Understanding the Attackers: Cybercrime and the Cyber Underground Economy

Richard A. Kemmerer

Computer Security Group
Department of Computer Science
University of California, Santa Barbara

http://seclab.cs.ucsb.edu
Perfect Storm

• Hackers realize potential monetary gains associated with Internet fraud
  – Shift from “hacking for fun” to “hacking for profit”
• Traditional crime organizations realize the potential of the Internet for their endeavors
• Integration of hacker’s sophisticated computer attacks with organized crime’s well-established fraud attacks results in an underground economy similar to legitimate economies
Underground Economy

- Trades compromised hosts, personal information, and services
- Makes it possible to significantly increase the scale of the frauds carried out on the Internet
- Allows criminals to reach millions of potential victims
- Criminals are using
  - IRC channels to verify stolen credit cards
  - e-casinos to launder money
  - fast-flux networks to create attack-resilient services
Cybercrime

• **General definition**
  – Using a computer connected to the Internet for criminal purposes
    • Financial
    • Theft of intellectual property
    • Service disruption

• **Organized cybercrime**
  – Professional organizations that make a living off of electronic crimes
  – Affiliate networks
  – Commercial services
Approach to Understanding Cybercrime

• Developing novel techniques and tools to analyze the underground economy
• Goal is to obtain a comprehensive picture of the complete criminal process
• Create models of
  – Cyber-underground market
  – Actors in the market
  – Processes and interactions between actors
  – Underlying infrastructure
• Leverage these models and develop techniques to disrupt parts of the criminal process
Mission Cyber - Assets

Sensor Alerts
Correlation Engine
Impact Analysis
Simulation/Live Security Exercises

Real World Enterprise Network

Observations: Netflow, Probing, Time analysis

Analysis to get up-to-date view of cyber-assets

Analysis to determine dependencies between assets and missions

Create semantically-rich view of cyber-mission status

Impact Analysis

Data

COAs

Data

Predict Future Actions

Analyze and Characterize Attackers

Data

Simulation/Live Security Exercises

Mission Model
Cyber-Assets

Data

Data

Data

Observations: Netflow, Probing, Time analysis
Three Major Projects

• Taking over the Torpig botnet

• Analyzing Fake Antivirus sites

• Assessing the preparedness of power distribution system operators
Botnet Terminology

• **Bot**
  – an application that performs some action or set of actions on behalf of a remote controller
  – installed on a victim machine (zombie)
  – modular (plug in your functionality/exploit/payload)

• **Botnet**
  – network of infected machines controlled by a malicious entity

• **Control channel**
  – required to send commands to bots and obtain results and status messages
  – usually via IRC, HTTP, HTTPS, or Peer-to-Peer

• **Bot Herder**
  – aka botmaster or controller
  – owns control channel, sends commands to botnet army
  – motivations are usually power or money
Torpig

• Trojan horse
  – distributed via the Mebroot “malware platform”
  – injects itself into 29 different applications as DLL
  – steals sensitive information (passwords, HTTP POST data)
  – HTTP injection for phishing
  – uses “encrypted” HTTP as C&C protocol
  – uses domain flux to locate C&C server

• Mebroot
  – spreads via drive-by downloads
  – sophisticated rootkit (overwrites master boot record)
Innocent victim

"Hacked" web servers

"Drive-By Download" server

Mebroot C&C

Injection server

Commands + torpig

Stolen data
Example Phishing Page
Sinkholing Torpig C&C Overview

• Reverse engineered name generation algorithm and C&C protocol
• Observed that domains for 01/25 – 02/15 unregistered
• Registered these domains ourselves
• Unfortunately, Mebroot pushed new Torpig binary on 02/04
• We controlled the botnet for ~10 days
• Data
  – 8.7 GB Apache logs
  – 69 GB pcap data (contains stolen information)
Conclusions

• Unique opportunity to understand potential for profit and malicious activity of botnet’s creators
• Previous evaluations of botnet sizes based on distinct IPs may be grossly overestimated
• Botnet victims are users with poorly maintained machines and choose easily guessable passwords to protect sensitive data
• Interacting with registrars, hosting facilities, victim institutions, and law enforcement can be a complicated process
Fake Antivirus Sites
New Windows Defender 2010

Fast. Safer. Easier to use.

- Identity Protection for safe banking and shopping
- LinkScanner® for safe surfing and searching
- WebShield for safe social networking, chatting and downloading
- Anti-phishing and anti-spam for a safe, uncluttered inbox
- High-speed anti-virus/anti-spyware with auto updates
- Enhanced firewall to keep hackers out of your PC

Why Windows Defender 2010?

Windows Defender 2010 has led the world in free anti-virus protection for years. 80 million people around the globe rely on Windows Defender 2010 to protect them while they're online or offline. Threats today go way beyond viruses and only Windows Defender 2010 adds the extra layers of protection against today's biggest online threats.

How do we do it?

Windows Defender 2010 LinkScanner®
LinkScanner®, included in all Windows Defender 2010 security products, protects you from the increasing number of "here today, gone tomorrow" threats on the web. These threats can be hidden on any type of website, from governments to big, well-known brands to small businesses, and they rarely stick around on those sites for more than 24 hours. LinkScanner® protects you by analyzing the web pages behind all the links on any web page you're viewing and making sure they’re safe at the time that matters, when you’re about to click that link.

Windows Defender 2010 Identity Protection
Identity Protection is included in Windows Defender 2010 and available as a standalone product to enhance the protection offered by any anti-virus product, not just Windows Defender 2010's. Identity Protection makes sure your confidential information stays safe while you're banking, shopping, or otherwise engaging in online transactions involving your credit card numbers, bank account information, passwords, and other private information. It's constantly watching how programs on your computer interact with each other and, if something doesn't
**New XP Internet Security**

**Fast, Safe, Easier to use.**

XP Internet Security multiple layers of protection means identity theft, spam and viruses are a thing of the past.

- **6 Months License** - $49.95
  (Full & Month License including Auto activation and Premium 24/7x365 Support)
  - BUY NOW

- **1 Year License** - $59.95
  (Full 1 Year License including Auto activation and Premium 24/7x365 Support)
  - BUY NOW

- **2 Years License** - $69.95
  (Full 2 Years License including Auto activation and Premium 24/7x365 Support)
  - BUY NOW

**Great Features**

- **Identity Protection** - up-to-the-minute banking and shopping protection
- **Webshield** - safe, unthreatened email
- **Anti-Spam** - safe, uncluttered email
- **Anti-Virus and Anti-Spyware** - safe computers
- **Enhanced Firewall** - block hackers

What do our Facebook fans think about the product?
Your Computer is infected

- Trojan Horse IRC/Backdoor.Sdbot4.FRV (Medium)
- Adware.Win32.Winad (Critical)
- Trojan-PSW.Win32.LdPinch.abm (Critical)
- W32.Benjamin.Worm (High)
- W95/Elkern F-Secure (High)

Recommend: Click "Start Protection" button to erase all threats
Register Extra Antivirus to get full protection against potentially unwanted software, viruses and malware.

Warning! Your system is not scanned yet!
Press "Scan NOW" button to search for potentially malicious software and other threats.

Security essentials
To help protect your computer, make sure the four security essentials below are marked ON or OFF.

- Extra Antivirus Firewall: OFF
- Automatic updates: OFF
- Malware protection: OFF
- Other security settings: OFF

Status
- Last scan: 4/20/2009 9:41:06 AM (None)
- Last schedule: Daily around 2:02 AM.
- Last update: 4/19/2009 2:07:36 AM (1 days) update now
- Definition version: 3112 (2009420) Created on 4/20/2009
Scareware

• Scareware is any program that infiltrates a victim’s PC to display fake security alerts with the intent of frightening the user into paying for worthless security software
• Best known example is fake anti-virus software
• Sometimes called “Rogue Security Software”
The Money Trail

1. Victim provides credit card information
2. Credit card data is forwarded to payment processor
3. Payment information forwarded to credit card company
4. Issuing bank approves transaction
5. Bank charges victim's credit card account
6. Merchant Payments
7. Withdraw funds
8. Commission
Studied Three Fake AV Operations

- **Operation AV_1**
  - 3 months: Net income $11,303,494
  - 189,342 sales
  - 3% chargebacks

- **Operation AV_2**
  - 16 months: Net income $5,046,508
  - 137,219 sales
  - 2% chargebacks

- **Operation AV_3**
  - 28 months: Net income $116,941,854
  - 1,969,953 sales
  - 7.1% chargebacks
Refunds and Chargebacks

• Chargeback is when a victim reports a fraudulent transaction to credit card issuer and gets a credit
  – Too many chargebacks may result in merchant being dropped by credit card processor
  – Credit card processor may also be dropped by credit card company
  – Therefore, merchant wants to reduce chargebacks

• Refund is when a victim reports dissatisfaction to the merchant and gets money back
  – Too many refunds hurts the merchant’s bottom line
  – Merchant wants to grant a small number of refunds
Refunds

Operation $AV_1$
• 5,669 refunds
• 189,342 sales
• Refund rate: 3%
  – $346,039

Operation $AV_2$
• 11,681 refunds
• 137,219 sales
• Refund rate: 8.5%
  – $759,666

Operation $AV_3$
• 151,553 refunds
• 1,969,953 sales
• Refund rate: 7.7%
  – $10,951,191
Refunds vs Chargebacks

AV₁

AV₂

AV₃
What can be done to stop scareware?

• Take out the financial incentives
  – Pressure credit card companies and processors
    • Visa, Mastercard, etc should never do business with Chronopay!

• Take out the backend servers
  – Taking down the front-end servers has little effect
    • Highly automated process of creating proxies
  – But…
    • All front-end servers must know the location of the back-end server(s)
    • Useful for researchers / LE to find the backend
  – Requires cooperation with hosting providers

• Pressure foreign governments to implement tougher cybercrime laws
Cyber Situation Awareness of Power Distribution System Operators

• Systematic Assessment through qualitative interviews
• Interviewed Distribution System Operators (DSOs) for six large power distributors in Norway
  – Includes the four largest distributors
  – 3 of 6 have outsourced IT operations
  – DSOs operate the low voltage power grid
Interview Guide

• Based on cyber situation awareness capabilities and tools
• Four sections:
  – General: Role, size, risk perception
  – Policies: Assessments, documentation, procedures
  – Preparedness: Awareness, exercises
  – Technical security mechanisms
• Distributed the interview guide in advance
• Asked for someone who was ”responsible for IT security in the control systems”
Conclusions

• Distribution system operators are not well prepared for targeted nor more traditional security attacks
  – They lack tools for monitoring and detecting attacks
  – They lack systematic approaches to follow-up on logs and alerts
• Regulations work
  – DSOs were obligated to conduct periodic dependency, vulnerability, and risk analysis, so they did
  – Requirements for incident response were more vague, so nothing was done
• Misconceptions and wrong threat perceptions
  – DSOs downplayed the probability of a successful cyber attack
• Stronger evidence is needed to make conclusions about control systems in general
Questions?
Economic Model

\[ r f_t = \alpha \cdot r q_t \]

- \( rf_t \): Refunds given at time \( t \)
- \( rq_t \): Poisson random variable capturing the expected portion of buyers at time \( t-1 \) who request a refund in time \( t \)
- \( cb \): Chargeback threshold where a payment processor will terminate the merchant’s account
- \( \{ A \} \): 1 if the event occurs, 0 otherwise
Economic Model

\[ rf_t = \beta_0 + \beta_1 cb_t + \beta_2 cb_{t-1} + \beta_3 \overline{s}_t + u_t \]

1. Coefficients capture the increase in refunds on day \( t \) brought about by an increase in chargebacks on day \( t \) and day \( t-1 \) holding previous sales constant.

2. Captures the increase in refunds due to an increase in average sales over the past three days.

3. \( u_t \) Random error that encompasses all other factors that influence refunds on that day.
Case I: $\beta_2 = 0$, current day’s chargebacks + 3 day average sales

Case II: chargebacks, lagged chargebacks, and 3-day average sales

Case (III): Account for time variations, day of the week and day of the month