Detecting the Network Behavior of Malware

Roberto Perdisci
**Malware = Malicious Software**

- Most modern cyber crimes are carried out using malicious software

*Spam, Identity Theft, DDoS…*

95% of all Spam sent using malware-infected machines
Malware = Malicious Software

- Most modern cyber crimes are carried out using malicious software
  - *Spam, Identity Theft, DDoS…*

  95% of all Spam sent using malware-infected machines

- Many different types of malware
  - *Trojans*
  - *Bots*
  - *Spyware*
  - *Adware*
  - *Scareware...*
Malware is a global problem

One quarter of the Internet is infected by malware
Source: Vint Cerf, “father of the Internet”

The annual financial loss for US organizations amounts to hundreds of millions of dollars.
Malware Infection Vectors

“Drive-by” Malware Downloads

- Simply visiting a legitimate (compromised) Website can cause a malware infection!
A friend just sent you a birthday gift...

cake.exe

Social engineering attacks!

Infected external disk!

Direct remote exploits!
Traditional AVs are not enough!

AV scan

Malware

Benign

Original Malware

Executable Packing (obfuscation)

Hidden Malware

AV industry in 1998

AV industry in 2008
What can we do to secure the Internet?

- No silver bullet solution...
- Different approaches to tackle the problem from different points of views
  - Host-level solutions
  - Network-level solutions
  - Usable security
  - Educate users

Defense-in-Depth strategy
Our Approach

- Detect the Network Behavior of Malware
- Complement existing host-based detection systems
- Improve “coverage”
Key observations

- Most malware need a network connection to perpetrate malicious activities
  - **Bots** need to contact C&C server, send spam, etc...
  - **Spyware** need to exfiltrate private info
  - **Trojan droppers** need to download further malicious software ...

- Obfuscated variants of the same malware can evade AVs
  - When executed they generate *similar malicious behavior*
Attractive Properties of Network-based Approach

• Monitor large number of machines with no overhead at the end host
  – Host-based malware behavior detection often requires costly VM monitoring

• Leverage existing *network perimeter* monitoring infrastructure
  – Enable detection of malware behavior
Challenges

- Detecting malware traffic is hard
  - Many different types of malware
  - Different communication protocols
  - Malware can use legitimate protocols to communicate (e.g., HTTP)
  - Identify malware traffic among very large volumes of legitimate traffic

Find a needle in haystack!
Behavioral Clustering of HTTP-based Malware and Signature Generation using Malicious Network Traces

Roberto Perdisci, Wenke Lee, Nick Feamster

USENIX NSDI 2010
Web-based Malware

- Use HTTP protocol
- Bypass existing network defenses
  - Firewalls
- Web kits for malware control available
Detecting Web-based Malware

Enterprise Network

Web-Proxy

FW

Web-Proxy

IDS

Behavioral Analysis

Malware detection models

Network Admin

Malware Collection
System Overview

Malware Traffic:

1. GET /in.php?affid=94901&url=5&win=Windows%20XP+2.0&sts=|US|1|6|4|1|284|0
2. GET /in.php?affid=43403&url=5&win=Windows%20XP+2.0&sts=
3. GET /in.php?affid=94924&url=5&win=Windows%20XP+2.0&sts=|US|1|6|8|1|184|0

Malware Detection Signature:

GET /in\.php\?affid=.*&url=5&win=Windows%20XP\+2\.0&sts=.*
Behavioral Malware Clustering

- System-level approaches
  - Based on *dynamic analysis*
    - Automated analysis of Internet malware [Bailey et al., RAID 2007]
    - Scalable malware clustering [Bayer et al., NDSS 2009]
  - Based on *static analysis*
    - Malware indexing using function-call graphs [Hu et al., CCS 2009]

source: honeyblog.org
Malware with similar network behavior may behave differently at the system level (and vice versa!)

- **Our approach**
  - Focus on *network-level behavior*
  - Clusters and related signatures should be independent from specific server IPs or domain names
  - Better *network-based* malware detection signatures compared to using host-level approaches
Network Behavioral Clustering

- Three-step clustering refinement process
- Good trade-off between efficiency and accuracy
- High-quality clusters are essential to extract good signatures
Network Behavioral Clustering

Malware Traces

Coarse-grained

Fine-grained

Meta-clusters

Honeypot

GET /bins/int/9kgen_up.int?fxp=6d HTTP/1.1
User-Agent: Download
Host: X1569.nb.host192-168-1-2.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Connection: close
Server: Yaws/1.68 Yet Another Web Server
Date: Mon, 15 Mar 2010 11:47:11 GMT
Content-Length: 573444
Content-Type: application/octet-stream
Network-level Clustering

Malware Traces → Coarse-grained → Fine-grained → Meta-clusters

Statistical Features:
- # GET req
- # POST req
- avg(len(url))
- avg(len(data_sent))
- avg(len(response))
- ...

Hierarchical Clustering

Dendrogram Cut

Davies-Bouldin validity index
Network-level Clustering

Malware Traces → Coarse-grained → Fine-grained → Meta-clusters

Structural Features

Malware Trace $m_1$
- GET /in.php?affid=94900
- GET /bins/int/9kgen_up.int?fxp=6dc23
- POST /jump2/?affiliate=boo1
- POST /trf?q=Keyword1&bd=-5%236

$\ldots \quad d(m_1, m_2) \quad \ldots \quad DC$

Malware Trace $m_2$
- GET /index.php?v=1.3&os=WinXP
- GET /kgen/config.txt
- POST /bots/command.php?a=6.6.6.6
- POST /attack.php?ip=10.0.1.2&c=dos
Network-level Clustering

- **Meta-clustering** recovers from possible mistakes made in previous steps

- Improves overall **quality** of malware clusters and malware detection models
Network-level Clustering

Malware Traces -> Coarse-grained -> Fine-grained -> Meta-clusters

Compute Centroids

Measure Distance $d(C_1, C_2)$

Hierarchical Clustering

DC

GET /in.php?affid=234
GET /bins/in\int?fxp=02
POST /j?affiliate=boo1
POST /trf?q=bd=-1%236

Centroid

Token Subsequences Algorithm

(Polygraph, IEEE S&P 2005)
Evaluating the Quality of Clusters

- **Hard task, no standard way to do it...**

  Clustering can be viewed as an unsupervised learning task, and analyzing the validity of the clustering results is intrinsically hard.

  Cluster validity analysis often involves the use of a subjective criterion of optimality.

- **Previous work** [Bayer et al., NDSS 2009]
  - compare to AV family labels
  - (semi-)manual *reference clustering*
  - Precision and Recall
Our Cluster Validity Analysis

<table>
<thead>
<tr>
<th>Malware Cluster</th>
<th>McAfee</th>
<th>Avira</th>
<th>Trend Micro</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>W32/Virut.gen</td>
<td>WORM/Rbot.50176.5</td>
<td>PE_VIRUT.D-1</td>
</tr>
<tr>
<td>M2</td>
<td>W32/Virut.gen</td>
<td>WORM/Rbot.50176.5</td>
<td>PE_VIRUT.D-2</td>
</tr>
<tr>
<td>M3</td>
<td>W32/Virut.gen</td>
<td>W32/Virut.Gen</td>
<td>PE_VIRUT.D-4</td>
</tr>
<tr>
<td>M4</td>
<td>W32/Virut.gen</td>
<td>W32/Virut.X</td>
<td>PE_VIRUT.XO-2</td>
</tr>
<tr>
<td>M5</td>
<td>W32/Virut.gen</td>
<td>WORM/Rbot.50176.5</td>
<td>PE_VIRUT.D-2</td>
</tr>
<tr>
<td>M6</td>
<td>W32/Virut.gen</td>
<td>W32/Virut.H</td>
<td>PE_VIRUT.NS-2</td>
</tr>
<tr>
<td>M7</td>
<td>W32/Virut.gen</td>
<td>WORM/Rbot.50176.5</td>
<td>PE_VIRUT.D-2</td>
</tr>
<tr>
<td>M8</td>
<td>W32/Virut.gen</td>
<td>WORM/Rbot.50176.5</td>
<td>PE_VIRUT.D-1</td>
</tr>
</tbody>
</table>

**Cohesion Index**

\[
c(C_i) = 1 - \frac{1}{\gamma n \cdot v(n \cdot v - 1)} \sum_{l_1 < l_2} \delta_{l_1, l_2}
\]

**Separation Index**

\[
s(C_i, C_j) = \frac{1}{\gamma \text{avg}_{k,h} \{\Delta(V_k^{(i)}, V_h^{(j)})\}}
\]

AV-Label Graph

- M_W32/Virut
- A_W32/Virut
- T_PE_VIRUT

Nodes labeled with index values:
- M_W32/Virut: 1 - 3/8
- A_W32/Virut: 0
- T_PE_VIRUT: 1 - 5/8

Nodes labeled with index values:
- M_W32/Virut: 1 - 3/8
- A_W32/Virut: 0
- T_PE_VIRUT: 1 - 5/8
Signature Generation and Pruning

Original Signature Set

Final Malware Clusters

Token Subsequences Algorithm
(Polygraph, IEEE S&P 2005)
Signature Generation and Pruning

Original Signature Set

Final Malware Clusters

Pruned Signature Set

IDS

GET /in\php\?affid=.*
GET /bins/int/9kgen_up\int\?fxp=.*
GET /img/logo.jpg
POST /jump2\?affiliate=boo.*
POST /trf\?q=Keyword.*&bd=*%23.*
GET /index\asp\?version=.*
Signature Generation and Pruning

Original Signature Set

IDS

Legitimate Traffic

Enterprise Network

Pruned Signature Set

GET /in\.php\?affid=.*
GET /bins/int/9kgen_up\.int\?fxp=.*
GET /img/logo.jpg
POST /jump2/\?affiliate=boo.*
POST /trf\?q=Keyword.*&bd=.*%23.*
GET /index\.asp\?version=.*
Experimental Results

• **Malware Dataset**
  - 6 months of malware collection (Feb-Jul 2009)
  - ~25k distinct *real-world* malware samples

• **Clustering Results**

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Samples</th>
<th>Malware Families</th>
<th>Modeled Samples</th>
<th>Signatures</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb-2009</td>
<td>4,758</td>
<td>234</td>
<td>3,494</td>
<td>446</td>
<td>~8h</td>
</tr>
</tbody>
</table>

Cluster Validity Analysis

Compact and well Separated Clusters
Malware Detection Results

Detection Test on All Samples

<table>
<thead>
<tr>
<th></th>
<th>Feb09</th>
<th>Mar09</th>
<th>Apr09</th>
<th>May09</th>
<th>Jun09</th>
<th>Jul09</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig. Feb09</td>
<td>85.9%</td>
<td>50.4%</td>
<td>47.8%</td>
<td>27.0%</td>
<td>21.7%</td>
<td>23.8%</td>
</tr>
</tbody>
</table>

Detection Test on Malware undetected by commercial AVs

<table>
<thead>
<tr>
<th></th>
<th>Feb09</th>
<th>Mar09</th>
<th>Apr09</th>
<th>May09</th>
<th>Jun09</th>
<th>Jul09</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig. Feb09</td>
<td>54.8%</td>
<td>52.8%</td>
<td>29.4%</td>
<td>6.1%</td>
<td>3.6%</td>
<td>4.0%</td>
</tr>
</tbody>
</table>

Sig. Feb09  No False Alerts → Tested on 12M legitimate HTTP queries
Comparison with other approaches

Signature extracted from reduced malware set of ~2k malware samples

Using only fine-grained clustering

Using approach proposed in [Bayer et al. NDSS 2009]
Real-World Signature Deployment

- Deployed in large enterprise network
  - ~ 2k-3k active nodes
  - 4 days of testing
  - ~2k distinct signatures
- Findings
  - 25 machines infected by *spyware*
  - 19 machines infected by *scareware* (fake AVs)
  - 1 *bot*-compromised machine
  - 1 machine compromised by *banker trojan*
Detecting Zero Day Malware

- **Guilty by association** policy
  - EXEs that cluster with known malware are bad!

<table>
<thead>
<tr>
<th>cluster_id</th>
<th>md5</th>
<th>scanner_name</th>
<th>virus_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>80594</td>
<td>102244534227faa399703abe1da9e9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80594</td>
<td>6f9e18753c9ce480e9b8b7d4cb109d8</td>
<td></td>
<td>TR/Crypt.XPACK.Gen</td>
</tr>
<tr>
<td>80594</td>
<td>4b6c9e9ce171a1ebe9d9c07969a374</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80594</td>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>avira</td>
<td>TROJ_OFICLA.SM</td>
</tr>
<tr>
<td>80594</td>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>symantec</td>
<td>Trojan.FakeAV</td>
</tr>
<tr>
<td>80594</td>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>trend</td>
<td>TROJ_OFICLA.SM</td>
</tr>
<tr>
<td>80594</td>
<td>cb5689c4982f05ca1027472ecff33ff</td>
<td>avira</td>
<td>TR/Crypt.XPACK.Gen</td>
</tr>
<tr>
<td>80594</td>
<td>cb5689c4982f05ca1027472ecff33ff</td>
<td>symantec</td>
<td>Trojan.FakeAV</td>
</tr>
<tr>
<td>80594</td>
<td>cb5689c4982f05ca1027472ecff33ff</td>
<td>trend</td>
<td>TROJ_OFICLA.SM</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>md5</th>
<th>url</th>
<th>host</th>
<th>user_agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>GET /loads.php?code=</td>
<td>domen-zaibisy.com</td>
<td>wget</td>
</tr>
<tr>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>GET /firewall.dll</td>
<td>domen-zaibisy.com</td>
<td>wget</td>
</tr>
<tr>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>GET /cgi-bin/ware.cgi?adv=</td>
<td>domen-zaibisy.com</td>
<td>wget</td>
</tr>
<tr>
<td>9ce21ca9ad7bc2f6be266786bf44cd</td>
<td>GET /cgi-bin/get.pl?l=</td>
<td>kakleglo2335.com</td>
<td>wget</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>md5</th>
<th>url</th>
<th>host</th>
<th>user_agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>6f9e18753c9ce480e9b8b7d4cb109d8</td>
<td>GET /loads.php?code=</td>
<td>get-money-now.net</td>
<td>wget</td>
</tr>
<tr>
<td>6f9e18753c9ce480e9b8b7d4cb109d8</td>
<td>GET /firewall.dll</td>
<td>get-money-now.net</td>
<td>wget</td>
</tr>
<tr>
<td>6f9e18753c9ce480e9b8b7d4cb109d8</td>
<td>GET /cgi-bin/ware.cgi?adv=</td>
<td>get-money-now.net</td>
<td>wget</td>
</tr>
<tr>
<td>6f9e18753c9ce480e9b8b7d4cb109d8</td>
<td>GET /cgi-bin/get.pl?l=</td>
<td>mamapapalol.com</td>
<td>wget</td>
</tr>
</tbody>
</table>
Technology Transfer

- **HTTPrecon**
  - Filed for US patent
  - Deployed since January 2010
  - Analysis of ~10k distinct malware samples/month
  - Used to categorize groups of bot-malware into distinct *botnets*
  - Finds previously unknown compromised assets
  - Results analyzed on a daily bases by Damballa's Threat Analysts
Future Research

- More efficient clustering process
- Generalize to all kinds of malware, not only HTTP-based
- Automatic generation of "signature-less" statistical detection models
Thank You!

Questions?

perdisci@gtisc.gatech.edu
Appendix
AV malware detection stats

Source: Oberheide et al., USENIX Security 2008
Experimental Results

6 months malware collection → over 25k distinct samples

<table>
<thead>
<tr>
<th>dataset</th>
<th>samples</th>
<th>undetected by all AVs</th>
<th>undetected by best AV</th>
<th>Number of Clusters</th>
<th>Processing Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>coarse fine meta</td>
<td>coarse fine meta+sig</td>
</tr>
<tr>
<td>Feb09</td>
<td>4,758</td>
<td>208 (4.4%)</td>
<td>327 (6.9%)</td>
<td>2,538 2,660 1,499</td>
<td>34min 22min 6h55min</td>
</tr>
<tr>
<td>Mar09</td>
<td>3,563</td>
<td>252 (7.1%)</td>
<td>302 (8.6%)</td>
<td>2,160 2,196 1,779</td>
<td>19min 3min 1h3min</td>
</tr>
<tr>
<td>Apr09</td>
<td>2,274</td>
<td>142 (6.2%)</td>
<td>175 (7.7%)</td>
<td>1,325 1,330 1,167</td>
<td>8min 5min 28min</td>
</tr>
<tr>
<td>May09</td>
<td>4,861</td>
<td>997 (20.5%)</td>
<td>1,127 (23.2%)</td>
<td>3,339 3,423 2,593</td>
<td>56min 8min 2h52min</td>
</tr>
<tr>
<td>Jun09</td>
<td>4,677</td>
<td>1,038 (22.2%)</td>
<td>1,164 (24.9%)</td>
<td>3,304 3,344 2,537</td>
<td>57min 3min 37min</td>
</tr>
<tr>
<td>Jul09</td>
<td>5,587</td>
<td>1,569 (28.1%)</td>
<td>1,665 (29.8%)</td>
<td>3,358 3,390 2,724</td>
<td>1h5min 5min 2h22min</td>
</tr>
</tbody>
</table>

Compact and well Separated Clusters

Cluster Validity Analysis

AV Label Cluster Cohesion

AV Label Cluster Separation
Experimental Results

Malware Detection rate (all samples)

<table>
<thead>
<tr>
<th></th>
<th>Feb09</th>
<th>Mar09</th>
<th>Apr09</th>
<th>May09</th>
<th>Jun09</th>
<th>Jul09</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig_Feb09</td>
<td>85.9%</td>
<td>50.4%</td>
<td>47.8%</td>
<td>27.0%</td>
<td>21.7%</td>
<td>23.8%</td>
</tr>
<tr>
<td>Sig_Mar09</td>
<td>-</td>
<td>64.2%</td>
<td>38.1%</td>
<td>25.6%</td>
<td>23.3%</td>
<td>28.6%</td>
</tr>
<tr>
<td>Sig_Apr09</td>
<td>-</td>
<td>-</td>
<td>63.1%</td>
<td>26.4%</td>
<td>27.6%</td>
<td>21.6%</td>
</tr>
<tr>
<td>Sig_May09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>59.5%</td>
<td>46.7%</td>
<td>42.5%</td>
</tr>
<tr>
<td>Sig_Jun09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>58.9%</td>
<td>38.5%</td>
</tr>
<tr>
<td>Sig_Jul09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>65.1%</td>
</tr>
</tbody>
</table>

False Positives as measured on 12M legitimate HTTP requests from 2,010 clients

<table>
<thead>
<tr>
<th></th>
<th>Sig_Feb09</th>
<th>Sig_Mar09</th>
<th>Sig_Apr09</th>
<th>Sig_May09</th>
<th>Sig_Jun09</th>
<th>Sig_Jul09</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP rate</td>
<td>0% (0)</td>
<td>3 \times 10^{-4}% (38)</td>
<td>8 \times 10^{-6}% (1)</td>
<td>5 \times 10^{-5}% (6)</td>
<td>2 \times 10^{-4}% (26)</td>
<td>10^{-4}% (18)</td>
</tr>
<tr>
<td>Distinct IPs</td>
<td>0% (0)</td>
<td>0.3% (6)</td>
<td>0.05% (1)</td>
<td>0.2% (4)</td>
<td>0.4% (9)</td>
<td>0.3% (7)</td>
</tr>
<tr>
<td>Processing Time</td>
<td>13 min</td>
<td>10 min</td>
<td>6 min</td>
<td>9 min</td>
<td>12 min</td>
<td>38 min</td>
</tr>
</tbody>
</table>

“Zero-Day” Malware Detection rate

<table>
<thead>
<tr>
<th></th>
<th>Feb09</th>
<th>Mar09</th>
<th>Apr09</th>
<th>May09</th>
<th>Jun09</th>
<th>Jul09</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sig_Feb09</td>
<td>54.8%</td>
<td>52.8%</td>
<td>29.4%</td>
<td>6.1%</td>
<td>3.6%</td>
<td>4.0%</td>
</tr>
<tr>
<td>Sig_Mar09</td>
<td>-</td>
<td>54.1%</td>
<td>20.6%</td>
<td>5.0%</td>
<td>3.1%</td>
<td>5.4%</td>
</tr>
<tr>
<td>Sig_Apr09</td>
<td>-</td>
<td>-</td>
<td>41.9%</td>
<td>5.8%</td>
<td>3.8%</td>
<td>5.2%</td>
</tr>
<tr>
<td>Sig_May09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>66.7%</td>
<td>38.8%</td>
<td>16.1%</td>
</tr>
<tr>
<td>Sig_Jun09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>48.9%</td>
<td>21.8%</td>
</tr>
<tr>
<td>Sig_Jul09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>62.9%</td>
</tr>
</tbody>
</table>

Dets significant fraction of current and future malware variants

Complements traditional AV detection systems
Comparison with other approaches

Reduced dataset of ~4k malware samples

**net-clusters** = our three-step clustering approach

**net-fg-clusters** = only fine-grained clustering

**sys-clusters** = using approach proposed in [Bayer et al. NDSS 2009]
Network-level Clustering

Malware Traces

Coarse-grained

Fine-grained

Meta-clusters

GET /in.php?affid=94900
GET /bins/int/9kgen_up.int?fxp=6dc23
POST /jump2/?affiliate=boo1
POST /trf?q=Keyword1&bd=-5%236
GET /p6.asp?MAC=00-0C-26-F7-BD-AE

Hierarchical Clustering

Structural Features

POST /trf?q=Keyword1&bd=-5%236
POST /trf?q=Keyword3&bd=-1%231

\[ d_r(r_k, r_h) = w_m \cdot d_m(r_k, r_h) + w_p \cdot d_p(r_k, r_h) + w_n \cdot d_n(r_k, r_h) + w_v \cdot d_v(r_k, r_h) \]
Network-level Clustering

Malware Traces → Coarse-grained → Fine-grained → Meta-clusters

Centroid Signatures:
- GET /in\.php\?affid=.*
- GET /bins/int/9kgen_up\int\?fxp=.*
- POST /jump2\?affiliate=boo.*
- POST /trf\?q=Keyword.*&bd=.*%23.*
- GET /p6\.asp\?MAC=.*
- POST /trf\?q=Keyword.*&bd=+.*%236
- POST /trf\?q=Keyword.*&bd=-1%20.*

Hierarchical Clustering

Distance Function:
\[ d(s_i, s_j) = \frac{agrep(s_i, s'_j)}{\text{length}(s'_i)} \]