

## Zeus Botnets: Malware and ACH/EFT Fraud

PAUL MELSON



## What's a botnet?



## What's a botnet?

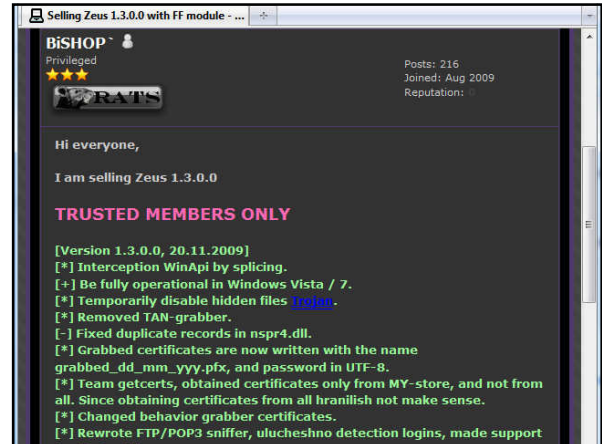
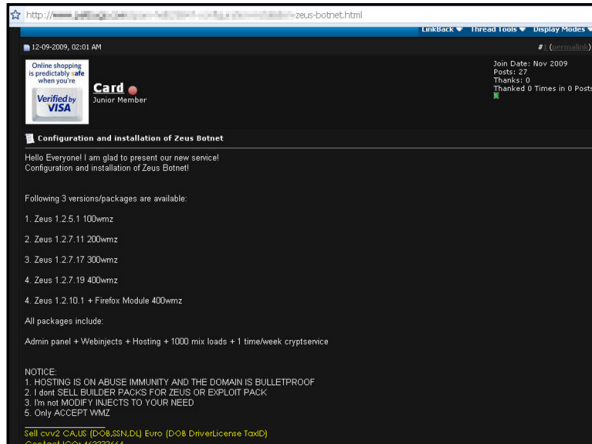
- A. This is where spam comes from
- B. DDoS for hire
- C. Fraud & identity theft
- D. All of the above

- Compromised computers running malware
- Centrally controlled
  - IRC, P2P, HTTP/HTTPS, DNS



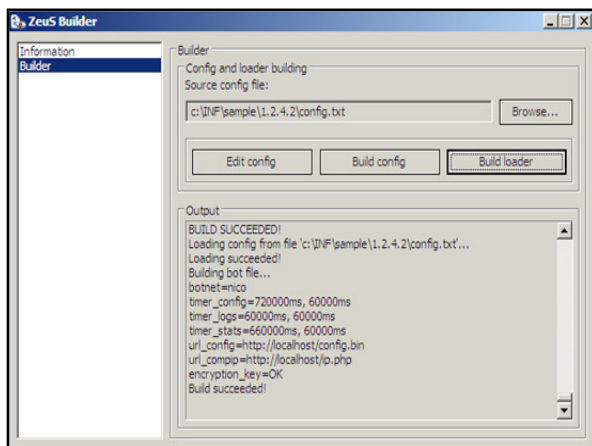
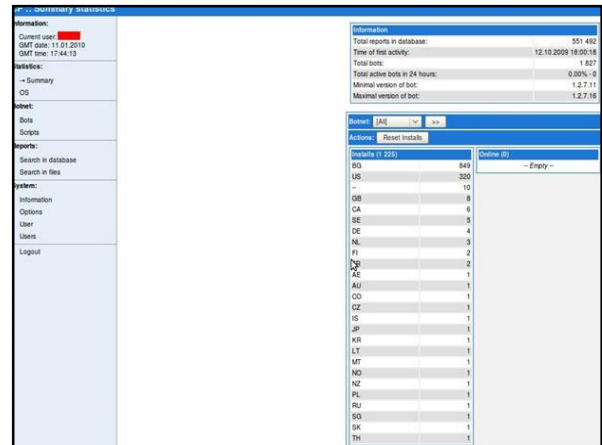
## The Zeus Botnet Kit

- Thought to be responsible for most of the reported ACH fraud incidents last year
- Made-to-order malware
- Reportedly, cost to criminal for custom version is \$3000 depending on options
- Unlike other kits like YES and BlackSun, Zeus does not sell exploits with its kit



## The Zeus Botnet Kit

- Components
  - Webkit command & control console (PHP/MySQL)
  - Zeus Builder binary generator
- Custom command & control options
  - Encrypted HTTP
  - Jabber
  - VNC (over encrypted HTTP)



## The Zeus Botnet Kit

- Self-protection features
  - %SystemRoot%\system32\drivers\etc\hosts file tampering
  - Automatic repacking of binaries
  - Polymorphic encryption (1.4.x and later)
- Data theft
  - Stored IE passwords
  - Web injection, aka login form stealing for Firefox & IE
  - Digital certificates used for authentication

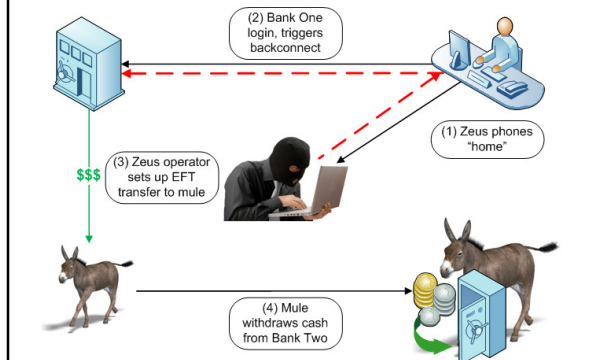
## Malware Man-In-The-Browser

- Presents fake login page / logout button to user
- Upon recognized bank login, phones home to waiting operator
- Steals bank website login information
- Steals Security Certificates
  - Used by Bank of America
- Hijacks sessions that use RSA tokens
  - Used by E\*Trade, Credit Suisse
  - This is reportedly a \$1,500 option for Zeus

## How ACH / EFT Fraud Works

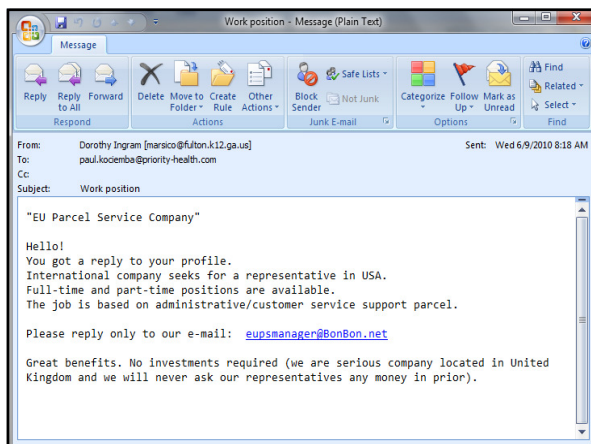
- Corporate login to bank website is stolen
- Thief transfers funds to “mule” accounts in the US
- Mules withdraw money in cash
- Mules wire cash to foreign countries in the form of a money order
- Thief cashes money order

## How ACH / EFT Fraud Works



## Mule Recruiting

- “Work From Home” scam
- Person is told they are working in a customer service or billing position
- Person uses their personal checking account to receive funds
- And after they do the wire transfer and are burned...
- ...their identity is sold on the black market and they get burned a second time



## Money Laundering

- Mule withdraws cash
- Cash is then wired via Western Union to an alias in a foreign country
  - Ukraine
  - China
  - Australia
  - Nigeria
- Money is picked up by another local mule
- ...and then it's *really* gone

## Michigan Case Study #1

- Insurance Services Firm on East side of Michigan
- \$150K stolen from trust account
- Transfer amounts just under \$10K to avoid IRS notification
- Sent to individual accounts across USA
- Victim has recovered approx. \$70K so far
- Confirmed instance of Zeus variant

## Michigan Case Study #2

- Construction company in central Michigan
- \$700K stolen from a payroll account
- Bank website used RSA token for login
- Transfer amounts just under \$10K to avoid IRS notification
- Transfers withdrawn in cash by “mules”
- Confirmed instance of ZeuS variant

## Detecting Zeus on Your Network

- UPnP search queries
  - 3x UDP packets to 239.255.255.250 on port 1900
- HTTP GET
  - pulls down config file on initial infection
  - default filename is /config.bin
  - server response is binary file (application/octet-stream)
- HTTP POST
  - check-ins use HTTP POST to send an RC4-encrypted string
  - Server responses are RC4-encrypted using the same key
- LuckySploit
  - "Welcome to LuckySploit:) \n ITS TOASTED";

## Risk Areas in Your Business

- Payroll
- Accounts Payable
- Insurance Claims
- Commissions
- Point of Sale
- Anything that can use EFT to send money

## Countermeasures

- Dual control for banking web sites
- Dedicated workstations
- Specialized Security Software
  - Trusteer Rapport
- Bank on a Mac?

## I Thought the FBI Busted Zeus?

- 9/28 – 15 arrested in UK
- 9/30 – 10 arrested in US
- Ties to organized crime in Ukraine
- Targeted customers of UK banks: HSBC, Royal Bank of Scotland, Barclays, Lloyds TSB
- Few details are publicly available as of right now
- This is one of many known active Zeus botnets
- This is *not* Kneber
- This is *not* a fast-flux botnet

## Underground Mergers?!

- In October, following the FBI arrests, Monstr announces his retirement on several carding web sites.
- Within days of his announcement, Harderman announces that he will begin supporting any existing ZeuS customers and that he has purchased the source code from Monstr.
- In January, we see the first hybrid release of SpyEye, which incorporates several ZeuS features.



## Discussion

Paul Melson  
 pmelson@gmail.com  
 twitter.com/pmelson  
 pmelson.blogspot.com