CERT La Poste

Group Infosec Observatory

40th TF-CSIRT meeting
London – 2013.09.27

frederic.lebastard@laposte.fr
Introduction – CERT La Poste

Detailed missions
- SISO
- Watch
- Compliance

Short focus on « Malware Trap »
Le Groupe La Poste

1st
French retail network
L’Enseigne
17000 points of sale
Including MVNO : La Poste Mobile (700k+ subscribers)

2nd
European postal operator (gross sales)
Mail : Le Courrier

2nd
European parcel & express operator (gross sales)
5 billion parcels delivered each year (20% of european market shares)

3rd
French retail bank
La Banque Postale
10 millions of active clients

- Annual sales 2012 : 21,6 billion €
- France’s leading employer with 270 700 professionnals
- 17 082 public outlets all over France
- 250 subsidiaries in 40 countries over 4 continents
2 main missions:

- Surveillance
- Anticipation

Observatory is a transversal team, on duty for Business Units:

- IR consistency through the Group
- Global (theoretical ...) visibility of the threat level for the Group
Built in 2008, after a massive worm infection

- 10-people team, based in Nantes, FR
  - 3 dedicated to security watch
  - 2 dedicated to anti-phishing, anti-fraud
  - 1 pentester, compliance issues
  - 2 main incidents responders
  - 2 SIEM / log management experts

- Backoffice for a 24/7 supervision service

- We’re hiring!
CERT La Poste perspectives

- Listed in TF-CSIRT/ Trusted introducer since march 2012
- Active member of french national CSIRT group (interCERT-FR)
- Committed to become a TI accredited team in the next 6 months
  - Share knowledge
  - Share tools
  - Enhance fight capabilities against frauds & criminal activities
Summary

Introduction – CERT La Poste

Detailed missions
- SISO
- Watch
- Compliance

Short focus on « Malware Trap »
Internal security supervision service : SISO

- 24/7/365 Security supervision of infrastructures connected to the outer world (internet, partners, subsidiaries)

- Based on log management / SIEM. Correlation rules focused on compliance (Law, Rules of Procedures, Internal infosec policy)

- Handling daily 300 million messages (logs) correlated to 150 security alerts, leading to a pair of qualified incidents

Now looking forward to :

- Complete infrastructures supervision with business supervision (ie. Fraud detection)
- Get our hands on real world « APT »
- Share our 5 years experience with the community!
Watch: infosec, phishing, DNS

- Infosec watch
  - Threats watch, Vulnerabilities watch

- Active fight against phishing & brands spoofing. Built on inhouse-crafted tools based on OSINT:
  - Parking sites / fraudulent domain names,
  - Banking phishing - labanquepostale.fr
  - Webmail phishing - laposte.net
  - Funds transfer phishing - Mandat-Cash Urgent
Mapping of Group’s websites on the Internet

- Recurring inventory of exposed websites
- Automated & recurring vulnerability audits
- Vulnerability notifications to BU
- Scheduled pentests
Summary

Introduction – CERT La Poste

Detailed missions
  SISO
  Watch
  Compliance

Short focus on « Malware Trap »
Observations:
- Limited AV efficiency (50% ?)
- Unreliable patch management
- Limited access to 150,000 endpoints
- Theory of evolution: BYOD, tethering, …

Raw material available:
- Internet proxies logs
- Internal DNS resolvers logs
- External trusted repositories (RBL, ZeuS Tracker, AV partnerships, …)
Malware Trap

Basic steps:
- Mix available materials
- Build an interactive trap
- Consolidate results

First results (2011):
- 12 malicious domains targeted (around Rimecud / Mariposa)
- Roughly 3000 endpoints compromised
- A few months later, <50 compromised endpoints
- Win!
Malware Trap

The hard points
- Automated semantical analysis of FQDNs does not work well
- Automated updates of internal DNS zones scares everyone
- Endpoints cleaning is a neverending story

What worked?
- Integration of the results in the industrial workflow of the SIEM
- Progressive feeding with public RBL
- … hopefully soon, automated netflow analysis
Thanks for your attention ! (*)