ANATOMY OF A FINANCIAL CRIME

Hal Pomeranz
Deer Run Associates

Copyright © Hal Pomeranz (hal@deer-run.com) and Deer Run Associates. All rights reserved.
The FBI and international law enforcement, working in an unprecedented partnership, have disrupted a large-scale, international organized cybercrime operation active in several countries that resulted in numerous search warrants and arrests.

Operation Trident Beach began in May 2009, when FBI agents in Omaha, Nebraska, were alerted to automated clearing house (ACH) batch payments to 15 separate bank accounts throughout the United States. Agents quickly traced the scope of the crime and partnered with local, state, and federal partners, cybercrime task forces, working groups, and foreign police agencies in the Netherlands, Ukraine, and the United Kingdom to bring those responsible to justice.

The cyber thieves targeted small- to medium-sized businesses, municipalities, churches, and individuals, infecting their computers using a version of the Zeus Botnet. The malware centered on stealing account...
http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits
http://www.youtube.com/watch?v=CzdBCDPETxk
http://www.fortiguard.com/analysis/zeusanalysis.html
Meet Zeus

- Complete crimeware kit
- Entry-level cost of $3000-$4000
- Continually evolving

How Computers Are Infected

- Drive-By Malware
- Phishing Scams
- Malicious Email Attachments
- Bogus Zeus crimeware downloads
http://voices.washingtonpost.com/securityfix/2009/10/ubiquitous_zeus_trojan_targets.html
http://news.cnet.com/8301-27080_3-20002425-245.html
Immediately Post-Infection

- Zeus downloads encrypted config file
- Transmits system details to C2 server
- May receive additional commands
What Can Attackers Do?

- Capture (banking) credentials
- Web injection
- Remote control
- Keystroke logging
- Screen grabs
- Proxy services
- Spamming
A Typical Theft (2)

- Attackers steal credentials
- Set up bogus employee or vendor accts
- Accounts are actually "mules"
- Transfers typically kept under $10K
- Mules wire money (less commission)
- Money sent to Eastern Europe
- Mules end up being on the hook for funds
A Word About Mules

- Often recruited via legitimate job sites
- Receive instructions via legitimate-seeming web sites
- Used to:
  - "Process payments"
  - Trans-ship stolen merchandise ("Pack Mules")
  - Fix attackers' grammar and spelling

Bad News for Small Business

Financial Services Information Security News:

ACHI fraud scams total $100 million, FBI says

By Marcia Savage, Site Editor
03 Nov 2009 / SearchFinancialSecurity.com

The surge of Automated Clearing House (ACHI) fraud committed by criminals stealing the online banking credentials of small and midsize businesses has resulted in approximately $100 million in attempted losses, according to the FBI.

Criminals are hitting businesses at a rapid clip, with several new cases opened each week, the FBI said in an IC3 alert released Tuesday by the Internet Crime Complaint Center (IC3).

"FBI analysis has found in most cases, the victim's accounts are held at local community banks and credit unions, some of which use third-party service providers to process ACH transactions," the IC3 reported. "The bank account holders are often small- to medium-sized businesses across the United States, in addition to court systems, school districts, and other public institutions."

The IC3 alert comes less than a week after the Federal Deposit Insurance Corporation warned of an increase in schemes that recruit "money mules" to siphon money from business bank accounts through fraudulent electronic funds transfers, such as ACH transfers. The FDIC issued an alert on Aug. 26 about increased reports of fraudulent EFTs hitting bank business customers.

IC3, which is a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice

http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1373452,0,0.html
Combatting Zeus – Client Side

- Crimeware revs rapidly
- Uses encryption and packing
- Typical endpoint detection not working

- *FBI recommendation is to use dedicated computer for on-line banking*

http://news.cnet.com/8301-27080_3-10370164-245.html
https://zeustracker.abuse.ch/index.php
C2 Servers (Continued)

- Use "fast flux" domains
- "Bullet-proof hosting" arrangements
- Often located in unfriendly jurisdictions

Bottom line: difficult targets
http://blogs.zdnet.com/security/?p=5110
Take-Aways

- Zeus crimeware is widespread
- End-point protections not working
- Current on-line security not working
- Small businesses being targeted
- Significant financial losses
- Don’t become a mule!

"Let’s be careful out there…"
Wrapping Up

- Any final questions?
- As always, thanks for listening...