APT in Finland

Juhani Eronen and
Sauli Pahlman of
CERT-FI

Background

- APT: A synonym for a targeted attack
  - a class of cyberattacks and malware destined for only a few (or even one) specific organization or branch of industry/government
- Indicator: Any factor identifying a target. Most commonly an IP address or md5 but can include:
  - From/to/subject/message id of email messages
  - Filenames, XOR keys, Mutexes, other malware details
  - Names, emails and other data in domain registrations
  - …

Some history

- Nearly a decade of APT in Finland
- 2004: First campaigns
- 2007: Targeted attacks using common document formats
  - » Trends: .doc, .ppt, .xls -> .pdf
  - » First cases analyzed, mostly attempting to gain a bridgehead position
- Indicator data mostly from trusted third parties

Some history

- Ongoing semi-active information gathering on Finnish targets: contact details, key persons, active projects, software used by the target organization
- 2011: HAVARO monitoring for the relevant network identities
- 2012: Browser exploit kits, watering hole attacks and spear phishing sites, more similar to normal exploitation

Advanced?

- Phishing an internal site, i.e. corporate email
  - » http://intranet/ anyone?
- Fake corporate websites□
- Targeting gmail accounts of employees, or using deceptive gmail accounts
- Working on tools on the fly
  - » 2 hours from compilation to use in a campaign
  - » The most important thing about the attack tools is to avoid AV detection, possible bugs can be corrected later

Persistent?

- The data might be gone in minutes
  - » The attackers may not leave the network but their main objective is fulfilled
  - » SIEM or log analysis does not usually help you here
- On the other hand persistence in the key when the attacker's objective is to maintain control of, e.g., an industrial control system (or to continue receiving the confidential documents)

Threat?

- Most attacks are not APT, but are a threat
- How great risk does APT cause on the Finnish infrastructure?
  - » So far we've seen only data theft or attacks breaching data confidentiality
  - » Perhaps greater damage via compromising part of the critical infrastructure, but requires an attacker with a motivation to cause havoc
  - » Problem: We only talk what we have seen, not what we do not know about

APT in Finland(?)

- CERT-FI mainly shares targeted spear phishing emails and network identities (DNS names, IP addresses etc.) involved in APT
  - » We seldom hear anything back
  - » Hardly any first hand APT discoveries – typically we hear about these from fellow CERTs
  - » We seldom get to investigate any successful cases
    - But when we do, the things we see make us believe there has to be more victims than the ones we are aware of
  - » Who has the best visibility for APT in .fi? CERT-FI? SUPO? F-Secure? Forensics consultancies? Security companies? "Unspecified foreign entities"?

APT in Finland

- In many of the successful cases we've seen the victim has been rather easy targets
  - Known good practices still work against them
  - Assume that the attacker gets to deliver his malware inside your network and design your defense keeping that in mind
  - The attacker will most probably need to own just one or two computers inside then network, and he will use legitimate remote administration tools from there
  - Most target networks have been compromised for months

Lessons learned

- The attacker has a strong incentive to cover his trails -> memory forensics emphasized
- Total infrastructure compromise is a good starting assumption
  - » Two-way strategy: investigate the event to gain things to look for in our infrastructure
- From anti-analysis to anti-forensics

What more could we do?

- We are mostly reactive and lacking active and proactive measures to detect and counter
- We should improve in sharing the information regarding successful attacks
  - » Valuable information for others to defend against APT

Viestintävirasto

Finnish Communications Regulatory Authority

www.ficora.fi