Anti Virus Industry‘s Future Challenge:
PUA
PUA STANDS FOR ...

Advertisement

Expectations

Reality
PUA and Security

Security

- **Install root certificate**
- Provide an **entry door for malware** (through exploits)
- Causing **issues on the system** – leading the user to remove/change the AV Software
- **Keylogger/KeyGenerator/PasswordReader** etc…
- ….

Basically is a potentially dangerous nuisance for the user and those poor admins fixing their parents device every weekend
Monetization

Non-objectionable means

- Share/Trialware
- SAAS or plain buying
- Advertisement on product webpage (Help, Forum etc.)
- Advertisement in products (App Stores apps)
- Non aggressive bundling

Questionable means

- Distribution through bundlers
- Information Harvesting
- Aggressive Advertisement
SOME PRETTY PICTURES – PUA BEHAVIOR

Sources
* http://www.nirsoft.net/utils/mailpv.html
* http://deletemalware.blogspot.de/2012/01/pupcnetadwarebundle-uninstall-guide.html

AV Future Challenge: PUA
DISTRIBUTION COMPARED TO MALWARE

Malware vs. PUA

10 million unique Files/Month

Windows, Linux, Android and Mac

AV Future Challenge: PUA
“IN THE WILD” PUA VS BENIGN APPS, WINDOWS

Benign vs. PUA

14,000 unique Installer/Month
“IN THE WILD” PUA VS BENIGN APPS, ANDROID

Benign vs. PUA including Malware

20,000 unique APKs/Month
ISSUES WITH MONETIZATION STRATEGIES
1.000 Malware, 600 PUA and 600 Benign unique samples
1.000 Malware, 600 PUA and 600 Benign unique samples
Permission classification provided by Google and Permissions set in Manifest
CLASSIFICATION OF REQUESTED PERMISSIONS

Permission classification provided by Google and Permissions set in Manifest

08.05.2017

AV Future Challenge: PUA
CLASSIFICATION OF REQUESTED PERMISSIONS CONT.

<table>
<thead>
<tr>
<th>Type</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>D D D D D D Nor Nor Nor Non S Nor Nor D D</td>
</tr>
<tr>
<td>PUA</td>
<td></td>
</tr>
<tr>
<td>Benign</td>
<td></td>
</tr>
</tbody>
</table>

July 2016
### Android

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Benign</th>
<th>PUA</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMEI (International Mobile Station Equipment Identity)</td>
<td>0,00%</td>
<td>27,56%</td>
</tr>
<tr>
<td>Device id (unique device identifier)</td>
<td>0,00%</td>
<td>2,95%</td>
</tr>
<tr>
<td>Root (device rooted or not)</td>
<td>0,00%</td>
<td>3,64%</td>
</tr>
<tr>
<td>Agent (user agent of browser)</td>
<td>0,16%</td>
<td>3,29%</td>
</tr>
<tr>
<td>IP Dest (IP destination)</td>
<td>0,32%</td>
<td>2,25%</td>
</tr>
<tr>
<td>Mac (unique network adapter address)</td>
<td>2,23%</td>
<td>10,57%</td>
</tr>
<tr>
<td>Device Model</td>
<td>9,38%</td>
<td>28,25%</td>
</tr>
<tr>
<td>OS Version</td>
<td>7,00%</td>
<td>15,42%</td>
</tr>
</tbody>
</table>

### Windows

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Benign</th>
<th>PUA</th>
<th>Malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relevant transmitted PUA data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer name</td>
<td>0,10%</td>
<td>7,36%</td>
<td>0,14%</td>
</tr>
<tr>
<td>Country</td>
<td>0,66%</td>
<td>8,23%</td>
<td>0,07%</td>
</tr>
<tr>
<td>City</td>
<td>0,00%</td>
<td>1,25%</td>
<td>0,00%</td>
</tr>
<tr>
<td>Relevant transmitted malware data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Browser details</td>
<td>0,05%</td>
<td>1,25%</td>
<td>13,16%</td>
</tr>
<tr>
<td>Region</td>
<td>0,00%</td>
<td>1,37%</td>
<td>4,46%</td>
</tr>
</tbody>
</table>
DESTINATION OF DATA TRANSMITTED, ANDROID

Benign Traffic Destination

- China: 48%
- United States: 18%
- Germany: 14%
- Netherlands: 10%
- Russian Federation: 6%
- Other Europe: 2%
- Other: 2%

PUA Traffic Destination

- China: 52%
- United States: 25%
- Germany: 7%
- Netherlands: 4%
- Russian Federation: 4%
- Other Europe: 6%
- Other: 4%

AV Future Challenge: PUA

July 2016
**DESTINATION OF DATA TRANSMITTED, WINDOWS**

**Benign Traffic Destination**
- United States: 77%
- Germany: 5%
- Netherlands: 1%
- China: 1%
- France: 2%
- United Kingdom: 2%
- Russian Federation: 3%
- Other Europe: 4%

**PUA Traffic Destination**
- United States: 68%
- Germany: 4%
- Netherlands: 4%
- China: 4%
- France: 4%
- United Kingdom: 2%
- Russian Federation: 1%
- Other Europe: 3%

**Malware Traffic Destination**
- United States: 50%
- Germany: 8%
- Netherlands: 6%
- China: 8%
- France: 17%
- United Kingdom: 6%
- Russian Federation: 6%
- Other Europe: 5%

**AV Future Challenge: PUA**

July 2016
Where AVs fit in

Protection against malware and infections

Providing additional Security features like reputation of files and webpages, secure banking, file vaults, parental control etc.

Provide a hassle free usage of device by not slowing the computer and being mostly invisible

Protect Privacy

... And provide protection against disruptive software
## PUA DETECTION

### Windows vs. Android

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows</th>
<th>Android</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUA detection choice during Setup</td>
<td>03/35</td>
<td>1/22</td>
</tr>
<tr>
<td>In-App Option change PUA Settings (activated by default)</td>
<td>17/35</td>
<td>05/22</td>
</tr>
<tr>
<td>In-App Option change PUA Settings (deactivated by default)</td>
<td>04/35</td>
<td>04/22</td>
</tr>
<tr>
<td>PUA detection present but no option to change settings</td>
<td>08/35</td>
<td>10/22</td>
</tr>
<tr>
<td>No Option to detect PUA, low detection rate</td>
<td>03/35</td>
<td>02/22</td>
</tr>
<tr>
<td>Malware Average detection rate</td>
<td>98,18%</td>
<td>99,63%</td>
</tr>
<tr>
<td>PUA Average detection rate</td>
<td>87,31%</td>
<td>93,98%</td>
</tr>
</tbody>
</table>
PUA vs. Malware detection rate per product (on-demand)

PUA detection rate: \( \bar{x} = 87.31\% \)
Malware detection rate: \( \bar{x} = 98.18\% \)

August 2016
PUA vs. Malware detection rate per product

PUA detection rate

Malware detection rate

PUA $\bar{x} = 93.98\%$

Malware $\bar{x} = 99.63\%$

July 2016
CONCLUSION

PUA is a problem as prevalent as Malware, maybe more…

Users are more likely to ‘see’ PUA instead of Malware.

More private data saved on digital/mobile devices.

Data is targeted by everyone, governments, vendors, distributors.

Users expect AV to protect or at least warn them.

Even more focus must be put on protecting data on devices.
@avtestorg (English) & @avtestde (German)

Follow us on facebook.com/avtestorg

Latest test results on https://www.av-test.org

Thank you for your attention!