

ON THE STRONGPITY WATERING HOLE ATTACKS

GREAT
2016

Kurt Baumgartner

Principal Security Researcher



@k_sec

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

Download:

WARNING: Using TrueCrypt is not secure

You should download TrueCrypt **only if you are migrating data encrypted by TrueCrypt.**

[TrueCrypt 7.2](#) [sig key](#)

If you use TrueCrypt on other platform than Windows, click [here](#).

Session/data in motion encryption

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

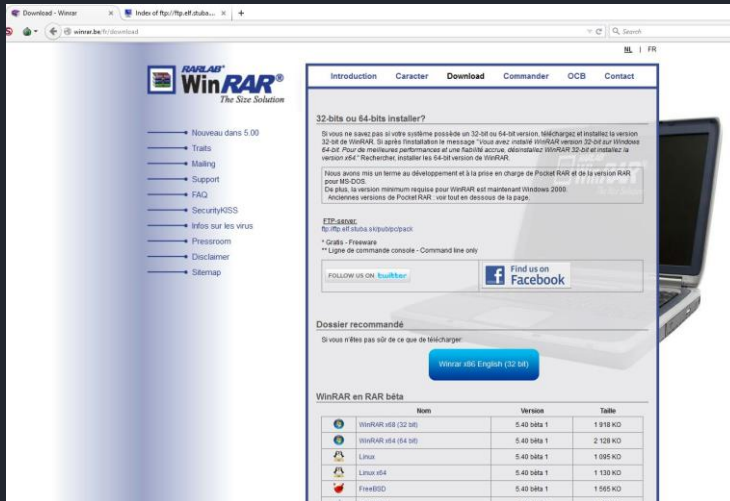


source: mideastfood.about.com

Distribution methods

Strong and weak

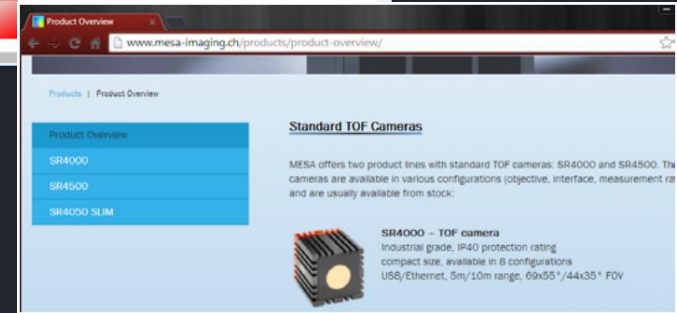
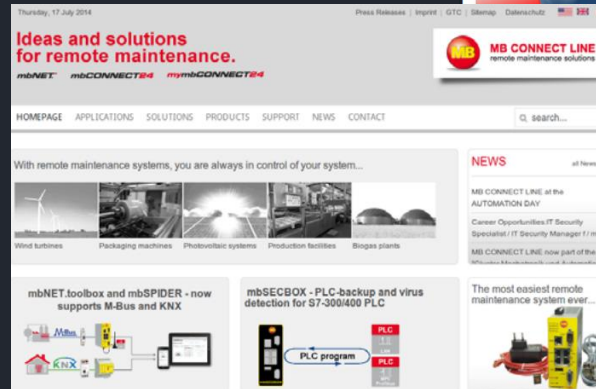
- Sourceforge (+mirrors)
- Resellers and distributors



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

Watering Holes - previous activity

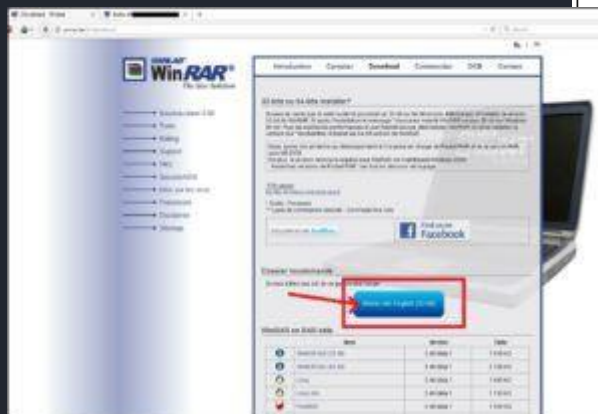
- Crouching Yeti – poisoned installers, ICS focused



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

Watering Holes – StrongPity Tactics

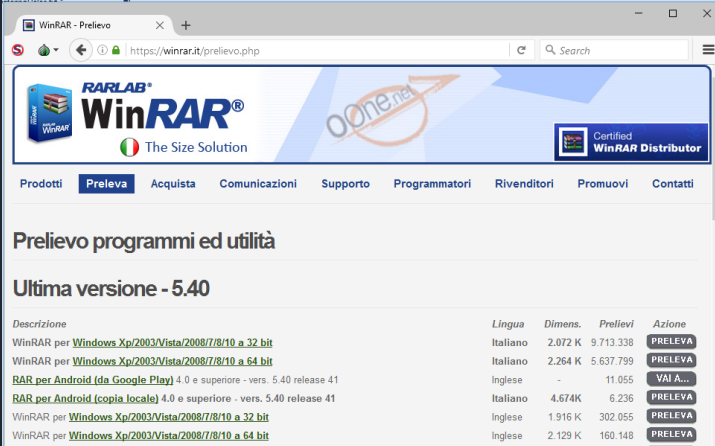
- Ralrab.com – spoof of Rarlab.com
- Redirect from redistributor site



A screenshot of a web browser window. The address bar shows 'www.ralrab.com/rar/'. The page title is 'Index of /rar'. Below the title is a table with columns for Name, Last modified, Size, and Description. The table lists several files, including 'winrar-x64-531.exe', 'winrar-x64-531nl.exe', 'wrar531.exe', 'wrar531ar.exe', 'wrar531fr.exe', and 'wrar531nl.exe'. Below the table, there is a link for 'Parent Directory' and a footer that reads 'Apache/2.4.10 (Debian) Server at www.ralrab.com Port 80'.

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

hxxps://www.winrar[.]it/prelievo/WinRAR-x64-531it.exe
hxxps://www.winrar[.]it/prelievo/WRAR531it.exe

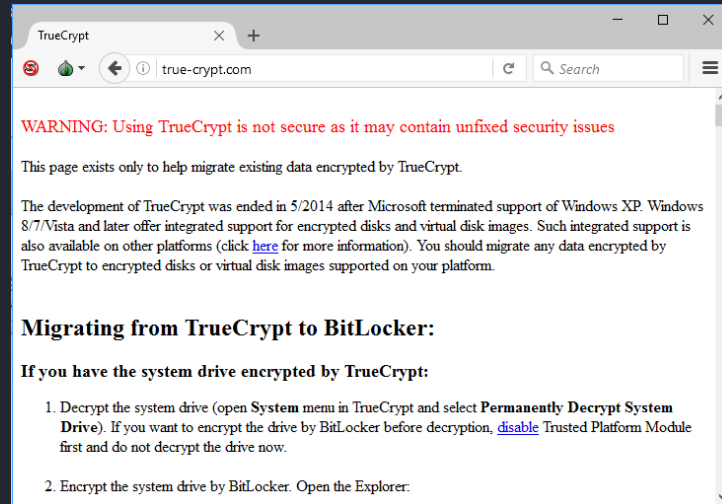
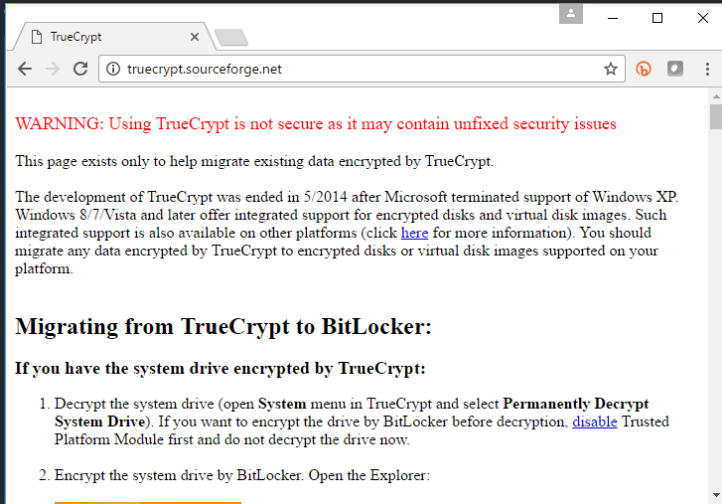


The screenshot shows a web browser window displaying the WinRAR website. The page features the WinRAR logo and navigation menu. Below the navigation menu, there is a section titled "Prelievo programmi ed utilità" with a sub-section "Ultima versione - 5.40". A table lists download links for different operating systems and languages, each with a "PRELEVA" button.

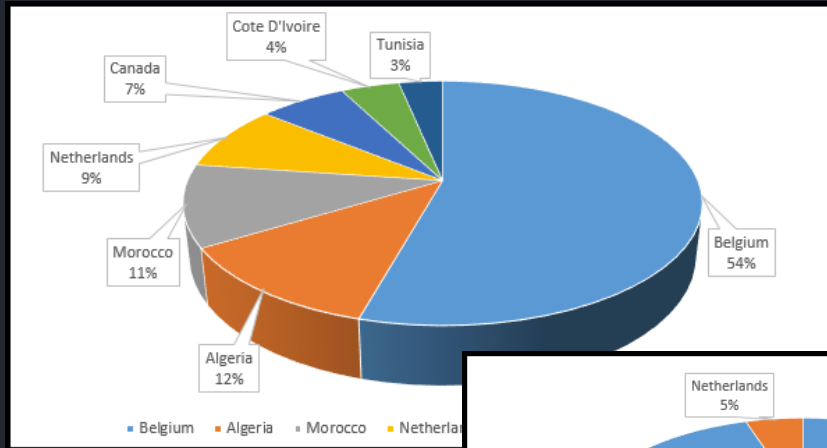
Descrizione	Lingua	Dimens.	Prelevi	Azione
WinRAR per Windows Xp/2003/Vista/2008/7/8/10 a 32 bit	Italiano	2.072 K	9.713.338	PRELEVA
WinRAR per Windows Xp/2003/Vista/2008/7/8/10 a 64 bit	Italiano	2.264 K	5.637.799	PRELEVA
RAR per Android (da Google Play) 4.0 e superiore - vers. 5.40 release 41	Inglese	-	11.055	VAI A...
RAR per Android (copia locale) 4.0 e superiore - vers. 5.40 release 41	Italiano	4.674K	6.236	PRELEVA
WinRAR per Windows Xp/2003/Vista/2008/7/8/10 a 32 bit	Inglese	1.916 K	302.055	PRELEVA
WinRAR per Windows Xp/2003/Vista/2008/7/8/10 a 64 bit	Inglese	2.129 K	160.148	PRELEVA

Watering Holes – TrueCrypt Spoofing

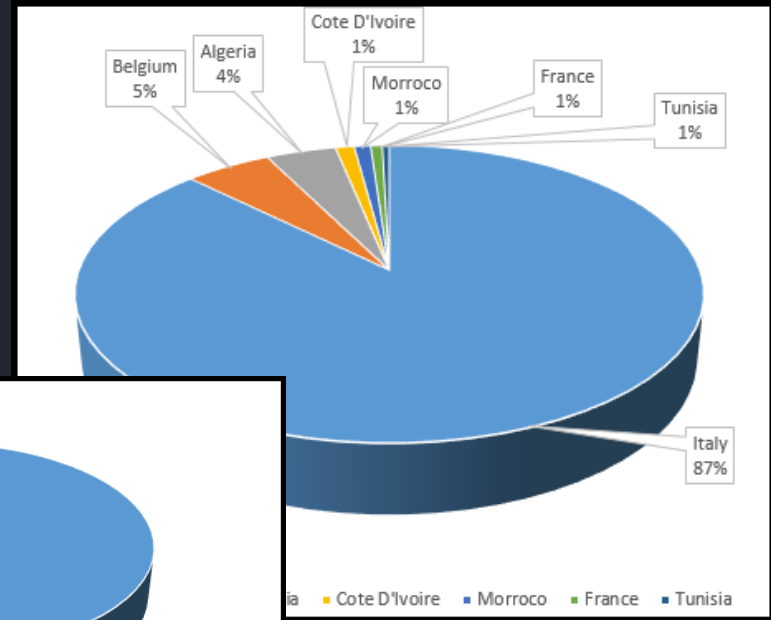
hxxp://www.true-crypt[.]com/download/TrueCrypt-Setup-7.1a.exe
hxxp://true-crypt[.]com/files/TrueCrypt-7.2.exe



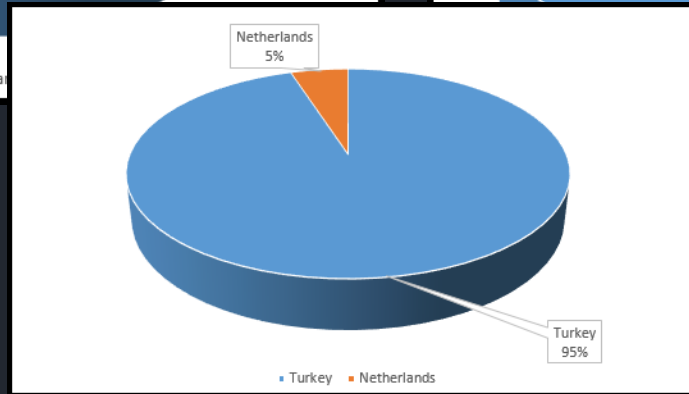
Watering Holes – Geolocation Targeting



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

THANK YOU



@k_sec