Torpig

By Contributors to Wikimedia projects

Published: 2007-05-09 · Archived: 2026-04-05 17:37:32 UTC

From Wikipedia, the free encyclopedia

Torpig, also known as **Anserin** or **Sinowal** is a type of botnet spread through systems compromised by the Mebroot rootkit by a variety of trojan horses for the purpose of collecting sensitive personal and corporate data such as bank account and credit card information. It targets computers that use Microsoft Windows, recruiting a network of zombies for the botnet. Torpig circumvents antivirus software through the use of rootkit technology and scans the infected system for credentials, accounts and passwords as well as potentially allowing attackers full access to the computer. It is also purportedly capable of modifying data on the computer, and can perform man-in-the-browser attacks.

By November 2008, it was estimated that Torpig had stolen the details of about 500,000 online bank accounts and credit and debit cards and was described as "one of the most advanced pieces of crimeware ever created".[1]

Torpig reportedly began development in 2005, evolving from that point to more effectively evade detection by the host system and antivirus software.[2]

In early 2009, a team of security researchers from University of California, Santa Barbara took control of the botnet for ten days. During that time, they extracted an unprecedented amount (over 70 GB) of stolen data and redirected 1.2 million IPs on to their private command and control server. The report[3] goes into great detail about how the botnet operates. During the UCSB research team's ten-day takeover of the botnet, Torpig was able to retrieve login information for 8,310 accounts at 410 different institutions, and 1,660 unique credit and debit card numbers from victims in the U.S. (49%), Italy (12%), Spain (8%), and 40 other countries, including cards from Visa (1,056), MasterCard (447), American Express (81), Maestro (36), and Discover (24).[4]

Initially, a great deal of Torpig's spread was attributable to phishing emails that tricked users into installing the malicious software. More sophisticated delivery methods developed since that time use malicious banner ads which take advantage of exploits found in outdated of versions of Java, or Adobe Acrobat Reader, Flash Player, Shockwave Player. A type of Drive-by download, this method typically does not require the user to click on the ad, and the download may commence without any visible indications after the malicious ad recognizes the old software version and redirects the browser to the Torpig download site. To complete its installation into the infected computer's Master Boot Record (MBR), the trojan will restart the computer.[2]

During the main stage of the infection, the malware will upload information from the computer twenty minutes at a time, including financial data like credit card numbers and credentials for banking accounts, as well as e-mail accounts, Windows passwords, FTP credentials, and POP/SMTP accounts.[4]

- Mebroot

- Drive-by download
- Phishing
- Man-in-the-browser
- Conficker a worm that also uses domain name generation (or domain flux)
- Timeline of computer viruses and worms

1. ^ BBC News: Trojan virus steals bank info
2. ^ Jump up to: *a* *b* *Carnegie Mellon University. "Torpig". Archived from the original on 19 May 2015. Retrieved 25 July 2015.*
3. ^ UCSB Torpig report
4. ^ Jump up to: *a* *b* *Naraine, Ryan (4 May 2009). "Botnet hijack: Inside the Torpig malware operation". ZDNet. Archived from the original on 1 August 2015. Retrieved 1 August 2015.*

- Taking over the Torpig botnet, *IEEE Security & Privacy*, Jan/Feb 2011

- UCSB Analysis
- One Sinowal Trojan + One Gang = Hundreds of Thousands of Compromised Accounts by RSA FraudAction Research Lab, October 2008
- Don't be a victim of Sinowal, the super-Trojan by Woody Leonhard, WindowsSecrets.com, November 2008
- Antivirus tools try to remove Sinowal/Mebroot by Woody Leonhard, WindowsSecrets.com, November 2008
- Torpig Botnet Hijacked and Dissected covered on Slashdot, May 2009
- How to Steal a Botnet and What Can Happen When You Do by Richard A. Kemmerer, GoogleTechTalks, September 2009
