

Recommended: New virus raids your bank account - but you won't notice

Recommended: Congress takes up controversial anti-piracy SOPA legislation

Recommended: After 16 hours on air at Wall Street protests, a Ustream star is born

Recommended: Chaos Computer Club: German gov't software can spy on citizens

advertisement

Corporate sneakiness. Government waste. Technology run amok. Outright scams. Our effort to unmask these 21st Century headaches and offer solutions that save you time and money.

About this blog Archives E-mail updates Follow on Twitter Subscribe to RSS Like 17k

Leave your comment below

Recommend 4k Tweet 1,337 7.3K

5 days ago

New virus raids your bank account - but you won't notice

The best way to protect yourself from an online financial scam is to diligently check your bank accounts. At least, until now.

Israeli-based Security firm Trusteer has found an elaborate new computer virus that not only helps fraudsters steal money from bank accounts -- it also covers its tracks.

Think of a crime plot involving a spy who plans to break into a high-security building and begins-by swapping out security camera video so guards don't notice anything is amiss. Known as a surveillance camera hack, the technique has been used in dozens of movies.

A new version of the widely prevalent SpyEye Trojan horse works much the same way, only it swaps out banking Web pages rather than video, preventing account holders from noticing that their money is gone.

The Trojan horse employs a powerful two-step process to commit the electronic crime. First, the virus lies in wait until a customer with an infected computer visits an online banking site, steals their login credentials and tricks the victim into divulging additional personal information such as debit card information. Then, after the stolen card number is used for a fraudulent purchase, the virus intercepts any further

advertisement



Raleigh: Mom Makes \$72/Hour Online
We Investigated How She Makes \$8,000/Month. You Won't Believe...



The E-Cigarette EXPOSED
Do not try until you read this new study on the results of using...

Solar Stock Alert - ONYX
Solar Company Secures Brilliant New Energy Technology. Once In... [OnyxService.com](#)

Raleigh: Dermatologists HATE her!
Mom Reveals \$3 Trick To Erase Wrinkles. Shocking Before... [consumerlifestylesonline...](#)

visits to the victim's banking site and scrubs transaction records clean of any fraud. That prevents -- or at least delays -- consumers from discovering fraud and reporting it to the bank, buying the fraudster critical extra time to complete the crime.



Bob Sullivan

Like 17,490

Follow @RedTapeChron 3,785 followers

Trusteer calls it a "post transaction" attack, because much of the virus' effectiveness is attributable to its ability to control what victims see after fraudulent transactions occur. Amit Klein, chief technology officer

for Trusteer, said he believes criminals have used the technique for a few months, and it has infected real consumers.

"I predict that the use of post transaction attack technology will significantly increase as it enables criminals to maximize the amount of fraud they can commit using their initial investment in malware toolkits and infection mechanisms," Klein said.

The new SpyEye came to Trusteer's attention when a large retail bank in the United States spotted it and shared with the firm, he said.

'A very scary tactic'

The virus' evidence-covering techniques are elaborate. First, it keeps track of all fraud committed by the criminal, and makes sure to remove those line items from online transaction lists. It also edits balance amounts to prevent consumers from getting suspicious.

"This is a very scary tactic," said Avivah Litan, a financial fraud analyst at consulting firm Gartner. "Everybody thinks all they have to do is check their transactions and their balances. That's not true anymore."

The new virus technique ups the ante in the cat-and-mouse game between security companies and the computer criminals who try to steal consumers' money. Consumer reports of fraud are still a very important part of fraud-fighting techniques, Litan said.

"Most banks 'let the first transaction through,' because if they stopped everything that was potentially fraud, consumers would get annoyed," she said. In some cases, fraud-checking tools kick in only after initial reports, so this version of SpyEye could buy criminals important time as they try to turn stolen data into cash.

"Usually they only need one day more to get the money, to push the fraud through," she said. "They always want to keep the security guys running after them."

Such cover-your-tracks techniques have been used before by virus writers, Klein said. In a simpler version, criminals who raided online bank accounts and wired money out of them would try to hide the transaction from

advertisement

EPSON
EXCEED YOUR VISION

WorkForce[®] Pro
Run your business at full speed for less.

Save on ink—
up to **50%**
vs. color laser.

[learn more](#)

51 Year Old Mom Looks 27
Raleigh: Mom Publishes Free Facelift Secret That has Angered... [consumerlifestyleonline...](#)



Raleigh: Mom Makes \$72/Hour Online
We Investigated How She Makes \$8,000/Month. You Won't Believe...

The E-Cigarette EXPOSED
Do not try until you read this new study on the results of using...

Raleigh: Mom Makes \$72/Hour Online
We Investigated How She Makes \$8,000/Month. You Won't... [homejobmanual.com](#)

victims using the same Web page interception trick. But this new flavor has more potential for success, because it involves stolen debit card numbers used at third-party merchants, creating complex transactions involving multiple banks and multiple security systems.

Victim account holders who check their balance at an ATM -- or even at a second uninfected computer -- would be able to spot the fraudulent transactions. The virus doesn't impact bank systems, merely the characters that are displayed within the infected system's Web browser. That means paper statements would reveal the fraud, too.

Of course, consumers who rely on paper statements could be a full 30 days behind when it comes to spotting fraudulent transactions.

While Klein is worried about the "post transaction" attack, he said consumers who have vulnerable Web browsers are bound to be victims of one fraudster or another.

"My take is that if your computer is infected with financial malware, it's game over anyway," he said. "My takeaway is you need to prevent getting infected with financial malware in the first place."

Don't miss the next Red Tape:

*Get Red Tape headlines on your [Facebook Wall](#)

*Follow Bob on [Twitter](#).

*Get an [e-mail newsletter](#) with Red Tape stories (requires Newsvine registration).

Explore related topics: [featured](#), [virus](#), [online-banking](#), [trojan-horse](#), [trusteer](#), [troj](#)

Most popular posts

New virus raids your bank account - but you won't notice

5 days ago

[Tweet](#) 1,337
[Recommend](#) 4k

Cordray tells msnbc.com new bureau will help consumers 'muscle up'

2 days ago

[Tweet](#) 13
[Recommend](#) 12

Of course upward mobility is the problem; we're stuck in our homes

6 days ago

[Tweet](#) 13
[Recommend](#) 27

Want to learn about Santorum? You might not want to search the Web at work

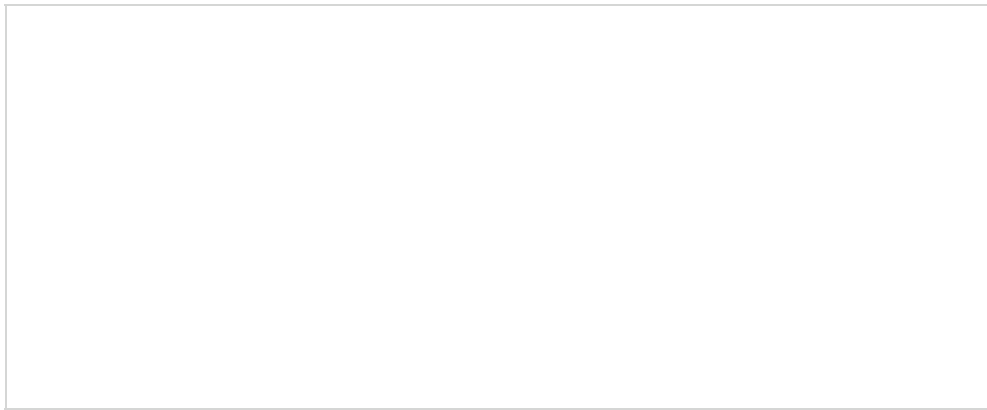
4 Jan 2012 11:05am, EST

[Tweet](#) 73
[Recommend](#) 156

Huge Eurobank, rated 'Britain's worst,' now accused of gouging US consumers

9 Dec 2011 6:31am, EST



[Tweet](#) 105
[Recommend](#) 1k



Discuss this post

* After entering a Facebook comment, your image and name may display on this page. All privacy settings are controlled within your Facebook account.

140 comments


 Post to Facebook Posting as Amanda Rhode ([Change](#))



CJ Fricke · Top Commenter · Assassin at Large

We only have enough money in there for them to go to KFC for a 2 wing basket.

[Reply](#) · [143](#) · [Like](#) · [Follow Post](#) · January 6 at 7:54am



Carl Corbett · Seymour Senior High School

Cj: That is hilarious... GREAT comment – and sadly, so true for most of us Americans nowadays...

[Reply](#) · [17](#) · [Like](#) · January 6 at 9:36am



Betty Carnes · Top Commenter

The problem is they can get the money by overdrawing your account leaving you with the over draft fees!

[Reply](#) · [4](#) · [Like](#) · January 6 at 10:24am



Kaj Sorensen · WarehouseIT at Pacific Blue Micro

@ CJ Fricke I can so relate to you thanks for the morning laugh lol

[Reply](#) · [6](#) · [Like](#) · January 6 at 11:15am

[View 6 more](#)



CJ Fricke · Top Commenter · Assassin at Large

Another poorly researched and written article. How is the Trojan horse put into your system? Attachments? What browsers are vulnerable, which are protected? What do we do to be protected? Wow, poor writing skills – and I am out of work.

[Reply](#) · [60](#) · [Like](#) · [Follow Post](#) · January 6 at 8:09am



Ragan Davis · Works at FWT LLC

Don't open any attachments you aren't sure of, disable cross site scripting in your internet options settings for your browser on the advanced tab and you should be fairly protected at that point but use anti-virus and malware software like malware bytes or Avast and scan your workstation often, its best to be pro active against these things.

[Reply](#) · [25](#) · [Like](#) · January 6 at 9:05am



Irvin Greene · Owner at Self employed

McDonalds is always hiring!

[Reply](#) · [11](#) · [Like](#) · January 6 at 9:13am



Shane Andrews · Grovetown, Georgia



Ragan Davis Also, having more than one method of checking your bank accounts is useful. If you normally use your home PC/laptop to do it, and you have another way, i.e. work computer, smartphone, or even calling the 'robot' at your bank's 1-800 number, you can get around this.

An up-to-date antivirus solution should be the front-line defense against this though.

Reply · 10 · Like · January 6 at 9:41am

[View 15 more](#)



Rg Riggs

So do the latest web browsers have what it takes to fight this post transaction attack? I like how it says to have it but not how to get it.

Reply · 16 · Like · Follow Post · January 6 at 6:24am



Kelly Rife

I was thinking the same thing. Only reporting the problem and not the solution ... Thanks a ton red tape!

Reply · 9 · Like · January 6 at 3:08pm



Kyrillos Wickenberg · Top Commenter

It is not the browser, it is the operating system aka Windows, Mac OS, Linux, that allows operations to be performed on the computer. Lots of smart phones use an Operating System like iOS (apple) and Android phones are now becoming infected with virus because people are indiscriminately downloading and installing apps on them then using them to access their bank accounts. These too can access infected web sites which inturn infect the device.

Reply · 2 · Like · January 7 at 9:48pm



Jason Hernandez · William Howard Taft High School

Kyrillos Wickenberg –well said

Reply · Like · Monday at 5:33pm

[View 137 more](#)

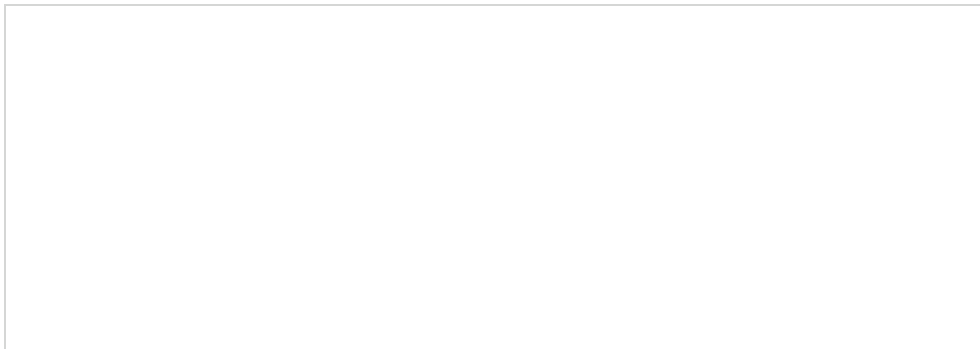
Facebook social plugin



Browse

[credit](#), [featured](#), [privacy](#), [consumer](#), [fees](#), [rights](#), [cards](#), [and](#), [lending](#), [computer](#), [security](#), [redtaperoadtrip2011](#), [sneaky](#), [hackers](#), [identity-theft](#), [to](#), [how](#), [on](#), [money](#), [save](#), [ads](#), [redtaperoadtrip2010](#), [theft](#), [online](#), [facebook](#), [in](#), [truth](#), [cell-phones](#), [bank](#), [scams](#), [spam](#), [identity](#), [safety](#), [child](#), [cybercrime](#), [parenting-debates](#), [jp-morgan-chase](#), [fc](#), [comcast](#), [credit-cards](#), [tv](#), [computer-security](#), [banks](#), [internet](#), [lucky](#), [fraud](#), [credit-and-lending](#), [twitter](#)

advertisement





Bob Sullivan

I'm a reporter for msnbc.com and I try to write stories that make the world a little bit more fair. My blog, The Red Tape Chronicles, is among the most popular consumer affairs columns on the Web. My recent book, Gotcha Capitalism, was a New York Times best seller. Since 1995, I've written about the troubles created for consumers by both technology, covering topics like privacy, identity theft, computer viruses and hackers.

Bob Sullivan Blogroll

[Consumerist](#)

[Life Inc - The economy and you](#)

Archives

- 2012 January (4)
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005

Recent Posts

- Cordray tells msnbc.com new bureau will help consumers 'muscle up'
- New virus raids your bank account - but you won't notice
- Of course upward mobility is the problem; we're stuck in our homes
- Want to learn about Santorum? You might not want to search the Web at work
- Huge Eurobank, rated 'Britain's worst,' now accused of gouging US consumers
- Senate GOP blocks consumer agency nominee Cordray, but who's to blame? (1)
- Consumer: Trove of evidence didn't persuade credit bureau to fix error (2)
- Consumer agency shares top beefs against credit card issuers

Other blogs

- The Body Odd
- Cosmic Log
- PhotoBlog
- Gadgetbox
- Technolog
- Daryl Cagle's Cartoon Blog
- Open Channel
- InGame



top stories

- Moment of truth for the GOP field in SC
- Romney wins big in NH: What now for November?
- Natalee Holloway suspect: I killed Peru woman
- Tensions rise as Pakistan PM fires defense secretary
- Mrs Obama: Tired of 'angry black woman' stereotype
- Stuck in ice: Alaska fuel convoy moves just 50 feet
- Video: Police say gunman targeted rich elderly couple
- US denies killing Iran nuke expert with magnet bomb
- French journalist, several others killed in Syria

US: Billionaire fugitive is 'most powerful' trafficker