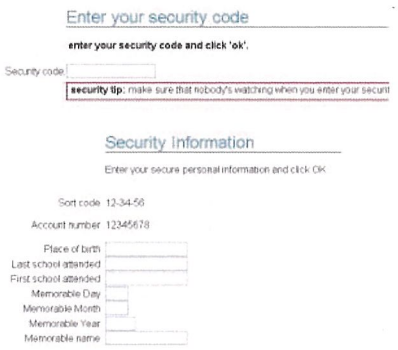
About the Author
Blog Advertising

24
Aug 11

Hybrid Hydras and Green Stealing Machines

Hybrids seem to be all the rage in the automobile industry, so it's unsurprising that hybrid threats are the new thing in another industry that reliably ships updated product lines: The computer crime world. The public release of the source code for the infamous **ZeuS Trojan** earlier this year is spawning novel attack tools. And just as hybrid cars hold the promise of greater fuel efficiency, these nascent threats show the potential of the ZeuS source code leak for morphing ordinary, run-of-the-mill malware into far more efficient data-stealing machines.

Researchers at **Trusteer** have unearthed evidence that portions of the leaked ZeuS source code have been fused with recent versions of Ramnit, a computer worm first spotted in January 2010. Amid thousands of other password-stealing, file-infecting worms capable of spreading via networked drives, Ramnit is unremarkable except in one respect: It is hugely prolific. According to a report (PDF) from **Symantec**, Ramnit accounted for 17.3 percent of all malicious software that the company detected in July 2011.



A sample Ramnit injection. Image courtesy Trusteer.

Trusteer says this Ramnit strain includes a component that allows it to modify Web pages as they are being displayed in the victim's browser. It is this very feature — code injection — that has made ZeuS such a potent weapon in defeating the security mechanisms that many commercial and retail banks use to authenticate their customers.

As this Ramnit variant demonstrates, the real threat from the ZeuS source leak is that it *greatly facilitates the addition of this code-injection capability into tons of other ordinary malware*. I think we can expect other established malware families to undergo a similar metamorphosis in the months ahead.

It is fitting that the ZeuS leak was the apparent outcome of an earlier hybridization: The merger of ZeuS with SpyEye. One of the more tantalizing conspiracy theories I've heard to explain the release of the ZeuS code is that it was done intentionally as part of a marketing ploy to create demand for peripheral code and services. This is not so far-fetched. As I wrote in July, malware writing gangs have taken to posting banner ads to lure talented programmers into the lucrative market for "Web injects" and other innovations designed to make existing malware stealthier and more feature-rich.

Security experts this week cataloged another evolution tied to the ZeuS source spill: On Tuesday, **Kaspersky Lab** published a blog post on **Ice IX**, which it claimed was the first crimeware based on the leaked code. Kaspersky said Ice IX, sold in the criminal underground for $1,800, "is the first new generation of web applications developed to manage centralized botnets through the HTTP protocol based on leaked ZeuS source code."

Tags: Ramnit, spyeye, Symantec, Trusteer, web injects, zeus

This entry was posted on Wednesday, August 24th, 2011 at 3:02 pm and is filed under Latest Warnings, The Coming Storm. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

8 comments

1.  *JCitizen*
   August 25, 2011 at 12:37 am

   At first I though this article was going to point to criminals cracking the On Star system in so many upscale vehicles, and then taking control of the maintenance management system to somehow damage the victim's vehicle. But then I couldn't see a way to make money by doing that. My bad!

It is a scary thought that the sophisticated computer network in a hybrid vehicle would be especially vulnerable – and since customers can interact with it to pay for services – who knows? If nothing else, the criminal could find out even more about his victim by listening in through the on-board cell system, and On Star communications, to better gather intelligence on his target. Then maybe turn of his motor at a dangerous point in a traffic incident. :O!

To get back to the point of the article Brian; I have a client who apparently has been a victim of this in the Microsoft partners network, and who I feel may have been a target of just such an attack. The victim lost control of the account and was never able to regain the assets available at the site. Even emails were intercepted and never reached Microsoft support. Oddly enough, the phones were failing at inopportune occasions while try to contact anyone referring to this incident, including me. This may have been poor trunk line service, because Comcast has since done underground repairs. The internet and phone problems surfaced as separate incidents however.

This condition even redirected the victim to a fake Microsoft update service that continued to make things worse as time progressed, until all communication became impossible. The victim did not know that Windows 7 does not use the IE browser to update the operating system. I am fairly convinced someone had remote control of the PC at one time, and even reconfigured the router, to enforce continued control over the victim. Needless to say – things pretty much blew up after I started nailing down the hatches; but I can't even trust the hard drive on this machine anymore. Microsoft seems nonplussed about it despite the loss in tens of thousands of software and services assets. I'm beginning to wonder just who is running things at Redmond?!

- *vhslady*
  August 26, 2011 at 8:43 am

  Omg. Yr post could hv been written about my life the last six months. No security site. Software. Cloud or person seems to be able to help me. So now instead of xbox I wage daily battles with this vicious program. It battles back too! If I. Didn't hate it so much I would almost be proud of. Its stubborn tenacity.

  -  *JCitizen*
    August 28, 2011 at 6:59 pm

    You are going to have to re-install the operating system to be sure it is gone – providing a rootkit is not part of the hybrid Brian is talking about. Wiping the drive is not always a panacea for those; but my client did get rid of it by doing a factory restore from the built in partition. That victim was lucky; but keeps re-acquiring the malware by re-visiting same said site, and Facebook.

    Rapport is the only way I know to stop browser injection attacks like these; running CCleaner regularly before rebooting or shutting off the PC may thwart the restarting of the malware in the start-up folder – WinPatrol may help there, or at least it would let you know something new has started up with your computer.

    You might do a trial of Mamutu after recovery, but it is a paid solution; maybe better to use Commodo with only the firewall and Defense + enabled. I'm not sure if Rapport and Defense + will get along, but it is worth trying even if you have to disable that feature. I will warn you that learning the Def+ alerts will be a steep learning curve. Mamutu is a little easier, and will list all protected processes. I've never seen anything get past it yet. Even secret digital right management spyware is stopped by this Emisoft product.

    Emisoft – the maker of Mamutu – has one of the best free firewalls going, called Online Armor, and I'm not sure you won't get the same protection from it – and for free too!

    What ever you do, don't bother trying any of these until you computer is likely to be cleaned up – a low level format of the hard drive may be necessary. Wait at least two weeks before restoring any backups, so you can scan them with any of the really good anti-malware utilities, because they will be more likely to have the definition on board before your restoration.

    I do not work for any person or vendor, just to be clear here. I am not a software salesman.

2.  *andy*
   August 25, 2011 at 12:01 pm

   I have already seen the use of zeus/ramnit combo, and it is nasty, quick and wide spread infection and redirection to banking/phishing sites asking for full details (luckily my client was able to notice the scam here) but protection was fully removed by threat and went undetected.

3. *KFritz*
August 25, 2011 at 3:19 pm

Open Source Malware. Even a wonderful concept like Open Source can be perverted.

4. *lyecdevf*
August 26, 2011 at 11:45 am

Every time I read some article about malware I can not help but to be amazed at all these new techniques. For instance this is the first time I read about, "web injects."

5. *DiamondGeeza*
August 28, 2011 at 9:55 pm

It looks like the developer of Ice IX has been watching too many hollywood movies … the film "The Recruit" (2003), starring Colin Farrell and Al Pacino, featured a fictional computer virus called "Ice 9" which would propagate itself over unprotected power sources and erase any hard disks it came into contact with. Lets hope the real Ice IX's M.O. isn't as advanced as that!

   - *JCitizen*
August 29, 2011 at 1:14 am

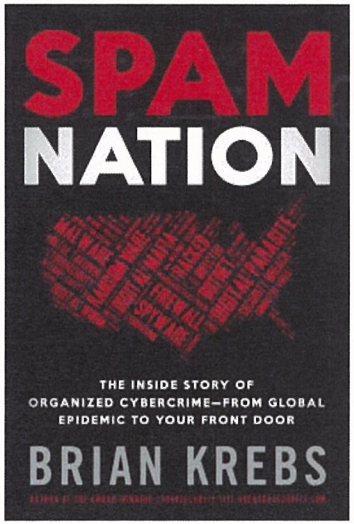
Good one DiamondGeeza!

About the only thing I've seen on regular PCs is reading the keyboard trough the house current source. It can be accomplished using plain old Radio Shack technology. A power conditioner, or UPS can pretty much defeat this, however.

I agree that other capabilities can get greatly inflated, especially through the news media.

-

- **My New Book!**



A New York Times Bestseller!

- Buy at Amazon
- BARNES&NOBLE BOOKSELLERS BUY NOW
- SHOP indie BUY IT NOW AT POLITICS AND PROSE

Recent Posts

- Toward Better Privacy, Data Breach Laws
- KrebsOnSecurity Wins Ntl' Journalism Award
- Lizard Stresser Runs on Hacked Home Routers
- Thieves Jackpot ATMs With 'Black Box' Attack
- Who's Attacking Whom? Realtime Attack Trackers

Subscribe by email

Your email:
Enter email address...

Subscribe Unsubscribe

- **Support KrebsOnSecurity!**

- **SANS Orlando 2015**

Use "SANS_Krebs200"' for $200 off any (4-6 day) class

- **Categories**
  - A Little Sunshine
  - All About Skimmers
  - Breadcrumbs
  - Data Breaches
  - How to Break Into Security
  - Latest Warnings
  - Ne'er-Do-Well News
  - Other
  - Pharma Wars
  - Security Tools
  - Spam Nation
  - Target: Small Businesses
  - The Coming Storm
  - Time to Patch
  - Web Fraud 2.0

- **All About ATM Skimmers**

Click image for my skimmer series.

Archives

- 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 avivah litan chrome chronopay cyberheist f-secure Facebook fbi firefox Glavmed gmail google Google Chrome Igor Gusev internet explorer java Liberty Reserve Mac mastercard mcafee microsoft money mules opera Oracle patch tuesday pavel vrublevsky RSA Spamit spyeye Symantec target data breach trend micro twitter U.S. Secret Service Visa webmoney windows zero day zeus ZeuS Trojan

- **Tools for a Safer PC**

Tools for a Safer PC

- **Blogroll**

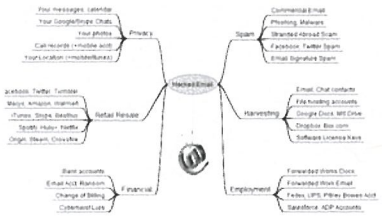
  - Arbor Networks Blog
  - Bleeping Computer
  - CERIAS / Spaf
  - Contagio Malware Dump
  - Cyber Crime & Doing Time
  - Cyveillance Blog
  - DHS Daily Report
  - DSL Reports
  - ESET Threat Blog
  - F-Secure Blog
  - FireEye Malware Intel Lab
  - Fortinet Blog
  - Fox-IT International
  - Google Online Security Blog
  - Imperva Blog
  - Malcovery Security
  - Malware Domain List Forum
  - Malware Don't Need Coffee
  - Microsoft Malware Protection Center
  - Naked Security (Sophos)
  - SANS Internet Storm Center
  - Schneier on Security
  - SecureWorks

- Securing the Human
- Securosis
- Spamtitan Blog
- Steve Gibson/Security Now
- 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

Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

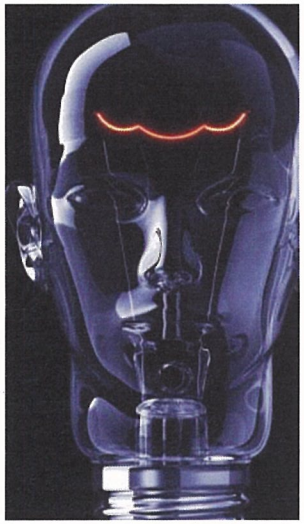
- **eBanking Best Practices**

eBanking Best Practices for Businesses

- **Most Popular Posts**

  - Sources: Target Investigating Data Breach (620)
  - Cards Stolen in Target Breach Flood Underground Markets (445)
  - Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
  - True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
  - Following the Money, ePassporte Edition (353)
  - U.S. Government Seizes LibertyReserve.com (315)
  - Banks: Credit Card Breach at Home Depot (305)
  - Sony Pictures Plans Movie About Yours Truly (273)
  - Who's Selling Credit Cards from Target? (269)
  - Target Hackers Broke in Via HVAC Company (268)

- **Category: Web Fraud 2.0**



Innovations from the Underground

- 

ID Protection Services Examined

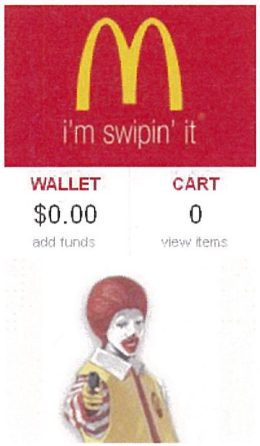
- **Is Antivirus Dead?**

The reasons for its decline

- **The Growing Tax Fraud Menace**

File 'em Before the Bad Guys Can

- **Inside a Carding Shop**



A crash course in carding.

- **Beware Social Security Fraud**

Sign up, or Be Signed Up!
