Announcements

• **Final exam** in Hearst Gym, 5/14, arrive by 7PM
  – Last names A-L: 230 Hearst Gym
  – Last names M-Z: 237 Hearst Gym

• Course surveys at end of Friday’s lecture: please attend!

• Review sessions next MWF 3-4pm here, with TAs
  – Monday 5/5: Network security
  – Wednesday 5/7: Web security
  – Friday 5/5: Cryptography
Goals For Today

• A look at profit-driven cybercrime …
  – Monetization of malware
  – Monetization of spam
• … including the *Underground Economy*
  – Elements
  – Significance
  – Infiltration/disruption
Cybercrime
Suppose you’ve hacked a bunch of machines. How could you make money from this?
Monetizing Malware on 1 Machine

• General malware monetization approaches:
  – Keylogging: steal financial/email/social network accounts
  – Ransomware
  – Scareware ("fake AV")
System scan progress

Shared Documents: 97 trojans
My Documents: 334 trojans

Hard drives
Local Disk (C): 353 trojans
Local Disk (D): 78 trojans

DVD
DVD-ROM Drive (E):

Scan procedures finished. 431 Probably harmful items was found.

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!

http://protection-check07.com
Potentially dangerous software. These programs may damage your computer and steal your private information. Online Security Checker needs Personal Antivirus components to repair your computer. Please click Ok to download and install Personal Antivirus tool.

OK

http://protection-check07.com
Your computer remains infected by threats! They might lead to data loss and file structure damage, and needed to be heal as soon as possible.

Return to Personal Antivirus and download it secure to your PC.

Cancel   OK
Monetizing Malware on 1 Machine

• 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 it: brand holders
Anatomy of a modern Pharmaceutical spam campaign

Spammer
- Paid commission
  - Bulk email sender
  - Open proxies/botnet

Spam emails
- Email recipient
  - Impotent? Curious?
  - Clicks on link
  - Email with link

Other recipients
- Email target page (disposable hosting)

redirects

Affiliate program
- Commission (up to 40%)
- Sale made
  - Viagra/pharmacy site
  - Typical value $50-100?

Generic pills (Sildenafil citrate)
- Non-US supply (India, Mexico, etc.)
  - Patent expired
  - Mere cents per pill = massive markup

Shipped to customer
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 it: 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, cont.

• 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, cont.

• 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, cont.

• 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, cont.

• Scheme #5: **pump-and-dump**
  – Example: “Falcon Energy (FPK) 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 Storm Spambot

Infected systems

Reachability check

Overnet (UDP)
The **Storm** Botnet

Operated using “bulletproof hosting”
Spam “Campaign” Mechanics

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP
- Workers
Campaign Mechanics: Harvest

- Botmaster
- HTTP proxies
- HTTP
- Proxy bots
- TCP
- Workers
Campaign Mechanics: Spamming

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

Workers
Campaign Mechanics: Spamming

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP
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 v3.1 Public Edition.
allBots Inc.

Social Networking Bots

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

Winsock (Multi-threaded) Bots

Click here for 30+ MySpace Bots

Become an Affiliate and Start Earning Now

<table>
<thead>
<tr>
<th>Accounts Creator</th>
<th>(You Just Need To Type In The CAPTCHAs To Create Accounts)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Social Networks</strong></td>
<td></td>
</tr>
<tr>
<td>MySpace Accounts Creator with Picture Uploader, Profile &amp; Layout Manager</td>
<td><img src="image" alt="PayPal" /> $180.95 - $140.00</td>
</tr>
<tr>
<td>MySpace Accounts Creator (Winsock)</td>
<td><img src="image" alt="PayPal" /> $360.95 - $320.00</td>
</tr>
<tr>
<td>YouTube Accounts Creator</td>
<td><img src="image" alt="PayPal" /> $120.95 - $95.00</td>
</tr>
<tr>
<td>Friendster Accounts Creator</td>
<td><img src="image" alt="PayPal" /> $120.95 - $95.00</td>
</tr>
<tr>
<td>Hi5 Accounts Creator</td>
<td><img src="image" alt="PayPal" /> $120.95 - $95.00</td>
</tr>
<tr>
<td>TagWorld Accounts Creator</td>
<td><img src="image" alt="PayPal" /></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 залива 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
Одобрятор друзей - Мой мир

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

Заработай на продаже аккаунтов

Купить аккаунты Одноклассников
Купить аккаунты Вконтакте

Сейчас в продаже

<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>

Новости

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 холдера.

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 id. 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 гарантий сервис приветствуется.

Мои цены:

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$
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 Services

The graph shows the percentage of labeled data for different ad types.

- **Cashier Available** has the highest percentage, significantly higher than the other ad types.
- **Cashier Wanted**, **Confirmers Available**, **DoS Available**, **Phisher Wanted**, and **Confirmers Wanted** have relatively low percentages.
- **Carder Wanted**, **Phisher Available**, **Carder Available**, and **DoS Wanted** have the lowest percentages, with very little data labeled for these ad types.

The x-axis represents the ad types, and the y-axis shows the percentage of labeled data.
Pay-Per-Install (PPI)
Installs4Sale.net - надежный сервис по загрузкам, достойный доверия

Контакты:
- 560869831
- 550525933
info [at ] installs4sale.net

Приемущества:
- Быстро осуществляем отгрузку практически в любой регион. Принимаем заказы на миксы 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$</td>
</tr>
<tr>
<td>PT</td>
<td>30$</td>
</tr>
<tr>
<td>LB</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, cont.

• 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
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 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.

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*

– 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
Merchant Bank bottlenecks

3 banks host 95+% of all sales
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.
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.
Infiltration opportunity

1. Fake AV
2. Spambot
3. Keylogger
4. PPI Service

Clients
PPI Affiliate
Target Host
Downloader
Install
Payment
Via protocol emulation, extracted ("milked") > 1M malicious binaries over 6 months
The majority of the world’s top malware appeared in PPI downloads.

Table 2: FireEye’s top 20 malware families observed in their MAX Cloud network on the April–June 2010 time.
Наш магазин аккаунтов рад предложить аккаунты различных почтовых служб и бесплатных хостингов для любых задач. Вы получите аккаунты СРАЗУ после оплаты заказа через Webmoney.

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

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

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

Заработай на продаже аккаунтов

Купить аккаунты Одноклассников
Купить 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>158111</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
If you need quality **bulk accounts**, you've come to the right place. You can get your accounts immediately after your payment - there is no need to wait.

All the accounts are provided in **any format** you like. Just use our **free account converter** to get them in the way you need.

Special rates are applied if you purchase less than 1000 accounts.

We accept Liberty Reserve and Paypal.

Please, review our **terms and conditions** before purchasing any accounts.

---

<table>
<thead>
<tr>
<th>Provider</th>
<th>Quantity</th>
<th>1K-10K</th>
<th>10K-20K</th>
<th>20K+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotmail.com</td>
<td>449292</td>
<td>$5</td>
<td>$4.5</td>
<td>$4</td>
</tr>
<tr>
<td>Hotmail.com Verified</td>
<td>423418</td>
<td>$6</td>
<td>$5.5</td>
<td>$5</td>
</tr>
<tr>
<td>Outlook.com Plus</td>
<td>9661</td>
<td>$4</td>
<td>$3.5</td>
<td>$3</td>
</tr>
<tr>
<td>Gmail.com USA PVA</td>
<td>4340</td>
<td>$100</td>
<td>$95</td>
<td>$90</td>
</tr>
<tr>
<td>Yahoo.com</td>
<td>14058</td>
<td>$8</td>
<td>$7.5</td>
<td>$7</td>
</tr>
<tr>
<td>Yahoo.com USA</td>
<td>8688</td>
<td>$15</td>
<td>$15</td>
<td>$15</td>
</tr>
<tr>
<td>Nokiamail.com</td>
<td>0</td>
<td>$10</td>
<td>$10</td>
<td>$9</td>
</tr>
</tbody>
</table>

---

**06 Apr 2013**

Twitter accounts are not available. We will start selling them shortly.

---

**06 Apr 2013**

Twitter accounts are not available. We will start selling them shortly.

**07 Feb 2013**

Added Instagram accounts at a great rate: **$50 per 1000**.

**04 Dec 2012**

Just added Fully Profilled Twitter Accounts at a great rate - **$30 per 1000**. Accounts come with avatar, bio and random background.

**19 Nov 2012**

Great prices for wholesale Twitter.com and Hotmail.com orders!
Infiltration

- ShadowCrew
  - Infiltrated (Secret Service)
- CarderPlanet
- CardersMarket
- DarkMarket
  - Infiltrated (FBI)
State-sponsored Adversaries
Russian election protests – Saturday 10 December 2011
- Largest political event of its kind since the fall of the USSR
- An estimated 50,000 people gathered in Moscow and 10,000 in St Petersburg
- They allege widespread fraud in Sunday's polls
- More than 1,000 arrests
- Protestors pledge to take to the streets again on December 24
- They want Sunday's election results annulled

#триумфальная (#triumphal)

26K Twitter accounts tweet 440K junk messages to drown out discourse / coordination.
Geolocation of Logins

Nonspam Logins

56%
Geolocation of Logins

26K accounts purchased from spam-as-a-service program. Part of a “lot” of 975K. Used ~20K distinct IP addresses.
Takeaways

• Rise of cybercrime is a major challenge for security, because adversaries have become far more capable…

• But cybercriminals are lazy and look for easiest way to make a buck. So, focus defenses on the easiest ways to turn a technical security breach into money.

• “Follow the money.”
Extra Material
Welcome to Storm! What can we sell you?
Kirill Levchenko
klevchen@cs.ucsd.edu

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
Synthetic diversity aims to thwart content-based anti-spam filtering.
<table>
<thead>
<tr>
<th>MACRO</th>
<th>SEEN LIVE</th>
<th>FUNCTIONALITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>(0)</td>
<td>✓</td>
<td>Spam target email address.</td>
</tr>
<tr>
<td>(A)</td>
<td>✓</td>
<td>FQDN of sending bot, as reported to the bot as part of the preceding C&amp;C exchange.</td>
</tr>
<tr>
<td>(B)</td>
<td></td>
<td>Creates content-boundary strings for multi-part messages.</td>
</tr>
<tr>
<td>(Cnum)</td>
<td>✓</td>
<td>Labels a field’s resulting content, so it can be used elsewhere through (V); see below.</td>
</tr>
<tr>
<td>(D)</td>
<td>✓</td>
<td>Date and time, formatted per RFC 2822.</td>
</tr>
<tr>
<td>(E)</td>
<td></td>
<td>ROT-3–encodes the target email address.</td>
</tr>
<tr>
<td>(Fstring)</td>
<td>✓</td>
<td>Random value from the dictionary named string.</td>
</tr>
<tr>
<td>(Gstring)</td>
<td>✓</td>
<td>Line-wrap string into 72 characters per line.</td>
</tr>
<tr>
<td>(Hstring)</td>
<td></td>
<td>Defines hidden text snippets with substitutions, for use in HTML- and plain-text parts.</td>
</tr>
<tr>
<td>(I)</td>
<td>✓</td>
<td>Random number between 1 and 255, used to generate fake IP addresses.</td>
</tr>
<tr>
<td>(Istring)</td>
<td></td>
<td>Produces quoted-printable “=20” linewrapping.</td>
</tr>
<tr>
<td>(K)</td>
<td></td>
<td>IP address of SMTP client.</td>
</tr>
<tr>
<td>(M)</td>
<td>✓</td>
<td>6-character string compatible with Exim’s message identifiers (keyed on time).</td>
</tr>
<tr>
<td>(N)</td>
<td></td>
<td>16-bit prefix of SMTP client’s IP address.</td>
</tr>
<tr>
<td>(Ostring: num)</td>
<td>✓</td>
<td>Randomized message identifier element compatible with Microsoft SMTPSVC.</td>
</tr>
<tr>
<td>(Pnum₁[-num₂]:string)</td>
<td>✓</td>
<td>Random string of num₁ (up to num₂, if provided) characters taken from string.</td>
</tr>
<tr>
<td>(Qstring)</td>
<td></td>
<td>Quoted-printable “=” linewrapping.</td>
</tr>
<tr>
<td>(Rnum₁-num₂)</td>
<td>✓</td>
<td>Random number between num₁ and num₂. Note, special-cased when used with (D). Randomized percent-encoding of string.</td>
</tr>
<tr>
<td>(Ustring)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Vnum)</td>
<td>✓</td>
<td>Inserts the value of the field identified by (Cnum).</td>
</tr>
<tr>
<td>(W)</td>
<td></td>
<td>Time and date as plain numbers, e.g. “20080225190434”.</td>
</tr>
<tr>
<td>(X)</td>
<td></td>
<td>Previously selected member of the “names” dictionary.</td>
</tr>
<tr>
<td>(Ynum)</td>
<td>✓</td>
<td>8-character alphanumeric string, compatible with Sendmail message identifiers.</td>
</tr>
<tr>
<td>(Z)</td>
<td>✓</td>
<td>Another Sendmail-compatible generator for message identifiers.</td>
</tr>
</tbody>
</table>

Table 2: Storm’s spam-generation templating language.
Campaign Mechanics: Reporting

Botmaster

HTTP proxies

HTTP

Proxy bots

TCP

SPAM
Template points to spammer's server.

Modified template points to our server.

Under our control:

- Bot Controller
- Proxying Bot
- Re-writing Proxy
- WWW server

n00b
- real email accounts
- our webmail accounts
- our domain
Axiom of Criminal Laziness
Axiom* of Criminal Laziness

Cybercrooks will work energetically to sustain their current cash flow …

… but will not look out strategically beyond it to serve their long-term interests

(* This is a working hypothesis to explain the observed pace of attacker innovation – not something definitively established)
Phases of the Spam Value Chain

If we were to “snip” a link in this chain, which one would be the most disruptive for our least expenditure?

Measuring URLs, DNS servers, HTTP redirection, etc. all a matter of energetic crawling & recording.

But merchant banks / Visa / “fulfillment”?
CASH PARADISE UNIVERSITY
ТВОЙ КЛЮЧ К БОГАТСТВУ
YOUR KEY TO WEALTH

ICQ 29-7777898
JABBER: cc@neomail.org

Study programs: