# Project Blitzkrieg

By Emily Laughren

# What is Project Blitzkrieg?

- A man-in-the-middle session highjacking attack for stealing money from bank accounts
- Targeted at 30 large US banks, with C&C servers located in Eastern Europe
- Based on malware of the name “Gozi Prinimalka,” from the Gozi Trojan family, which uses similar tactics to steal information and send it back to a C&C server.
- First announced in October 2012, determined to be a threat in December 2012
- Anticipated attack date: Spring 2013

# Initial Infection

- The malware infects systems via typical phishing methods.  A user installs what they believe to be a safe file or software update that contains malicious files.
- The downloaded object contains a backdoor called “BKDR_URSINF.B,” which drops the following into the victim's user profile folder:
  - govXXXX.exe- set to run whenever the user logs in
  - govold.exe
  - govtemp1.exe
  - govcookies.txt
  - govcookies.dat
- The malware is also able to set up a Telnet connection (to send/receive backdoor commands) and a SOCKS proxy connection on the victim's PC.

# Gaining Victim Information

- The malware depends on a combination of webinjects and “function hooking” to collect user information.  Function hooks allow the malware to modify the behavior of common API functions already in the system by causing the system to jump to the malware's malicious implementation of the function when it is called.
- Webinjects allow the attacker to collect usernames, passwords when victims visit their banking websites (at URLs hardcoded into a configuration file in the malware), and this information is sent to the attacker.
- Attacker is also able to collect system information such as OS version, time zone, browser version, etc.

# Transferring Money

- The attacker has collected account and system information from the victim, and also has established a proxy connection on the victim's computer.
- The attacker uses this information to create a virtual machine “clone” of the victim's PC, goes to their banking website, and makes a transfer.
- Prinimalka backend provides information for how/where to drop transferred funds.

# Phone Flooding

- Many banks call or send text messages to customers when large transfers occur.
- Gozi Prinimalka uses “phone flooding” to prevent banks from being able to get in contact with account holders
- Phone flooding: continuous calls to a phone number via VoIP (in this case, Skype).

# How Bad Is It?

- 300-500 computers in the US are infected
- Not much news since October from vorVzakone
- Targeted attacks: Attack a few accounts with high balances and instead of several with lower balances

# How Do We Prevent It?

- Don't download suspicious files, avoid suspicious emails.
- ***Two factor authentication should be required for US banks***

# Sources


http://ddos.arbornetworks.com/2012/10/trojan-prinimalka-bits-and-pieces/

http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf

http://krebsonsecurity.com/2012/12/new-findings-lend-credence-to-project-blitzkrieg/

http://blog.trendmicro.com/trendlabs-security-intelligence/probing-the-gozi-prinimalka-malware/

http://blogs.rsa.com/cyber-gang-seeks-botmasters-to-wage-massive-wave-of-trojan-attacks-against-u-s-banks/

http://www.secureworks.com/cyber-threat-intelligence/threats/gozi/

http://en.wikipedia.org/wiki/SOCKS

http://en.wikipedia.org/wiki/Telnet

http://en.wikipedia.org/wiki/Hooking

http://www.symantec.com/security_response/writeup.jsp?docid=2009-060121-0427-99&tabid=2

http://www.codeproject.com/Articles/37228/API-Hooking-LoadLibrary

http://about-threats.trendmicro.com/Malware.aspx?language=au&name=BKDR_URSNIF.B

http://www.bankinfosecurity.com/banks-prepared-for-new-trojan-a-5224/op-1