SECURITY READING GROUP

Today’s Talks:
Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services - Ziyun Zhu

Upcoming Talks:
HoTSoS 2017 (4-5 Apr) - http://hot-sos.com
http://cps-vo.org/group/hotsos/registration - Nevermore!
Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services

Platon Kotzias, Leyla Bilge, Juan Caballero
Potential Unwanted Programs (PUP)
Potential Unwanted Programs (PUP)
PUP vs Malware

Install Vuze Offer

By clicking "Next" you agree to the Terms of Use and Privacy Policy.

Express Install includes the Extensions by Spider (Browser Extensions(IE), Shopping Assistant/New Tab Helper(GC), Slick Savings/StarPage/Ebay Assistant(FF)), Set Yahoo! as my default, home, and new tab pages (IE,FF,G). The Spider Terms of Use applies to the Browser Extensions (which includes Browser Extensions in Internet Explorer, Shopping Assistant/New Tab Helper in Google Chrome, Slick Savings/StarPage/Ebay Assistant in Mozilla Firefox) and Search Protection ("Program"), which is built and maintained by Spider, Inc. ("We", "your", or "us"), whether in uppercase, lowercase, or a combination. The Program allows you a convenient way to help find search results online by collecting your requests for information and processing them through our search engine partners. Our partners may compensate us for making the information available to you. Use of the Program is free of charge to you. Use of the Program and its features as described below requires that you agree to the following Terms of Use (the "Terms"). You agree to be legally bound by these Terms clicking the "I Accept", "Next", "Run", "Install", or "Yes" button provided. These Terms are a legal contract between us and you, an individual user of at least 18 years of age, or if you are using the Program on behalf of any entity -- including a company, organization, or trust, no matter the legal form of the entity -- ("Entity"), then you represent and warrant that you are an authorized representative of that entity.

Custom install (for advanced users): Make Yahoo! my default search (IE,FF,G). Make Yahoo! my home & startup page (IE,FF,G). Install the Extensions by Spider (Browser Extensions(IE), GC, Shopping Assistant/New Tab Helper(GC), Slick Savings/StarPage/Ebay Assistant(FF)).

VLC classic Setup

TELL YOUR FRIENDS EXACTLY WHAT YOU WANT!

Adds "I Want This" button to your favorite shopping sites.
Clicking "I Want This" adds items you want to your wishlist.
Wishlist items can be automatically posted to your wall so friends and family can buy them.

I Want This is ad-supported software that is provided at no cost and may display advertisements in websites as you view them.
By clicking "Accept" you agree to install I Want This and to its license agreement and Privacy policy.
PUP vs Malware

When Adware Goes Bad: The Installbrain and Sefnit Connection

Posted on: July 7, 2014 at 8:30 am  Posted in: Bad Sites, Malware  Author: Trend Micro
Evidence of PUP Prevalence

Evidence of PUP Prevalence


- 5% of unique IPs accessing Google have injected advertisements

Evidence of PUP Prevalence

How many users are affected by PUP?


- 5% of unique IPs accessing Google have injected advertisements

Pay-Per-Install (PPI) Ecosystem
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service

Affiliate Publishers

VLC
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service

Affiliate Publishers

VLC
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service

Affiliate Publishers

Target Hosts
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service

Affiliate Publishers

Target Hosts

VLC

Tell Your Friends
EXACTLY WHAT YOU WANT

Add "Want This" to your favorite shopping sites.

Creating "Want This" will save you money at your favorite stores.

Also share "Want This" with your friends to help them save too.

http://www.wantthis.com

Terms of Service and Privacy Policy
Pay-Per-Install (PPI) Ecosystem

Advertisers

PPI Service

Publishers = Software owners

Affiliate Publishers

Target Hosts

Publishers = Software owners
Pay-Per-Install (PPI) Ecosystem

How many PPI services?
What type of PUP is advertised?
Contributions

Measure PUP prevalence and its distribution through PPI services
Measure PUP prevalence and its distribution through PPI services

Build publisher graph to captures who-installs-who relationships among PUP Publishers

Identify the prevalent PPI services and advertisers
Contributions

Measure PUP prevalence and its distribution through PPI services

Build publisher graph to captures who-installs-who relationships among PUP Publishers
Identify the prevalent PPI services and advertisers

Examine PUP-Malware relationships
Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach
Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach

Analysis period

<table>
<thead>
<tr>
<th>19 months</th>
<th>12 months</th>
</tr>
</thead>
</table>

PUP Prev. 23 PPI 77 Adv.

4 PPI

Safe Browsing data
Adv. SW
PPI Measurements

3.9M WINE Dataset
Comparison with Simultaneous Work

- Complementary works
- Bottom-to-top compared to top-to-bottom approach

- Analysis period

- Geographical coverage
Datasets

11M reports of malicious/undesirable software
Datasets

11M reports of malicious/undesirable software

Malsign dataset

142K signed malware and PUP (binaries & clustering families)

[Kotzias et al. CCS ’15]
Datasets

**VirusTotal**
- 11M reports of malicious/undesirable software

**Malsign dataset**
- 142K signed malware and PUP (binaries & clustering families)
  
  [Kotzias et al. CCS ’15]

**Symantec WINE Dataset**
- AV telemetry from 3.9M real Windows hosts
- 8B events for 19 months (Jan ‘13 – July ‘14)
Datasets

**Virustotal**

11M reports of malicious/undesirable software

**WINE Dataset**

142K signed malware and PUP (binaries & clustering families)

[Kotzias et al. CCS ’15]

**Malsign dataset**

AV telemetry from 3.9M real Windows hosts

8B events for 19 months (Jan ‘13 – July ‘14)

**Symantec**

Parent

Uncompress

Child
Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP \cite{Kotzias et al. CCS ‘15}
Identify PUP Publishers

Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]

11M hashes
Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]
Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]
Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]
Focus on signed executables → Digital signatures allow attribution of software publisher

Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]
Focus on signed executables → Digital signatures allow attribution of software publisher
Properly signed executables flagged by AVs are predominantly PUP [Kotzias et al. CCS ‘15]
Publisher name similarity

Tuguu Israel Ltd
TUGUU SLU
Tuguu sl
Tuguu S.L.U.

Tuguu
Clustering Publishers

Publisher name similarity

Tuguu Israel Ltd
TUGUU SLU
Tuguu s.l
Tuguu S.L.U.

Tuguu

Child download domains

Publisher A
Publisher B
Publisher C

Parent download domains

Publisher A
Publisher B
Publisher C
Clustering Publishers

Publisher name similarity
- Tuguu Israel Ltd
- TUGUU SLU
- Tuguu sl
- Tuguu S.L.U.

Child download domains
- Maldown.com
- EXE
- Publisher A
- EXE
- Publisher B
- EXE
- Publisher C

Malsign clustering
- 142K signed samples

Parent download domains
- 2.2K clusters

Publisher A
- EXE
- Publisher B
- EXE
- Publisher C
- EXE
Clustering Publishers

Publisher name similarity
Tuguu Israel Ltd
TUGUUU SLU
Tuguu sl
Tuguu S.L.U.

Child download domains
Publisher A
Publisher B
Publisher C
Maldown.com

Malsign clustering
142K signed samples
2.2K clusters

5K Publisher clusters
Maldown.com
Publisher A
Publisher B
Publisher C
Clustering Publishers

Publisher name similarity

Tuguu Israel Ltd
TUGUU SLU
Tuguu S.L.U.
Tuguu Maldown.com

Child download domains

Publisher A
Publisher B
Publisher C

Parent download domains

142K signed samples
2.2K clusters

High DR

Publisher Detection Ratio (DR) = \# EXEs flagged by AVs / All EXEs

5K Publisher clusters
915 PUP Publisher clusters

915

Publisher A
Publisher B
Publisher C

Maldown.com
Road Map

- Intro
- PUP Prevalence
- PPI Ecosystem
PUP Prevalence

Internet Users

Symantec Users

WINE Opted-in

Users with PUP
54% (2.1M) of WINE hosts have at least one PUP executable installed.
PUP Prevalence

Internet Users

Symantec Users

WINE Opted-in

Users with PUP

~210M Internet users affected

54% (2.1M) of WINE hosts have at least one PUP executable installed
# Publisher Ranking

<table>
<thead>
<tr>
<th>#</th>
<th>Cluster</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft</td>
<td>3.9M</td>
</tr>
<tr>
<td>2</td>
<td>Symantec</td>
<td>3.8M</td>
</tr>
<tr>
<td>3</td>
<td>Adobe Systems</td>
<td>3.5M</td>
</tr>
<tr>
<td>4</td>
<td>Google</td>
<td>3.1M</td>
</tr>
<tr>
<td>5</td>
<td>Apple</td>
<td>1.8M</td>
</tr>
<tr>
<td>6</td>
<td>Intel</td>
<td>1.6M</td>
</tr>
<tr>
<td>7</td>
<td>Sun Microsystems</td>
<td>1.6M</td>
</tr>
<tr>
<td>8</td>
<td>Cyberlink</td>
<td>1.6M</td>
</tr>
<tr>
<td>9</td>
<td>GEAR Software</td>
<td>1.5M</td>
</tr>
<tr>
<td>10</td>
<td>Hewlett-Packard</td>
<td>1.5M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>Cluster</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Oracle</td>
<td>1.4M</td>
</tr>
<tr>
<td>12</td>
<td>Skype Technologies</td>
<td>1.3M</td>
</tr>
<tr>
<td>13</td>
<td>Mozilla Corporation</td>
<td>1.0M</td>
</tr>
<tr>
<td>14</td>
<td>McAfee</td>
<td>1.0M</td>
</tr>
<tr>
<td>15</td>
<td>Perion Network/Conduit</td>
<td>1.0M</td>
</tr>
<tr>
<td>24</td>
<td>Mindspark</td>
<td>533K</td>
</tr>
</tbody>
</table>
### Publisher Ranking

<table>
<thead>
<tr>
<th>#</th>
<th>Cluster</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft</td>
<td>3.9M</td>
</tr>
<tr>
<td>2</td>
<td>Symantec</td>
<td>3.8M</td>
</tr>
<tr>
<td>3</td>
<td>Adobe Systems</td>
<td>3.5M</td>
</tr>
<tr>
<td>4</td>
<td>Google</td>
<td>3.1M</td>
</tr>
<tr>
<td>5</td>
<td>Apple</td>
<td>1.8M</td>
</tr>
<tr>
<td>6</td>
<td>Intel</td>
<td>1.6M</td>
</tr>
<tr>
<td>7</td>
<td>Sun Microsystems</td>
<td>1.6M</td>
</tr>
<tr>
<td>8</td>
<td>Cyberlink</td>
<td>1.6M</td>
</tr>
<tr>
<td>9</td>
<td>GEAR Software</td>
<td>1.5M</td>
</tr>
<tr>
<td>10</td>
<td>Hewlett-Packard</td>
<td>1.5M</td>
</tr>
<tr>
<td>11</td>
<td>Oracle</td>
<td>1.4M</td>
</tr>
<tr>
<td>12</td>
<td>Skype Technologies</td>
<td>1.3M</td>
</tr>
<tr>
<td>13</td>
<td>Mozilla Corporation</td>
<td>1.0M</td>
</tr>
<tr>
<td>14</td>
<td>McAfee</td>
<td>1.0M</td>
</tr>
<tr>
<td>15</td>
<td>Perion Network/Conduit</td>
<td>1.0M</td>
</tr>
</tbody>
</table>

PUP publishers are among the most widely installed software publishers.
Road Map

- Intro
- PUP Prevalence
- PPI Ecosystem
How many PPI services exist?

What type of PUP is distributed?

How is PUP distributed?

PUP – Malware relationship?
Publisher graph captures the who-installs-who relationships
Publisher graph captures the who-installs-who relationships

#Events: 10K
#Hosts: 1K

#Events: 2K
#Hosts: 500

Publisher Graph
Publisher graph captures the who-installs-who relationships
How many PPI services exist?

High DR and High ID and High OD
How many PPI services exist?

High DR and High ID and High OD

5K Publishers → Rule → 49 Candidates → Manual Analysis → 24 PPIs
How many PPI services exist?

High DR and High ID and High OD

5K Publishers

Rule

49 Candidates

Manual Analysis

24 PPIs

<table>
<thead>
<tr>
<th>PPI cluster</th>
<th>DR</th>
<th>ID</th>
<th>OD</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perion Network/Conduit</td>
<td>52%</td>
<td>168</td>
<td>63</td>
<td>1M</td>
</tr>
<tr>
<td>Web Pick</td>
<td>79%</td>
<td>65</td>
<td>22</td>
<td>346K</td>
</tr>
<tr>
<td>iBario</td>
<td>84%</td>
<td>62</td>
<td>36</td>
<td>336K</td>
</tr>
<tr>
<td>IronSource</td>
<td>81%</td>
<td>73</td>
<td>112</td>
<td>332K</td>
</tr>
<tr>
<td>OpenCandy</td>
<td>55%</td>
<td>91</td>
<td>36</td>
<td>311K</td>
</tr>
</tbody>
</table>
### How many PPI services exist?

#### PPI cluster

<table>
<thead>
<tr>
<th>PPI cluster</th>
<th>DR</th>
<th>ID</th>
<th>OD</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perion Network/Conduit</td>
<td>52%</td>
<td>168</td>
<td>63</td>
<td>1M</td>
</tr>
<tr>
<td>Web Pick</td>
<td>79%</td>
<td>65</td>
<td>22</td>
<td>346K</td>
</tr>
<tr>
<td>iBario</td>
<td>84%</td>
<td>62</td>
<td>36</td>
<td>336K</td>
</tr>
<tr>
<td>IronSource</td>
<td>81%</td>
<td>73</td>
<td>112</td>
<td>332K</td>
</tr>
<tr>
<td>OpenCandy</td>
<td>55%</td>
<td>91</td>
<td>36</td>
<td>311K</td>
</tr>
</tbody>
</table>

**3/Top 5 most popular PUP publishers are PPI services**
How many PPI services exist?

High DR and High ID and High OD

- 5K Publishers
- Rule to 49 Candidates
- Manual Analysis to 24 PPIs

3/Top 5 most popular PUP publishers are PPI services

- 12 other PPIs not seen:
  - Not popular or gain popularity later
  - Distribute unsigned bundles
  - Resellers

<table>
<thead>
<tr>
<th>PPI cluster</th>
<th>DR</th>
<th>ID</th>
<th>OD</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perion Network/Conduit</td>
<td>52%</td>
<td>168</td>
<td>63</td>
<td>1M</td>
</tr>
<tr>
<td>Web Pick</td>
<td>79%</td>
<td>65</td>
<td>22</td>
<td>346K</td>
</tr>
<tr>
<td>iBario</td>
<td>84%</td>
<td>62</td>
<td>36</td>
<td>336K</td>
</tr>
<tr>
<td>IronSource</td>
<td>81%</td>
<td>73</td>
<td>112</td>
<td>332K</td>
</tr>
<tr>
<td>OpenCandy</td>
<td>55%</td>
<td>91</td>
<td>36</td>
<td>311K</td>
</tr>
</tbody>
</table>
What type of PUP is distributed?

High DR and High ID and Low OD and Parent PPI > 0
What type of PUP is distributed?

High DR and High ID and Low OD and Parent PPI > 0
What type of PUP is distributed?

High DR and High ID and Low OD and Parent PPI > 0

18/30 Add-ons

Modify default search engine

Inject shopping deals & price comparisons

77 Advertisers
What type of PUP is distributed?

High DR and High ID and Low OD and Parent PPI > 0

18/30 Add-ons

Modify default search engine

6/30 Rogueware

Performance Optimizers

77 Advertisers

Inject shopping deals & price comparisons
What type of PUP is distributed?

- High DR and High ID and Low OD and Parent PPI > 0

18/30 Add-ons

- Delta Search
- iminent

Modify default search engine

6/30 Rogueware

- Uniblue SpeedUpMyPC
- Systweak Regclean Pro

6/30 Other

- myPC Backup.com
- Gom-Player
- FS

Performance Optimizers

Inject shopping deals & price comparisons

Advertisers

77

Modify default search engine

Inject shopping deals & price comparisons

Add-ons

Rogueware

Other

Performance Optimizers

Backup tools

Multimedia players
How is PUP distributed?
How is PUP distributed?
How is PUP distributed?

71% signed parents
How is PUP distributed?

71% are signed parents

74% are PUP parents

PUPs are generally installed by other PUPs
How is PUP distributed?

PUPs are generally installed by other PUPs

71% signed parents

74% are PUP parents

26% are PPI services

PPI services play an important role in the distribution of PUP
PUP - Malware Relationship

- **Challenge**: Accurately label malware in WINE dataset
PUP - Malware Relationship

- **Challenge**: Accurately label malware in WINE dataset

- **AVClass** malware labeling tool *Sebastián et al. RAID ´16*:
  
github.com/malicialab/avclass

\[
\begin{align*}
1be77f9e3abb48a481b1e683d617904a \\
8aeb7793645c05c6fe6e3c017703e45f \\
88f21f6a38bd35673dde705839885cce \\
1db177e0235fc32873973328f8f4f9b2
\end{align*}
\]
**PUP - Malware Relationship**

- **Challenge**: Accurately label malware in WINE dataset

- **AVClass** malware labeling tool [*Sebastián et al. RAID ´16*]:
  
  [GitHub](https://github.com/malicialab/avclass)

- Selected 70 popular malware families (e.g., zbot, zeroaccess, reveton, virut, salty)

![AVClass](https://example.com/avclass_icon.png)
PUP - Malware Relationship
PUP - Malware Relationship

Does PUP download malware?

71 PUP Publishers

40 families

5.6K (0.01%) download events

Examples:

- Perion Network dropping Zbot, Shylock trojans
- InstallBrain downloading Mevade/Sefnit as reported by TrendMicro
PUP - Malware Relationship

Does PUP download malware?

71 PUP Publishers

40 families

5.6K (0.01%) download events

Examples:

- Perion Network dropping Zbot, Shylock trojans
- InstallBrain downloading Mevade/Sefnit as reported by TrendMicro

Does malware download PUP?

25 families

98 PUP Publishers

11K (0.03%) download events
PUP - Malware Relationship

Does PUP download malware?

- 71 PUP Publishers
- 40 families
- 5.6K (0.01%) download events

Examples:
- Perion Network dropping Zbot, Shylock trojans
- InstallBrain downloading Mevade/Sefnit as reported by TrendMicro

Does malware download PUP?

- 25 families
- 98 PUP Publishers
- 11K (0.03%) download events

Malware distribution seems disjoint from PUP distribution
Summary

- **54%** of **3.9M** real hosts examined have PUP installed

- **Birds-eye view of the PPI ecosystem**
  - **24** PPI services that distribute **26%** of all signed PUP
  - **77** advertiser clusters (mostly BAO) that monetize in various ways

- Malware distribution seems disjoint from PUP distribution
Measuring PUP Prevalence and PUP Distribution through Pay-Per-Install Services

Platon Kotzias, Leyla Bilge, Juan Caballero