

Virtual Heist Nets 500,000+ Bank, Credit Accounts

Washington Post - <http://blog.washingtonpost.com/securityfix/?hpid=sec-tech>

A single cyber crime group has stolen more than a half million bank, credit and debit card accounts over the past two-and-a-half years using one of the most advanced strains of computer spyware in existence, according to research to be published today. The discovery is among the largest stolen data caches ever recovered.

Researchers at **RSA's FraudAction Research Lab** unearthed the massive trove of purloined data while tracking the activities of a family of spyware known as the "**Sinowal**" Trojan, designed to steal data from **Microsoft Windows PCs**.

RSA investigators found more than 270,000 online banking account credentials, as well as roughly 240,000 credit and debit account numbers and associated personal information on Web servers the Sinowal authors were using to set up their attacks. The company says the cache was the bounty collected from computers infected with Sinowal going back to February 2006.

"Almost three years is a very, very long time for just one online gang to maintain the lifecycle and operations in order to utilize just one Trojan," said **Sean Brady**, manager of identity protection for RSA, the security division of **EMC**. "Only rarely do we come across crimeware that has been continually stealing and collecting personal information and payment card data, and compromising bank accounts as far back as 2006."

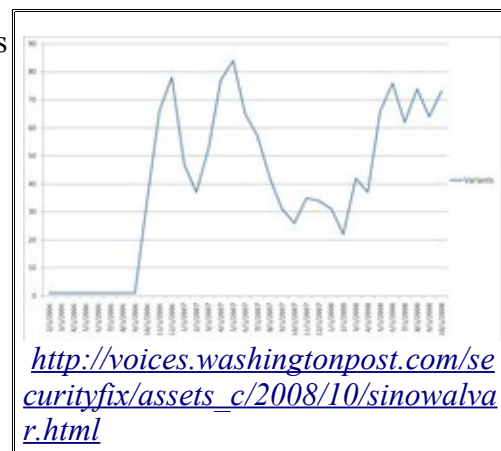
Sinowal, also called "**Torpig**" and "**Mebroot**" by various anti-virus companies, constantly morphs its appearance to slip past security software. Between April and October, researchers spotted an average of 60 to 80 new Sinowal variants per month (see graphic above). Indeed, in the 24 hours ending Oct 30, security researchers at **ThreatExpert.com** saw at least three new versions of Sinowal being released into the wild.

On Oct. 21, [a new Sinowal variant](#) was submitted to **Virustotal.com**, which scans incoming files against nearly three dozen commercial anti-virus programs and maintains a historical record of those results. Only [10 out of 35 of those security programs](#) - or 28.5 percent - identified it as such or even flagged it as suspicious. Another scan of a Sinowal variant sent to VirusTotal a week earlier yielded slightly better results, with just over half of the anti-virus tools detecting it as malicious.

Sinowal also is unique in that hides in the deepest recesses of a host computer, an area known as the "Master Boot Record." The MBR is akin to a computer's table of contents, a file system that loads even before the operating system boots up. According to security experts, many anti-virus programs will remain oblivious to such a fundamental compromise. What's more, completely removing the Trojan from an infected machine often requires reformatting the system and wiping any data stored on it.

The Trojan lies in wait until the victim visits one of more than 2,700 bank and e-commerce sites hard-coded into the malware, at which point it injects new Web pages or information fields into the victim's Web browser. For example, Sinowal can falsely prompt an unsuspecting victim for personal information, such as a Social Security number or password when he or she visits one of the targeted financial institution Web sites. Any stolen data is regularly uploaded to Web servers controlled by the Trojan's authors.

The makers of Sinowal typically have spread their Trojan by sewing malicious code into the fabric of large numbers of legitimate, hacked Web sites. When an unsuspecting **Windows user** visits one of these sites, the



code left on the site tries to install the Trojan using one of several **known Web browser security holes**, such as vulnerabilities found in popular video and music player plug-ins like **Macromedia Flash** and **Apple's QuickTime player**.

The Sinowal gang appear to have profited handsomely from a spate of high-profile Web compromises reported of late: More than 100,000 bank account credentials were stolen by the Trojan in the last six months alone, RSA found (see graphic above).

It's not clear exactly who's behind these attacks, but evidence points to Russian malware gangs. Brady said Sinowal had early ties with the [Russian Business Network](#), a notorious, cyber-crime friendly Web hosting firm in St. Petersburg, Russia, that was [dispersed](#) last year due to international media attention. While the Sinowal authors no longer use RBN as a home base, Brady said his team could find no trace of a single Russian victim in the entire database of credentials and identities stolen from customers of hundreds of banks across the United States, Europe and Asia, and at least 27 other countries.

According to several analysts at [iDefense](#), a security intelligence firm in Sterling, Va., more than a dozen criminals operating the Sinowal data theft network have been thumbing their noses at authorities for some time. While examining a Web server used in a Sinowal attack earlier this year, iDefense found a spoof of the [U.S. Marshals Web site](#) apparently created by the criminals (click the image above to enlarge).

iDefense said each nickname on the fake site corresponds to the digital credentials that gang members used to access the Web server. The bogus wanted poster includes caricatures of such famous figures as Mikhail Gorbachev; Leonid Brezhnev, Joseph Stalin (Perevodchik, "translator" in Russian); Vladimir Lenin; and Russian Prime Minister Vladimir Putin ("Shaitan," or "devil").

