PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion

Jon Oberheide, Michael Bailey, Farnam Jahanian
University of Michigan

August 10th, 2009

WOOT '09
Can AV protect us from non-fictional threats too?
Game Plan

- AV and Packer Diversity
- The PolyPack Service
- The Rise of CaaS
- Demo and Wrap-up
There exists a wide diversity in AV detection capabilities

We can leverage diversity of multiple engines in the cloud
Diversity

“What AV engine has the best detection?”

- AV fails against recent threats
  - What else is new?
- Diversity in AV capabilities is significant

“What packer is most effective for attackers?”

- Similar diversity in packer effectiveness?
  - Single best packer?
  - Or case-by-case basis?
Packers in the Wild

- Packers
  - crypt/armor/compress
  - obfuscate/resist RCE
- Packer identification
  - 98,801 malware samples
  - PEiD:
    - Identified: 59,070 (60%)
    - Top 10: 33.3%
  - SigBuster
    - Identified: 69,974 (71%)
    - Top 10: 55.3%
- Unidentified
  - 80% compress < 20%
  - High entropy, small IATs
- Overall: > 90% packed

<table>
<thead>
<tr>
<th>PEiD</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPX</td>
<td>11244</td>
</tr>
<tr>
<td>Upack</td>
<td>6079</td>
</tr>
<tr>
<td>PECompact</td>
<td>4672</td>
</tr>
<tr>
<td>Nullsoft</td>
<td>2295</td>
</tr>
<tr>
<td>Themida</td>
<td>1688</td>
</tr>
<tr>
<td>FSG</td>
<td>1633</td>
</tr>
<tr>
<td>tElock</td>
<td>1398</td>
</tr>
<tr>
<td>NsPack</td>
<td>1375</td>
</tr>
<tr>
<td>ASpack</td>
<td>1283</td>
</tr>
<tr>
<td>WinUpack</td>
<td>1234</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SigBuster</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allaple</td>
<td>22050</td>
</tr>
<tr>
<td>UPX</td>
<td>11324</td>
</tr>
<tr>
<td>PECompact</td>
<td>5278</td>
</tr>
<tr>
<td>FSG</td>
<td>5080</td>
</tr>
<tr>
<td>Upack</td>
<td>3639</td>
</tr>
<tr>
<td>Themida</td>
<td>1679</td>
</tr>
<tr>
<td>NsPack</td>
<td>1645</td>
</tr>
<tr>
<td>ASpack</td>
<td>1505</td>
</tr>
<tr>
<td>tElock</td>
<td>1332</td>
</tr>
<tr>
<td>Nullsoft</td>
<td>1058</td>
</tr>
</tbody>
</table>
Diversity in AV detection and packer evasion is present across the board.
Game Plan

- AV and Packer Diversity
- The PolyPack Service
- The Rise of CaaS
- Demo and Wrap-up
The PolyPack Service

- The PolyPack Service
  - Impact of packers on AV detection

- Online submission service
  - Pack submitted binary with $N$ packers
  - Analyze each packed with $M$ AV engines
  - Evaluate evasion results of each packer

- Current implementation
  - 10 popular antivirus engines
  - 10 most common packers
The PolyPack Architecture

The PolyPack architecture is a web service that uses an array of packers and antivirus engines as a feedback mechanism to select the packer that will result in the optimal evasion of the antivirus engines. Our current implementation, based on the CloudAV backend, employs 10 packers and 10 popular antivirus engines. More information about PolyPack is available in our paper:

**PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion**

Jan Oberheide, Michael Bailey, and Farnam Jahanian

Workshop on Offensive Technologies (WOOT'09)

### PolyPack Service

**Upload a Binary**

Upload an unpacked PE binary. Or take a look at [some example results](#).

[Upload Binary]

**STATUS:** All packers and antivirus engines are online and operational.

### About PolyPack

PolyPack is a web service that uses an array of packers and antivirus engines as a feedback mechanism to select the packer that will result in the optimal evasion of the antivirus engines. Our current implementation, based on the CloudAV backend, employs 10 packers and 10 popular antivirus engines. More information about PolyPack is available in our paper:

**PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion**

Jan Oberheide, Michael Bailey, and Farnam Jahanian

Workshop on Offensive Technologies (WOOT'09)

### PolyPack Results

**Summary**

- SHA-1: 94db8c5ea44108d775bb7585b3c80b2e506f5a99
- Submitted: Sun Jul 19 16:21:11 2009
- File Size: 234496 bytes
- Current Status: **COMPLETE**
- Comments: N/A

**Evasion Recommendation**

- The unpacked binary was detected by 9 out of the 10 antivirus engines.
- Packing the binary resulted in evasion gains in 5 cases (Nilssoft, PECompact, IEblock, Themida, Yoda).
- The best evasion, 9 out of the 10 antivirus engines, was provided by Themida.
PolyPack Use Cases

- Researchers / defenders
  - Understand limitations of AV w.r.t. packers

- Penetration testers
  - Pick best packer for engagements w/unknown AV
  - Confidentiality, evasion metrics

- Already in use by both
Evaluation

- Malware dataset
  - 208 malware samples compiled from source
  - 2288 total (208 unpacked + 2080 packed)

<table>
<thead>
<tr>
<th>Packer</th>
<th>Total</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unpacked</td>
<td>212</td>
<td>1.02</td>
</tr>
<tr>
<td>ASpack</td>
<td>+128</td>
<td>+0.61</td>
</tr>
<tr>
<td>FSG</td>
<td>+39</td>
<td>+0.19</td>
</tr>
<tr>
<td>NsPack</td>
<td>+239</td>
<td>+1.15</td>
</tr>
<tr>
<td>Nullsoft</td>
<td>+646</td>
<td>+3.11</td>
</tr>
<tr>
<td>PECompact</td>
<td>+509</td>
<td>+2.45</td>
</tr>
<tr>
<td>tElock</td>
<td>+424</td>
<td>+2.04</td>
</tr>
<tr>
<td>Themida</td>
<td>+935</td>
<td>+4.50</td>
</tr>
<tr>
<td>UPX</td>
<td>+91</td>
<td>+0.44</td>
</tr>
<tr>
<td>WinUpack</td>
<td>+230</td>
<td>+1.11</td>
</tr>
<tr>
<td>Yoda</td>
<td>+654</td>
<td>+3.14</td>
</tr>
<tr>
<td>Average</td>
<td>+389</td>
<td>+1.87</td>
</tr>
<tr>
<td>PolyPack</td>
<td>+1005</td>
<td>+4.73</td>
</tr>
</tbody>
</table>

PolyPack is >250% more effective at evading AV than picking a packer at random.

<table>
<thead>
<tr>
<th>Packer</th>
<th>Best Choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Themida</td>
<td>122</td>
</tr>
<tr>
<td>Nullsoft</td>
<td>59</td>
</tr>
<tr>
<td>Yoda</td>
<td>24</td>
</tr>
<tr>
<td>PECompact</td>
<td>3</td>
</tr>
</tbody>
</table>

Themida is best individually, but PolyPack picks a better packer for >40% of the samples.
Game Plan

- AV and Packer Diversity
- The PolyPack Service
- The Rise of CaaS
- Demo and Wrap-up
Existing Crimeware

- Packers/cryptors
- Exploit bundles
- Phishing kits
“Evil” In-Cloud Services

- Crimeware
  - Traditionally deployed and sold ad-hoc
  - Piracy/reselling is rampant
  - Can be deployed in SaaS model

- Advantages of cloud not limited to legit apps
  - CloudAV versus Cloud Anti-AV

- PolyPack as a crystal ball
  - Ease of construction and efficacy
Crimeware as a Service (CaaS)

- Service/subscription model
- More control / more money
- Parallels between cloud apps / crimeware:

<table>
<thead>
<tr>
<th>Cloud Type</th>
<th>Legitimate</th>
<th>Crimeware</th>
</tr>
</thead>
<tbody>
<tr>
<td>IaaS</td>
<td>Amazon EC2, Mosso</td>
<td>Renting out infected bots</td>
</tr>
<tr>
<td>PaaS</td>
<td>Google App Engine, Azure</td>
<td>Botnet-backed spam services</td>
</tr>
<tr>
<td>SaaS</td>
<td>SalesForce, SAP ByDesign</td>
<td>Packing services, Decaptcha!</td>
</tr>
</tbody>
</table>
Real-World CaaS

- Recent CaaS activity in the wild
- Rudimentary crimeware/online packing services already starting to appear

Screenshots thanks to Jorge Mieres / Evil Fingers!
Game Plan

- AV and Packer Diversity
- The PolyPack Service
- The Rise of CaaS
- Demo and Wrap-up
DEMO TIME!
Wrap-up

- Diversity as a strength and weakness
  - But why? Crack the AV blackbox!

- PolyPack Service
  - Feedback from pen testers
  - More packers, AVs, file formats, unpackers!

- The rise of CaaS
  - Attractive model for crimeware authors
  - Undoubtedly increased sophistication in future
Questions?

PolyPack website: https://polypack.eecs.umich.edu/

- Contact information
  - Jon Oberheide
  - University of Michigan
  - jonojono@umich.edu
  - http://www.eecs.umich.edu/fjgroup/