

# **PolyPack:**

An Automated Online Packing Service  
for Optimal Antivirus Evasion

*Jon Oberheide, Michael Bailey, Farnam Jahanian*  
*University of Michigan*

**August 10th, 2009**

**WOOT '09**



# Box Office Threats



**STRIKE FIRST**  
WITH THE SPEED OF NORTON

LOG IN / REGISTER

**PROTECTORS**

*Threats are no match for G.I. JOE and Norton Special Forces*

**TREATS**

With cunning, stealth and a penchant for destruction, the COBRA agenda is to wreak havoc whenever and wherever possible.

Relying on a talented crew built from heroic, trustworthy, and intelligent soldiers, the Joe team fearlessly defends against COBRA's evil intentions.

Norton Special Forces are no different. With services that range from the all-encompassing to the uber-specialized, you can rest assured your system is safeguarded from any enemy invaders.

*Click on the character icons below*  
to learn how Norton and the G.I. JOE team stack up against enemy threats.

**G.I. JOE** VS **COBRA**

Home Norton Special Forces Instant Win Buy Norton Now Watch G.I. JOE Trailer SFX ON/OFF

**Norton**  
from symantec

Official Rules | FAQs | Privacy Policy | Find us on Facebook  
Legal Notices | Site Feedback | License Agreements | Contact Us

© 2009 Symantec Corporation © 2009 Paramount © 2009 Hasbro

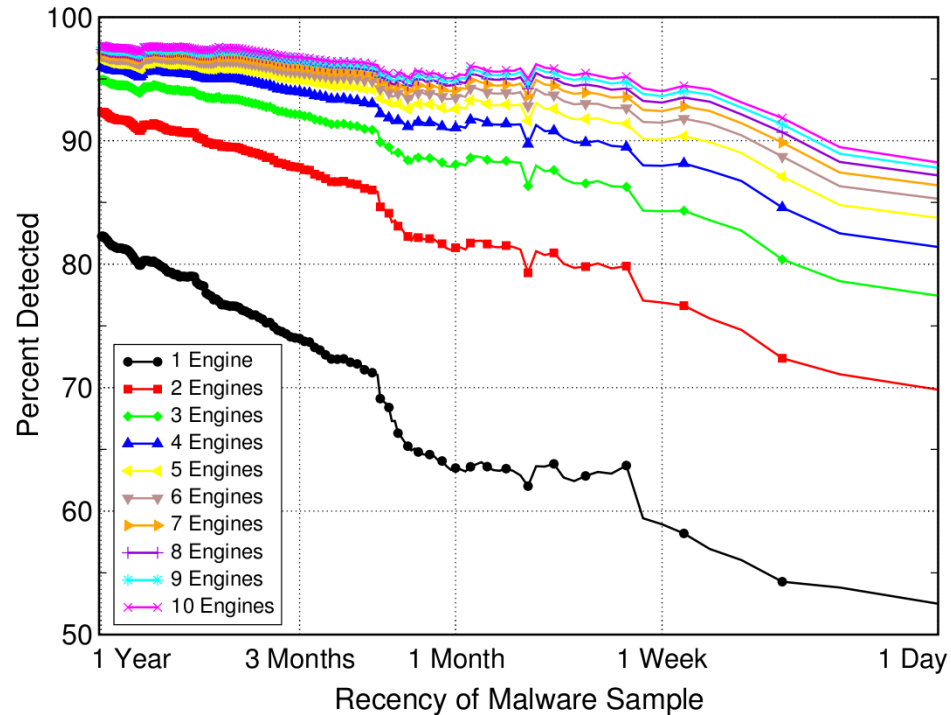
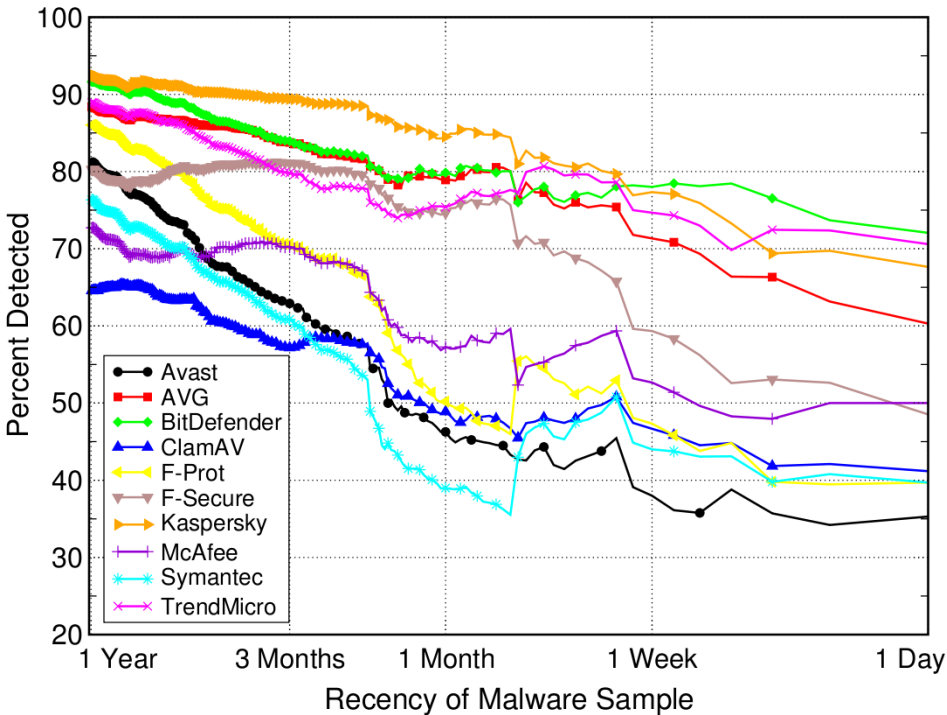
**G.I. JOE**  
THE RISE OF COBRA  
ONLY IN THEATERS

Can AV protect us from non-fictional threats too?



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

# CloudAV: AV Diversity



There exists a wide diversity in AV detection capabilities

We can leverage diversity of multiple engines in the cloud



“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

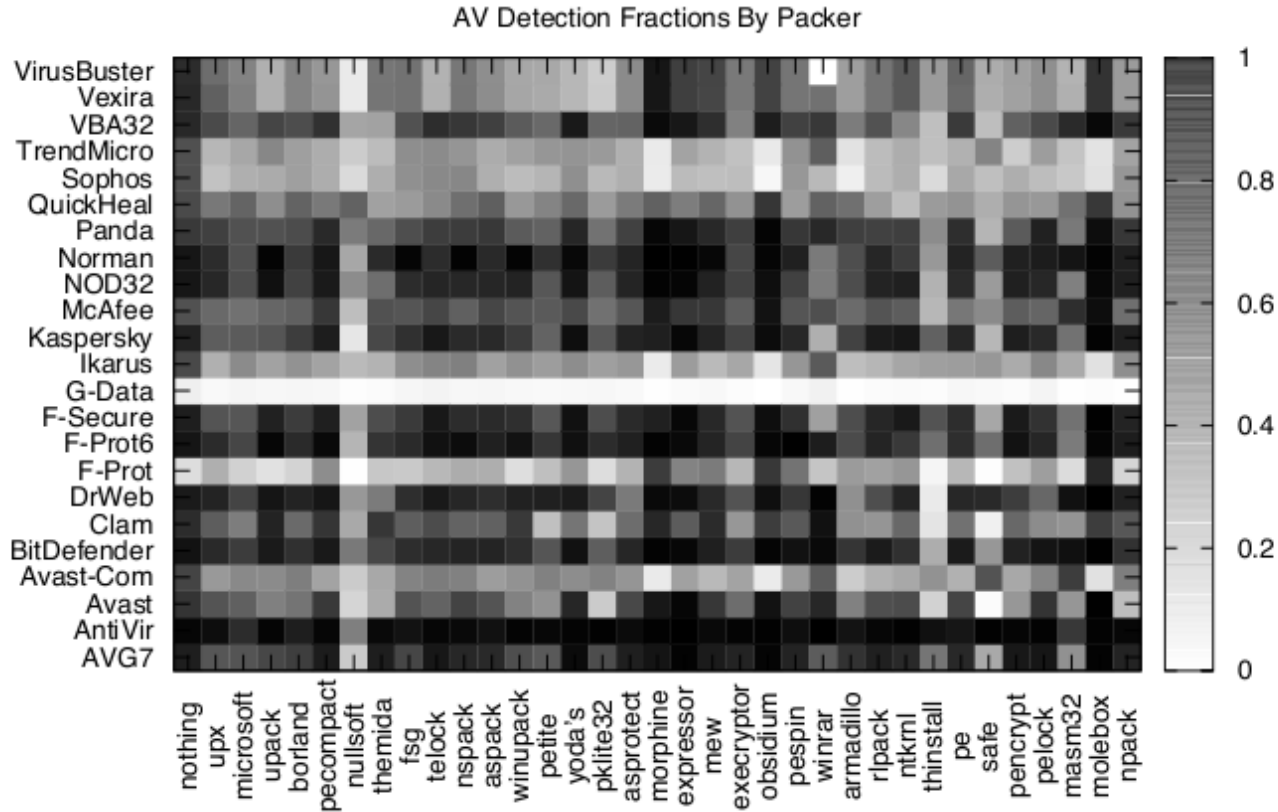


- Packers
  - crypt/armor/compress
  - obfuscate/resist RCE
- Packer identification
  - 98,801 malware samples
  - PEiD:
    - Identified: 59,070 (60%)
    - Top 10: 33.3%
  - SigBuster
    - Identified: 69,974 (71%)
    - Top 10: 55.3%
  - Unidentified
    - 80% compress < 20%
    - High entropy, small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

PEiD	Count
UPX	11244
Upack	6079
PECompact	4672
Nullsoft	2295
Themida	1688
FSG	1633
tElock	1398
NsPack	1375
ASpack	1283
WinUpack	1234

SigBuster	Count
Allaple	22050
UPX	11324
PECompact	5278
FSG	5080
Upack	3639
Themida	1679
NsPack	1645
ASpack	1505
tElock	1332
Nullsoft	1058

# AvP: Antivirus vs. Packers



Diversity in AV detection and packer evasion is present across the board.



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























# The PolyPack Service

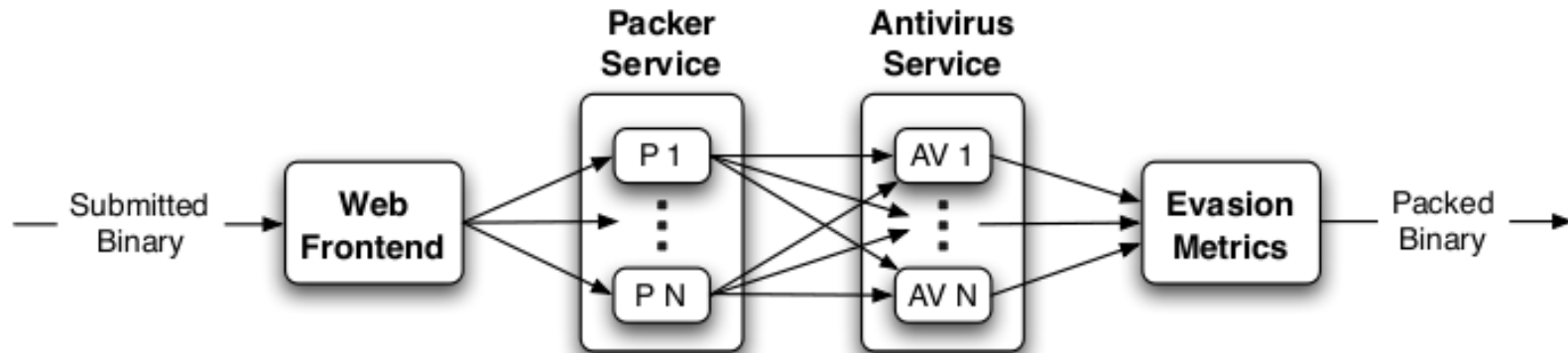


- The PolyPack Service
  - Impact of packers on AV detection
- Online submission service
  - Pack submitted binary with  $N$  packers
  - Analyze each packed with  $M$  AV engines
  - Evaluate evasion results of each packer
- Current implementation
  - 10 popular antivirus engines
  - 10 most common packers

## Supported Antivirus Supported Packers

	Avast		ASPack
	AVG		FSG
	BitDefender		NsPack
	ClamAV		Nullsoft
	F-Prot		PECompact
	F-Secure		tElock
	Kaspersky		Themida
	McAfee		UPX
	Symantec		WinUpack
	Trend Micro		Yoda

# The PolyPack Architecture



## POLYPACK

### PolyPack Service

#### Upload a Binary

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

**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**

Jon Oberheide, Michael Bailey, and Farnam Jahanian

Workshop on Offensive Technologies (WOOT'09)

## POLYPACK

### PolyPack Results

#### Summary

SHA-1: 94db8c5ea448108d775bb7785ec80b2e506ffa99

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 (Nullsoft, PECompact, tElock, 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)

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

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

Packer	Best Choice
Themida	122
Nullsoft	59
Yoda	24
PECompact	3

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



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

# Existing Crimeware



- Packers/cryptors
- Exploit bundles
- Phishing kits

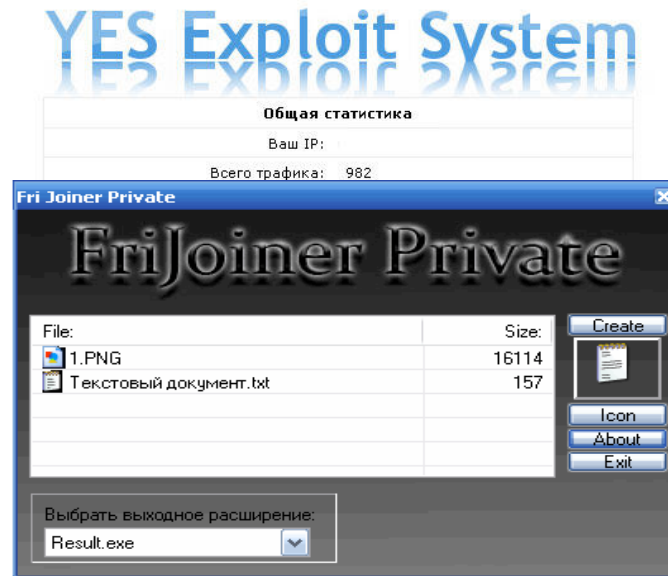
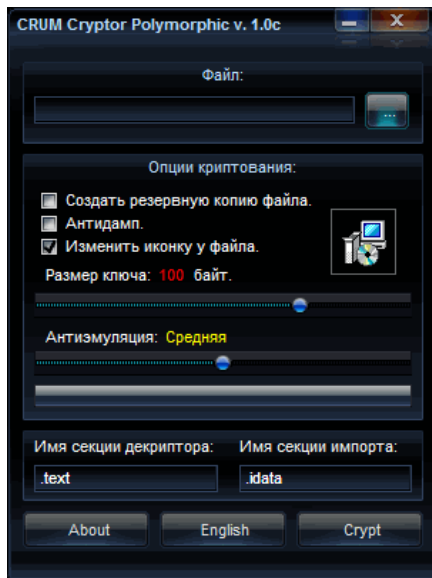
## UNIQUE PACK

Unique sheaf spoils

Spoils:		Info:
9. Adobe Collab.getIcon + util.printf + Collab.collectEmailInfo (up to 9)		<a href="http://google.com/">http://google.com/</a>
2. Foxit Reader 3.0 (<= Build 1301) PDF Buffer Overflow Exploit		<a href="http://www.securitylab.ru/vulnerability/369891.php">http://www.securitylab.ru/vulnerability/369891.php</a>
4. Opera CSS "operaconfig" && execute code		<a href="http://google.com/">http://google.com/</a>
5. Internet Explorer 7 Uninitialized Memory Corruption Vulnerability		<a href="http://www.checkpoint.com/defense/advisories/public/2009/cpai-03-Feb.html">http://www.checkpoint.com/defense/advisories/public/2009/cpai-03-Feb.html</a>
6. Microsoft Internet Explorer Data Binding Memory Corruption (XML)		<a href="http://www.microsoft.com/technet/security/advisory/961051.mspx">http://www.microsoft.com/technet/security/advisory/961051.mspx</a>
7. Snapshot Viewer for Microsoft Access ActiveX Control Arbitrary File Download		<a href="http://www.securityfocus.com/bid/30114">http://www.securityfocus.com/bid/30114</a>
8. IE6 splMegaPack		<a href="http://www.securitylab.ru/poc/270820.php">http://www.securitylab.ru/poc/270820.php</a>

Browsers:	List spoils:
	<ul style="list-style-type: none"> <li>   x Foxit Reader 3.0 (&lt;= Build 1301)</li> <li>   x Adobe SplPack (Collab.getIcon, Collab.collectEmailInfo, util.printf)</li> </ul>



MPack v0.90 stats

Attacked hosts (total - uniq)		Traffic (total - uniq)	
IE XP ALL	114721 - 96104	Total traff	159073 - 129089
QuickTime	2175 - 2048	Exploited	44804 - 35574
Win2000	7033 - 6260	Loads count	17408 - 15968
Firefox	12885 - 12514	Loader's response	38.85% - 44.89%
Opera7	1271 - 1264	<b>Efficiency 10.94% - 12.37%</b>	

Browser stats (total)		Modules state	
MSIE	4 0%	Statistic type	MySQL-based
Opera	1 0%	User blocking	ON
		Country blocking	OFF

Country	Traff	Loads	Efficiency
RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
IT - Italy	7045 4.4%	593 3.4%	8.42%
GE - Georgia	5775 3.6%	673 3.9%	11.65%
BY - Belarus	5419 3.4%	657 3.8%	12.12%
KZ - Kazakhstan	3098 1.9%	376 2.2%	12.14%
US - United states	1117 0.7%	50 0.3%	4.48%
AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
MD - Moldova, republic of	683	101	14.79%

# “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

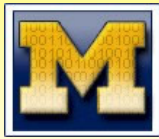
# Crimeware as a Service (CaaS)



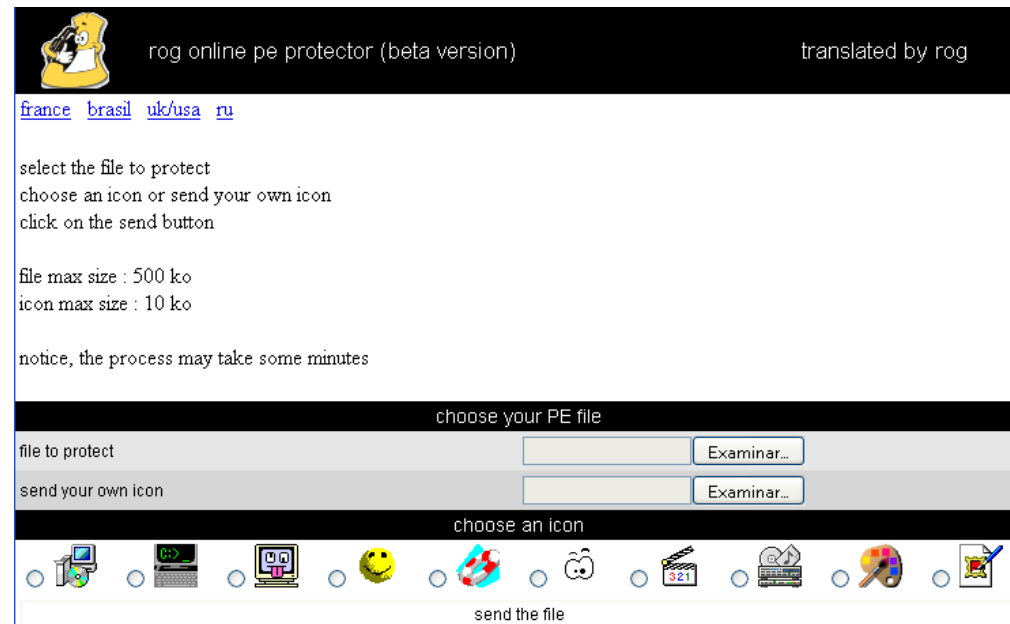
- Service/subscription model
- More control / more money
- Parallels between cloud apps / crimeware:

Cloud Type	Legitimate	Crimeware
IaaS	Amazon EC2, Mosso	Renting out infected bots
PaaS	Google App Engine, Azure	Botnet-backed spam services
SaaS	SalesForce, SAP ByDesign	Packing services, Decaptcha!





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



Screenshots thanks to Jorge Mieres / Evil Fingers!



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



# DEMO TIME!



- 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](mailto:jonojono@umich.edu)
  - <http://www.eecs.umich.edu/fjgroup/>