BIZCOMMUNITY

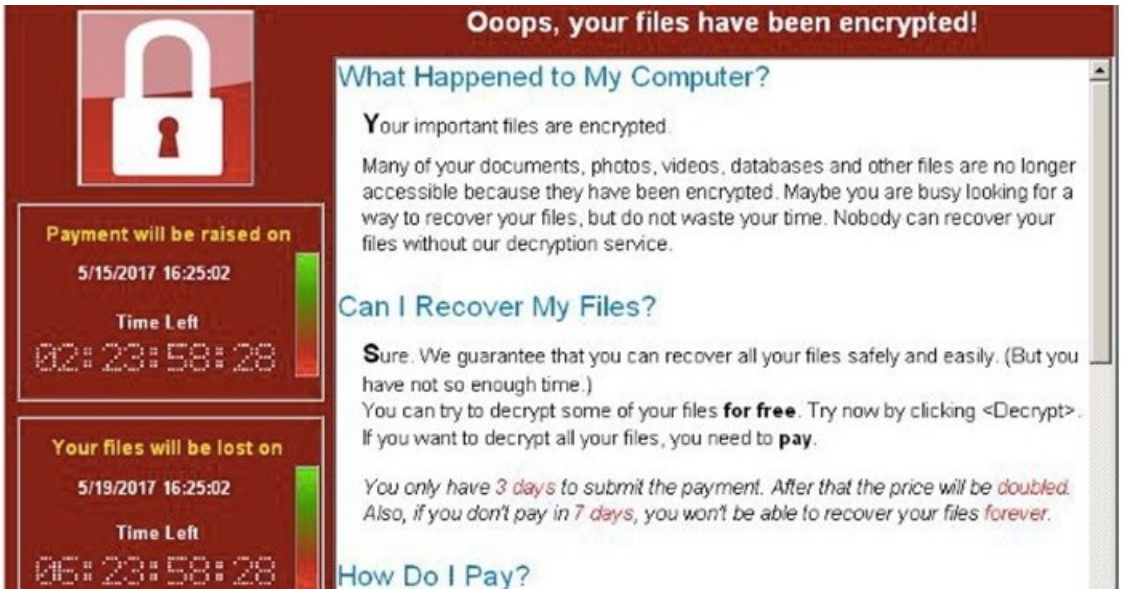
The six worst ransomware

By Colin Thornton

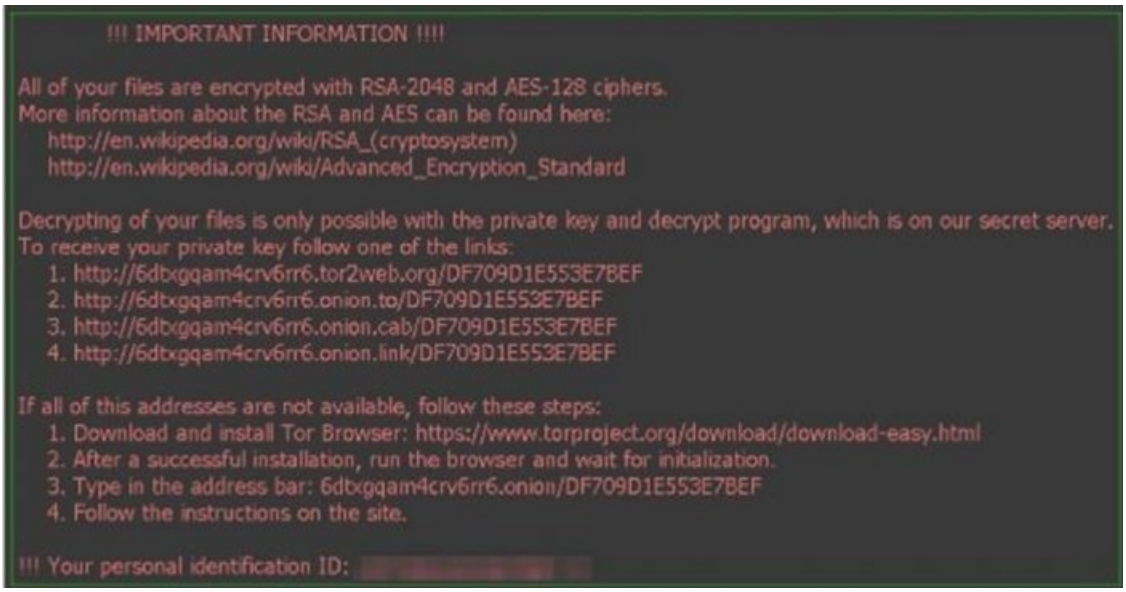
20 Jul 2017

It's hard to keep track of the cybercriminal world as it seems these dark web creatures are constantly trying to outwit, outlast, and outplay each other with their destructive viruses. These are, however, currently the six worst ransomware to protect yourself against.

1. **WannaCry:** WannaCry wreaks its havoc by encrypting most or even all of the files on a user's computer. Then, it demands that a ransom be paid in order to have the files decrypted. WannaCry demands that the victim pays a ransom of $300 in bitcoins at the time of infection. If the user doesn't pay the ransom within three days, the amount doubles to $600. After seven days without payment, WannaCry will delete all of the encrypted files and all data will be lost.

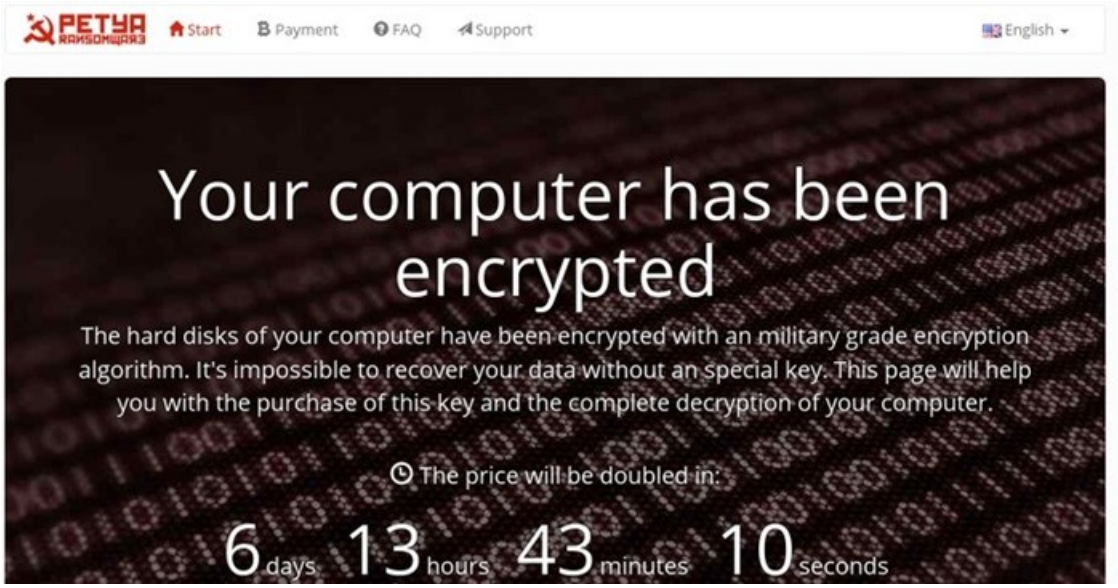


2. **Locky ransomware:** This pernicious ransomware is meant to lock you out of your data on the system, which, admittedly, is the aim of any ransomware…however, Locky changes your file extension to keep your data out of your reach. It encrypts your files and changes your file extension to lock the data down. It uses '.locky' as its file extension with RSA-2048+AES-128 encryption.



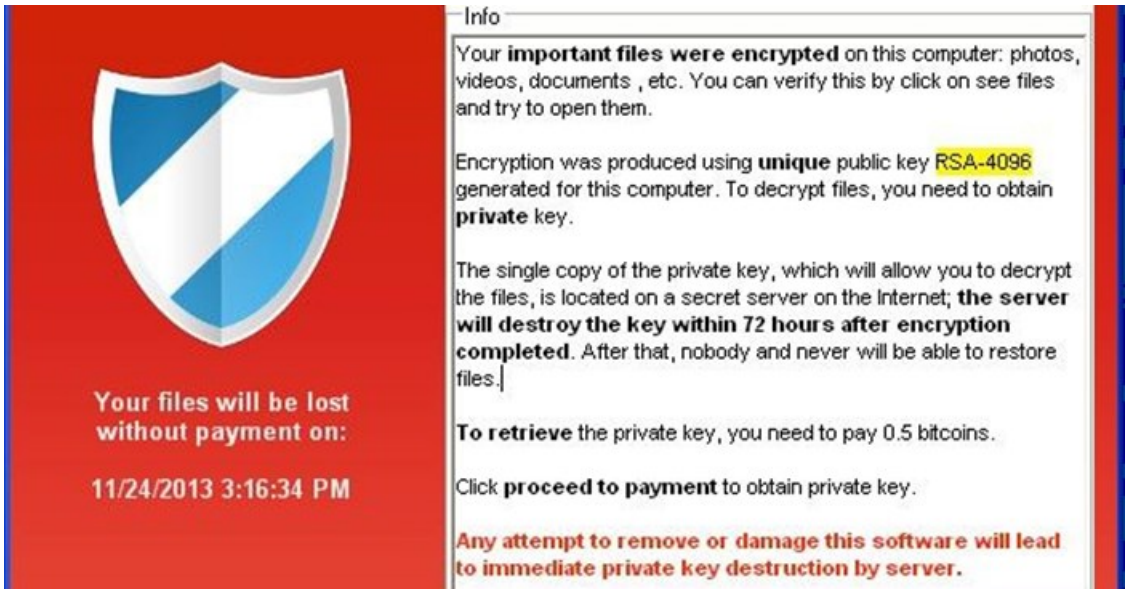
This is considered to be one of the most dangerous ransomware. It generally targets systems with spam email attachments. Once you download the attachment, Locky ransomware gets installed on the system to lock your files and data. Despite all the issues related to this ransomware, it is still not a good approach to pay to release the data affected by Locky ransomware. By applying certain Locky ransomware removal steps, you can actually prevent your data loss (to some extent).

3. **Petya:** Petya ransomware attacks differently, because instead of encrypting files one by one, it blocks access to the full system by attacking low-level structures on the disk.
   The Petya ransomware attacks each system's boot drive's existing master boot record, with an affected and malicious loader.

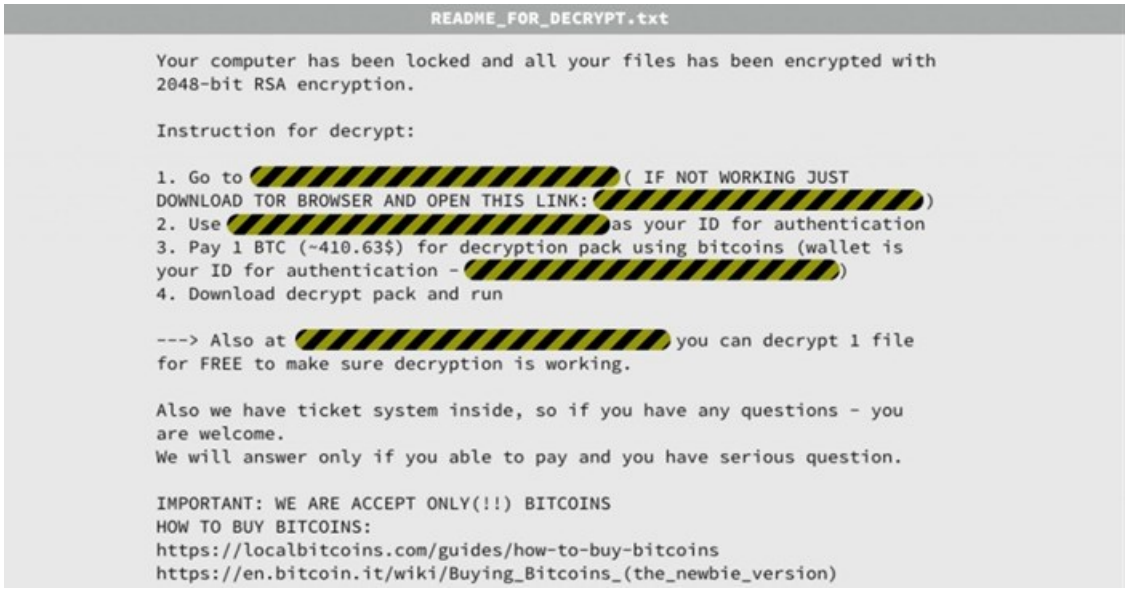


Notably, this malicious boot loader overwrites the affected system's MBR – as it loads a tiny malicious kernel that proceeds with further encryption of existing data. This way, it encrypts a portion of the system's hard drive. Additionally, it blocks access to Windows – so that you cannot access the system at all. This ransomware is delivered via spam emails to target systems. Another malicious payload is Mischa, which is considered to be the updated version of Petya ransomware.

4. **CryptoLocker:** This is considered to be one of the nastiest ransomware, as it not only prohibits you from accessing your data - but once attacked by this malware you can lose your important data permanently! It is spread using malicious attachments sent via emails disguised as coming from a trusted institution or company. CryptoLocker encrypts your data and demands payment to release it. It virtually locks down your system entirely…

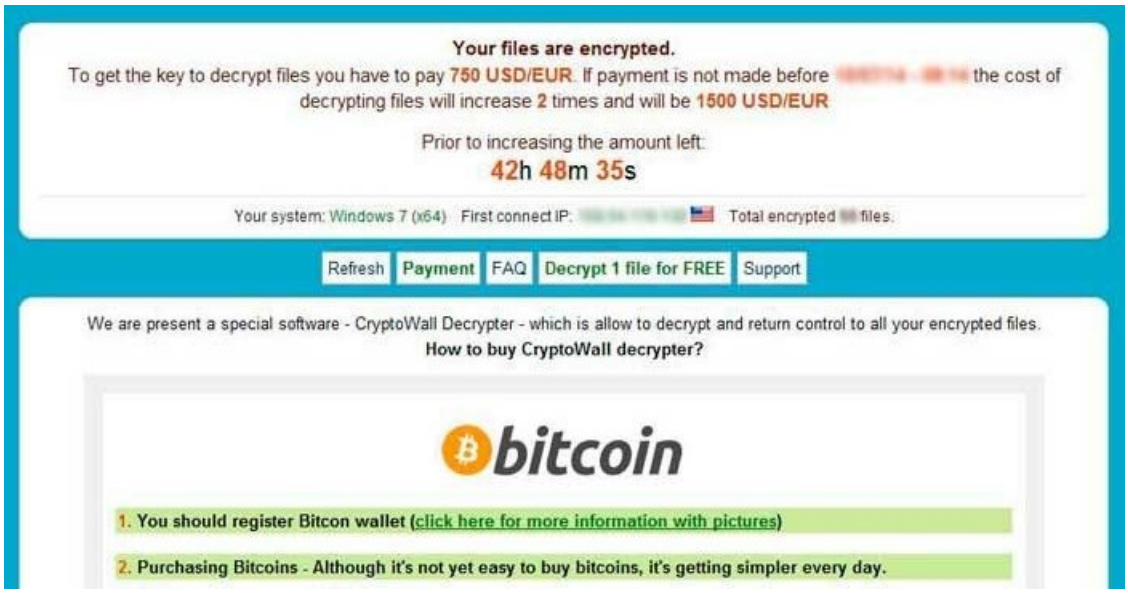


5. **KeRanger:** This is the first-ever ransomware that has attacked Mac. Palo Alto Networks discovered this first Mac ransomware, which was found to be infecting the Transmission - a widely used open-source platform for file sharing that has affected the BitTorrent client.
   This ransomware is able to encrypt everything in the user's folder, along with files using common document extensions found in the volumes folder.



6. **CryptoWall:** CryptoWall is from the family of file-encrypting ransomware that first appeared in early 2014. It is

primarily distributed using various exploit kits, spam campaigns, and malvertising techniques. This ransomware attacks systems in a fashion similar to CryptoLocker, and it attacks particularly important files and data within each victim's system (such as tax receipts, bills, financial data, etc). CryptoWall demands a few hundred dollars, which can be doubled if certain deadlines are not met.



Recently, CryptoWall was updated to version 3.0, which has made it even more dangerous. CryptoWall 3.0 encrypts the user's files with the system of intelligent scanning - and it then generates a unique link for the user. It can hide the identity of the attackers, making it very hard for law enforcement to uncover the source.

ABOUT COLIN THORNTON

Colin founded Dial a Nerd in 1998 as a consumer IT support company and in 2002 the business- focused division was founded. Supporting SMEs is now its primary focus. In 2015 his company, merged with Turrito Networks who provided niche internet services outside of the local network. These two companies have created an end-to-end IT and Communication solution for SME's. Colin has subsequently become the managing director of Turrito. Contact him at info@dialanerd.co.za

- Understanding SA's 5G reality - 4 Apr 2019
- Why your business needs a cloud architect - 21 Feb 2019
- Privacy vs Profit: Will 2019 be the year of consumer paranoia? - 26 Nov 2018
- Why SMEs should be looking at cyber insurance - 28 Sep 2018
- Why your future digital ID should harness blockchain technology - 23 Aug 2018

View my profile and articles...