Zeus (malware)

By Contributors to Wikimedia projects

Published: 2009-11-19 · Archived: 2026-04-05 21:46:01 UTC

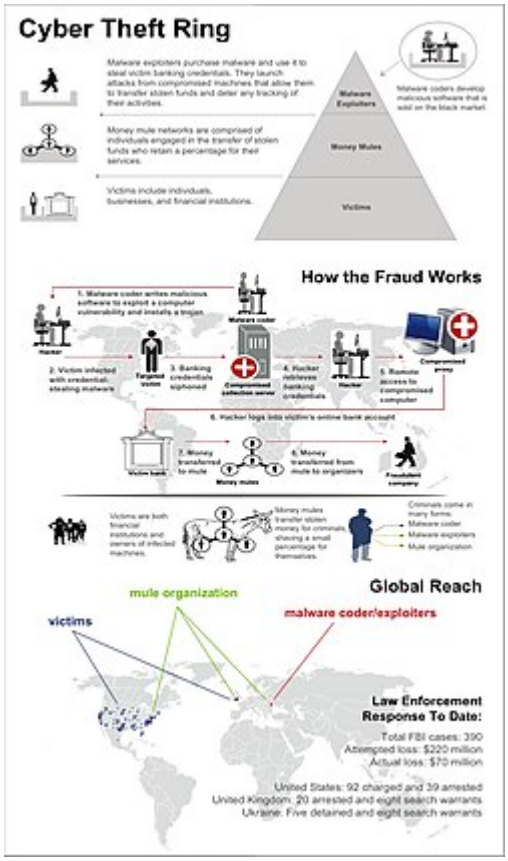
From Wikipedia, the free encyclopedia

"Zbot" redirects here. For the action figures, see Zbots.

Zeus	
Malware details	
Type	Trojan Horse
Origin	July 2007

Zeus is a Trojan horse malware package that runs on versions of Microsoft Windows. It is often used to steal banking information by man-in-the-browser keystroke logging and form grabbing.[1] Zeus is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation,[2] it became more widespread in March 2009. In June 2009 security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and *BusinessWeek*.[3] Similarly to Koobface, Zeus has also been used to trick victims of technical support scams into giving the scam artists money through pop-up messages that claim the user has a virus, when in reality they might have no viruses at all. The scammers may use programs such as Command prompt or Event viewer to make the user believe that their computer is infected.[4]

Zeus is very difficult to detect even with up-to-date antivirus and other security software as it hides itself using stealth techniques.[5] It is considered that this is the primary reason why the Zeus malware then had become the largest botnet on the Internet: Damballa estimated that the malware infected 3.6 million PCs in the U.S. in 2009.[6] Security experts are advising that businesses continue to offer training to users to teach them not to click on hostile or suspicious links in emails or Web sites, and to keep antivirus protection up to date. Antivirus software does not claim to reliably prevent infection; for example Symantec's Browser Protection says that it can prevent "some infection attempts".[7]



FBI: The Zeus Fraud Scheme

In October 2010 the US FBI announced that hackers in Eastern Europe had managed to infect computers around the world using Zeus.[8] The virus was distributed in an e-mail, and when targeted individuals at businesses and municipalities opened the e-mail, the trojan software installed itself on the victimized computer, secretly capturing passwords, account numbers, and other data used to log into online banking accounts.

The hackers then used this information to take over the victims' bank accounts and make unauthorized transfers of thousands of dollars at a time, often routing the funds to other accounts controlled by a network of money mules, paid a commission. Many of the U.S. money mules were recruited from overseas. They created bank accounts using fake documents and false names. Once the money was in the accounts, the mules would either wire it back to their bosses in Eastern Europe, or withdraw it in cash and smuggle it out of the country.[9]

More than 100 people were arrested on charges of conspiracy to commit bank fraud and money laundering, over 90 in the US, and the others in the UK and Ukraine.[10] Members of the ring had stolen $70 million.

In 2013 Hamza Bendelladj, known as Bx1 online, was arrested in Thailand[11] and deported to Atlanta, Georgia, USA. Early reports said that he was the mastermind behind ZeuS. He was accused of operating SpyEye (a bot functionally similar to ZeuS) botnets, and suspected of also operating ZeuS botnets. He was charged with several counts of wire fraud and computer fraud and abuse.[12] Court papers allege that from 2009 to 2011 Bendelladj and others "developed, marketed, and sold various versions of the SpyEye virus and component parts on the Internet and allowed cybercriminals to customize their purchases to include tailor-made methods of obtaining victims' personal and financial information". It was also alleged that Bendelladj advertised SpyEye on Internet forums

devoted to cyber- and other crimes and operated Command and Control servers.[13] The charges in Georgia relate only to SpyEye, as a SpyEye botnet control server was based in Atlanta.

Possible retirement of creator

[edit]

In late 2010, a number of Internet security vendors including McAfee and Internet Identity claimed that the creator of Zeus had said that he was retiring and had given the source code and rights to sell Zeus to his biggest competitor, the creator of the SpyEye trojan. However, those same experts warned the retirement was a ruse and expect the developer to return with new tricks.[14][15]

- Conficker
- Command and control (malware)
- Gameover ZeuS, the successor to ZeuS
- Jabber Zeus
- Operation Tovar
- Timeline of computer viruses and worms
- Tiny Banker Trojan
- Torpig
- Zombie (computer science)

1. ^ *Abrams, Lawrence. "CryptoLocker Ransomware Information Guide and FAQ". Bleeping Computer. Retrieved 25 October 2013.*
2. ^ *Jim Finkle (17 July 2007). "Hackers steal U.S. government, corporate data from PCs". Reuters. Retrieved 17 November 2009.*
3. ^ *Steve Ragan (29 June 2009). "ZBot data dump discovered with over 74,000 FTP credentials". The Tech Herald. Archived from the original on 25 November 2009. Retrieved 17 November 2009.*
4. ^ *"How to Recognize a Fake Virus Warning". Retrieved 28 July 2016.*
5. ^ *"ZeuS Banking Trojan Report". Dell SecuWorks. 10 March 2010. Retrieved 2 March 2016.*
6. ^ *"The Hunt for the Financial Industry's Most-Wanted Hacker". Bloomberg. Bloomberg Business. 18 June 2015. Retrieved 2 March 2016.*
7. ^ *"Trojan.Zbot". Symantec. Archived from the original on 30 January 2010. Retrieved 19 February 2010.*
8. ^ *"Cyber Banking Fraud". The Federal Bureau of Investigation. Retrieved 2 March 2016.*
9. ^ *FBI (1 October 2010). "CYBER BANKING FRAUD Global Partnerships Lead to Major Arrests". Archived from the original on 3 October 2010. Retrieved 2 October 2010.*
10. ^ *BBC (1 October 2010). "More than 100 arrests, as FBI uncovers cyber crime ring". BBC News. Retrieved 2 October 2010.*
11. ^ *Al Jazeera (21 September 2015). "Hamza Bendelladj: Is the Algerian hacker a hero?". AJE News. Retrieved 21 March 2016.*
12. ^ *Zetter, Kim. "Alleged 'SpyEye' Botmaster Ends Up in America, Handcuffs, Kim Zetter, Wired, 3 May 2013". Wired. Wired.com. Retrieved 30 January 2014.*

13. ^ *"Alleged "SpyEye" mastermind extradited to US, Lisa Vaas, 7 May 2013, Sophos nakedsecurity"*. *Nakedsecurity.sophos.com. 7 May 2013. Archived from the original on 21 April 2022. Retrieved 30 January 2014.*
14. ^ *Diane Bartz (29 October 2010). "Top hacker "retires"; experts brace for his return". Reuters. Retrieved 16 December 2010.*
15. ^ *Internet Identity (6 December 2010). "Growth in Social Networking, Mobile and Infrastructure Attacks Threaten Corporate Security in 2011". Yahoo! Finance. Retrieved 16 December 2010.*

- "Measuring the in-the-wild effectiveness of Antivirus against Zeus" Study by Internet security firm Trusteer.
- "A summary of the ZeuS Bot" A summary of ZeuS as a Trojan and Botnet, plus vector of attacks.
- "The Kneber BotNet" by Alex Cox Archived 21 April 2022 at the Wayback Machine NetWitness Whitepaper on the Kneber botnet.
- "België legt fraude met onlinebankieren bloot" Dutch news article about a banking trojan
- "Indications in affected systems" Archived 8 January 2018 at the Wayback Machine Files and registry keys created by different versions of Zeus Trojan.
- Zeus, le dieu des virus contre les banques Archived 27 January 2022 at the Wayback Machine (in French)
- Zeus Bot's User Guide
- Zeus source code at GitHub
- Botnet Bust - SpyEye Malware Mastermind Pleads Guilty, FBI
