Aw, Snap!

It looks like this page crashed.

Download and install update to fix this problem
Aw, Snap!

It looks like this page crashed.

Download and install update to fix this problem
Aw, Snap!

It looks like this page crashed.

Download and install update to fix this problem

Click and run Plugin Update below.
Click and run Plugin Update below.

pluginupdate.exe appears malicious.  Discard
CAMP
Content Agnostic Malware Protection

Moheeb Abu Rajab, Lucas Ballard, Noé Lutz, Panayiotis Mavrommatis and Niels Provos

Google Safe Browsing Team
Current Situation

- Web still used for malware distribution
- Browsers and plug-ins are more secure
- Drive-by-downloads become challenging
- Social Engineering attacks on the rise
Challenges

- Exploit detection mechanism fail
- URL malware lists can be ineffective
- AVs struggle with polymorphic binaries
- Binary whitelists do not scale
Objective
Contributions

• Content agnostic malware protection
• Real-time detection of malware
• Hybrid detection approach
• 6 month evaluation with 200M users
Overview

• System Architecture
• Evaluation
• Case study
• Conclusion
System Architecture

Client Request → Reputation Engine

Verdict ← Reputation Engine

Whitelists

Malware List

Reputation Data

IP, Site, aggregates
Verdict in Chrome

unknown.exe is not commonly downloaded and could be dangerous.

content.exe appears malicious. Discard
System Architecture

Client Request -> Reputation Engine

Reputation Engine -> Verdict

Client Request

Whitelists

Malware List

Reputation Data

IP, Site, aggregates
# Reputation Engine

Aggregate:  # bad / # total events

<table>
<thead>
<tr>
<th>Feature / Aggregation Key</th>
<th>Baseline Aggregates</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP:1.2.3.4</td>
<td>98 / 109</td>
</tr>
<tr>
<td>site:foo.com/</td>
<td>1039 / 5694</td>
</tr>
<tr>
<td>host:a.foo.com/</td>
<td>0 / 0</td>
</tr>
</tbody>
</table>
Overview

- System Architecture
- Evaluation
- Case study
- Conclusion
Evaluation

- 6 month evaluation, 200M Chrome users
- 15M download requests / day
- 500K warnings shown / day
Evaluation - Labeling

Client Requests → Safe Browsing Frontend → Aggregation

URLs → Binary Analysis → Aggregation

IP:1.2.3.4: 30 / 100

IP:1.2.3.4: 98 / 109

Reputation Data
Evaluation - Labeling

1% FP

12% FN

Malicious

Benign

Binary Analysis
VT

1100
1089

1100
968
Evaluation - Reputation

TPR
TNR
FPR
FNR

03/01
04/01
05/01
06/01
07/01
## Overall Accuracy

<table>
<thead>
<tr>
<th></th>
<th>Reputation Engine</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>98%</td>
<td>99.5%</td>
</tr>
<tr>
<td>FPR</td>
<td>2%</td>
<td>0.6%</td>
</tr>
</tbody>
</table>
CAMP Reputation vs. AVs

Flagged

Benign

CAMP AV-1 AV-2 AV-3 AV-4

CAMP AV-1 AV-2 AV-3 AV-4
Overview

- System Architecture
- Evaluation
- Case study
- Conclusion
Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

• 13K unique hostnames over 2 week period
• Domain rotation every 7 minutes
Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- 13K unique hostnames over 2 week period
- Domain rotation every 7 minutes

URL Malware lists didn’t work here
Case Study
(srv|www|server|update)\d{2}.\w+.uni.me

- Binary changed roughly every 10 minutes
- Saw >900 distinct content hashes
- Only 1/40 Virus Total AV flagged binary
Case Study

(srv|www|server|update)\d{2}.\w+.uni.me

- Binary changed roughly every 10 minutes
- Saw >900 distinct content hashes
- Only 1/40 Virus Total AV flagged binary

Content based approaches didn’t work here
Overview

- System Architecture
- Evaluation
- Case study
- Conclusion
Summary

• Content agnostic reputation approach
• Scalable to 200M users
• High accuracy with low false positive rate