



ADVERTISEMENT

Low graphics | Accessibility Help


 Search

Explore the BBC

[▶ Watch](#) ONE-MINUTE WORLD NEWS

Page last updated at 13:15 GMT, Friday, 31 October 2008

[✉ E-mail this to a friend](#)

[🖨️ Printable version](#)

Trojan virus steals banking info

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

The details of about 500,000 online bank accounts and credit and debit cards have been stolen by a virus described as "one of the most advanced pieces of crimeware ever created".



Sinowal infects victims' computers without leaving any trace

The Sinowal trojan has been tracked by RSA, which helps to secure networks in Fortune 500 companies.

RSA said the trojan virus has infected computers all over the planet.

"The effect has been really global with over 2000 domains compromised," said Sean Brady of RSA's security division.

He told the BBC: "This is a serious incident on a very noticeable scale and we have seen an increase in the number of trojans and their variants, particularly in the States and Canada."

The RSA's Fraud Action Research Lab said it first detected the Windows Sinowal trojan in Feb 2006.

Since then, Mr Brady said, more than 270,000 banking accounts and 240,000 credit and debit cards have been compromised from financial institutions in countries including the US, UK, Australia and Poland.

The lab said no Russian accounts were hit by Sinowal.

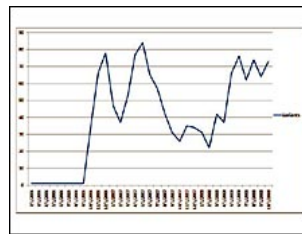
"Drive-by downloads"

RSA described the Sinowal as "one of the most serious threats to anyone with an internet connection" because it works behind the scenes using a common infection method known as "drive-by downloads".

Users can get infected without knowing if they visit a website that has been booby-trapped with the Sinowal malicious code.

Mr Brady said the worrying aspect about Sinowal, which is also known as Torpig and Mebroot, is that it has been operating for so long.

"One of the key points of interest about this particular trojan is that it has existed for two and a half years quietly collecting information," he said. "Any IT professional will tell you it costs a lot to maintain and to store the information it is gathering.



Sinowal has been constantly updated with new variants



ADVERTISEMENT

[LEARN MORE ▶▶](#)

Responsibility. What's your policy?



News Front Page



- Africa
- Americas
- Asia-Pacific
- Europe
- Middle East
- South Asia
- UK
- Business
- Health
- Science & Environment
- Technology
- Entertainment
- Also in the news
- Video and Audio
- Have Your Say
- In Pictures
- Country Profiles
- Special Reports
- Related BBC sites
- Sport
- Weather
- On This Day
- Editors' Blog
- BBC World Service
- Site Version
- UK Version
- International Version
- About the versions

SEE ALSO

- Cybercrime wave sweeping Britain
30 Oct 08 | Technology
- Police stalking cyber fraudsters
17 Oct 08 | UK
- Don't have security nightmares
21 Oct 08 | Technology
- Fraudsters' website shut in swoop
17 Oct 08 | UK
- Bank turmoil fuels phishing boom
10 Oct 08 | Technology
- How secure is your card info?
06 Aug 08 | Technology

RELATED INTERNET LINKS

- RSA
- Fortinet

The BBC is not responsible for the content of external internet sites

TOP TECHNOLOGY STORIES

- Trojan virus steals banking info
- PC users to invent ideal machine
- Joystick gold for action shooter
- [RSS](#) | News feeds

MOST POPULAR STORIES NOW

- [E-MAILED](#) [READ](#) [WATCHED/LISTENED](#)
- Sarah Palin duped by prank call
- US rivals target knife-edge races
- Man who breathed in anthrax dies

"The group behind it have made sure to invest in the infrastructure no doubt because the return and the potential return is so great."

RSA's researchers said the trojan's creators periodically release new variants to ensure it stays ahead of detection and maintain "its uninterrupted grip on infected computers."

While RSA's lab has been tracking the trojan since 2006, Mr Brady admitted that they know a lot about its design and infrastructure but little about who is behind Sinowal.

"There is a lot of talk about where it comes from and anecdotal evidence points to Russia and Eastern Europe. Historically there have been connections with an online gang connected to the Russian Business Network but in reality no one knows for sure."

That he said is because the group is able to use the web to cloak its identity.

Infection

In April 2007, researchers at Google discovered hundreds of thousands of web pages that initiated drive-by downloads. It estimated that one in ten of the 4.5 million pages it analysed were suspect.

Sophos researchers reported in 2008 it was finding more than 6,000 newly infected web pages every day, or about one every 14 seconds.

RSA's fraud action team said it noticed a spike in attacks from March through to September this year.

That is backed up by another online security company called Fortinet. It said from July 2008 to September 2008 the number of reported attacks rose from 10m to 30m. This included trojans, viruses, malware, phishing and mass mailings.



Since May, Sinowal has compromised over 100,000 online bank accounts

"The explosion in the number of attacks is alarming," said Derek Manky of Fortinet.

"But trojans are just one of the players in the game wreaking havoc in cyberspace."

Remedies

While attacks are on the increase, there are some simple steps that users can take to protect their information besides using security software.

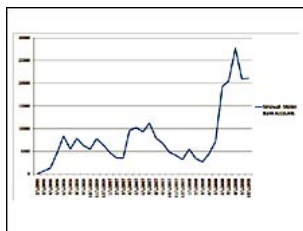
"We have a saying here which is 'think before you link,'" said Mr Manky.

"That just means observe where you are going on the web. Be wary of clicking on anything in a high traffic site like social networks.

"A lot of traffic in the eyes of cyber criminals means these sites are a target because to these people more traffic means more money," he said.

RSA also urged users to be wary if their bank started asking for different forms of authentication such as a social security number or other details.

"People think not clicking on a pop up or an attachment means they are safe. What people don't realise now is that just visiting a website is good enough to infect them."



The rate at which Sinowal has been compromising online bank accounts


RSA said it is co-operating with banks and financial institutions the world over to tell them about Sinowal. It has passed information about the virus to law enforcement agencies.

[Ryanair set for £8 flights to US](#)
[Saddam's luxury yacht up for sale](#)

[Most popular now, in detail](#)

Bookmark with:

[Delicious](#) [Digg](#) [reddit](#) [Facebook](#) [StumbleUpon](#)
What are these?

 [E-mail this to a friend](#)

 [Printable version](#)

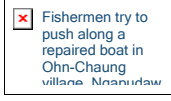
FEATURES, VIEWS, ANALYSIS



Voter power
US election day will see controversial referendums



Afghan stalemate?
Alastair Leithhead looks back on three years in Helmand



Six months on
Burmese seek to rebuild lives after Cyclone Nargis

[SKIP TO TOP](#)

PRODUCTS & SERVICES

[E-mail news](#)

[Mobiles](#)

[Alerts](#)

[News feeds](#)

[Podcasts](#)

 © MMVIII

The BBC is not responsible for the content of external internet sites.

[News Sources](#)
[About BBC News](#)

[About the BBC](#)
[BBC Help](#)
[Contact Us](#)
[Accessibility Help](#)
[Terms of Use](#)
[Jobs](#)
[Privacy & Cookies](#)
[Advertise With Us](#)