Anatomy of Attacks

Dmitry Samosseiko, SophosLabs
SophosLabs Team

• One global team – UK, US, Canada, Australia
• 24/7, 365 days/year
• ~100 Researchers and Developers globally
  ▪ Threat Operations
  ▪ Systems Development
  ▪ Advanced Research and Detection Development
• Highly trained
  ▪ ~6 month training program for new hires
  ▪ Strong focus on Software Reverse Engineering
  ▪ Broad skills set – malware, spam, web, exploits
WHO WRITES COMPUTER VIRUSES?
The good old days...
Today’s motives
Monetizing on malware?

- Spam bots
- Spyware (keyloggers, “phishing” password stealers)
- Ransomware
- Scareware
- Denial of service attacks
- Corporate data theft
- …
The value of “zombie” PC

Source: krebsonsecurity.com
Exponential growth
Variants and volumes

SophosLabs sees 200,000 samples per day

33% more than in 2011

And 20,000 new malicious URLs

80% were compromised legitimate sites
MALWARE DIVERSITY
Viruses

- Spread by infecting other files, executables
- Parasitic
- Not as common today as other forms of malware
- May require a special cleanup approach
Worms

- Spread via network connection
- Attack network shares, weak passwords/security
Trojan horses

• The most prevalent kind of malware today
• Often relies on social engineering
• Needs to be disguised as something normal
“Bankers”

- Steal banking account information
- Prevalent in South America
- Attempt to bypass online banking security measures
Rootkits

• Stealthy, avoid detection
• Subverts the OS operations
• Hard to detect and remove
• Bootkits – rootkits attacks MBRs, loads before OS kernel
• Examples:
  ▪ TDSS/TDL
  ▪ ZeroAccess
  ▪ Alureon
Botnets

Botnets for:

1. Email spam
   - “Grum” ~ 200,000 PCs
   - “Rustock” ~ 815,000 PCs
2. Web spam
3. DDoS
4. “Installs”
5. Info stealers (Zeus, Citadel)

Picture source: http://en.wikipedia.org/wiki/Botnet
Scareware / FakeAV

#1 threat today by prevalence

- Fake anti-virus
- Fake anti-spyware
- System “optimizers”

Videos at http://youtube.com/SophosLabs
Scareware for Macs
Ransomware

- Encrypts documents or
- Blocks screen/mouse/keyboard access
- Demands money to unlock (SMS, e-currency, prepaid cards)
Stop Online Piracy Automatic Protection System

If you see a warning.txt or warning screen, it means your IP address was included in S.O.P.A. Black List.

One or more of the following items were made from your PC:
1. Downloading or distributing audio or video files protected by Copyright Law.
2. Downloading or distributing illegal content (child porn, phishing software, etc.)
3. Downloading or distributing Software protected by Copyright Law.

As a result of these infringements based on Stop Online Piracy Act (H.R. 3261) you PC and files are now blocked. You can remove you IP from black list and unlock PC and files by paying a fine of 200 (USA and Canada) / 200EUR (via Western Union to other Countries)

STEP 1: Buy a moneypak prepaid voucher for the amount of $200 at the nearest store.

STEP 2: Enter your prepaid voucher number and your email address in the fields below then click PAY and you will be prompted to enter the unlock code. OR Send an e-mail at UNLOCK@SOPASYSTEM.COM. Indicate your ID in the message title and provide moneypak prepaid voucher number.

STEP 3: Check your e-mail. In 24 hours we will send your Unlock code once payment is verified. Then enter your unlock code that you received by email from us and click UNLOCK. Your computer will roll back to the ordinary state.

Your identification number: 1643
Your IP address: [REDACTED]

Q: How can I make sure that you can really decipher my files?
A: You can send one ciphered file on email UNLOCK@SOPASYSTEM.COM (Indicate your ID and IP address in the message title), in the response message you receive the deciphered file.

Q: Where can I purchase a MoneyPak?
A: MoneyPak can be purchased at thousands of stores nationwide, including major retailers such as Wal-Mart, Walgreens, CVS/pharmacy, Rite Aid, Kmart, Kroger and Meijer.

Q: How do I buy a MoneyPak at the store?
A: Pick up a MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the MoneyPak.

Q: What if I don’t have possibility to purchase prepaid voucher?
A: You can send money in amount of 200EUR by WesternUnion as alternative option.

WARNING!!!: If you don’t pay the fine within 72 HOURS at the amount of 200.00 USD, all your computer data will be erased.

If you have any questions please contact us unlock@sopasystem.com

We accept only Moneypak prepaid vouchers.
Visit for information: http://www.moneypak.com

SOPHOS
Main vectors

- Web
- Email spam
- Removable media (USB, phones)
Spam for malware distribution

Email messages containing malicious attachments

- Spam often used to distribute threats
- Attachments to the message
- Links in the message body
- Executable often in ZIP or RAR
- HTML attachments.
- Social engineering throughout
Social engineering

• “You need to install this codec to watch that video”
• “You are infected! Install XP Antivirus 2012!”
• “OMG! Your private video is online. Watch it here.”
• “Open the attachment to see your pay raise details!”
• “You’ve got a PayPal payment. Open to see”
• … there is one for everybody …

Forces you to act, not think…
Ok, we’re too smart to fall for this…
Software has “bugs”

- Bugs create vulnerabilities
- Vulnerabilities get exploited
- It may take weeks to patch a hole
- Exploit packs are sold online
They also have “holes”

Browsers & browser plugins:
• Java
• Flash
• PDF
• Quicktime
• Media players
• ActiveX
• Office documents
• Even images
Exploit packs = Silent installs

“drive-by” infections


Poly Exploit Pack  Red Exploit Pack  SEO Exploit Kit (Numerous, names unknown)  Siberia Pack  Smart Exploit Pack  Target Exploit Pack

BlackHole

• The most successful and prevalent exploit kit
• $1500 per year or from $50 a day
• PHP/MySQL backend
• Management console
• Version 2 (Oct 2012) includes Windows8 and mobile devices
IT’S ALL ABOUT WEB TRAFFIC
Web traffic generation

- Black SEO (doorways, content farms)
- Traffic hijacking
- “Malvertizing”
- …
SEO – How they do it?

Doorway – A web page that is designed to attract traffic from a search engine and then redirect it to another site or page.

Google results

Googlebot sees

Firefox/Chome/IE
Social networking malware

```javascript
var redirects = [
  ['facebook.com', 'abc+fb.php'],
  ['tagged.com', 'abc+tg.php'],
  ['friendster.com', 'abc+fr.php'],
  ['myspace.com', 'abc+ms.php'],
  ['myslinks.com', 'abc+ms.php'],
  ['myyearbook.com', 'abc+yb.php'],
  ['fubar.com', 'abc+fu.php'],
  ['hi5.com', 'abc+hi5.php'],
  ['twitter.com', 'abc+tw.php'],
  ['bebo.com', 'abc+be.php'],
];
```
Myth: I’m a safe surfer

Do you ever visit these sites?
Even those we trust most
Website infections

- FTP account hacking
- cPanel exploits
- SQL Injections
- Vulnerable webservers, CMS (Wordpress, Drupal, …), PHP, …
## Pharma profitability

This affiliate used 66 unique domains referencing his AffID

- 124 orders per day
- Average sale = $160
- 40% commission

\[124 \times 160 = 19840 \times 40\% = 7936/\text{day}\]

<table>
<thead>
<tr>
<th>Date</th>
<th>Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>30</td>
</tr>
<tr>
<td>02</td>
<td>74</td>
</tr>
<tr>
<td>03</td>
<td>216</td>
</tr>
<tr>
<td>04</td>
<td>193</td>
</tr>
<tr>
<td>05</td>
<td>231</td>
</tr>
<tr>
<td>06</td>
<td>191</td>
</tr>
<tr>
<td>07</td>
<td>189</td>
</tr>
<tr>
<td>08</td>
<td>78</td>
</tr>
<tr>
<td>09</td>
<td>99</td>
</tr>
<tr>
<td>10</td>
<td>128</td>
</tr>
<tr>
<td>11</td>
<td>52</td>
</tr>
<tr>
<td>12</td>
<td>7</td>
</tr>
</tbody>
</table>

Average sales per day 124
# Fake anti-virus profitability

Statistics from topsale2.ru

<table>
<thead>
<tr>
<th>Date</th>
<th>Visits</th>
<th>Buy page</th>
<th>Loads</th>
<th>Sales</th>
<th>Ratio (Uniq/Sales)</th>
<th>Ratio (Loads/Sales)</th>
<th>Ch-backs</th>
<th>Refunds</th>
<th>Referals</th>
<th>Sales</th>
<th>Money</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-03-01</td>
<td>15817</td>
<td>492</td>
<td>7980</td>
<td>37</td>
<td>1:427</td>
<td>1:215</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>1078.92</td>
<td>1078.92</td>
</tr>
<tr>
<td>2009-03-02</td>
<td>14013</td>
<td>409</td>
<td>5925</td>
<td>28</td>
<td>1:500</td>
<td>1:211</td>
<td>0</td>
<td>2</td>
<td>0.00</td>
<td>779.22</td>
<td>779.22</td>
</tr>
<tr>
<td>2009-03-03</td>
<td>9949</td>
<td>252</td>
<td>2832</td>
<td>21</td>
<td>1:473</td>
<td>1:134</td>
<td>0</td>
<td>2</td>
<td>0.00</td>
<td>569.43</td>
<td>569.43</td>
</tr>
<tr>
<td>2009-03-04</td>
<td>11765</td>
<td>298</td>
<td>3482</td>
<td>12</td>
<td>1:980</td>
<td>1:290</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>359.64</td>
<td>359.64</td>
</tr>
<tr>
<td>2009-03-05</td>
<td>7504</td>
<td>173</td>
<td>3064</td>
<td>2</td>
<td>1:3752</td>
<td>1:1532</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>59.94</td>
<td>59.94</td>
</tr>
<tr>
<td>2009-03-06</td>
<td>3023</td>
<td>106</td>
<td>3801</td>
<td>8</td>
<td>1:377</td>
<td>1:475</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>209.79</td>
<td>209.79</td>
</tr>
<tr>
<td>2009-03-07</td>
<td>2370</td>
<td>113</td>
<td>6416</td>
<td>9</td>
<td>1:263</td>
<td>1:712</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>239.76</td>
<td>239.76</td>
</tr>
<tr>
<td>2009-03-08</td>
<td>8841</td>
<td>278</td>
<td>6388</td>
<td>24</td>
<td>1:368</td>
<td>1:266</td>
<td>0</td>
<td>1</td>
<td>0.00</td>
<td>689.31</td>
<td>689.31</td>
</tr>
<tr>
<td>2009-03-09</td>
<td>10936</td>
<td>358</td>
<td>5234</td>
<td>6</td>
<td>1:1822</td>
<td>1:872</td>
<td>0</td>
<td>4</td>
<td>0.00</td>
<td>59.94</td>
<td>59.94</td>
</tr>
<tr>
<td>2009-03-10</td>
<td>12331</td>
<td>379</td>
<td>6862</td>
<td>24</td>
<td>1:513</td>
<td>1:285</td>
<td>7</td>
<td>2</td>
<td>0.00</td>
<td>482.05</td>
<td>482.05</td>
</tr>
<tr>
<td>2009-03-11</td>
<td>5384</td>
<td>194</td>
<td>833</td>
<td>13</td>
<td>1:414</td>
<td>1:64</td>
<td>0</td>
<td>0</td>
<td>0.00</td>
<td>388.31</td>
<td>388.31</td>
</tr>
<tr>
<td><strong>Total:</strong></td>
<td><strong>101933</strong></td>
<td><strong>3052</strong></td>
<td><strong>52817</strong></td>
<td><strong>184</strong></td>
<td><strong>1:553</strong></td>
<td><strong>1:287</strong></td>
<td><strong>7</strong></td>
<td><strong>14</strong></td>
<td><strong>0</strong></td>
<td><strong>4916.31</strong></td>
<td><strong>4916.31</strong></td>
</tr>
</tbody>
</table>
Fake AV recruitment – Topsale.ru

- $255 за продажу ан.
- exe, а также по запросу сделаем вам связку для iframe трафика.
- промо-фейковые сканеры для редирект трафа.
- холд 14 дней (напр. за 1-7 число выплата 21), антифродовые условия биллинга.
Top fake anti-virus affiliates

<table>
<thead>
<tr>
<th>Affiliate ID</th>
<th>Affiliate Username</th>
<th>Account Balance (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4928</td>
<td>nenastniy</td>
<td>$158,568.86</td>
</tr>
<tr>
<td>56</td>
<td>krab</td>
<td>$105,955.76</td>
</tr>
<tr>
<td>2</td>
<td>rstwm</td>
<td>$95,021.16</td>
</tr>
<tr>
<td>4748</td>
<td>newforis</td>
<td>$93,260.64</td>
</tr>
<tr>
<td>5016</td>
<td>slyers</td>
<td>$85,220.22</td>
</tr>
<tr>
<td>3684</td>
<td>ultra</td>
<td>$82,174.54</td>
</tr>
<tr>
<td>3750</td>
<td>cosma2k</td>
<td>$78,824.88</td>
</tr>
<tr>
<td>5050</td>
<td>dp322</td>
<td>$75,631.26</td>
</tr>
<tr>
<td>3886</td>
<td>iamthevip</td>
<td>$61,552.63</td>
</tr>
<tr>
<td>4048</td>
<td>dp32</td>
<td>$58,160.20</td>
</tr>
</tbody>
</table>
# Ransomware Profitability

<table>
<thead>
<tr>
<th>Rank</th>
<th>Country</th>
<th>Installs</th>
<th>Pins</th>
<th>Amount</th>
<th>Conversion</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Austria (14)</td>
<td>529</td>
<td>13</td>
<td>1100</td>
<td>2.08%</td>
</tr>
<tr>
<td>2</td>
<td>Sweden (221)</td>
<td>1066</td>
<td>87</td>
<td>5400</td>
<td>5.07%</td>
</tr>
<tr>
<td>3</td>
<td>France (84)</td>
<td>2998</td>
<td>113</td>
<td>11200</td>
<td>3.74%</td>
</tr>
<tr>
<td>4</td>
<td>Italy (118)</td>
<td>272</td>
<td>1</td>
<td>100</td>
<td>0.37%</td>
</tr>
<tr>
<td>5</td>
<td>Portugal (193)</td>
<td>283</td>
<td>1</td>
<td>100</td>
<td>0.35%</td>
</tr>
<tr>
<td>6</td>
<td>Spain (217)</td>
<td>1604</td>
<td>26</td>
<td>2450</td>
<td>1.53%</td>
</tr>
<tr>
<td>7</td>
<td>Poland (191)</td>
<td>1462</td>
<td>16</td>
<td>1600</td>
<td>1.09%</td>
</tr>
<tr>
<td>8</td>
<td>Netherlands (176)</td>
<td>1427</td>
<td>72</td>
<td>6650</td>
<td>4.66%</td>
</tr>
<tr>
<td>9</td>
<td>Finland (77)</td>
<td>1</td>
<td></td>
<td></td>
<td>0%</td>
</tr>
<tr>
<td>10</td>
<td>Belgium (21)</td>
<td>401</td>
<td>7</td>
<td>700</td>
<td>1.75%</td>
</tr>
<tr>
<td>11</td>
<td>Germany (94)</td>
<td>5376</td>
<td>167</td>
<td>14450</td>
<td>2.69%</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>15419</td>
<td>503</td>
<td>43750</td>
<td>2.84%</td>
</tr>
</tbody>
</table>
Arms Race ...
Evasion Techniques

- IP/network blocking
- HTTP_REFERER/cookie check
- “Time attacks”
- JavaScript obfuscations for redirect chain
- Browser detection
- Delays
- DOM tricks
- “Click to download” images
Exploit Code
Evasion Techniques

Everything is a moving target

• Binaries repackaged every 20 min (!) and AV tested + server side polymorphism
• 100s of payload domains created daily + payload sites hosted on “free TLDs” (.cz.cc …)
• 10,000s of new infected websites stealing legitimate traffic, found daily
• TDS domain turn over (relatively slow)
• IP hopping
AV Scanners for Virus writers
Crypto services for virus writers

- Meant to hide the payload behind a layer of packer/crypto
- Could include multiple layers, i.e. a VB malware wrapped in a C packer
- Service model
  - + Legitimate commercial packers
SSP

- SSP - Server-side polymorphism
- New binary for every download
Non-traditional malware

- APTs
- State-sponsored “cyber weapons” (Duqu, Stuxnet, Flame)
APT – What does it mean?

Advanced Persistent Threat

- A fancy name for targeted attacks
- A term describing the “daily onslaught of digital assaults launched by attackers who are considered highly-skilled, determined and possessed of a long-term perspective on their mission” (Wikipedia)
APT highlights for 2010/11

Threats left undiscovered for months, even years:

- Nov 2010 – operation “Aurora” – Google
- Jan 2011 – Canadian government organizations
- Feb 2011 - “Knight Dragon” – energy industries
- Mar 2011 - RSA
- Jun 2011 – Northrop Grumman (RSA hack)
- Jun 2011 - IMF
- Aug 2011 - “ShadyRat” – MANY governments and corporations worldwide
- Sept 2011 – Mitsubishi (nuclear plant, defense secrets)
Intellectual property is the new gold

- Zero day Flash vulnerability
- Inadequate monitoring
- Victims of their own success

- Zero day IE6 vulnerability
- All systems “trustworthy”
- Allowed intruders too much privilege
What can be done?

Awareness

Security measures

Legal actions
Legal actions and takedown efforts

Takedown highlights

• Nov 2009 – “Mega-D” (30-35% of spam). Arrested
• Feb 2010 – “Mariposa” botnet, 12M PCs. Arrested.
• Mar 2010 – “Zeus” botnet. Arrested
• Oct 2010 – “Bredolab” botnet, 30M PCs!
• Sep 2011 – “Kelihos” botnet
• …
• Nov 2012 – “Nitol”
Anatomy of Defences
Modern AV

- Not just about viruses
- Not just about signatures
- Not just about executables
• Multi-layer defenses
• Static and runtime protection
• Behavioral malware profiles
• Malicious scripts, PDFs, Flash, Java, docs, exploits, packers, ...
• Emulation, unpacking
• “Cloud”-based reputation services
A typical web attack

Doorways / Infected
• Set the trap for users and draw them in

Traffic Distribution
• Directs victims to selected attacks

Penetration
• Getting around environmental defenses

Infection
• Binary threats downloaded and installed

Execution
• The threat is doing its dirty work
Layered protection
Stop attacks and breaches

Entry point
Traffic Distribution
Penetration
Infection
Execution

URL Reputation
Behavioral Profiling
HIPS
AV Lab Tasks

- Threat Visibility
- Sample Collection
- Analysis
- Protection
Threat Discovery

Through SophosLabs systems and products

• Product feedback
• Web crawling
• Spam traps
• Industry sharing
URL Analysis

Website URLs

• URL Patterns
• Domain age
• Popularity
• Location
• Network reputation
• Name servers (DNS)
• Scan results from various content engines
• Sources
• Manual analysis
File Analysis

Dynamic Files Analysis

• Samples executed
• Behavior observed, recorded and analyzed
• Dropped samples submitted for analysis
• Outbound network traffic (URLs, domains) captured and sent for analysis
• All analysis results are sent to correlation system for decision making
processes
process_action  "Started"

HIPS
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"
detection: "HIPS/IPConnect-003"

SAV

ip_connections
connection: 64.79.86.25:8392
connection: 64.120.176.66:8392

dns_requests
dns_query: findhobbits.com
dns_query: sendinvest.com

http_requests

autostart

files_created
file: C:\WINDOWS\system32\bpxr_788593173096

registry

SnapShot_overall_registry_and_file_changes

----------------------------------
Registry Added: 2
----------------------------------
HKLM\SOFTWARE\Microsoft\WBEM UpdateNew
18 76 7A C2 C3 B2 E3 40
HKLM\SOFTWARE\Microsoft\WBEM uid
ucsp0416
Static Analysis

Human Analysis

- Reverse Engineering with IDAPro
- Many internal tools
  - JS unpacking
  - File entropy
  - Strings extraction
  - File format handling, i.e. PDF tools
Reversing…
Automation is key

• “Big data” problems
• Fast turn around time
• Anti-anti-anti-* techniques
Attack Examples

A typical web attack and levels of protection offered
Doorways

- Filled with keywords
- Look different to Googlebots (cloaking)
- SEO Kits

Detection:
- Template detection, i.e. Mal/SEORed-*
Typical FakeAV

Doorway → TDS → Redirector → Promo → Payload → Install → Payment

Doorway page

Payload site

Redirect sites
Typical FakeAV

- SutraTDS, SimpleTDS, …
- Run on dedicated domains
- Redirecting traffic based on: country/city, browser, OS, search keywords, etc

Detection:
- TDS domain blocking
Typical FakeAV

Just another obfuscation layer

Detection:
- Domain/URL blocking
- JavaScript detection
  - Mal/ObfJS
  - Mal/JSRedir
Typical FakeAV

- Fake “My Computer” (or Finder) scanner page

Detection:
- URL/domain blocking
- HTML/JS content:
  - Mal/FakeAvJS
Typical FakeAV

- Often hosted on the same page as “promo”
- Hard to get to
- SSP

Detection:
- URL/domain blocking
- Binary detection
  - Mal/FakeAvJS
  - EnkPack
  - Cloud
Typical FakeAV

On endpoints:

- Context based detection – correlating registry keys, file names with binary "genes"
- HIPS – runtime behavior analysis
Thank you!

Some recommended resources

http://nakedsecurity.sophos.com

http://www.facebook.com/SophosSecurity

http://krebsonsecurity.com