Monetizing Attacks / The Underground Economy

CS 161: Computer Security
Prof. Vern Paxson

TAs: Jethro Beekman, Mobin Javed, Antonio Lupher, Paul Pearce & Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

April 30, 2013
Announcements

• **Final exam** in Wheeler auditorium (arrive by 7PM)

• HKN at end of this Thursday’s lecture

• **Course Summary/Review** lecture on Thurs
  – Chime in on Piazza w/ topics and/or +1s by tmw AM

• **Q/A w/ TAs** on Wed May 8
  – 10AM-5PM (except 12-1), 306 Soda, hour-long slots
  – Attend as many slots as you like
  – **Bring questions/topics**
Goals For Today

• Finish discussion of information leakage
  – Disclosing private information
  – Privacy protections

• A look at profit-driven cybercrime …
  – Monetization of malware
  – Monetization of spam

• … including the Underground Economy
  – Elements
  – Significance
  – Infiltration/disruption
I Can Stalk U
Raising awareness about inadvertent information sharing

Who have we stalked recently?

ICanStalkU was able to stalk RangeLifeEnt at 51 Great Jones St New York NY
1 minute ago · Map Location · View Tweet · View Picture · Reply to RangeLifeEnt

ICanStalkU was able to stalk Inicklsson at http://maps.google.com/?q=57.134444444,12.714166667
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Inicklsson

ICanStalkU was able to stalk Welerson13 at
http://maps.google.com/?q=-15.738055556,-47.898611111
2 minutes ago · Map Location · View Tweet · View Picture · Reply to Welerson13

ICanStalkU was able to stalk BritBangert at 920 Hawley St Taylorville IL
1 minute ago · Map Location · View Tweet · View Picture · Reply to BritBangert

ICanStalkU was able to stalk jiggy_Owla at
http://maps.google.com/?q=13.7830055879,100.518500685
4 minutes ago · Map Location · View Tweet · View Picture · Reply to jiggy_Owla

ICanStalkU was able to stalk gcolony at
http://maps.google.com/?q=37.785166667,-122.404166667
4 minutes ago · Map Location · View Tweet · View Picture · Reply to gcolony

Links
- Mayhemic Labs
- PaulDotCom
- SANS ISC
- Electronic Frontier Foundation
- Center for Democracy & Technology

How did you find me?
Did you know that a lot of smart phones encode the location of where pictures are taken? Anyone who has a copy can access this information.
read more

Help me fix this!
Disabling Geo-Tagging on your phone is easy. Click here for instructions.
My baby girl.... http://t.co/5qLfLV6

2 minutes ago via Twitter for Android

BritBangert
Brittany Bangert
@BritBangert
Brittany Bangert  April 5, 2011

Login to leave a comment
How To Gain Better Privacy?

• Force of law
  – Example #1: web site privacy policies
    • US sites that violate them commit false advertising
    • But: policy might be “Yep, we sell everything about you, Ha Ha!”
7. Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.
7. Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.
7. Collection of Viewing Information. You acknowledge that you are aware of and consent to the collection of your viewing information during your use of the Software and/or Content. Viewing information may include, without limitation, the time spent viewing specific pages, the order in which pages are viewed, the time of day pages are accessed, IP address and user ID. This viewing information may be linked to personally identifiable information, such as name or address and shared with third parties.
How To Gain Better Privacy?

• Force of law
  – Example #1: web site privacy policies
    • US sites that violate them commit false advertising
    • But: policy might be “Yep, we sell everything about you, Ha Ha!”
  – Example #2: SB 1386
    • Requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed)
    • Quite effective at getting sites to pay attention to securing personal information
May 8, 2009 1:53 PM PDT

UC Berkeley computers hacked, 160,000 at risk

by Michelle Meyers

This post was updated at 2:16 p.m. PDT with comment from an outside database security software vendor.

Hackers broke into the University of California at Berkeley's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced Friday.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waqqener, UCB’s chief technology officer, said in a press conference Friday afternoon.
Monetizing Malware Locally

• General malware monetization approaches:
  – Keylogging: steal financial/email/social network accounts
  – Ransomware
  – Scareware ("fake AV")
Your Computer is Infected!

Threats and actions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Risk level</th>
<th>Date</th>
<th>Files infected</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email-Worm.Win32.Myd</td>
<td>Critical</td>
<td>11.18.2008</td>
<td>65</td>
<td>Waiting removal</td>
</tr>
<tr>
<td>Win 32:Delf-XQ</td>
<td>Critical</td>
<td>11.18.2008</td>
<td>44</td>
<td>Waiting removal</td>
</tr>
</tbody>
</table>

Description:
This program is potentially dangerous for your system. **Trojan-Downloader** stealing passwords, credit cards and other personal information from your computer.

Advice:
You need to remove this threat as soon as possible!
Monetizing Malware Locally

• General malware monetization approaches:
  – Keylogging: steal financial/email/social network accounts
  – Ransomware
  – Scareware (“fake AV”)
  – *Transaction generators* (“man-in-the-browser”)
    • Malware watches user’s surfing …
    • … waits for them to log into banking site (say) …
    • … and then injects additional banking transactions like “*send $50,000 to Nigeria*” …
    • … and alters web server replies to mask the change in the user’s balance
Monetizing Large-Scale Malware

- Monetization that leverages *botnet scale*
  - DDoS (extortion)
  - Spam
  - *Click fraud*
  - Scam *infrastructure*
    - Hosting web pages (e.g., phishing)
    - Redirection to evade blacklisting/takedown (DNS)
    - Proxying traffic to thwart tracing / provide *IP diversity*

- Which of these cause serious pain for infected user?
  - **None.** Users have *little incentive* to prevent
    ⇒ *Externality* (cost one party’s actions impose on another)
Spam & Spam Profit
Monetizing Spam

• In what different ways can spammers make money off of sending spam?
  – And who has incentives to thwart these schemes?
    • (Other than law enforcement)

• Scheme #1: advertise goods or services
  – Examples: fake Rolexes, Viagra, university degrees
  – Profit angle: increased sales
  – Who’ll try to stop: brand holders
Anatomy of a modern Pharma spam campaign

Diagram by Stuart Brown
modernlifeisrubbish.co.uk
Monetizing Spam

• In what different ways can spammers make money off of sending spam?
  – And who has incentives to thwart these schemes?
    • (Other than law enforcement)

• Scheme #1: advertise goods or services
  – Examples: fake Rolexes, Viagra, university degrees
  – Profit angle: increased sales
  – Who’ll try to stop: brand holders

• Scheme #2: phishing
  – Profit angle: transfer $$$ out of accounts; sell accounts to others; use accounts for better spamming (e.g. Facebook)
  – Opponents: issuers of accounts
  – Note: targeted phishing (“spear-phishing”) doesn’t actually need much in the way of spam due to low volume
Monetizing Spam, con’t

• Scheme #3: scams
  – Examples: pen pal relationships, 419 (“Nigerian”)
  – Profit angle: con victim into sending money
  – Opponents: scambaiters (e.g., www.419eater.com)

• Scheme #4: recruiting crooks/underlings
  – Examples: money mules, reshippers
  – Profit angle: enables profiting from cybercrime
  – Opponents: ?
Monetizing Spam, con’t

• Scheme #3: scams
  – Examples: pen pal relationships, 419 (“Nigerian”)
  – Profit angle: con victim into sending money
  – Opponents: scambaiters (e.g., www.419eater.com)

Money mules take incoming (fraudulent) financial transfers to their bank accounts, wire-transfer 90% out of country, keep 10%

• Scheme #4: recruiting crooks/underlings
  – Examples: money mules, reshippers
  – Profit angle: enables profiting from cybercrime
  – Opponents: ?
Monetizing Spam, con’t

• Scheme #3: scams
  – Examples: pen pal relationships, 419 (“Nigerian”)
  – Profit angle: con victim into sending money
  – Opponents: scambaiters (e.g., www.419eater.com)

  Reshippers receive shipments of goods (e.g., a laptop bought using a stolen account) and re-mail them outside the country

• Scheme #4: recruiting crooks/underlings
  – Examples: money mules, reshippers
  – Profit angle: enables profiting from cybercrime
  – Opponents: ?
Monetizing Spam, con’t

• Scheme #5: pump-and-dump
  – Example: “Falcon Energy (FKP) is about to go through the roof! Don’t miss out on $eriou$ Profit$!”
  – Profit angle: penny-stock momentarily goes up, dump pre-bought shares when it does
  – Opponents: Securities and Exchange Commission
  – Note: unlike other monetization techniques, the “back channel” is out-of-band
    • No link in messages back to the scammer

• Scheme #6: recruiting bots
  – Examples: “important security patch!”, “someone sent you a greeting card!”
  – Profit angle: get malware installed on new machines
  – Opponents: ?
Welcome to Storm!

Would you like to be one of our newest bots? Just read your postcard!

(Or even easier: just wait 5 seconds!)
The Rise of the

Underground Economy
ProAgent Spy Software is one of the most powerful monitoring and surveillance applications available today.

It is an ultimate solution for monitoring spouses, children, employees, or anyone else!

ProAgent records all typed keystrokes, all active window texts, all visited web sites, usernames, passwords and more and sends e-mail reports to your e-mail address that you specified when creating the server, completely hidden!

ProAgent can work in all kind of networks. It doesn’t matter if the PC is behind a firewall or behind a router or in a LAN, ProAgent works in all of these conditions without any problems.

Click here to purchase ProAgent v2.1 Special Edition...

Click here to download ProAgent v2.1 Public Edition
**allBots Inc.**

**Social Networking Bots**

GOOD News!!! We have something more for you! Yes, we have just integrated **CAPTCHA Bypassers** in all of our bots.

**Winsock (Multi-threaded) Bots**

Click here for 30+ MySpace Bots

Become an **Affiliate** and **Start Earning Now**

---

### Accounts Creator

*(You Just Need To Type In The CAPTCHAs To Create Accounts)*

<table>
<thead>
<tr>
<th>Social Networks</th>
<th>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager</th>
<th>$180.95</th>
<th>$140.00</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager (Winsock)</td>
<td>$360.95</td>
<td>$320.00</td>
</tr>
<tr>
<td></td>
<td>YouTube Accounts Creator</td>
<td>$120.05</td>
<td>$95.00</td>
</tr>
<tr>
<td></td>
<td>Friendster Accounts Creator</td>
<td>$120.05</td>
<td>$95.00</td>
</tr>
<tr>
<td></td>
<td>Hi5 Accounts Creator</td>
<td>$120.05</td>
<td>$95.00</td>
</tr>
<tr>
<td></td>
<td>TagWorld Accounts Creator</td>
<td>$120.05</td>
<td>$95.00</td>
</tr>
</tbody>
</table>

---

**Friend Adders, Message Senders, Comment Posters & Others**

*(All Bots Work In A Conventional Manner, They Gather Friend IDs/Names And Send Friend Requests, Messages, Comments Automatically)*

**Chaining Feature** is Available On All Bots for All Networks Except Facebook
Наш магазин аккаунтов рад предложить аккаунты различных почтовых служб и бесплатных хостингов для любых задач. Вы получаете аккаунты СРАЗУ после оплаты заказа через Webmoney.

Также доступна услуга запуска редиректов на Pochta.ru, Cwahi.net и 0catch.com что является уникальной услугой - вы получаете готовые редиректы в течение часа после заказа. При покупке аккаунтов менее 1000 штук действует специальный тариф.

www.FreedomScripts.org - разработка софта на заказ
Mega Софт для дорвеев - Zerber
Одобратор друзей - Мой мир

Twidium - безопасный и профессиональный инструмент для раскрутки твиттера
накрутить фолловеров в Твиттер

Заработай на продаже аккаунтов
Купи аккаунты Одноклассников
Купи аккаунты Вконтакте

<table>
<thead>
<tr>
<th>Служба</th>
<th>Кол-во акков</th>
<th>Цена за 1K аккаунтов</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail.ru</td>
<td>117025</td>
<td>до 10K: $5</td>
</tr>
<tr>
<td>Mail.ru Mix</td>
<td>327199</td>
<td>до 10K: $5</td>
</tr>
<tr>
<td>Mail.ru Second Hand</td>
<td>0</td>
<td>до 10K: $4</td>
</tr>
<tr>
<td>Mail.ru Mix S/H</td>
<td>15811</td>
<td>до 10K: $4</td>
</tr>
<tr>
<td>Yandex.ru</td>
<td>4758</td>
<td>до 10K: $20</td>
</tr>
<tr>
<td>Narod.ru</td>
<td>5315</td>
<td>до 10K: $50</td>
</tr>
</tbody>
</table>

06 Апр 2013
Временно не продаем аккаунты Twitter.com

15 Мар 2013
Отличная цена на аккаунты Facebook.com! Всего $80 за 1000 шт. Дешевле не бывает!

07 Фев 2013
Сенсационная цена на аккаунты Yahoo.com. Теперь отличные аккаунты со всеми регистрационными данными по цене от $7 за 1000 шт!

06 Фев 2013
Список доступных акков

Сервис по продаже аккаунтов аукциона eBay.

Добрые юзеры аукциона eBay предлагают вашему вниманию свои аккаунты. Постоянным клиентам и тем, кто берет более 5 акков, различные бонусы и скидки. Все аккаунты с доступом к мылу ходлера.

Вы сами выбираете акк (несколько акков) из списка. Говорите мне. Оплачиваете и получаете.
 Все акки предварительно проверяются перед продажей, в случае, если что-то не работает - 100% замена.

Актив/не актив смотрите сами по юзер ид. По активности не сортирую, так как это для каждого субъективно.

Также в продаже бывают акки PayPal. Цены рыночные. Постоянно не продаю.

Оплата по WM.
Перед покупкой следует обязательно ознакомиться с FAQ.
По работе с товаром не консультирую.
Работа через гаранти сервис приветствуется.

Моя цена:
seller/баер акк до 10 фидов = 5$
seller/баер акк 10-25 фидов = 10$
seller/баер акк 25-50 фидов = 15$
seller/баер акк более 50 фидов = 25$
Advertisement

i have boa wells and barclays bank logins....

have hacked hosts, mail lists, php mailer send to all inbox

i need 1 mastercard i give 1 linux hacked root

i have verified paypal accounts with good balance...and i can cashout paypals
Marketplace Ads for Goods

Percentage of Labeled Data

Ad Type (Goods)
Pay-Per-Install (PPI)
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Контакты
- 560869831
- 560525933
- info[at]installs4sale.net

Приемущества
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миассы стран по вашему выбору.
- Для постоянных клиентов действуют скидки и бонусы в виде дополнительного объема загрузок.
- Договориться по всем ценам и получить индивидуальные условия вы можете в службе поддержки. Пишите!
GangstaBucks.com - it pays on time! We pay for all installs!

Join our ranks and by tomorrow you could get your first payout!
Goldinstall Rates for 1K Installs for each Country.

<table>
<thead>
<tr>
<th>Country</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>OTH</td>
<td>13$</td>
</tr>
<tr>
<td>US</td>
<td>150$</td>
</tr>
<tr>
<td>GB</td>
<td>110$</td>
</tr>
<tr>
<td>CA</td>
<td>110$</td>
</tr>
<tr>
<td>DE</td>
<td>30$</td>
</tr>
<tr>
<td>BE</td>
<td>20$</td>
</tr>
<tr>
<td>IT</td>
<td>65$</td>
</tr>
<tr>
<td>CH</td>
<td>20$</td>
</tr>
<tr>
<td>CZ</td>
<td>20$</td>
</tr>
<tr>
<td>DK</td>
<td>20$</td>
</tr>
<tr>
<td>ES</td>
<td>30$</td>
</tr>
<tr>
<td>AU</td>
<td>55$</td>
</tr>
<tr>
<td>FR</td>
<td>30$</td>
</tr>
<tr>
<td>NL</td>
<td>20$</td>
</tr>
<tr>
<td>NO</td>
<td>20$</td>
</tr>
<tr>
<td>PT</td>
<td>20$</td>
</tr>
<tr>
<td>LR</td>
<td>6$</td>
</tr>
</tbody>
</table>
The Underground Economy

• Why is its emergence significant?

• Markets enable efficiencies
  – *Specialization*: individuals rewarded for doing a single thing particularly well

• Lowers barrier-to-entry
  – Only need a single skill
  – Some underground market activities are legal

• Competition spurs innovation
  – Accelerates arms race
  – Defenders must assume a more pessimistic threat model

• Facilitates non-$ Internet attacks (political, nation-state)
  – Provides actors with cheap attack components
  – Provides stealthy actors with plausible cover
The Underground Economy, con’t

• What problems do underground markets face?

• Depending on marketplace architecture, can present a target / **single point of failure**

• By definition, deals are between **crooks**
  – Major issue of betrayal by “**rippers**”

• Markets only provide major efficiencies if they facilitate deals between strangers
  – Susceptible to **infiltration**
Welcome to Storm! What can we sell you?
I am a project scientist with the Systems and Networking group in the Computer Science department at the University of California, San Diego. My current research
Template points to spammer’s server

Modified template points to our server

Under our control

Bot Controller

Proxying Bot

Re-writing Proxy

WWW server

bot

... bot

real email accounts

our webmail accounts

our domain

n00b

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM

SPAM
Life As A Spammer …

- Storm infiltration study found:
  - Modern spam campaigns can send **10s of billions** of spams using mailing lists of **100s of millions** of addresses
  - **3/4 to 5/6** of all spam delivery attempts **fail** before the message is even sent to the receiver’s server …
    - … due to heavy & effective use of black-listing
  - It takes around **20,000 “postcard” spams** to get one person to visit the postcard site
    - 1 in 10 of the visitors will click to download the postcard
  - It takes around **12,000,000 Viagra spams** to get one person to visit the site and make a purchase (~$100)
  - Even given those low rates, huge volume ⇒ **profitable**

~ $1.5-2M/year revenue
Life As A Spammer …

• Storm infiltration study found:
  – Modern spam campaigns can send 10s of billions of spams
    – 3/4 to 5/6 of all spam delivery attempts fail before the message is even sent to the receiver’s server
  – It takes around 20,000 “postcard” spams to get one person to visit the postcard site
  – 1 in 10 of the visitors will click to download the postcard
    – It takes around 12,000,000 Viagra spams to get one person to visit the site and make a purchase (~$100)
    – Even given those low rates, huge volume ⇒ profitable ~ $1.5-2M/year revenue

Another study based on making purchases of spam-advertised pharmaceuticals found that 3 merchant banks hosted 95+% of all sales …

… suggesting a novel way to suppress spam is to undermine the credit-card processing
Уважаемые Вебмастера,
В связи с событиями произошедшими в течение последних двух месяцев, когда под удар попали все банковские и процессинговые счета компании, мы вынуждены сообщить, что, поскольку до сегодняшнего дня не удалось найти достаточно надежного решения для продолжения работы, а долги перед поставщиками и партнерами продолжают расти, мы вынуждены полностью остановить функционирование партнерской программы Medinc.
Мы были рады работать с вами, друзья, и нам жаль, что сотрудничество в рамках данного проекта более невозможно.
В случае, если нам удастся найти надежное, по нашему мнению, процессинговое решение и возобновить работу, все вебмастера получат уведомления на почтовые адреса, указанные при регистрации.

Dear webmasters,
Due to the recent developments which led to all our bank and processing accounts being jeopardized, we have to inform you, that functioning of the Medinc partnership program will be discontinued, as no reliable solution has been found to keep it working, and the debts to suppliers and partners keep increasing.
We were happy to work with all of you, and we are very sorry that we can’t cooperate with you anymore within this project. If we manage to find a reliable processing solution to resume working, all webmasters will receive an email notification sent to the address submitted during registration.
6/29/2012

Dear Partners,

As you may have noticed, in the last couple of days we've had problems with processing. We don't have a solution yet, and there is no concrete time when it will be resolved.

From this point forward, GlavMed is switching to a "PAUSED" mode. No new orders will be processed until the processing issue is resolved.

We urge you to temporarily switch your traffic to other shops/projects.