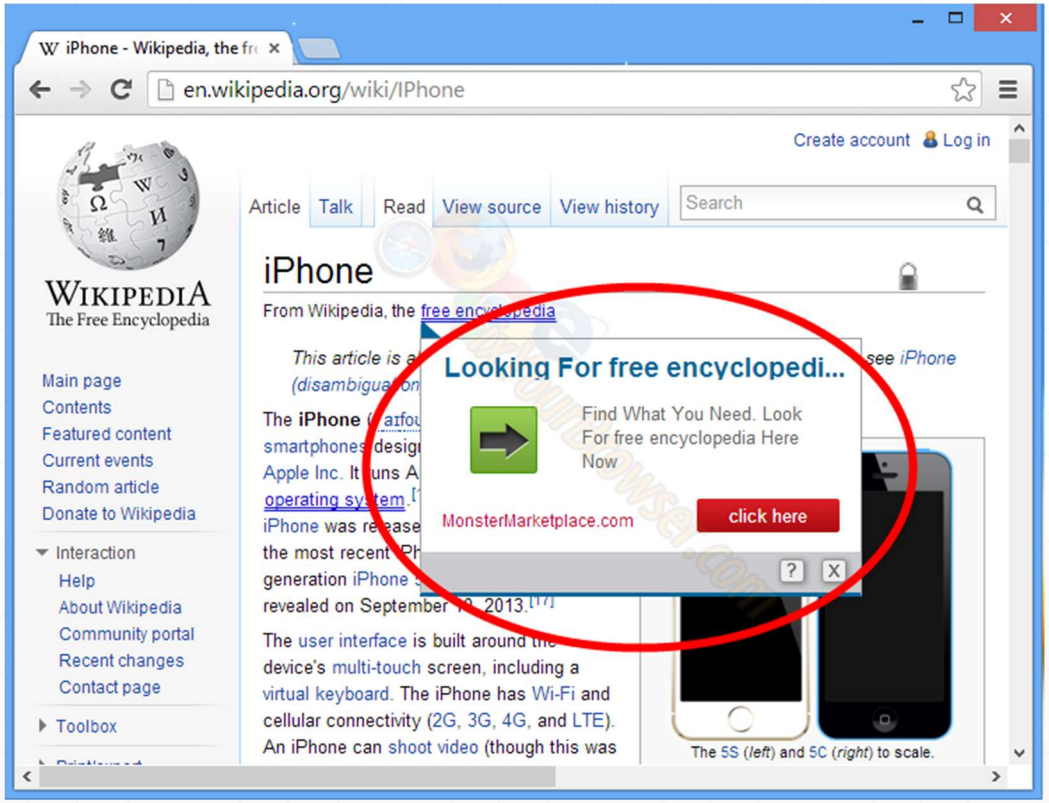
An Analysis of Pay-per-install Economics Using Entity Graphs

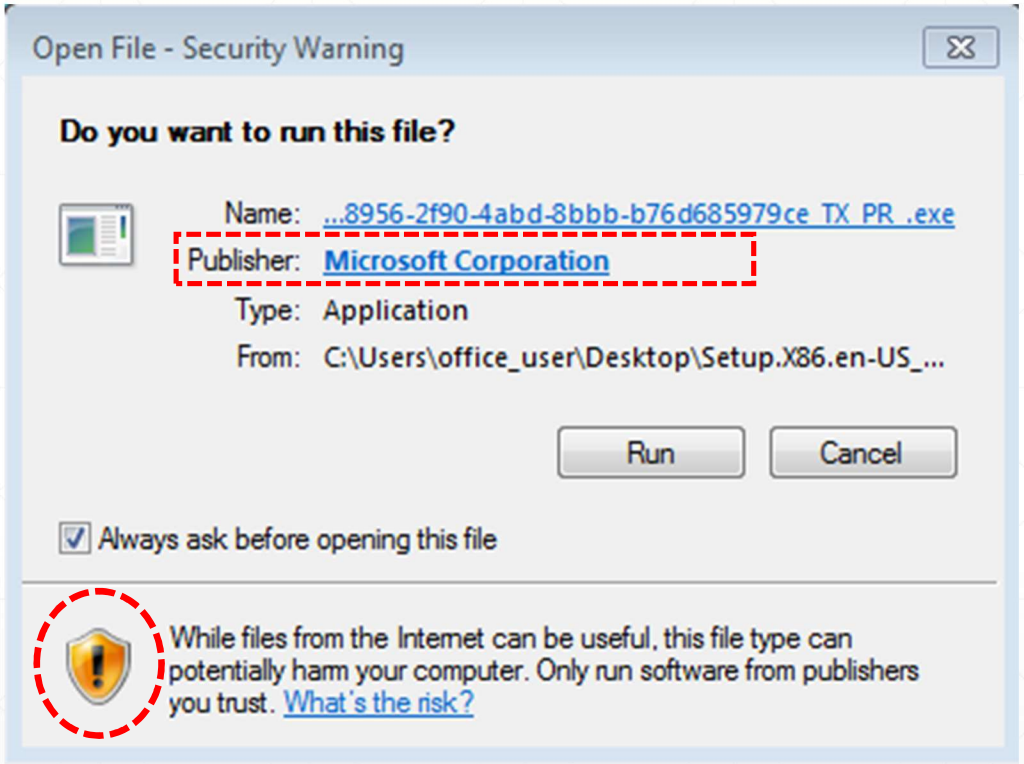
Platon Kotzias, Juan Caballero

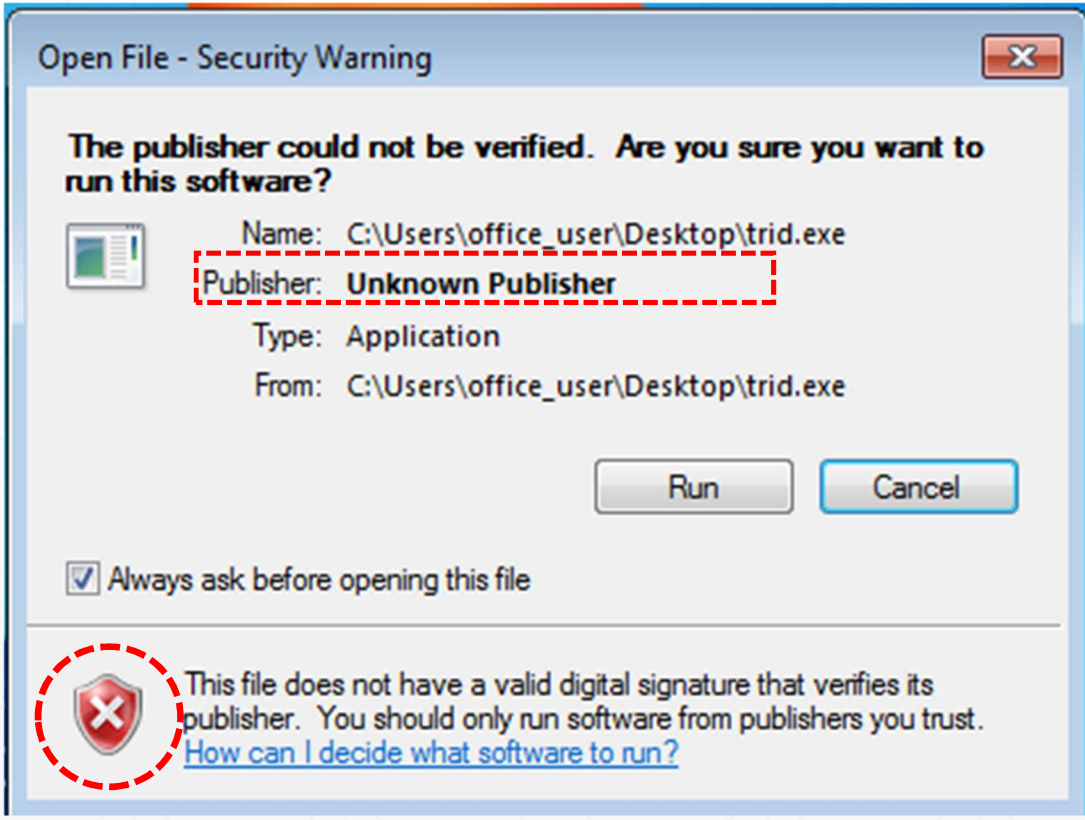
institute imdea software

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

Thomas et al. Ad injection at scale: Assessing deceptive advertisement modification. In Proceedings of the IEEE Symposium on Security and Privacy, 2015.

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

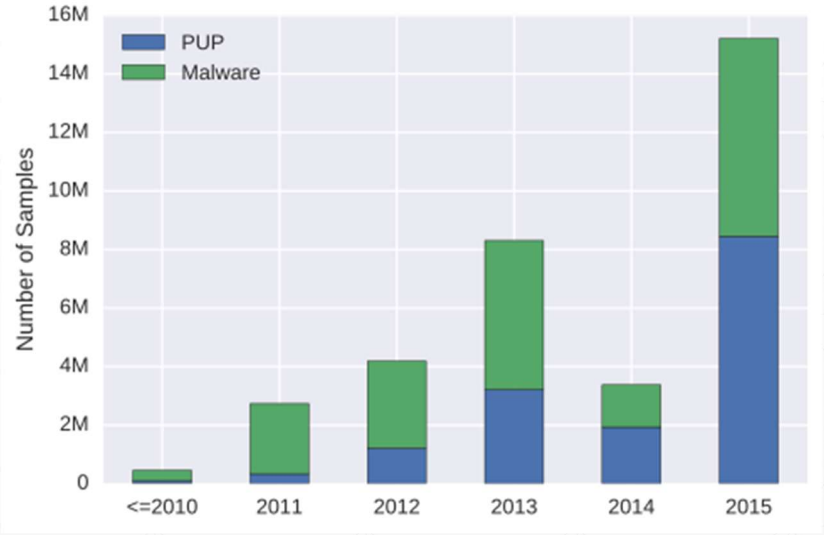
Thomas et al. Investigating Commercial Pay-Per-Install and the Distribution of Unwanted Software. In USENIX Security Symposium, 2016.

- 54% of 3.9M hosts examined had PUP installed

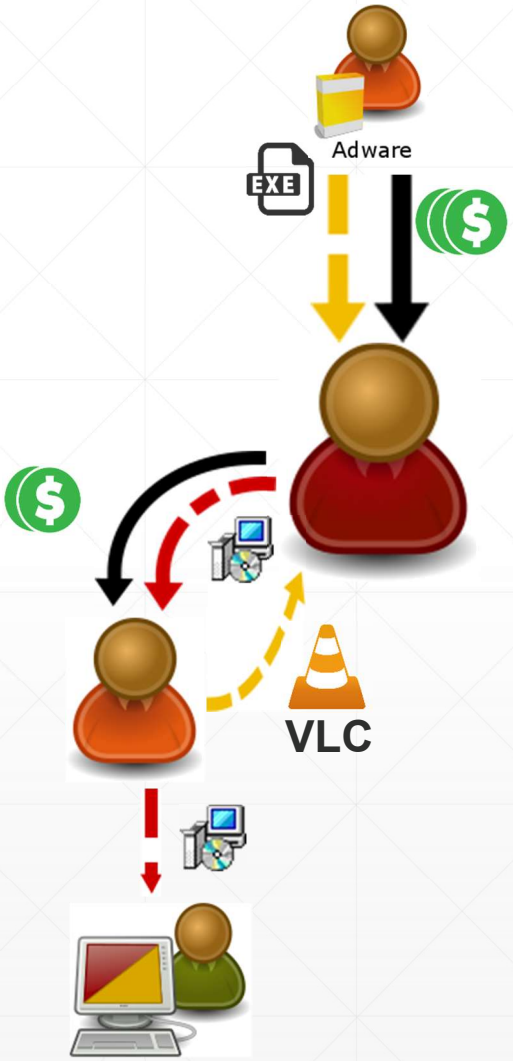
Kotzias et al. Measuring PUP prevalence and PUP Distribution through Pay-Per-Install Services. In USENIX Security Symposium, 2016.

- Increased of PUP samples over time on a dataset of 26.8M malware samples

Lever et al. A Lustrum of Malware Network Communication: Evolution and Insights. In Proceedings of the IEEE Symposium on Security and Privacy, 2017.



PUP distribution by commercial Pay-Per-Install (PPI) services



Advertisers

PPI Service

Affiliate Publishers

Target Hosts

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

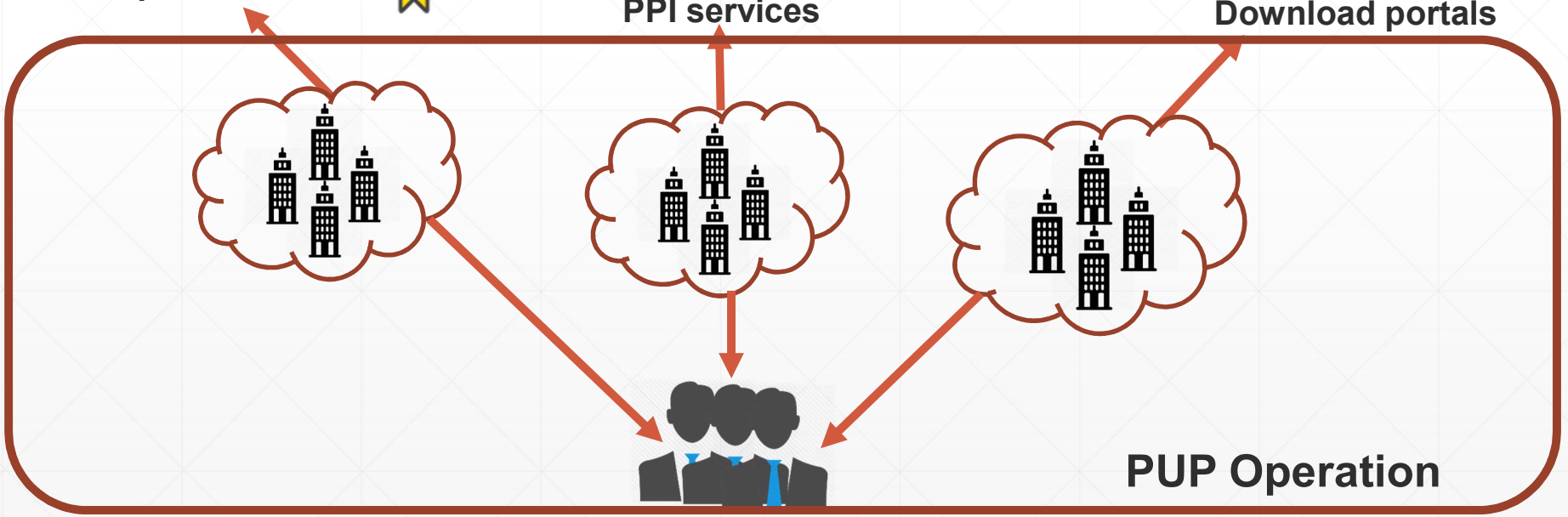
Download portals

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?

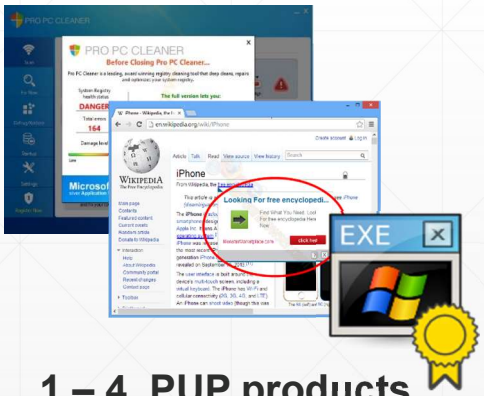
- All run their own PPI service

Millions of users

- Their samples observed in the wild

- Involved in various ways in PUP ecosystem

1 – 16 Download portals



1 – 4 PUP products

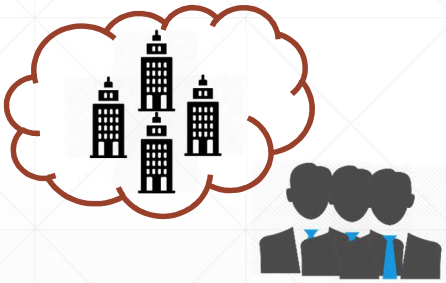
Are these 3 case studies representative?

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?*



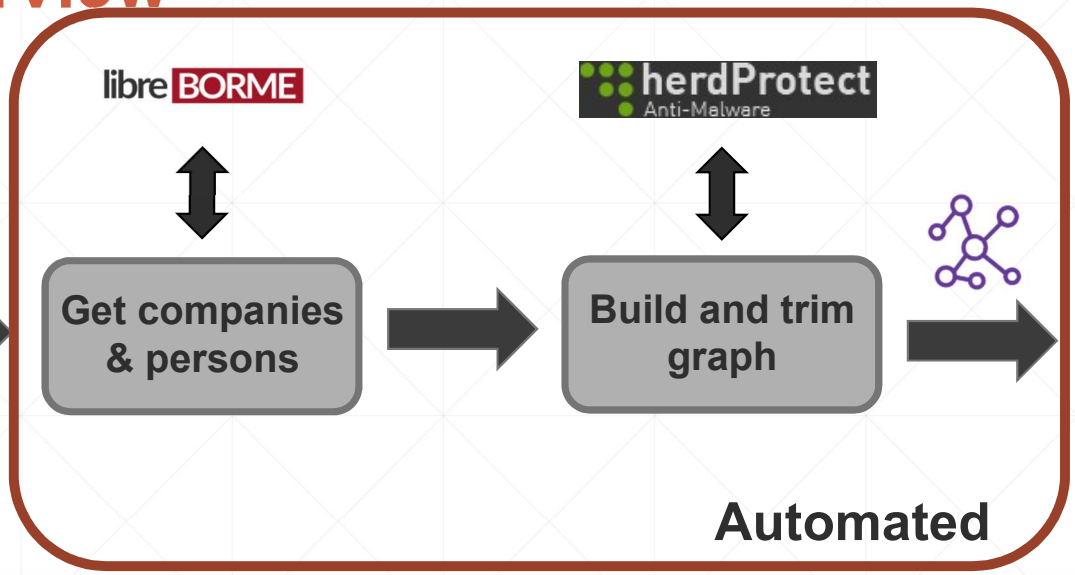
- *How many companies are involved in an operation?*
- *How many persons run an operation?*
- *How long have they been in operation?*

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

Approach Overview

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

PUP Entity graphs – OP1

Persons:

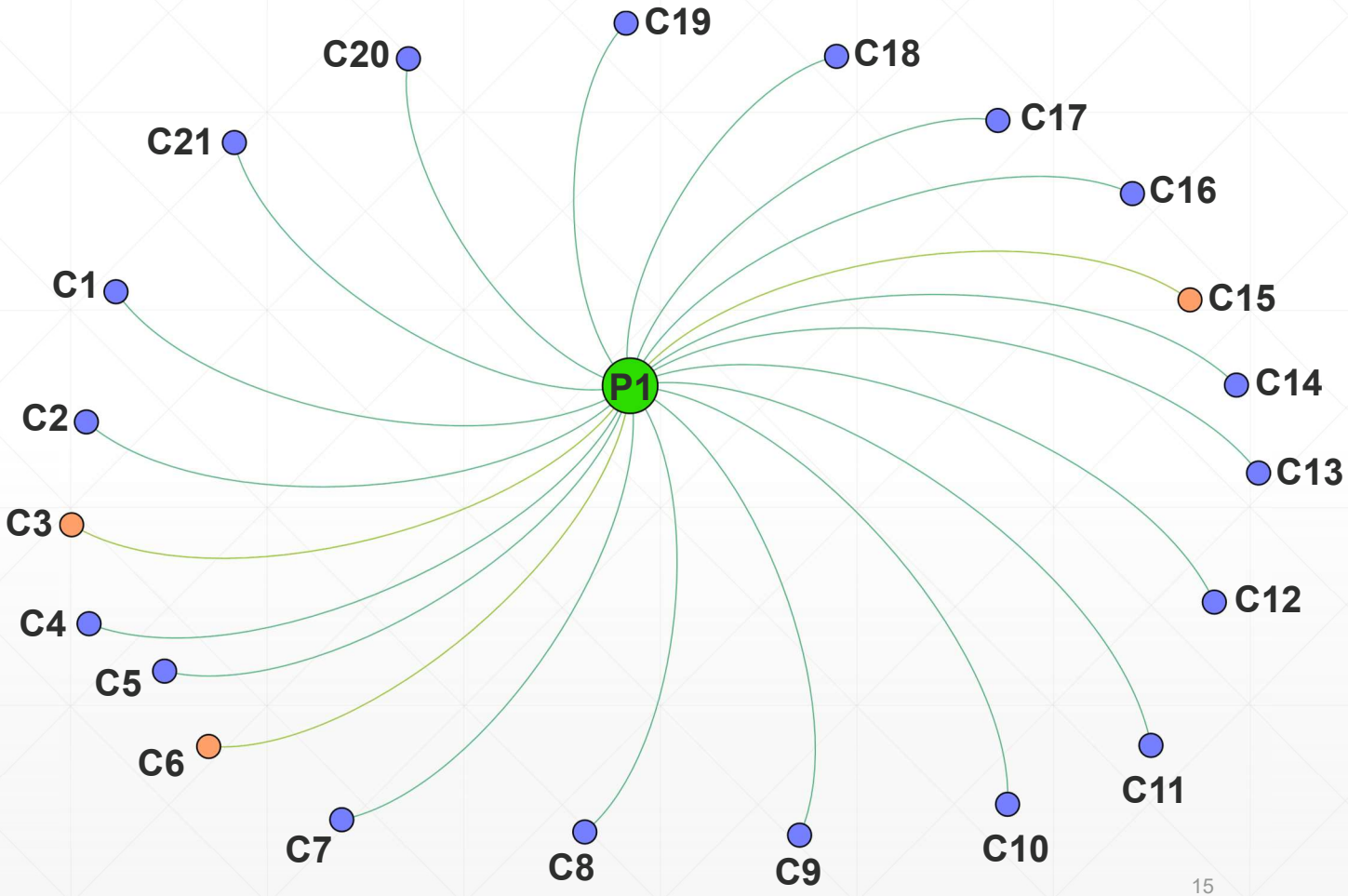
- Person name

Companies:

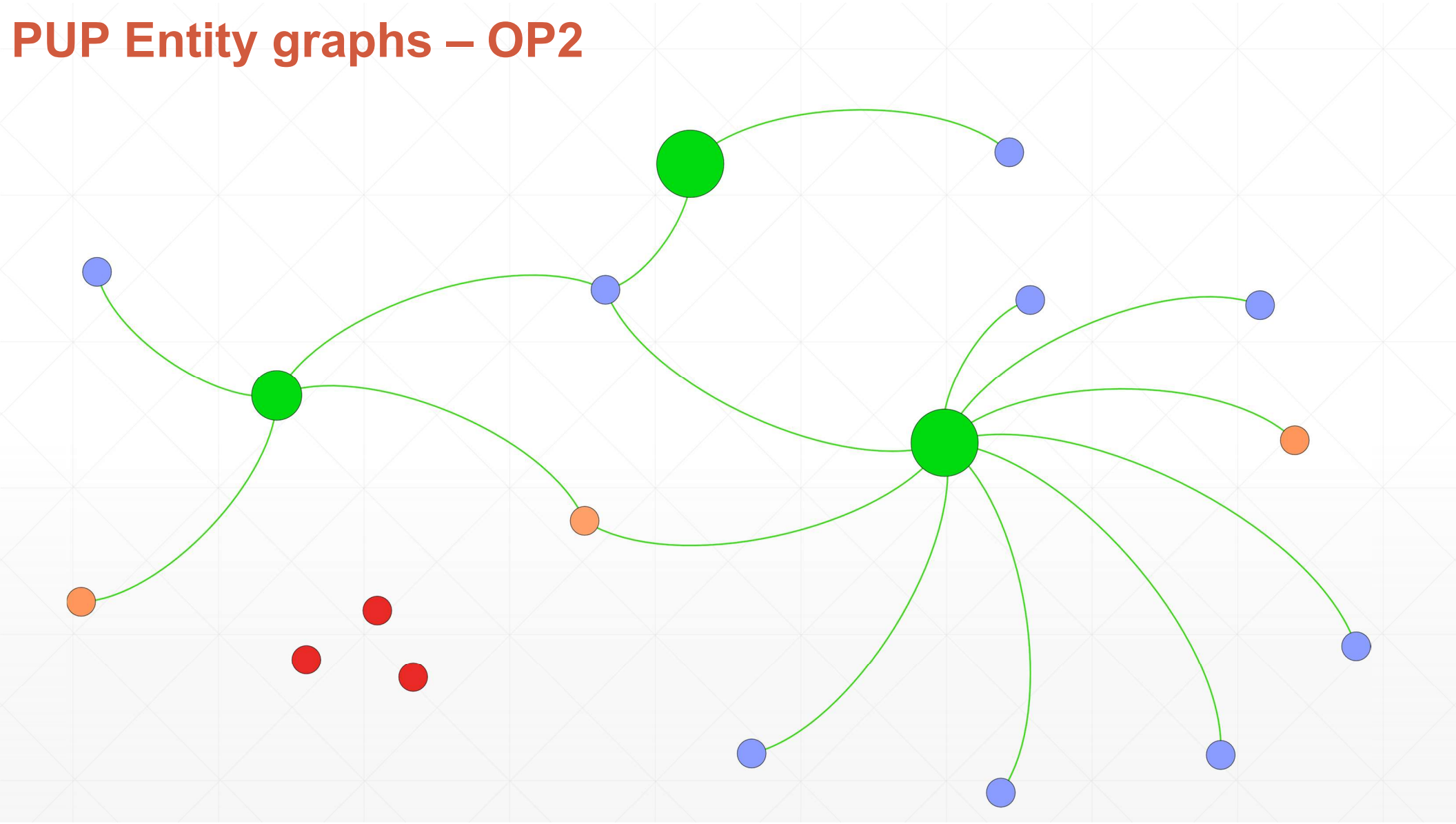
- Fiscal ID
- Company name(s)
- Company Type
- Economic activity
- Employees
- Telephone number
- Address
- City/Country
- Creation date
- Dissolution date
- Capital
- Earnings
- Revenue
- EBITDA
- Certificates
- Revoked

Edges:

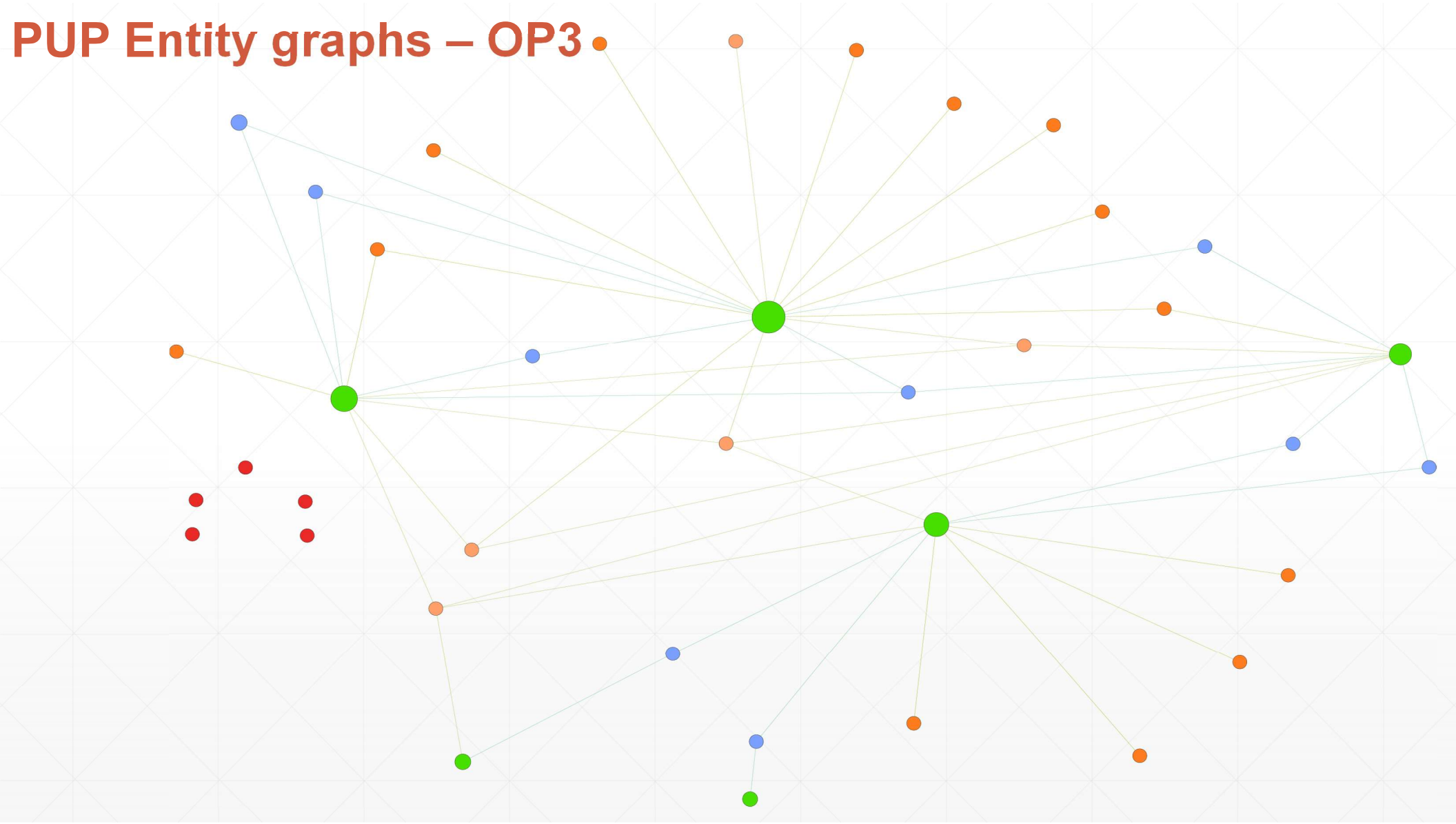
- Active roles
  (e.g., administrator, treasurer)
- Passive roles



PUP Entity graphs – OP2



PUP Entity graphs – OP3



How many companies are involved and for how long?

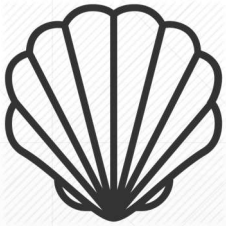
15 – 32 companies

7 – 13 years

- As early as 2003
- PPI services appear in 2010-2011

Most PUP Companies:

- Share addresses
- Have no employees
- Have no revenue
- Have no Web presence
- Created in batches



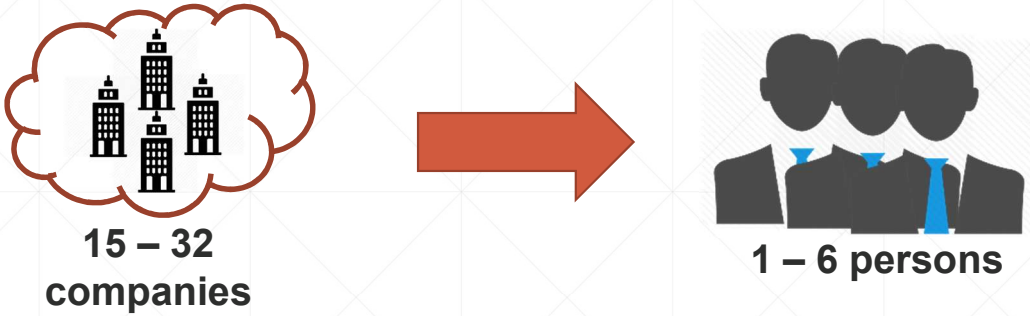
Shell Companies

Shell companies are used to obtain code signing certificates

On average 4 certificates per company

48-85 Certificates

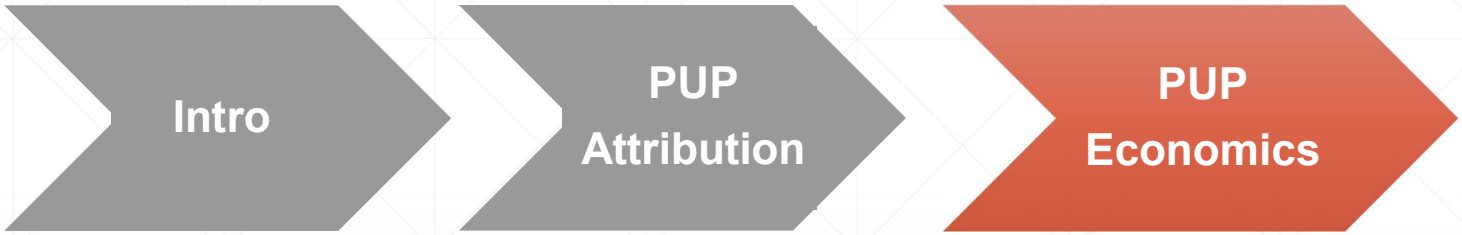
How many persons run an operation?



A small number of people manages the large number of companies

OP1 includes 21 companies, all managed by a single person

Road Map



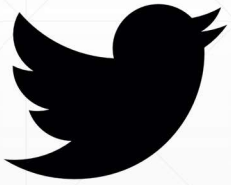
How profitable are PUP operations?

Operation	Period	Revenue (€)	Income (€)
OP1	2012-15	81.8M	8.2M
OP2	2013-15	92.2M	11.0M
OP3	2008-14	28.5M	3.8M
Total	**2008-15**	**202.5M**	**23.0M**

- Prior work has measured the economics of various malicious activities

Pharmaceutical affiliate programs

Fake AVs



Fraudulent Twitter accounts

ZeroAccess Botnet

CryptoLocker Ransomware

Our work measures both revenue and net income

What are the revenue sources?

Audit reports

Source	Total (€)
PPI	83.4M (90%)
Streaming Portal	3.1M (3.4%)
Mobile Advertisement	2.0M (2.0%)
Download Portals	1.4M (1.5%)
Rogueware	45.1K (<1%)

OP2 Revenue Split

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

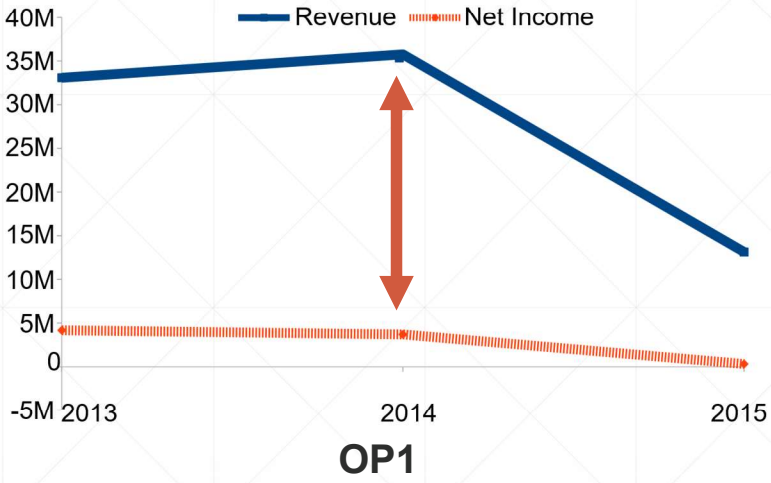
- PPI service is the main revenue source
- 87% of company revenue comes from outside EU
- Video streaming service launched in 2015

OP3 Revenue Split

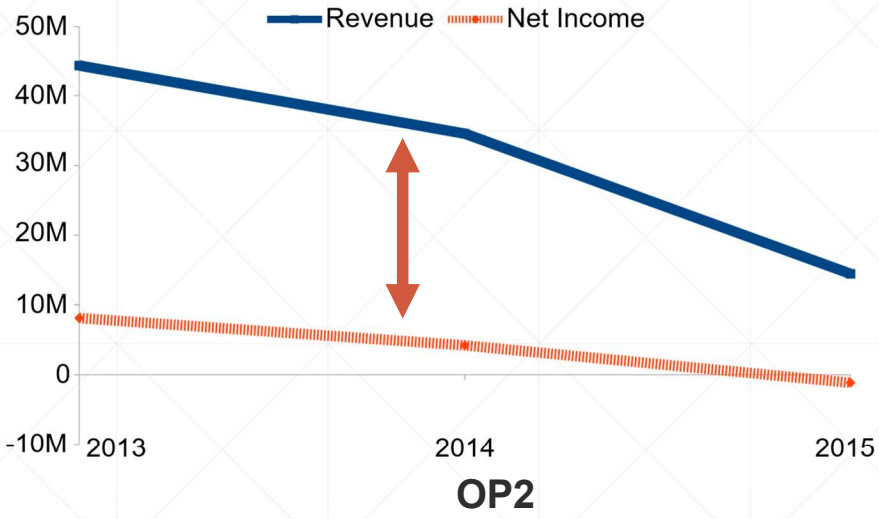
Source	Total (€)
PPI	7.9M (28%)
Advertising	0.7M (2.5%)
Software	44K (<1%)

PPI services are the largest source of revenue

PPI evolution over time – High expenses low profit margins



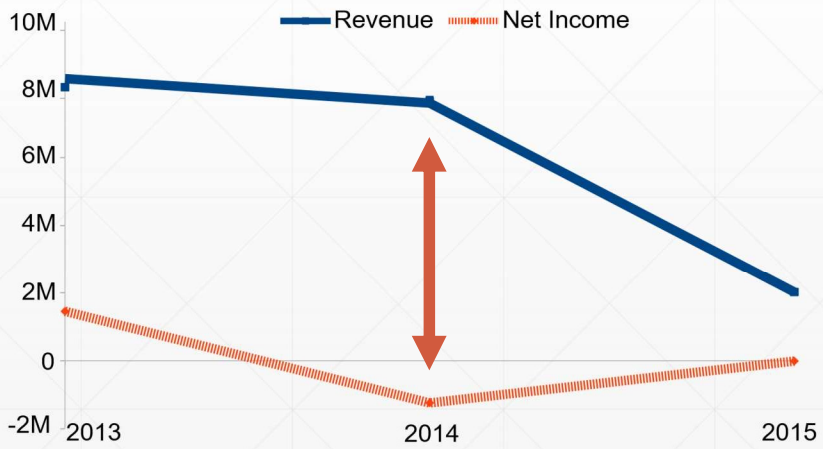
OP1



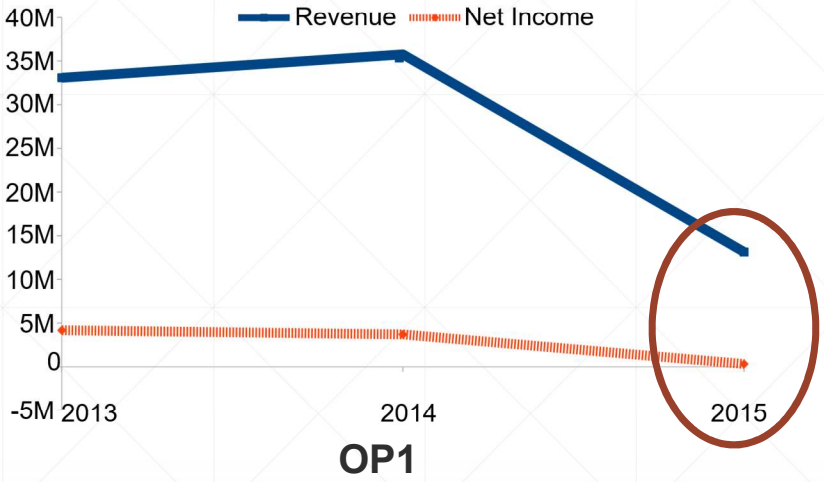
OP2

OP3

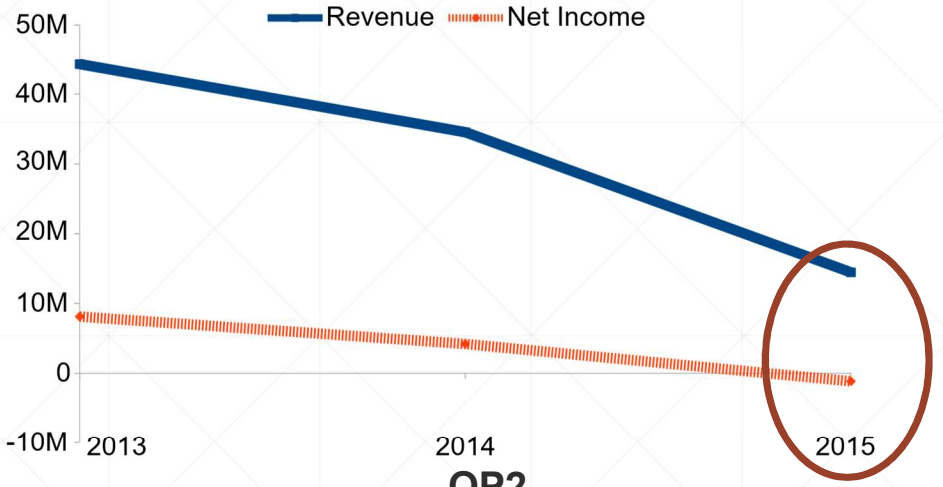
- Most expenses declared under generic categories (e.g. Supplies, Other costs)
- Personnel expenses from 6% - 17% of total revenue
- Observe transactions among companies of the same operation



PPI evolution over time – Revenue drop

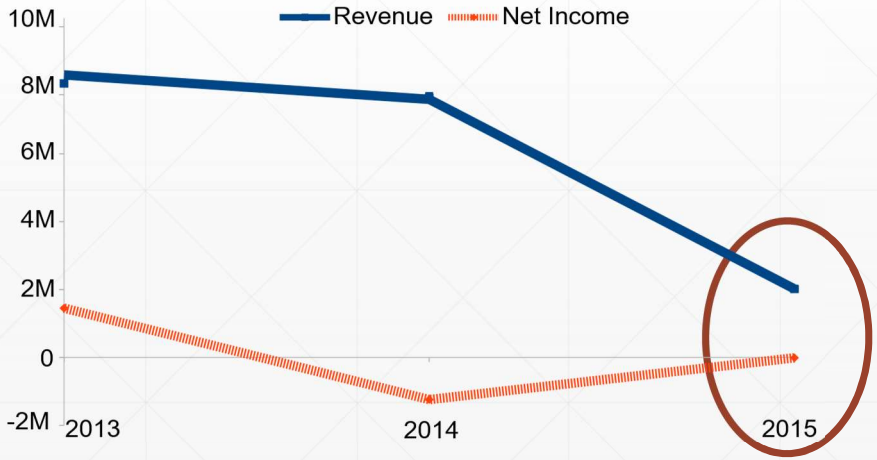


OP1



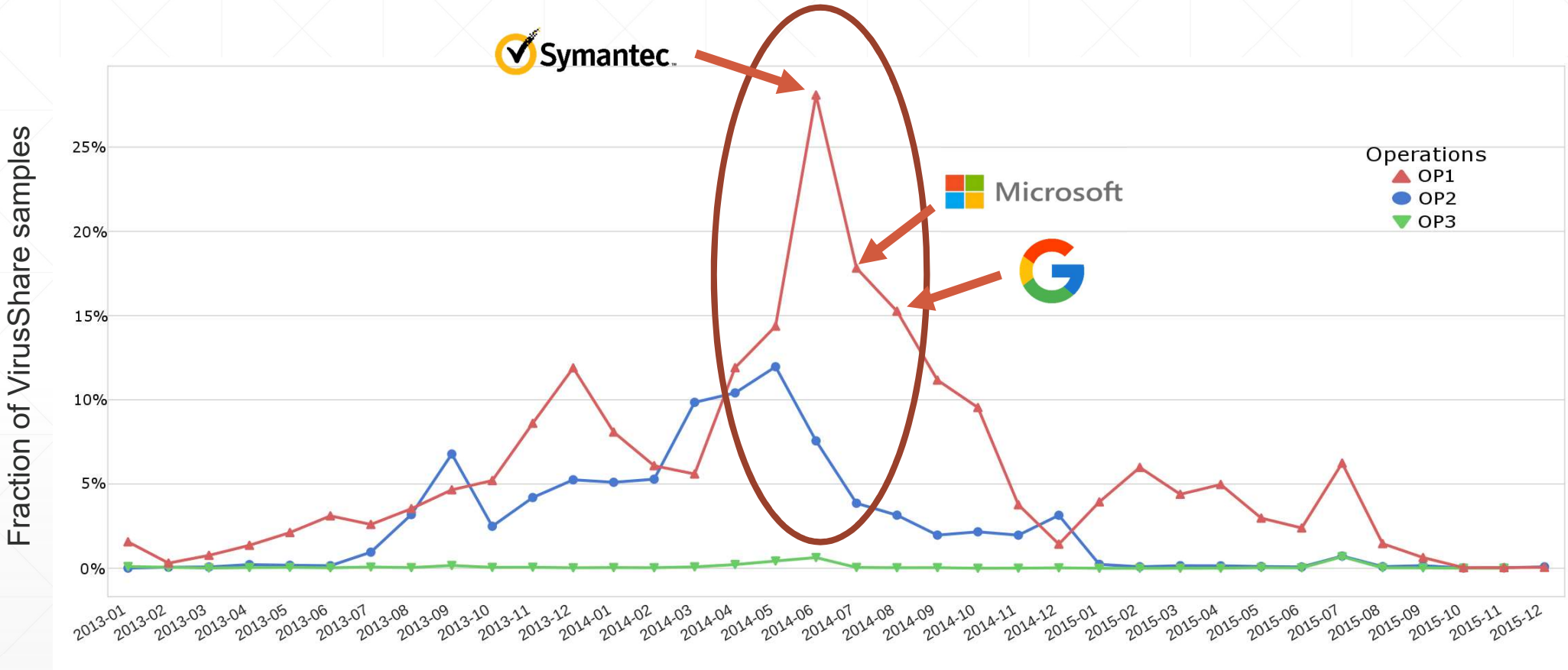
OP2

OP3



PUP samples over time

27.7M malware hashes



PUP defenses have significantly impacted the PPI market

Summary

❖ *How profitable are commercial PPI services and the operations behind them?*

202.5M € Total Revenue

23M € Total Income

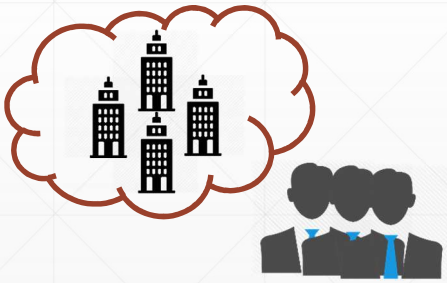
❖ *What are the revenue sources?*

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

institute imdea software

Workshop on the Economics of Information Security (WEIS) 2017