ON THE STRONGPITY WATERING HOLE ATTACKS

Kurt Baumgartner

Principal Security Researcher

@k_sec

GREAT

2016

Encryption Tech, Types of Tools

- TrueCrypt
- WinRAR
- IM Clients
- SSH Clients
- File transfer
  - Filezilla
  - Winscp
  - RDP clients

Watering Holes - previous watering holes

- Crouching Yeti – ICS related poisoned installers
- Fortune website
- Darkhotel - P2P distribution

Watering Holes – StrongPity Tactics

- Rarlab spoof
- WinRAR distributor link + redirect
- WinRAR distributor direct hosting
- TrueCrypt spoof

Watering Hole - StrongPity GeoTargeting

- Italy
- Belgium
- Turkey
- Algeria
- Morocco

StrongPity Malware – Poisoned Installers, Other

- Droppers
- Digital Certificates
- Clever crypto
- Spyware

source: klonblog.com

Strong Encryption Technology Types of Tools

Drive and file content / data at rest encryption

- TrueCrypt
- WinRAR

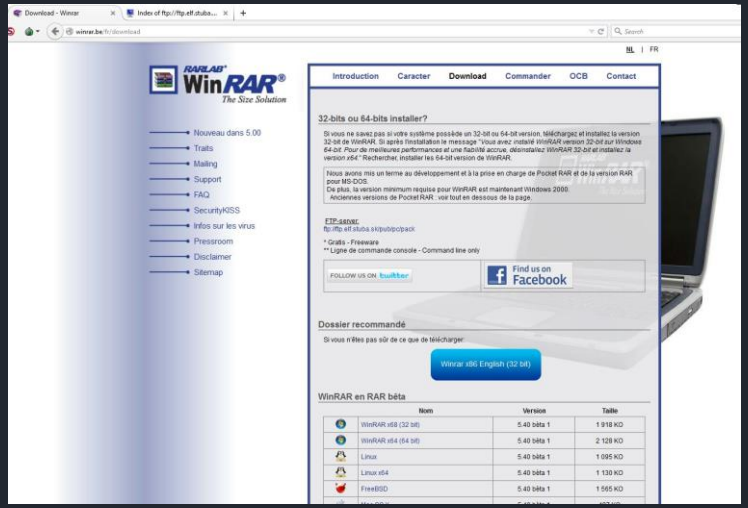
Session/data in motion encryption

- IM Clients
- SSH Clients
- File transfer
  - Filezilla
  - Winscp
  - RDP clients

source: mideastfood.about.com

Distribution methods
Strong and weak

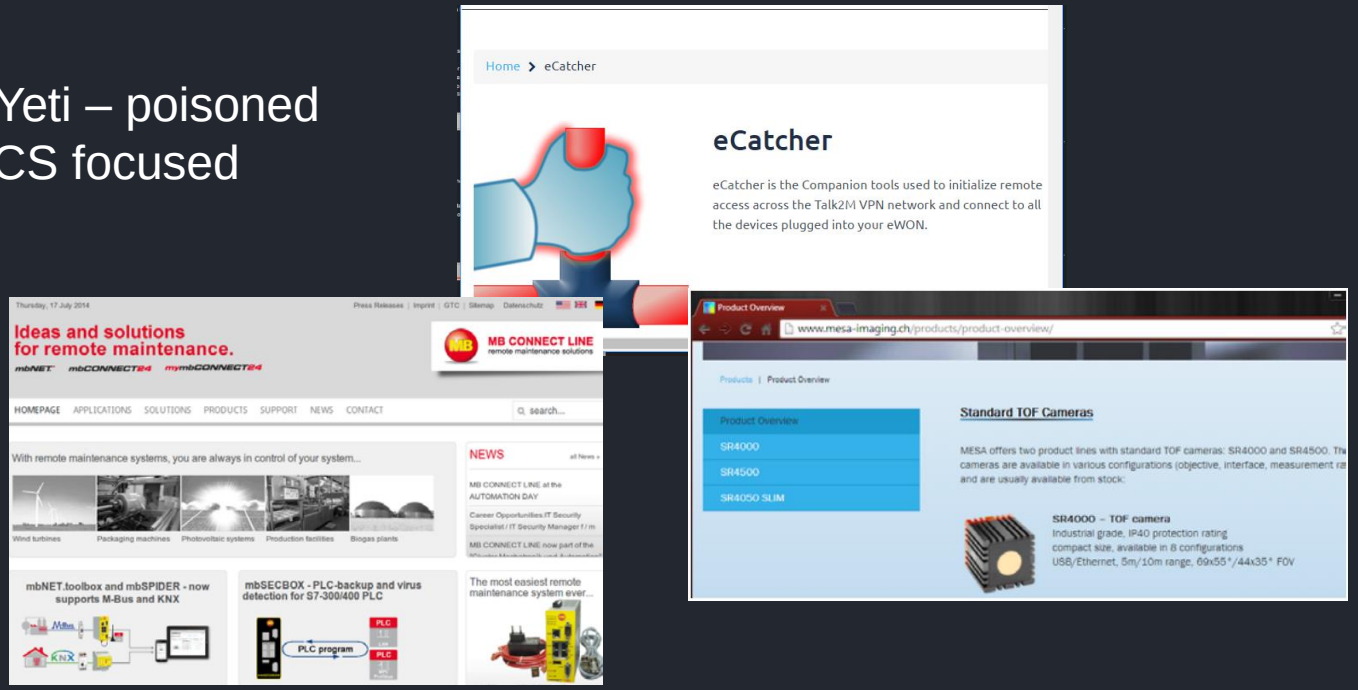
- Sourceforge (+mirrors)
- Resellers and distributors



- Microsoft Store and Microsoft Update
- Homebrew websites
- Maybe over http
- Signed (SHA1?) or unsigned, PGP

Watering Holes - previous activity

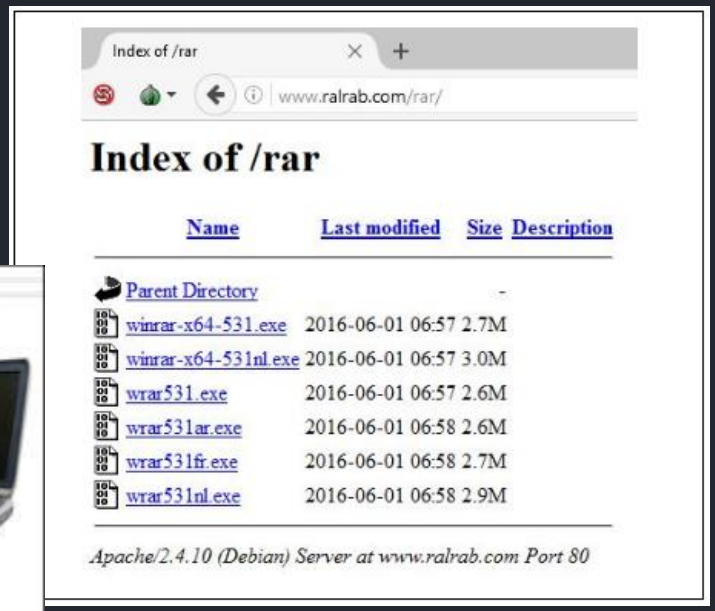
- Crouching Yeti – poisoned installers, ICS focused



https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf

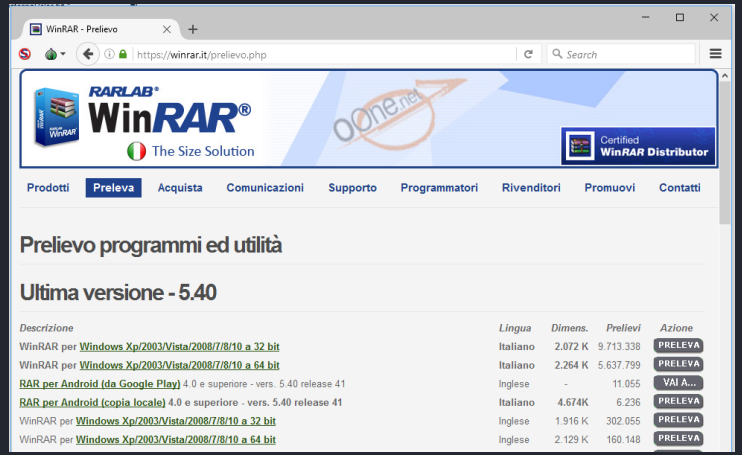
Watering Holes – StrongPity Tactics

- Ralrab.com – spoof of Rarlab.com
- Redirect from redistributor site



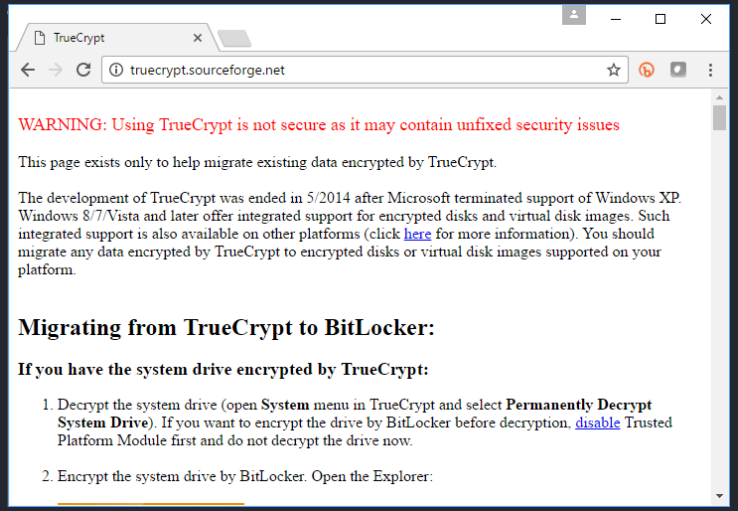
Watering Holes – hosted directly by redistributor (compromised, other?)

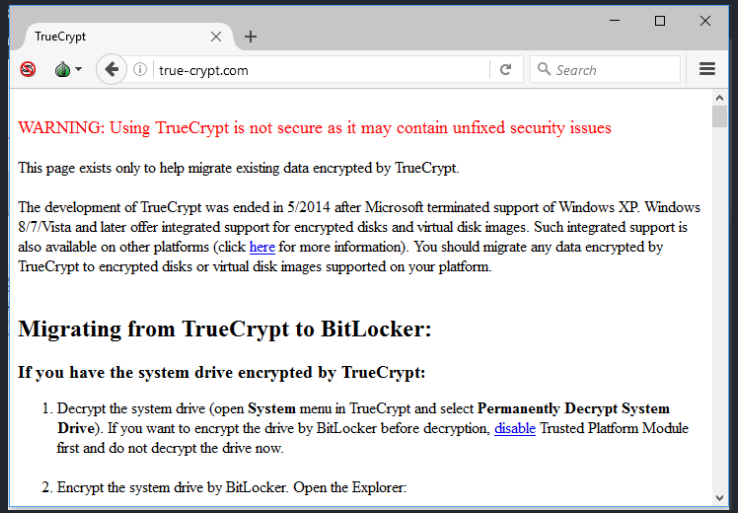
hxxps://www.winrar[.]it/prelievo/WinRAR-x64-531it.exe
hxxps://www.winrar[.]it/prelievo/WRar531it.exe



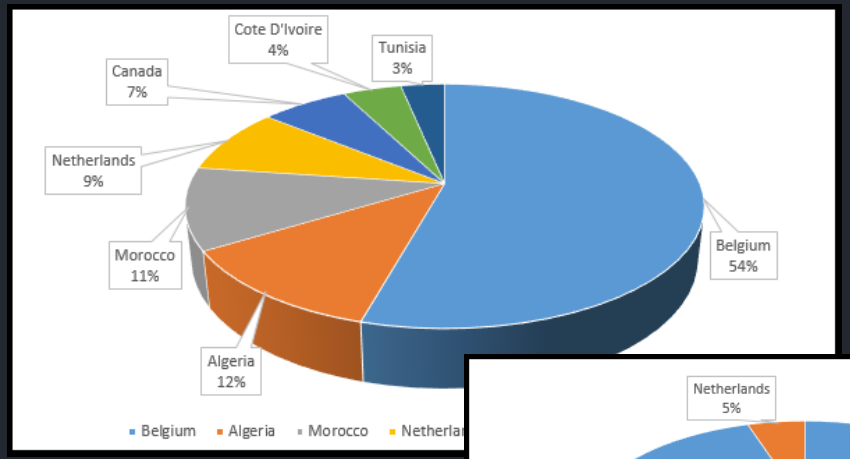
Watering Holes – TrueCrypt Spoofing

hxxp://www.true-crypt[.]com/download/TrueCrypt-Setup-7.1a.exe
hxxp://true-crypt[.]com/files/TrueCrypt-7.2.exe

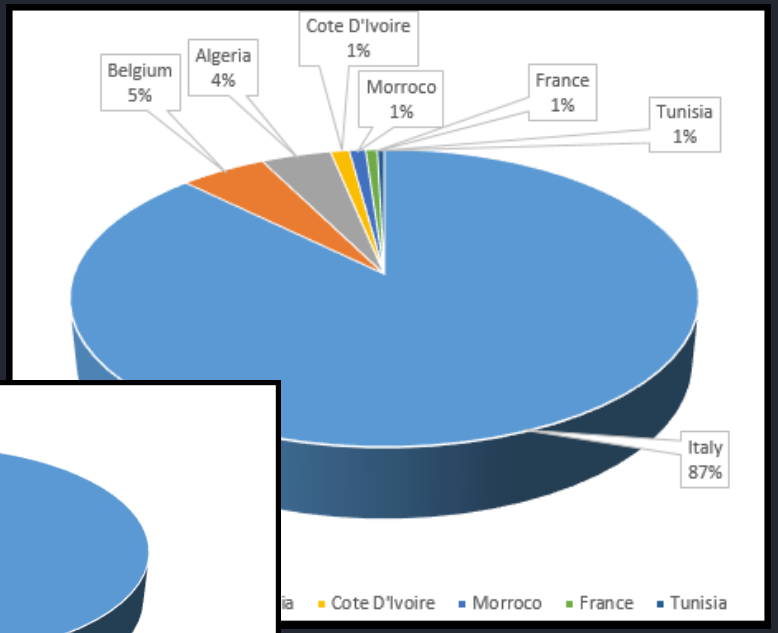




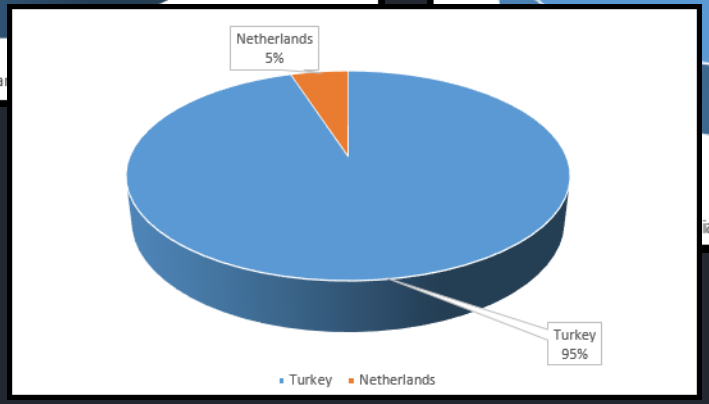
Watering Holes – Geolocation Targeting



winrar.be/ralrab.com detections



winrar.it detections



true-crypt.com detections

Watering Holes – Targeted Encryption

- putty.exe (a windows SSH client)
- filezilla.exe (supports ftps uploads)
- winscp.exe (a windows secure copy application)
- mstsc.exe (Windows Remote Desktop client)
- mRemoteNG.exe (supports SSH, RDP, and other encrypted protocols)
- IM Clients
    - keyloggers and additional data stealers

By Eaeeae - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=30396311

THANK YOU

@k_sec