On the StrongPity Waterhole Attacks Targeting Italian and Belgian Encryption Users

By Kurt Baumgartner

Published: 2016-10-03 · Archived: 2026-04-05 16:43:11 UTC

The StrongPity APT is a technically capable group operating under the radar for several years. The group has quietly deployed zero-day in the past, effectively spearphished targets, and maintains a modular toolset. What is most interesting about this group's more recent activity however, is their focus on users of encryption tools, peaking this summer. In particular, the focus was on Italian and Belgian users, but the StrongPity watering holes affected systems in far more locations than just those two. Adding in their creative waterholing and poisoned installer tactics, we describe the StrongPity APT as not only determined and well-resourced, but fairly reckless and innovative as well.

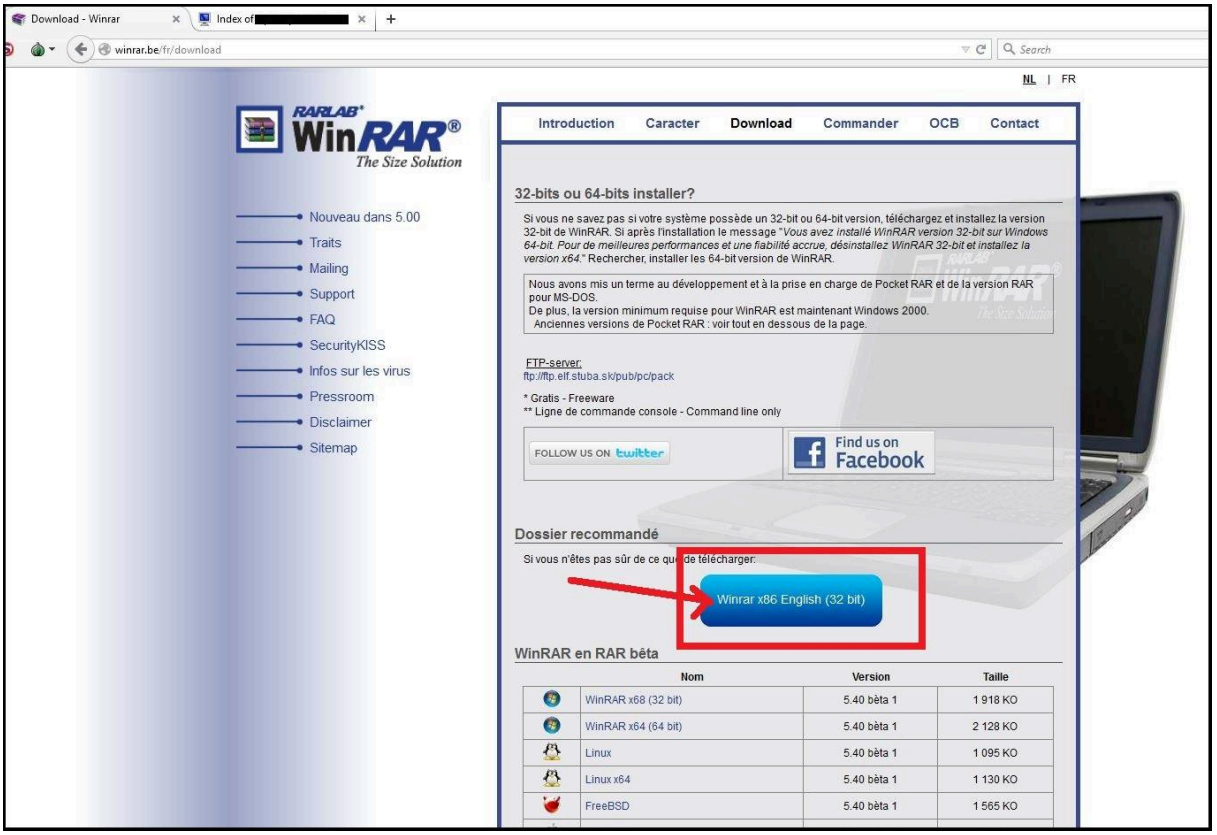
Clearly this APT is interested in encrypted data and communications. The tools targeted by this group enable practices for securing secrecy and integrity of data. For example, WinRAR packs and encrypts files with strong suites like AES-256, and TrueCrypt encrypts full hard drives all in one swoop. Both WinRAR and TrueCrypt help provide strong and reliable encryption. WinRAR enables a person to encrypt a file with AES-256 in CBC mode with a strong PBKDF2 HMAC-SHA256 based key. And, TrueCrypt provides an effective open-source full disk encryption solution for Windows, Apple, Linux, and Android systems. Using both of these tools together, a sort of one off, poor man's end-to-end encryption can be maintained for free by putting these two solutions together with free file sharing services.

Other software applications help to support encrypted sessions and communications. Well known applications supporting end-to-end encryption are used by hundreds of millions of folks, sometimes unknowingly, every day. IM clients like Microsoft's Skype implement 256-bit AES encrypted communications, while Putty, Winscp and Windows Remote Desktop help provide private communications and sessions with fully encrypted communications as well. Most of these communications across the wire are currently unbreakable when intercepted, at least, when the applications are configured properly.

Summer 2016 Watering Hole Resources and Trickery – WinRAR and TrueCrypt

This actor set up a particularly clever site to deliver trojanized WinRAR installers in the summer of 2016, appears to have compromised another, and this activity reminds us somewhat of the early 2014 Crouching Yeti activity. Much of the Crouching Yeti intrusions were enabled by trojanizing legitimate ICS-related IT software installers like SCADA environment vpn client installers and industrial camera software driver installers. Then, they would compromise the legitimate company software distribution sites and replace the legitimate installers with the Crouching Yeti trojanized versions. The tactics effectively compromised ICS and SCADA related facilities and networks around the world. Simply put, even when visiting a legitimate company distribution site, IT staff was downloading and installing ICS-focused malware. StrongPity's efforts did much the same.

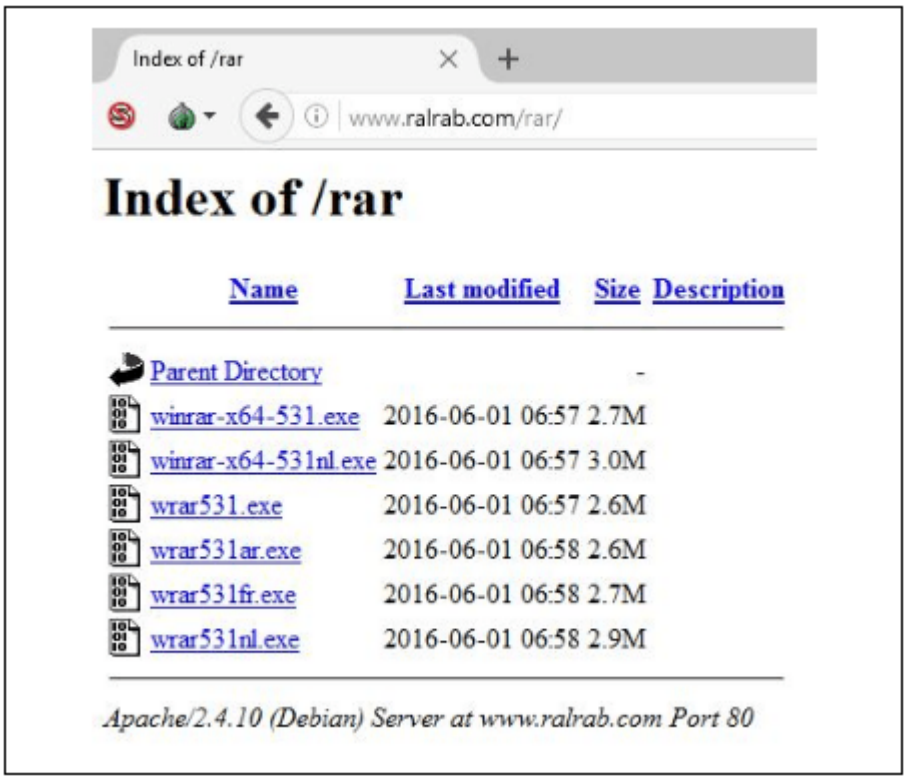
In the case of StrongPity, the attackers were not focused on ICS or SCADA. They set up a domain name (ralrab[.]com) mimicking the legitimate WinRAR distribution site (rarlab[.]com), and then placed links on a legitimate “certified distributor” site in Europe to redirect to their poisoned installers hosted on ralrab[.]com. In Belgium, the attackers placed a “recommended” link to their ralrab[.]com site in the middle of the localized WinRAR distribution page on winrar[.]be. The big blue recommended button (here in French) linked to the malicious installer, while all the other links on the page directed to legitimate software:



Winrar[.]be site with “recommended link” leading to malicious ralrab[.]com

The winrar[.]be site evaluated what “recommended” package a visitor may need based on browser localization and processor capability, and accordingly offered up appropriate trojanized versions. Installer resources named for french and dutch versions, along with 32-bit versus 64-bit compiled executables were provided over the summer:

- hxxp://www.ralrab[.]com/rar/winrar-x64-531.exe
- hxxp://www.ralrab[.]com/rar/winrar-x64-531fr.exe
- hxxp://www.ralrab[.]com/rar/winrar-x64-531nl.exe
- hxxp://www.ralrab[.]com/rar/wrar531.exe
- hxxp://www.ralrab[.]com/rar/wrar531fr.exe
- hxxp://www.ralrab[.]com/rar/wrar531nl.exe
- hxxp://ralrab[.]com/rar/winrar-x64-531.exe
- hxxp://ralrab[.]com/rar/winrar-x64-531nl.exe
- hxxp://ralrab[.]com/rar/wrar531fr.exe
- hxxp://ralrab[.]com/rar/wrar531nl.exe
- hxxp://ralrab[.]com/rar/wrar53b5.exe

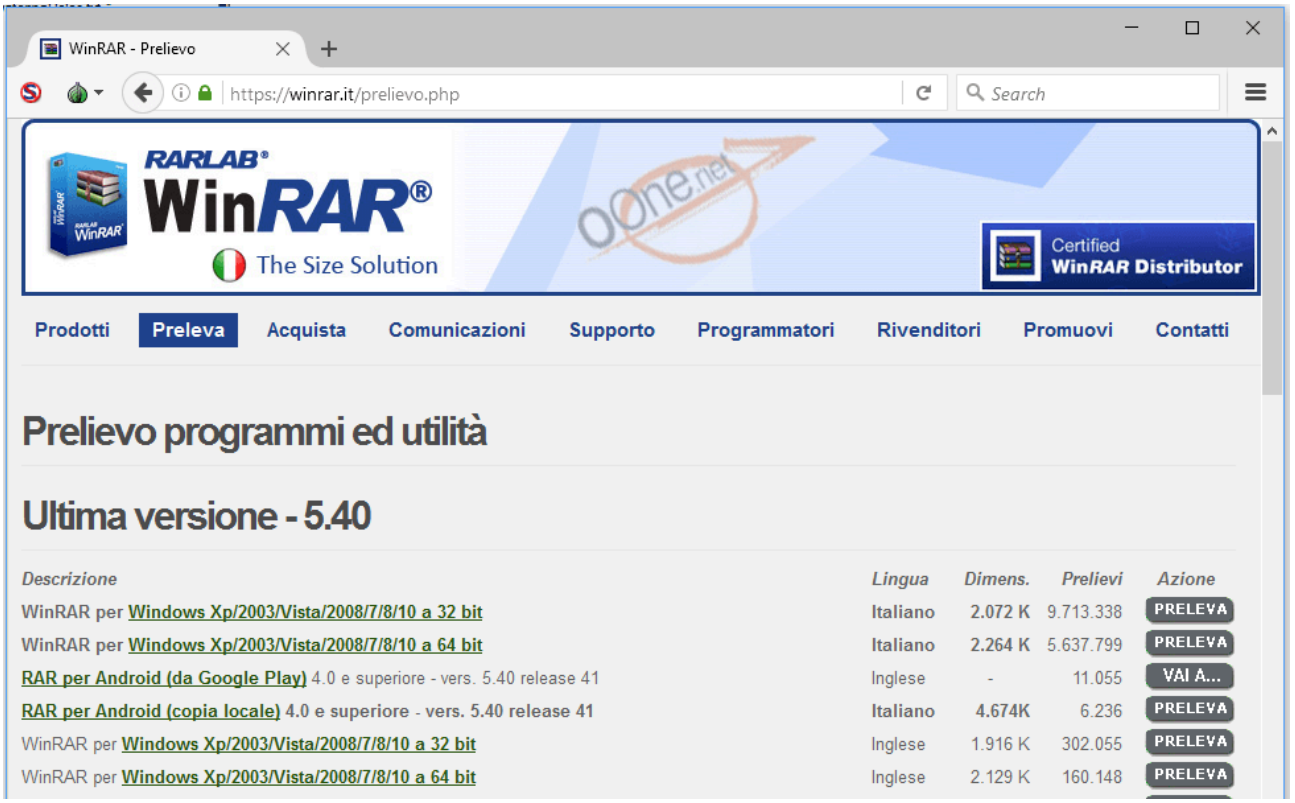


Directory listing, poisoned StrongPity installers, at rarlrab[.]com

The first available visitor redirects from winrar[.]be to ralrab[.]com first appeared on May 28th, 2016, from the dutch speaking version of the winrar.be site. And around the same time, another “certified distributor” winrar[.]it served trojanized installers as well. The major difference here is that we didn’t record redirections to ralrab[.]com, but it appears the site directly served StrongPity trojanized installers:

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

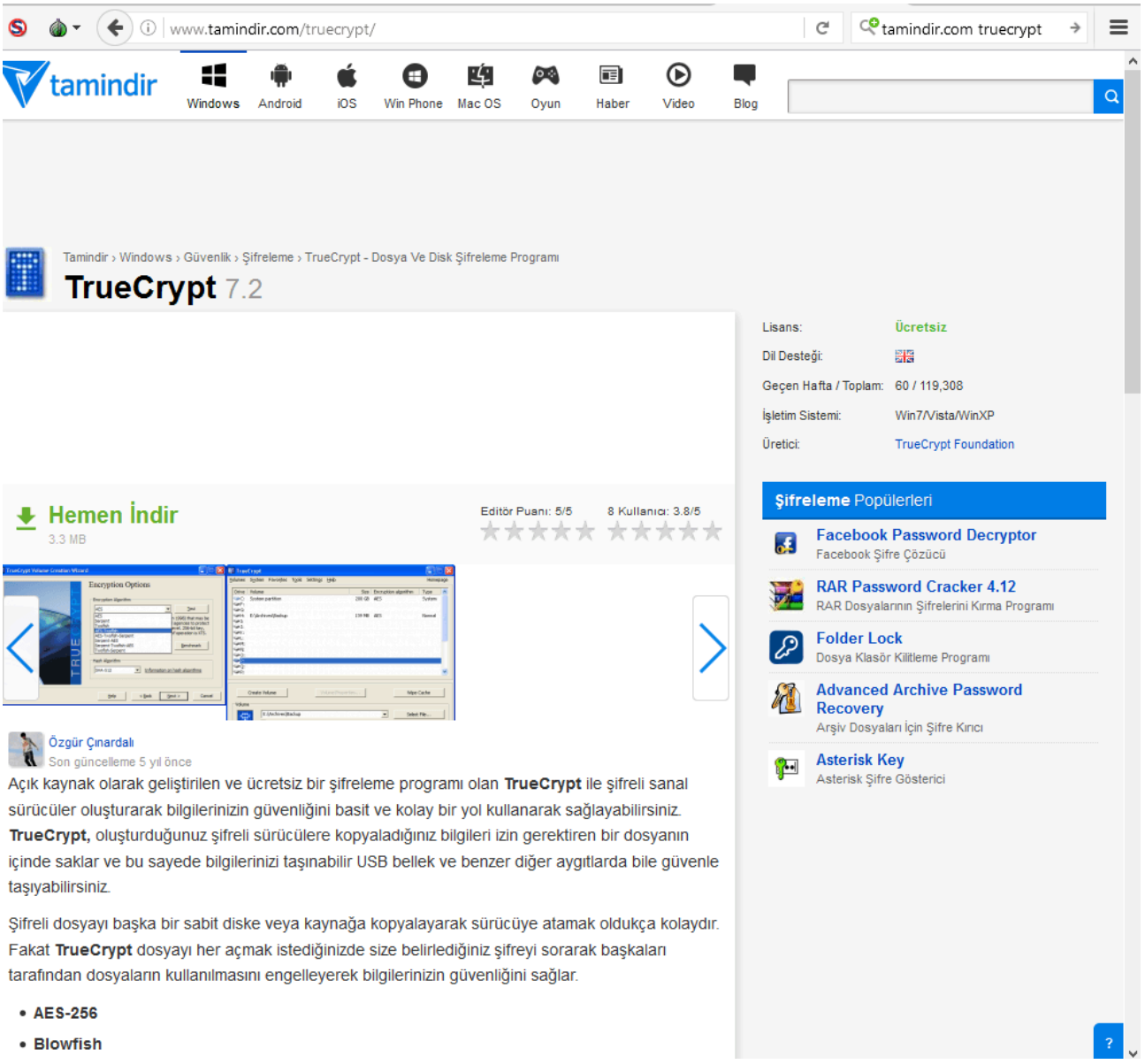
The site started serving these executables a couple of days earlier on 5/24, where a large majority of Italian visitors where affected.



Download page, winrar[.]it

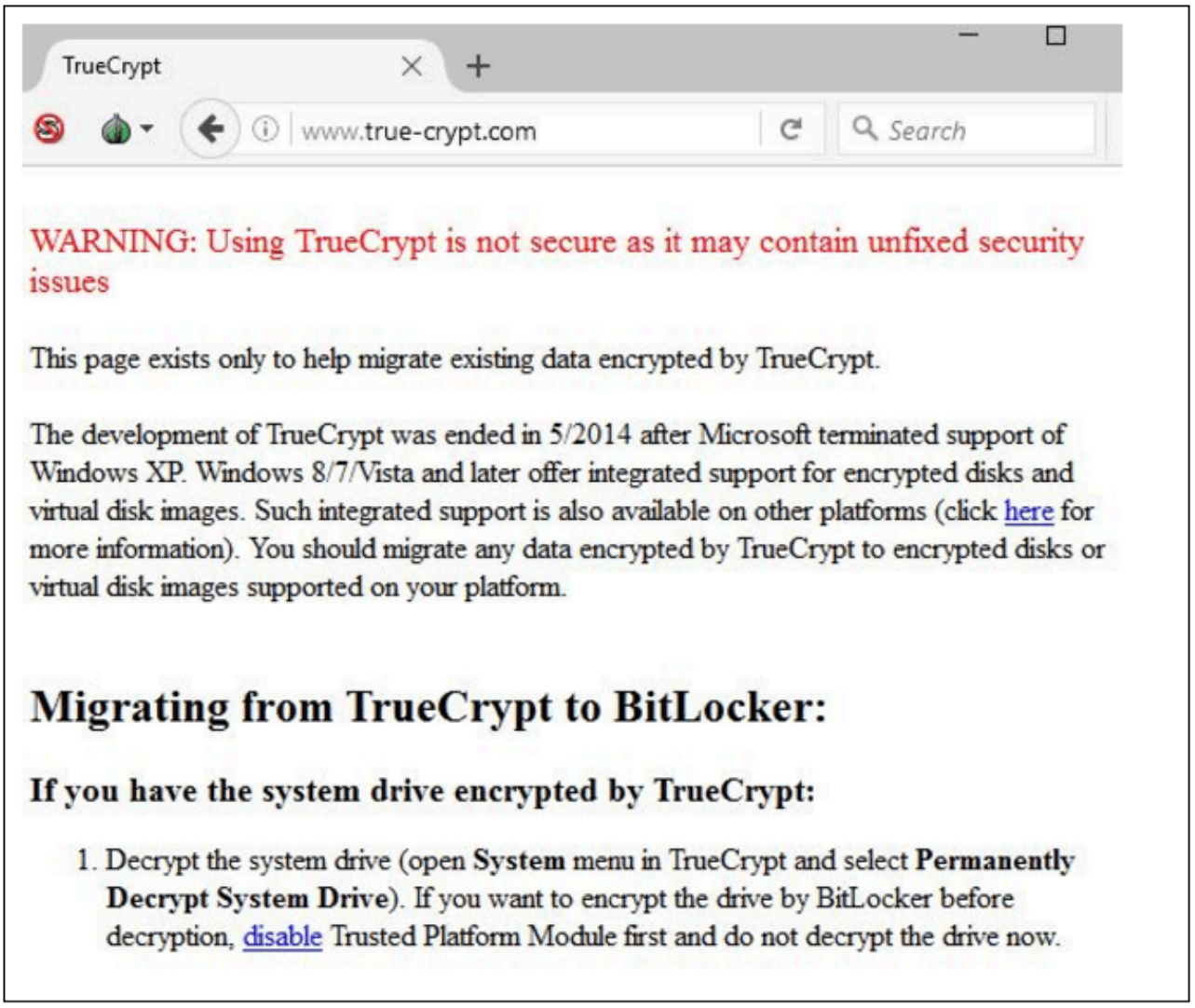
Quite simply, the download links on this site directed visitors to trojanized WinRAR installers hosted from the winrar.it site itself. It's interesting to note that both of the sites are "distributors", where the sites are owned and managed not by rarlabs, but by local owners in individual countries.

StrongPity also directed specific visitors from popular, localized software sharing sites directly to their trojanized installers. This activity continued into late September 2016. In particular, the group redirected visitors from software aggregation and sharing site tamindir[.]com to their attacker-controlled site at true-crypt[.]com. The StrongPity controlled Truecrypt site is a complete rip of the legitimate site, now hosted by Sourceforge. Here is the Tamindir truecrypt page, looks harmless enough.



TrueCrypt page, tamindir software sharing site

Unlike the newer poisoned WinRAR installers, StrongPity hosted several Much like the poisoned WinRAR installers, multiple filenames have been used to keep up with visitor interests. Visitors may have been directed to the site by other means and downloaded directly from the ripped and persuasive site.



true-crypt[.]com malicious StrongPity distribution site

At the very bottom of the page, there are a couple of links to the poisoned installers:

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

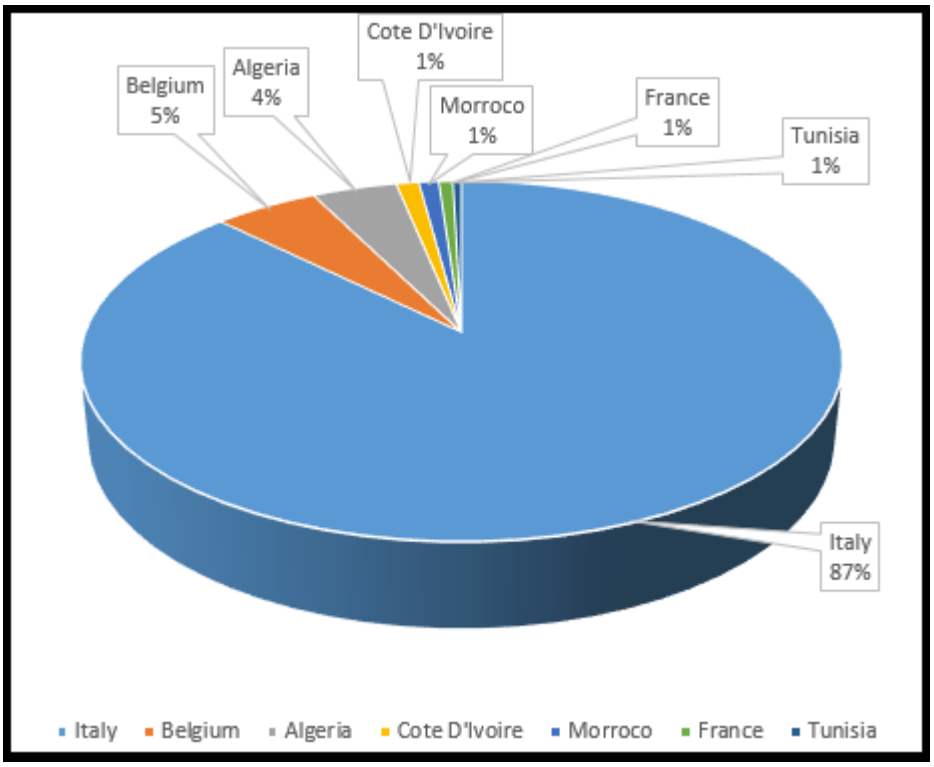
Referrers include these localized software aggregates and sharers:

- gezginler[.]net/indir/truecrypt.html
- tamindir[.]com/truecrypt/indir

It’s interesting that Ksn recorded appearance of the the file on two unique systems in December 2015, a third in January 2016, all in Turkey, and then nothing until May 2016. Then, deployment of the installers continued mostly within Turkey in July and September 2016.

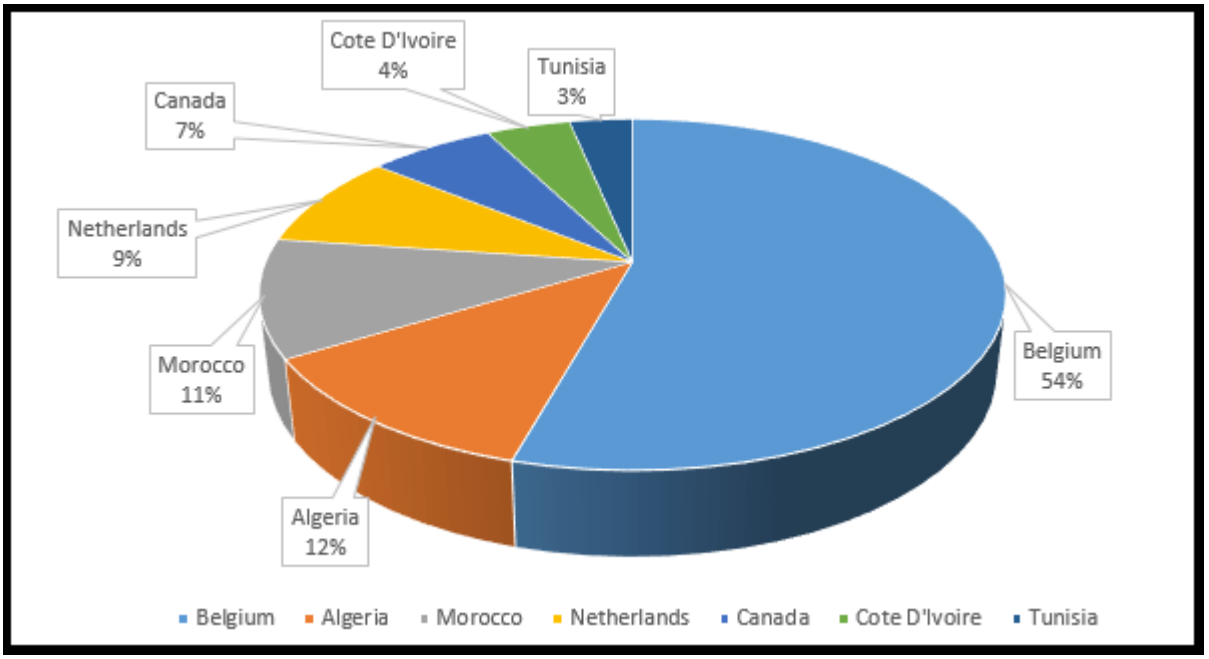
Summer 2016 Watering Hole Victim Geolocations – WinRAR and TrueCrypt

Over the course of a little over a week, malware delivered from winrar.it appeared on over 600 systems throughout Europe and Northern Africa/Middle East. Likely, many more infections actually occurred. Accordingly, the country with the overwhelming number of detections was in Italy followed by Belgium and Algeria. The top countries with StrongPity malware from the winrar.it site from May 25th through the first few days of June are Italy, Belgium, Algeria, Cote D'Ivoire, Morroco, France, and Tunisia.



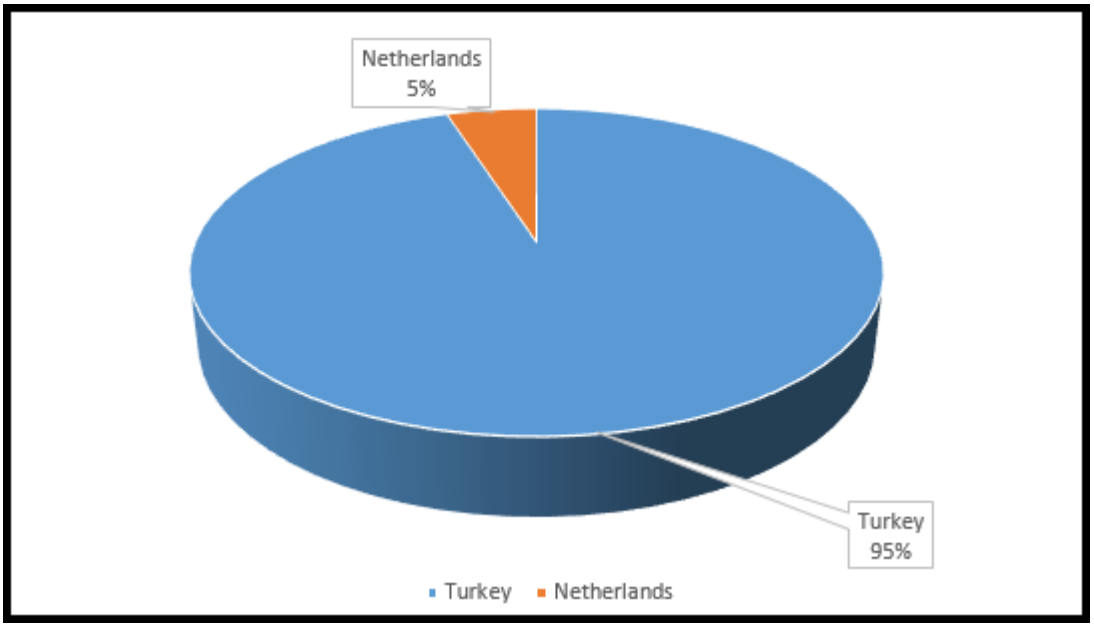
winrar[.]it StrongPity component geolocation distribution

In a similar time-span, the over sixty visitors redirected from winrar.be to ralrab.com for malicious file download were overwhelmingly located in one country. The top countries directed to StrongPity malware from the winrar.be site from May 25th through the first few days of June are Belgium, Algeria, Morroco, Netherlands, Canada, Cote D'Ivoire, and Tunisia.



winrar[.]be StrongPity component geolocation distribution

StrongPity previously set up TrueCrypt themed watering holes in late 2015. But their offensive activity surged in late summer 2016. The group set up a site directly pulled from the contents of the legitimate TrueCrypt website. From mid July to early September, dozens of visitors were redirected from tamindir[.]com to true-crypt[.]com with unsurprisingly almost all of the focus on systems in Turkey, with victims in the Netherlands as well.



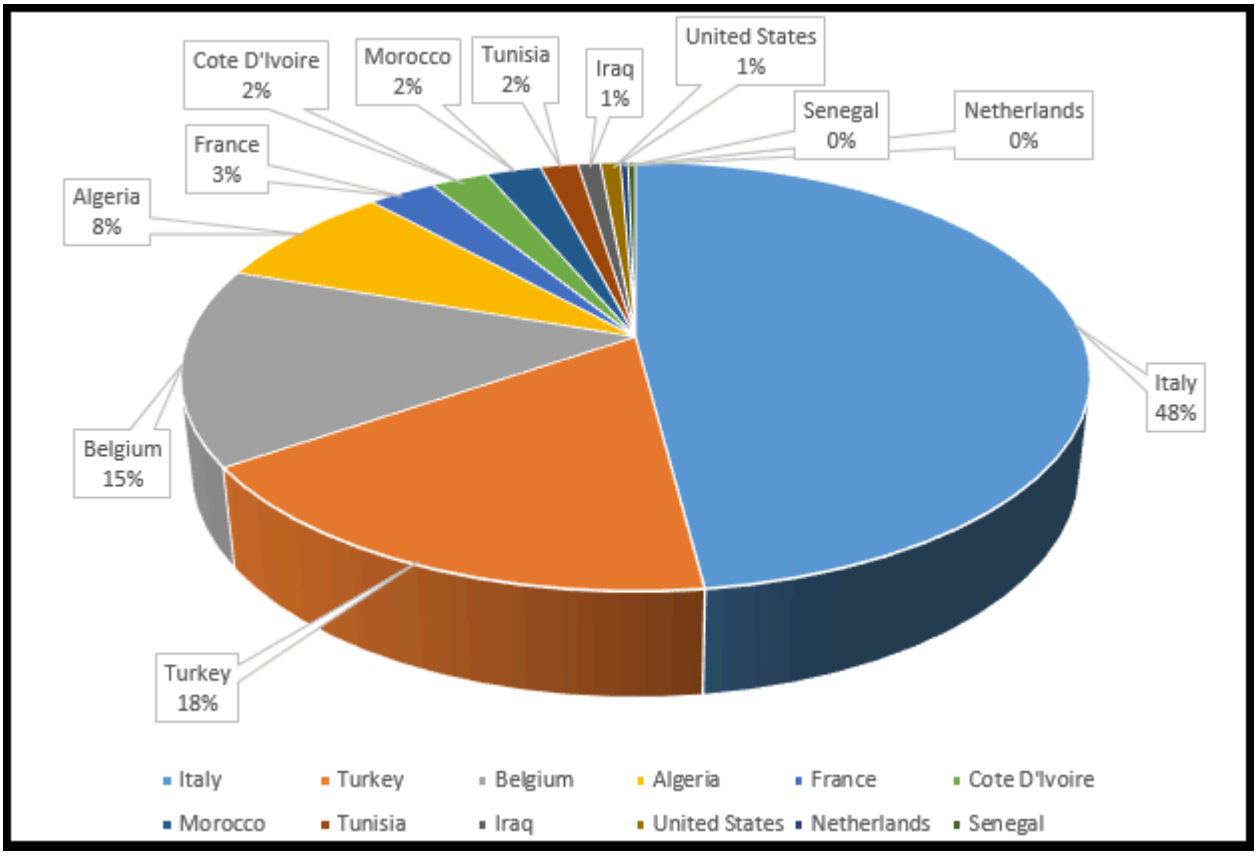
tamindir[.]com to true-crypt[.]com poisoned TrueCrypt installer redirects

StrongPity Malware

The StrongPity droppers were often signed with unusual digital certificates, dropping multiple components that not only provide complete control of the victim system, but effectively steal disk contents, and can download

components for further collection of various communications and contacts. Because we are talking about StrongPity watering holes, let's take a quick look at what is being delivered by the group from these sites.

When we count all systems from 2016 infected with any one of the StrongPity components or a dropper, we see a more expansive picture. This data includes over 1,000 systems infected with a StrongPity component. The top five countries include Italy, Turkey, Belgium, Algeria, and France.



In the case of the winrar[.]be/ralrab[.]com watering hole malware, each one of the six droppers that we observed created a similar set of dropped components on disk. And, in these cases, the attackers did not re-use their fake digital certificates. In addition to installing the legitimate version of WinRAR, the dropper installed the following StrongPity components:

- %temp%\procexp.exe
- %temp%\sega\
- nvvscv.exe
- prst.cab
- prst.dll
- wndplyr.exe
- wrlck.cab
- wrlck.dll

Of these files, two are configurable and encrypted with the same keyless cipher, "wrlck.cab" and "prst.cab". While one maintains several callback c2 for the backdoor to fetch more instructions and upload installed software and file paths, the other maintains something a bit more unusual. "prst.cab" maintains an encrypted list of programs

that maintain encrypted connections. This simple encoding takes the most significant nibble for each character, swaps the nibbles of that byte, and xors the result against the original value. Its code looks something like this:

- x = s[i];
- j = ((x & 0xF0)>>4);
- y = x ^ j;

Using that cipher in the ralrab[.]com malware, the package is configured to seek out several crypto-enabled software applications, highlighting the group's interest in users of more encryption-supported software suites.

- putty.exe (a windows SSH client)
- filezilla.exe (supports ftps uploads)
- winscp.exe (a windows secure copy application, providing encrypted and secure file transfer)
- mstsc.exe (Windows Remote Desktop client, providing an encrypted connection to remote systems)
- mRemoteNG.exe (a remote connections manager supporting SSH, RDP, and other encrypted protocols)

Also included in StrongPity components are keyloggers and additional data stealers.

Conclusion

Widely available, strong cryptography software tools help provide secure and private communications that are now easily obtained and usable. In the summer of 2016, multiple encryption-enabled software applications were targeted with watering hole, social engineering tactics, and spyware by the StrongPity APT. While watering holes and poisoned installers are tactics that have been effectively used by other APT, we have never seen the same focus on cryptographic-enabled software. When visiting sites and downloading encryption-enabled software, it has become necessary to verify the validity of the distribution site and the integrity of the downloaded file itself. Download sites not using PGP or strong digital code signing certificates need to re-examine the necessity of doing so for their own customers. We have seen other APT such as Crouching Yeti and Darkhotel distribute poisoned installers and poisoned executable code, then redistribute them through similar tactics and over p2p networks. Hopefully, simpler verification systems than the current batch of PGP and SSL applications will arise to be adopted in larger numbers. Until then, strong anti-malware and dynamic allowlisting solutions will be more necessary than ever.

More information about the StrongPity APT group is available to customers of Kaspersky Intelligent Services. Contact: intelreports@kaspersky.com

---