Troldesh ransomware influenced by (the) Da Vinci code

blogs.technet.microsoft.com/mmpc/2016/07/13/troldesh-ransomware-influenced-by-the-da-vinci-code/

July 13, 2016

*(Note: Read our latest comprehensive report on ransomware: **Ransomware 1H 2017 review: Global outbreaks reinforce the value of security hygiene**.)*

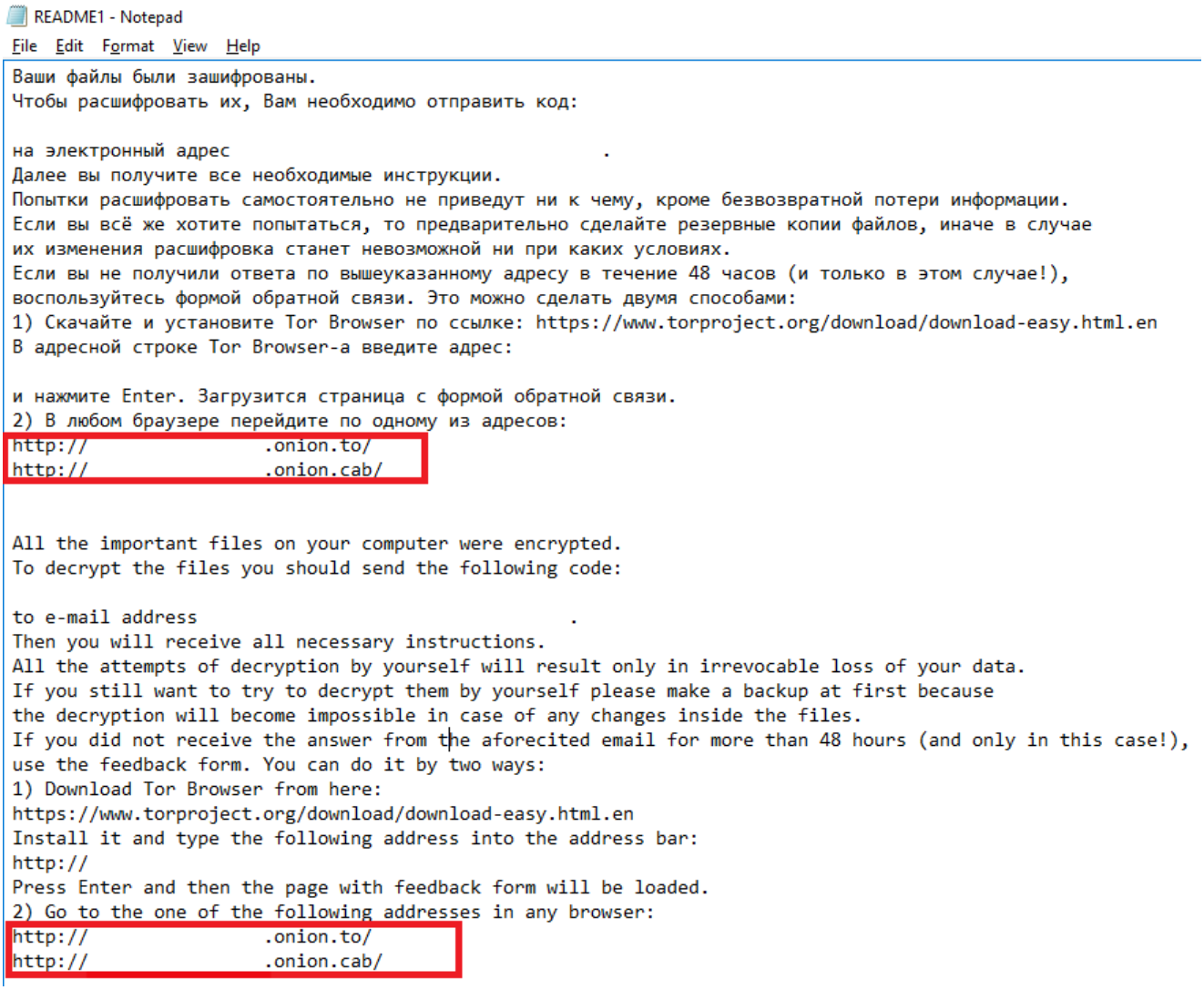
We at the MMPC are constantly tracking new and emerging ransomware threats so we can be one step ahead of active campaigns and help protect our users. As part of these efforts, we recently came across a new variant of the Win32/Troldesh ransomware family.

Ransomware, like most malware, is constantly trying to change itself in an attempt to evade detection. In this case, we've seen the following updates to Troldesh:

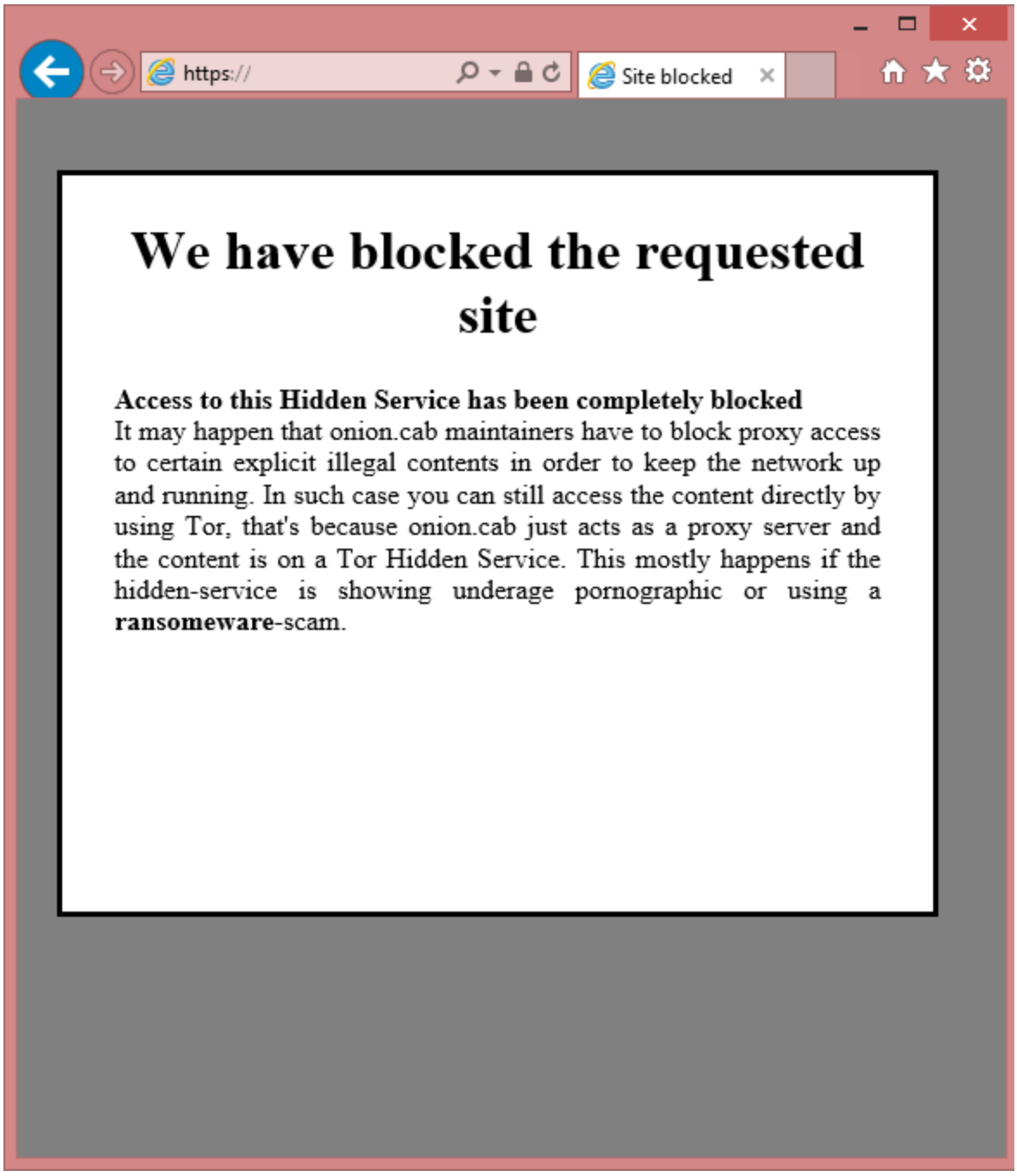
- Tor functionality
- Glyph/symbol errors on the wallpaper ransom note
- Modified extension names for encrypted files
- New malware being delivered (Trojan:Win32/Mexar.A)
- Updates the ransom note to cover the Tor functionality

The biggest change in this update is the addition of Tor links. Using Tor addresses as the ransom payment method (as opposed to standard www addresses) is the current fashion among ransomware.

The ransom note now includes links to the Tor address (previously, the only method provided for obtaining decryption was an email address):



However, upon investigation it appears that Tor has blocked the address:



Errors have been introduced into the image that replaces the user's desktop wallpaper (this occurred to several samples, but not all):

After encryption, Troldesh changes the file's extension. In the latest update, we've seen it use the following strings:

- .da_vinci_code
- .magic_software_syndicate

For example, an encrypted file might appear as follows:

Name	Date modified	Type	Size
oag6HJ25UnZr9sKxhDvzuwiJu6ulvQuhtbLT5VgTQpk=.BF4EB35FA84C95EE6783.da_vinci_code	7/7/2016 11:52 AM	DA_VINCI_CODE File	100 KB

The list of file types that Troldesh encrypts has also increased – see the Win32/Troldesh description for a full list.

Prevention

To help stay protected:

- Keep your Windows Operating System and antivirus up-to-date and, if you haven't already, upgrade to Windows 10.

- Regularly back-up your files in an external hard-drive
- Enable file history or system protection. On Windows 10 and Windows 8.1, set up a drive for file history
- Use OneDrive for Business
- Beware of phishing emails, spams, and clicking malicious attachment
- Use Microsoft Edge to get SmartScreen protection. It can help warn you about sites that are known to be hosting exploits, and help protect you from socially-engineered attacks such as phishing and malware downloads.
- Disable the loading of macros in your Office programs
- Disable your Remote Desktop feature whenever possible
- Use two factor authentication
- Use a safe Internet connection
- Avoid browsing web sites that are known for being malware breeding grounds (such as illegal music, movies and TV, and software download sites)

Detection

- Ensure your antimalware protection (such as Windows Defender) is up-to-date and working correctly.
- Enable Microsoft Active Protection Service (MAPS) to get the latest cloud-based ransomware detection and blocking.

Recovery

In the Office 365 "How to deal with ransomware" blog, there are several options on how you might be able to remediate or recover from a ransomware attack, including backup and recovery using File History in Windows 10 and System Restore in Windows 7.

You can also use OneDrive and SharePoint to backup and restore your files:

- OneDrive for Business and SharePoint:
  - Restore a previous version of a document in OneDrive for Business
  - Restore Option in SharePoint Online
- OneDrive for home users:
  - Find lost or missing files in OneDrive
  - Delete or restore files and folders

Patrick Estavillo

Talk to us

Questions, concerns, or insights on this story? Join discussions at the Microsoft community and Windows Defender Security Intelligence.