ZeuS Trojan

Taylor Kvarda

April 4, 2012

What is ZeuS?

- **Trojan**: standalone malicious program designed to give full control of infected PC to another PC.
- **Target**: Windows users.
- **Goal**: steal bank account information in order to steal money.

More background.

- The ZeuS trojan/botnet uses a client-server approach to control remotely. The trojan is available for purchase from underground forums ranging anywhere from 700 USD to 15000 USD, depending on which version you purchase. Furthermore, the trojan allows for customization on a per user basis to choose what information the owner specifically wants out of the trojan.

How it works.

1. Infects users machine through drive-by download or phishing.
2. Connects to the ZeuS botnet.
3. Owner of the specific trojan controls it from a remote location using provided PHP and SQL template files.
4. Steal bank account information depending on how the owner customized the trojan.
5. ????
6. Profit.

How part 2.

- Primary source of gathering information is through man-in-the-browser keystroke logging and form grabbing.
- Mainly gathers login credentials, although credit/debit card numbers and bank account information probably works as well.

How to get infected.

- Don’t follow smart internet browsing practices.
- Visit untrustworthy sites.
- Download and run anything and everything.

How to remove infection.

- You don't. ZeuS is a stealthy trojan. This means that it intercepts antivirus software requests to the OS and passes those requests to itself. It then returns an uninfected version of the file it is located in, making the file seem harmless.
- Some antivirus software can counter stealth, but it is very difficult and not reliable.
- The only reliable means of removing a stealthy trojan is to reinstall a known clean version/backup of the OS.

Am I infected?

- An estimated 3.6 million PCs are infected in the US alone.
- Since ZeuS is stealthy, it is hard to tell if you are infected. If you've ever had money stolen from an account, you may want to reinstall your OS just in case.

What damage has been done?

- In 2010, more than 100 people were arrested for conspiracy to commit bank fraud and money laundering.
- 90 of these people were in the US, with the other 10 in the UK and Ukraine.
- These 100 people managed to steal $70 million combined.

What is being done to prevent ZeuS?

- Besides the aforementioned arrests, Microsoft has accused 39 unnamed individuals controlling portions of the botnet of stealing $100 million and spamming.
- Multiple C&C (command and control) servers were seized from Lombard, IL, and Scranton, PA.
- Microsoft's legal team used the RICO Act to make the accusations.

Where is ZeuS heading?

- Source code of a specific version was released in May 2011.
- A new build is in the works that relies on P2P capabilities instead of client-server conversation.
- Experts say that this will make it more difficult to determine the location of owners of the software since they wont be on centralized servers.

References

http://www.pandasecurity.com/homeusers/security-info/classic-malware/trojan/
http://www.secureworks.com/research/threats/zeus/?threat=zeus http://www.abuse.ch/?p=3499
http://www.bbc.co.uk/news/world-us-canada-11457611 http://csis.dk/en/csis/blog/3229/
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf http://en.wikipedia.org/wiki/Zeus_(trojan_horse)