An Analysis of Pay-per-install Economics Using Entity Graphs

Platon Kotzias, Juan Caballero

Workshop on the Economics of Information Security (WEIS) 2017
Potential Unwanted Programs (PUP)
Open File - Security Warning

Do you want to run this file?

Name: .8956-2f90-4abd-8bbb-b76d685979ce TX PR.exe
Publisher: Microsoft Corporation
Type: Application
From: C:\Users\office_user\Desktop\Setup.X86.en-US...

Run | Cancel

Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. [What's the risk?]

Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: C:\Users\office_user\Desktop\trid.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Users\office_user\Desktop\trid.exe

Run | Cancel

Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. [How can I decide what software to run?]
PUP prevalence

- 5% of unique IPs accessing Google have injected advertisements
  

- Google’s Safe Browsing generates 60M PUP warnings - 3 times that of malware
  

- 54% of 3.9M hosts examined had PUP installed
  

- Increased of PUP samples over time on a dataset of 26.8M malware samples
  
PUP distribution by commercial Pay-Per-Install (PPI) services

- **Advertisers**
- **PPI Service**
- **Affiliate Publishers**
- **Target Hosts**

Diagram:
- Adware
- VLC

Diagram details:
- Advertisers pay PPI service.
- PPI service distributes adware.
- Affiliates receive payments from PPI service.
- Target hosts receive adware.
- Publishers may receive payments.

Image:
- VLC installation prompt.
PUP distribution through download portals

- Hundreds of download portals
- Some in the top Alexa (at least 3 in Top 200)
PUP ecosystem

PUP publishers → PPI services → Download portals
PUP ecosystem

PUP publishers

PPI services

Download portals

PUP Operation
PUP attribution

- National laws may require companies to publish their data
- In Spain
  - Register into national register
  - Publish yearly financial statements
  - External audits for large companies

- National register reports:
  - Creation/dissolution of companies
  - Changes in administrators
  - Capital increases and reductions
  - Corporate split-ups, absorptions
Are these 3 case studies representative?

- All run their own PPI service

- Their samples observed in the wild

- Involved in various ways in PUP ecosystem
Are these 3 case studies representative?

Disclaimer

Our ethics advisory board has mandated that we anonymize the operations to prevent putting the spotlight on the people running these three operations, and to avoid time-consuming legal actions. We anonymize the names of operations, as well as the names of the companies and persons involved in each operation.
Contributions

- How profitable are commercial PPI services and the operations behind them?
- What are the revenue sources?
- How has the PPI business evolved?

- How many companies are involved in an operation?
- How many persons run an operation?
- How long have they been in operation?

- Propose PUP attribution using entity graphs
- Generate entity graphs for 3 Spanish operations
**Approach Overview**

- **Get companies & persons**
  - Using libreBORME

- **Build and trim graph**
  - Using herdProtect

- **Collect financial data**

- **Automated**

**Malsign PUP dataset**

- **PUP companies**

**Business reports**
- 59 business reports
- Financial data: revenue, net income

**Audit reports**
- 5 reports for 3 companies (2013-15)
- Sources of income, reasons behind big revenue changes, etc.
Road Map

- Intro
- PUP Attribution
- PUP Economics
PUP Entity graphs – OP1

Persons:
- Person name

Companies:
- Fiscal ID
- Company name(s)
- Company Type
- Economic activity
- Employees
- Telephone number
- Address
- City/Country
- Creation date
- Dissolution date
- Capital
- Earnings
- Revenue
- EBITDA
- Certificates
- Revoked

Edges:
- Active roles
  (e.g., administrator, treasurer)
- Passive roles
PUP Entity graphs – OP2
PUP Entity graphs – OP3
How many companies are involved and for how long?

- 15 – 32 companies
- 7 – 13 years

Most PUP Companies:
- Share addresses
- Have no employees
- Have no revenue
- Have no Web presence
- Created in batches

Shell companies are used to obtain code signing certificates

On average 4 certificates per company
How many persons run an operation?

A small number of people manages the large number of companies

OP1 includes 21 companies, all managed by a single person
Road Map

Intro

PUP Attribution

PUP Economics
How profitable are PUP operations?

<table>
<thead>
<tr>
<th>Operation</th>
<th>Period</th>
<th>Revenue (€)</th>
<th>Income (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OP1</td>
<td>2012-15</td>
<td>81.8M</td>
<td>8.2M</td>
</tr>
<tr>
<td>OP2</td>
<td>2013-15</td>
<td>92.2M</td>
<td>11.0M</td>
</tr>
<tr>
<td>OP3</td>
<td>2008-14</td>
<td>28.5M</td>
<td>3.8M</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2008-15</strong></td>
<td><strong>202.5M</strong></td>
<td><strong>23.0M</strong></td>
</tr>
</tbody>
</table>

- Prior work has measured the economics of various malicious activities

Our work measures both revenue and net income
What are the revenue sources?

- PPI service is the main revenue source
- 87% of company revenue comes from outside EU
- Video streaming service launched in 2015

<table>
<thead>
<tr>
<th>Source</th>
<th>Total (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPI</td>
<td>83.4M (90%)</td>
</tr>
<tr>
<td>Streaming Portal</td>
<td>3.1M (3.4%)</td>
</tr>
<tr>
<td>Mobile Advertisement</td>
<td>2.0M (2.0%)</td>
</tr>
<tr>
<td>Download Portals</td>
<td>1.4M (1.5%)</td>
</tr>
<tr>
<td>Rogueware</td>
<td>45.1K (&lt;1%)</td>
</tr>
</tbody>
</table>

**OP2 Revenue Split**

- PPI service is an important revenue source
- 72% of PPI company revenue comes from outside EU

**OP3 Revenue Split**

<table>
<thead>
<tr>
<th>Source</th>
<th>Total (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPI</td>
<td>7.9M (28%)</td>
</tr>
<tr>
<td>Advertising</td>
<td>0.7M (2.5%)</td>
</tr>
<tr>
<td>Software</td>
<td>44K (&lt;1%)</td>
</tr>
</tbody>
</table>

PPI services are the largest source of revenue
PPI evolution over time – High expenses low profit margins

- Most expenses declared under generic categories (e.g. Supplies, Other costs)
- Personnel expenses from 6% - 17% of total revenue
- Observe transactions among companies of the same operation
PPI evolution over time – Revenue drop

OP1

OP3

OP2

Revenue
Net Income
PUP defenses have significantly impacted the PPI market

PUP samples over time

27.7M malware hashes
Summary

- How profitable are commercial PPI services and the operations behind them?
  - 202.5M €
    Total Revenue
  - 23M €
    Total Income

- What are the revenue sources?
  - PPI services are the largest source of revenue

- How has the PPI business evolved?
  - High expenses and low profit margins
  - Large drop on 2015

- How many companies are involved in an operation?
  - 15 – 32 comp./op.
  - Most are shell companies

- How many persons run an operation?
  - 1 – 6 persons/op.

- How long have they been in operation?
  - 7 – 13 years/op.
An Analysis of Pay-per-install Economics Using Entity Graphs

Platon Kotzias, Juan Caballero

Workshop on the Economics of Information Security (WEIS) 2017