CS5438: Security and Privacy: Practice and Case Studies

Cybercrime and Cyberwarfare

Instructors: Ari Juels and Vitaly Shmatikov
Spring 2016
Cybercrime
Cybercrime

• Today, we’ll talk about how criminals make money from compromised clients…

• To begin with, what’s better than a compromised machine?
  • A few hundred thousand of them…
Botnet

- **robot + network**

- A centrally and remotely controllable Internet-connected network of programs on (lots of) compromised systems

- Bots are called “zombies”
  - Users often don’t know about compromise
  - Enterprises often ignore botnet malware because they’ve got bigger problems (APTs)

- Botnet maintained and issued instructions by command and control (C&C) servers
In-class exercise

• Suppose you owned a botnet? How would you make money?

• How might ZeroAccess have done it?
• Bitcoins (BTC) may be generated anywhere by anyone in a process called “mining”
• Mining involves intensive computation, equipment, electricity
• So (computing) time = money

• PPC (pay-per-click) advertising: advertiser pays for each user who clicks on an ad
• Publishing networks generate traffic in return for payment
  • E.g., Google Adwords /Adsense
• Click fraud: Simulating user clicks on advertisements
Click traffic ecosystem

• Ways to benefit from click traffic:
  • Click fraud, plus...
  • Search engine optimization (SEO)
  • Degrading competitor resources
  • Boosting website visitor counts
Land Marketing Presents
TrafficDelivers!

THE MARKETERS CHOICE SINCE 2010
Daily Cash Prizes & Activity Rewards

Most Importantly We Deliver Real Traffic!

Sure we have Prizes-however if you want
Results from your Promotions then
TrafficDelivers is Perfect for YOU

You will NOT be Disappointed!
TrafficDelivers is a Real Traffic Exchange Where All
Admin Policies, Prizes, Promotions and
Program Tips are based on one thing, and One Thing Only -Getting YOU
CONVERSIONS*

We are not here Just to Entertain You-We WORK for You!
Click traffic ecosystem

[Adapted with permission from Tom Ristenpart]
The PeachySkin experiment

- Created content for a “cosmetic consulting site”
- Then they went and tried to buy some traffic...

Experimental methodology

- Set up several copies (xxx.sysnet.ucsd.edu)
- Attempted to purchase web traffic
  - Real name but temporary Visa number
- Sat back and let the data roll in…
# Click traffic resellers

<table>
<thead>
<tr>
<th>Website</th>
<th>10k Cost</th>
<th>Claimed Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.trafficdeliver.com">www.trafficdeliver.com</a></td>
<td>~$34.69</td>
<td>“Advertiser exchange”</td>
</tr>
<tr>
<td>revisitors.com</td>
<td>~$48.95</td>
<td>Recently expired domain redirection?</td>
</tr>
<tr>
<td>qualitytrafficsupply.com</td>
<td>~$55.00</td>
<td>Contextual advertisements</td>
</tr>
<tr>
<td>mediatraffic.com</td>
<td>~$70</td>
<td>AdWare (Voomba) pop-ups</td>
</tr>
</tbody>
</table>

*Adapted with permission from Tom Ristenpart*
Lesson 1: No (little) honor among thieves

revisitors.com
Took the money

qualitytrafficsupply.com
Took the money

mediatraffic.com
Wanted $200 deposit

www.trafficdeliver.com
Took the money

Sent “targeted” U.S. traffic

…and ran

…and gave it back!

[Adapted with permission from Tom Ristenpart]
Lesson 1:

No (little) honor among thieves

Took the money

Took the money

Wanted $200

Deposit

Sent “targeted”

U.S. traffic

…and ran

…and gave it back!

[Adapted with permission from Tom Ristenpart]
Lesson 2: Inorganic (funny-looking) traffic

- High degree of temporal proximity, i.e., bursty
- Many IP visit times clustered within seconds

[Adapted with permission from Tom Ristenpart]
Clicks on internal site links

Figure 2: Traffic to PeachySkin pages, normalized by the total number of all clicks to a site. Note that the y-axis is log-scale.
Mouse movements

Conclusion?
A riddle
You see this promising ad
Website looks legit!

Well, mostly!
You get the job!

From: Human Resource hr@sullivanmyers.com

Your documents has been verified and checked; you seem to be a suitable candidate for Junior Packing Specialists’ position and we are glad, that you are interested in this opening.

Following, you’ll find information about Sullivan & Myers and additional details about Junior Packing Specialist position.

This is a part-time job with a flexible schedule. Work time is not limited, but to be successful you need to devote at least 10hrs per week to it, though those who work up to 20hr/week have best results in the company.

The trial period is paid $1390 USD per month. For every successful mail/parcel forwarded you will receive $35, also you shall receive an additional bonus of $15 per parcel that you send at the day of delivery, for example, if you have received a parcel at 01.05.2010 and forwarded it at the same day, you shall receive not $35
All seems good

• The work is easy.
  • You receive electronic goods in the mail.
  • You repackage them and ship them abroad.
• And it’s reasonably well paid.
• What’s going on?
The answer

• **You’re a pack mule!**
  - When hackers steal credit-card numbers, they need to monetize them, so…
  - they buy goods and resell them.
• They don’t use their own physical addresses; they recruit mules
  - Mule provides layer of concealment
  - Often U.S. companies won’t ship to hackers’ locations
• **Mules also used to launder money**
  - Money wired to mule from hacked bank account
  - Mule wires money to criminals
  - Mule receives cut, but often unaware of scam and may also be victimized

A little investigation

- Domain www.sullivanmyers.com resolves to IP address 194.28.112.11
- IP address 194.28.112.11 also hosts
  - fotosharedownloads.com: delivers malware
  - fotoshare-dknc.com: delivers malware
  - azkinternational.com: pack mule recruiting site

A little investigation

- Domain www.sullivanmyers.com is registered to migray71@yahoo.com (“Michael Gray”).
- Using MalwareDomainList and ZeusTracker, we learn that migray71@yahoo.com registered domain names associated with
  - Drive-by-downloading such as Oficla/Sasfis, Fake Antivirus, and the RussKill DDoS tool
  - Multiple versions of the **ZeuS** Trojan
  - www.sosanni.com, a C&C for the Ambler botnet, which was controlled by the same actors who controlled several **ZeuS** botnets

ZeuS

- Trojan / crimeware
- Spreads via drive-by-download and phishing
- ZeuS kits sell for $700 - $15,000
- First detected after data theft from U.S. Dept. of Transportation in 2007
- Sophisticated anti-virus evasion
  - “Symantec Browser Protection is known to be effective at preventing some infection attempts made through the Web browser.”
- Used mainly to steal banking credentials via, e.g., keystroke logging
- Massive reach
  - At one time, 13+ million infections, including 90% of Fortune 500 companies
Example: Operation ACHing Mules

- Global ring spanning Eastern, Western Europe and U.S.
- Used ZeuS to infect machines, steal banking credentials
- Made off with $70 million
Global Reach

Law Enforcement Response To Date:
Total FBI cases: 360
Attempted loss: $220 million
Actual loss: $70 million

United States: 92 charged and 39 arrested
United Kingdom: 20 arrested and eight search warrants
Ukraine: Five detained and eight search warrants

 victims

 malware coder/exploiters

mule organization

Cyber Theft Ring
Malware exploiters purchase malware and use it to steal victim banking credentials. They launch attacks from compromised machines that allow them to transfer stolen funds and deter any tracking of their activities.

 victims

 Money Mules

 Malware Exploiters

Malware coders develop malicious software that is sold on the black market.

Victims include individuals, businesses, and financial institutions.

 How the Fraud Works

1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan

2. Victim infected with credential-stealing malware

3. Banking credentials stolen

4. Hacker retrieves banking credentials

5. Remote access to compromised computer

6. Hacker logs into victim’s online bank account

7. Money transferred to mule

8. Money transferred from mule to organizers

9. Criminals come in many forms:
   - Malware coder
   - Malware exploiters
   - Mule organization

Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

ACHing mules
How are cybercriminals identified?

• Case study: **Koobface** gang

  - Responsible for 2008-9 Facebook worm
    - Messages Facebook friends of infected users, tricks them into visiting a site with a malicious “Flash update”
  - Made at least $2 million a year from fake antivirus sales, spam ads, etc.
  - De-anonymized by in 2009-10 by
    - Jan Drömer, independent researcher
    - Dirk Kollberg, SophosLabs

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
Koobface deanonymization

• One of the command-and-control servers had a configuration mistake: any visitor can view all requests, revealing file and directory names.

• last.tar.bz2 file contained daily C&C software backup, including a PHP script for sending daily revenue statistics to five Russian mobile numbers.

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
Koobface deanonymization

- Search for the phone numbers found Russian online ads for a BMW car and Sphynx kittens

- Search for username “krotreal” found profiles in various social sites – with photos!

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
Koobface deanonymization

- One of the social-network profiles references an adult Russian website belonging to “Krotreal”
- “Whois” for the website lists full name of the owner, with a St. Petersburg phone number and another email (krotreal@mobsoft.com)

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
Koobface deanonymization

- Krotreal profile on vkontakte.ru (“Russian Facebook”) is restricted…
- … but he posted links to photos on Twitter, thus making photos publicly available
  - and revealing social relations

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
Koobface deanonymization

- The co-owner of one of the Mobsoft entities did not restrict her social profile
- She reveals the faces, usernames, relationships between gang members
  - E.g., holidays in Monte Carlo, Bali, Turkey

One photo shows Svyatoslav P. participating in a convention in Cyprus

“FUBAR webmaster” website has archive photo sets of Svyatoslav and wife at a convention

Username “Psychoman” on the badge!

[Source: http://nakedsecurity.sophos.com/koobrace; slides adapted by permission from Vitaly Shmatikov]
The Koobface gang

- Антон Коротченко
  - “KrotReal”
- Станислав Авдейко
  - “LeDed”
- Святослав Полышук
  - “PsViat”, “PsychoMan”
- Роман Котурбач
  - “PoMuc”
- Александр Колтышев
  - “Floppy”

[Source: http://nakedsecurity.sophos.com/koobface; slides adapted by permission from Vitaly Shmatikov]
On 17 January 2012

- The *NYTimes* revealed that Facebook planned to name five men as being involved in Koobface
- The apparent mastermind…

Stanislav A.
Example: Operation ACHing Mules

• 37 people charged by FBI in 2010

• Most ultimately arrested, but not all…

“Cyber’s most wanted fugitive” (FBI)

[http://www.fbi.gov/wanted/cyber/operation-aching-mules]
Cyberwarfare
In June 1982, a strange event occurred in a remote part of the Soviet Union:

- The White House was alerted to this event from U.S. early-warning satellites.
- NORAD initially feared that a nuclear missile launch had occurred at site not known to house missile facilities.
- Satellite images showed the largest non-nuclear explosion and fire ever seen from space.
What caused the explosion?

Malware!

Courtesy of the CIA…
What caused the explosion?

The backdrop:

- KGB defector Vladimir Vetrov leaked Farewell Dossier to French intelligence
- Dossier indicated that Soviet Union planed to steal Canadian technology for its trans-Siberian gas pipeline
  - Sophisticated SCADA (Supervisory Control and Data Acquisition) technology needed for pipeline management
- CIA learned of plan and planted a Trojan in the Canadian SCADA software targeted by the Soviets
- Trojan caused malfunction in pipeline, resulting in build up of excessive pressure
- Result: Explosion equivalent to 3 kilotons of TNT
  - (Estimated yield of Hiroshima bomb Little Boy was about 13 kilotons)
Siberian pipeline sabotage

• Early, crude form of cyberwarfare
• Today, we’ll talk about more modern ones...
Estonia (2007)

- Estonia relocated Bronze Soldier of Tallinn
  - Controversial Soviet WWII monument
  - Disagreement with Russia ensued
  - Cyberattacks disabled web sites of a number of Estonian institutions
    - Parliament, banks, newspapers, etc.
  - Mainly *distributed denial-of-service* (DDoS) attacks
- Pivotal instance of cyberwarfare
  - Raised awareness of military importance of internet
What's a DoS attack?

- **Goal**: Disable victim service (usually temporarily)
- **Means**: Amplification
  - Turn small amount of traffic into big amount
- **Two approaches**:
  - Exploit *vulnerability* that amplifies attack
  - Use *botnet* to generate flood of traffic
DNS amplification

- 50x amplification!
- (In extreme cases, as much as 100x)
- Open resolver project: 28 million open resolvers posing risk (27 Oct. 2013)
Even better


[Image 101x114 to 904x560]
Digital Attack Map

- http://www.digitalattackmap.com/
Case study:
Stuxnet (2010)

Based on the Symantec W32.Stuxnet Dossier
Background:
Industrial Control Systems (ICS)

- ICS is a general term for automated control systems used in factories, chemical plants, power plants, etc.
- Includes Programmable Logic Controllers (PLCs)
  - Computer-based devices that controls attached industrial equipment
  - Usually programmed via Windows using specialized assembly code
Stuxnet’s target

- Stuxnet targets a specific PLC
  - Infects Siemens SIMATIC Process Control System (PCS) 7 that specifically controls a
  - Siemens S7-300 PLC that specifically controls
  - variable-frequency drives (VFDs) from one of two specific vendors
    - Vacon (Finland)
    - Fararo Paya (Iran)
  - that specifically control attached motors spinning between 807 Hz and 1210 Hz
    - as determined after monitoring through Stuxnet infection

- For example…
- Centrifuges used to enrich uranium in Iran…

Natanz nuclear facility, Iran
Challenges

- Propagating stealthily outside target so that
  - Zero-days don’t get patched
  - Target isn’t alerted
- Evading intrusion detection tools at (high-security) target
- Jumping an air gap
  - Natanz machines were not networked!
  - So how does a worm reach them?
- Destroying centrifuges
  - Using software alone
  - While preventing operators from perceiving malfunction!
Stuxnet milestones

- Landmark in sophistication
  - Combines zero-day exploits, Windows rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, etc., etc.
- Probably the costliest malware development effort ever
  - Symantec estimates a team of up to thirty people over half a year
- First malware to exploit multiple *(four!)* zero-day attacks (Microsoft vulnerabilities)
  - Two for propagation
  - Two for privilege escalation
- Uses stolen signing keys from *two* certificate authorities
- First known programmable logic controller (PLC) rootkit
- Not first cyberphysical attack (as we’ve seen)
  - But first known to self-propagate via malware
Highly targeted attack

- Released in three waves against five “Domains” (organizations)
  - 10 initial infections (release from seeded USB drives)
- Fingerprints specific industrial control system: Siemens SIMATIC Step 7 software (as we’ve seen)
- Highly linear propagation
  - Performs rate limiting
  - Self-deletes from USB stick after third infection
  - In general, intentionally limited its spread
- E.g., Domain E
  - Targeted once, in May 2010
  - Three infections: same USB drive inserted into three machines
Spread beyond target

- Infections beyond Iran (five organizations) are collateral damage.
- Un intended propagation caused by collaboration with partner organizations.
- 12,000 infections in 1,800 domains traceable to five initially seeded domains.
- Collateral infection is how we know about Stuxnet.
How does it spread?

Network propagation methods:

• Infecting WinCC database servers
• Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability
• Propagating through the MS08-067 Windows Server Service Vulnerability
• Propagating through network shares
• Peer-to-peer communication and updates
But how does Stuxnet jump the air gap?
Removable drive (USB) propagation

- Key propagation method because of air gap:
  - Industrial control systems in secure facilities are commonly programmed via *non-networked* Windows computer
  - Operators exchange data among computers via removable (USB) drives
    - (Sometimes called a “sneaker net”)
- Stuxnet exploits LNK zero-day vulnerability (CVE-2010-2568)
  - Causes code execution when files on removable drive are viewed
Also involves digitally signed driver keys

• The stolen keys came from two Taiwanese semiconductor manufacturers.

• Both have offices in Hsinchu Science and Industrial Park…
  • Convenient for physical theft / bribery
  • Also convenient to create appearance of physical theft / bribery…
Command and Control (C&C)

- After installation file drops, Stuxnet attempts to contact C&C servers
  - (Works for instances that aren’t behind air gap)
- Tests network connectivity by contacting www.windowsupdate.com or www.msn.com
- Contacts C&C server via www.mypremierfutbol.com or www.todaysfutbol.com on port 80
  - Previously pointed to servers in Malaysia and Denmark; now redirected to disable Stuxnet C&C
- Sends host information
  - Time of infection, IP address, OS version, flag specifying if the host is part of a workgroup or domain, infected Step 7 project file name
- May receive backdoor code update from C&C server
The grand finale

- Infected PLC changes motor speed to 1410 Hz to 2 Hz to 1064 Hz (then repeats)
- Speeds up and slows down centrifuge at various times
- (Recall: normal operating range is 807-1210 Hz)
- All the while, normal behavior is simulated for operator…
Cyberattack against power generator
The result

- Sept. 2010: “delays”
  - Warm weather blamed
- Oct. 2010: “spies” arrested
  - Allegedly attempted to sabotage Iran’s nuclear program
- Nov. 2010: Iran acknowledges that its nuclear enrichment centrifuges were affected by a worm
  - Foreign minister: “Nothing would cause a delay in Iran’s nuclear activities”
  - Intelligence minister: “enemy spy services” responsible
- “In recent days, the retiring chief of Israel’s Mossad intelligence agency, Meir Dagan, and Secretary of State Hillary Rodham Clinton separately announced that they believed Iran’s efforts had been set back by several years.”
  —NYTimes, 15 Jan. 2011
WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran’s main nuclear enrichment facilities, significantly expanding America’s first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran’s Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.
Duqu

- Identified in Oct. 2011
- Closely related to Stuxnet
- Different objective than Stuxnet: Theft of data
- F-Secure initially mistook Duqu kernel driver JMINET7.SYS, for Stuxnet's MRXCLS.SYS
- Digitally signed driver using stolen private key
  - Stolen from C-Media, based in Taipei, Taiwan…
Flame

- Even more complex than Stuxnet
- Steals data, e.g.,
  - Activates microphones and webcam
  - Logs keystrokes
  - Takes screenshots
  - Extracts geolocation data from images
- Masquerades as Windows update proxy
  - (WPAD (Web Proxy Auto-Discovery Protocol) server)
  - Innovation: Signed using bogus Microsoft update certificate; certificate had valid-looking digital signature
  - How was certificate produced? Collision attack on the MD5 hash function!
    - (Cryptanalytic bravado!)
Gauss

- Information-stealing malware based on Flame
  - Discovered in Aug. 2012
- Innovation: Gödel module
  - “Warhead” encrypted using RC4
  - Key is derived from data extracted from host
  - But no target host has yet been identified
- So we don’t know what it does!
  - But the warhead is large and the worm appears to be highly targeted...