CompNetSys
Computer Network Systems

SPECIAL REPORT

Don’t Fall Victim to a Ransomware Attack.

Protect Your Data and Business From This Top Security Threat For 2017.

CompNetSys
Computer Network Systems

Ransomware attacks are on the rise. It's part of the top 10 threat predictions by security analysts and labs around the world. And for businesses that are victimized, the consequences can be paralyzing and destructive.

When ransomware infects your computer or mobile device, your organization's operations can come to a grinding halt. You'll be denied access to your computer and may even lose your data. Ransomware attacks have cost U.S. businesses millions of dollars in losses. Don't let your business be one of these.

Fast Facts:

- **Ransomware is the most malicious and frequently used form of malware today.**
- **There's more than one type of ransomware.**
- **It's important to know what to do if you experience a ransomware attack.**
- **The best way to protect your organization from ransomware is to prevent it from landing on your computers in the first place.**
- **Always back up your data so your IT professional can restore it in the event of an attack.**

Ransomware is the most malicious and frequently used form of malware today.

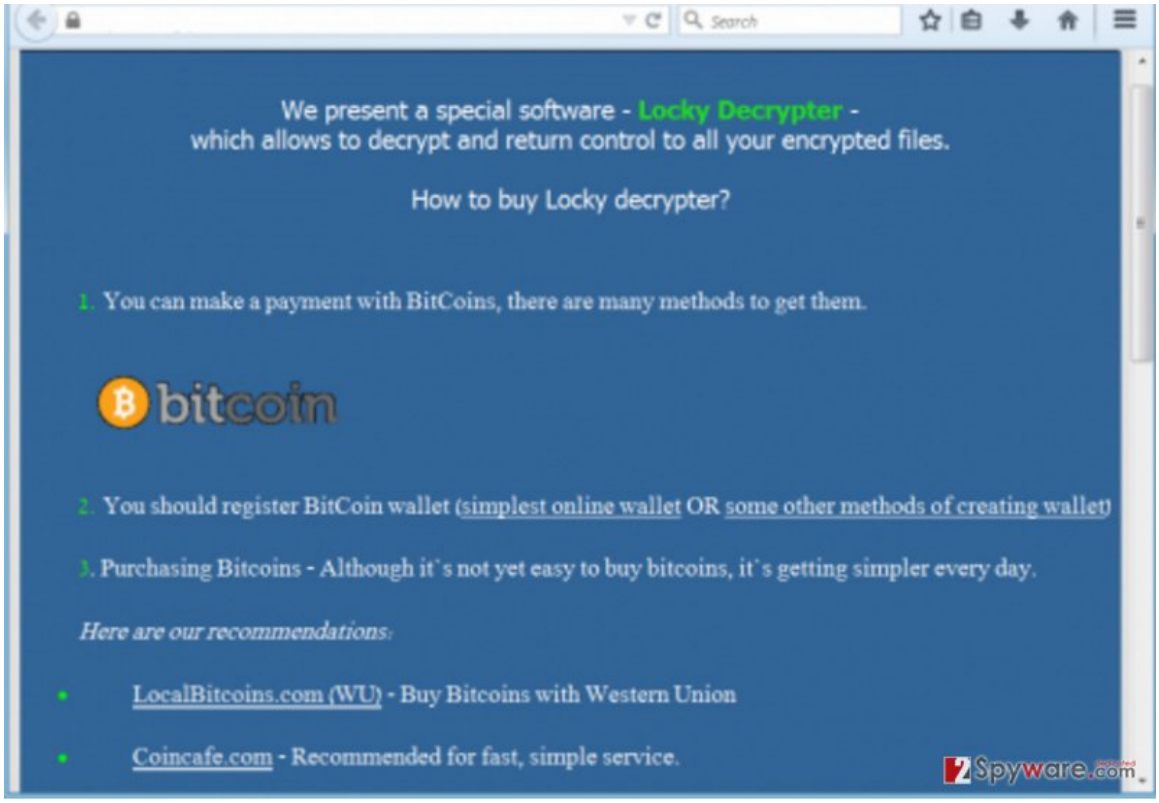
Ransomware blocks access to your data and demands payment through an anonymous system like Bitcoin to restore access. In the past few years many small businesses, government agencies and private users have been victims of ransomware. The criminals who distribute and operate these attacks are making millions of dollars. They extort money from you in exchange for a promise to unlock your computer files.

There's more than one type of ransomware.

Ransomware programs may be different but they can all wreak havoc with Windows and Macintosh computers, and even Android devices. The infection takes place when you open a malicious email attachment, visit an infected website, or download and install infected software from the Internet.

There are many different types of ransomware. The following are some that are currently used.

Locky: This is the most prevalent form of ransomware today. Locky was used in nearly all of the malicious email attacks in the third quarter of 2016. It's a screen-locking or "locker" ransomware that prevents you from using your device by freezing your computer interface. The way it's delivered is through a phishing email that tricks you into either opening malicious Microsoft Office documents or other infected attachments. Your screen will then display a banner saying that your computer has been "locked" by the FBI or other law-enforcement agency. Locky also encrypts files on your network and deletes any copies so they can't be used to restore your files. Unfortunately, there's no way to decrypt files that have been encrypted by Locky without paying a ransom.



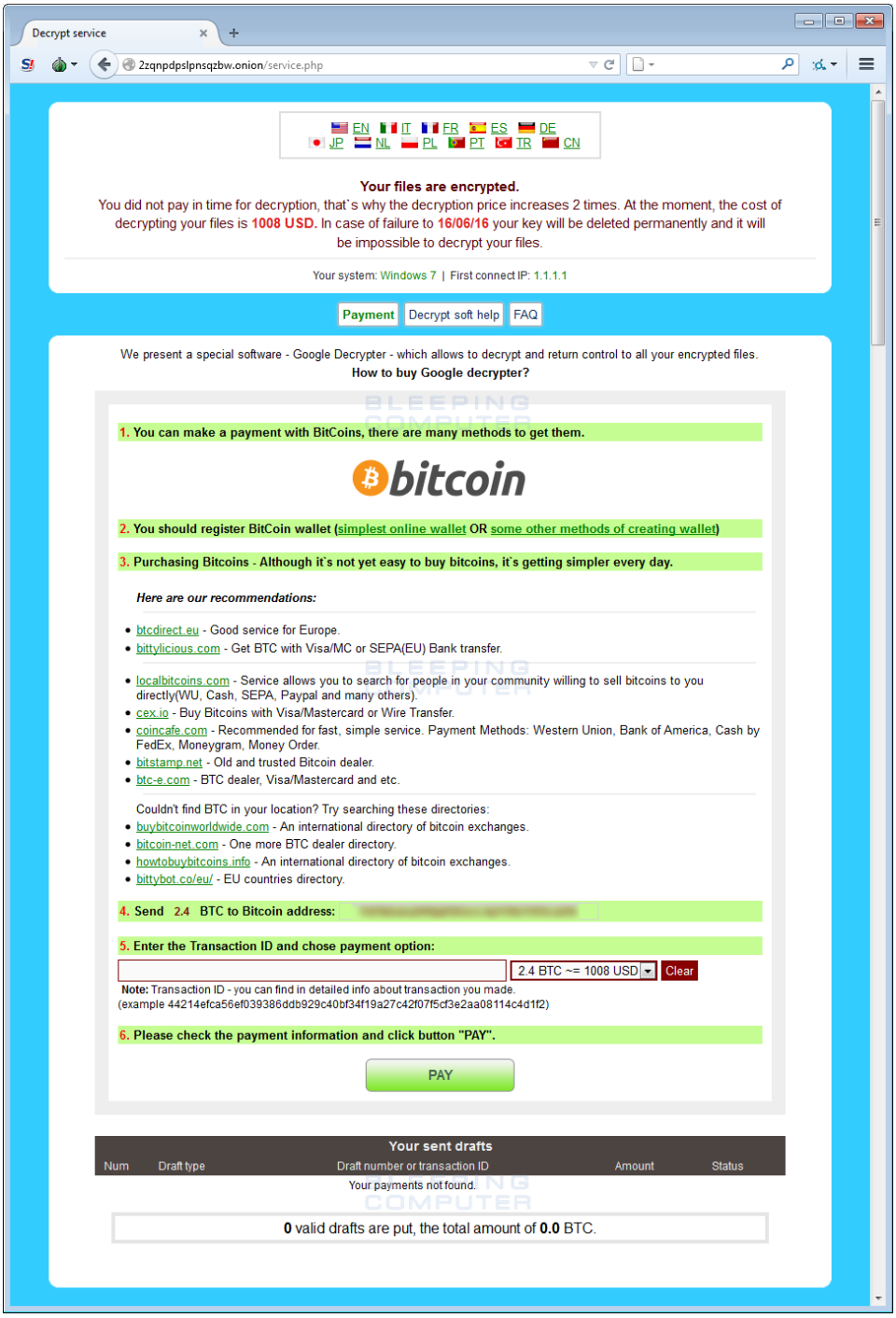
Crypto: Instead of freezing your computer interface, "crypto" ransomware searches your hard drive for common file types such as images and documents, and freezes them. It's often distributed through machines that have already been infected via malicious email attachments. When you click on this attachment it automatically installs malware on your computer. Once installed, the crypto ransomware sets keys in the Windows Registry of your computer so it can start itself automatically every time you boot your computer. The ransomware attacker will then send you a message saying your files have been encrypted, and that unless you pay their ransom it will be impossible to recover your files.

In either case you will be given specific instructions to pay a ransom. A deadline for paying is typically accompanied by a threat that your files will be deleted at specified intervals (typically every 30 minutes). After your payment is received and processed, you will be sent a numerical key to unlock your computer screen or encrypted files, or provided a serial key for activating a decryption program found on the attacker's website.

CryptXXX: This is a new, sophisticated ransomware that is now demanding $1,000 for their decryption key. It infects all versions of Windows. When your computer is infected with CryptXXX your files are encrypted with a .crypt extension, and you can't open them. Crypt XXX creates three types of files, similar to other types of ransomware:

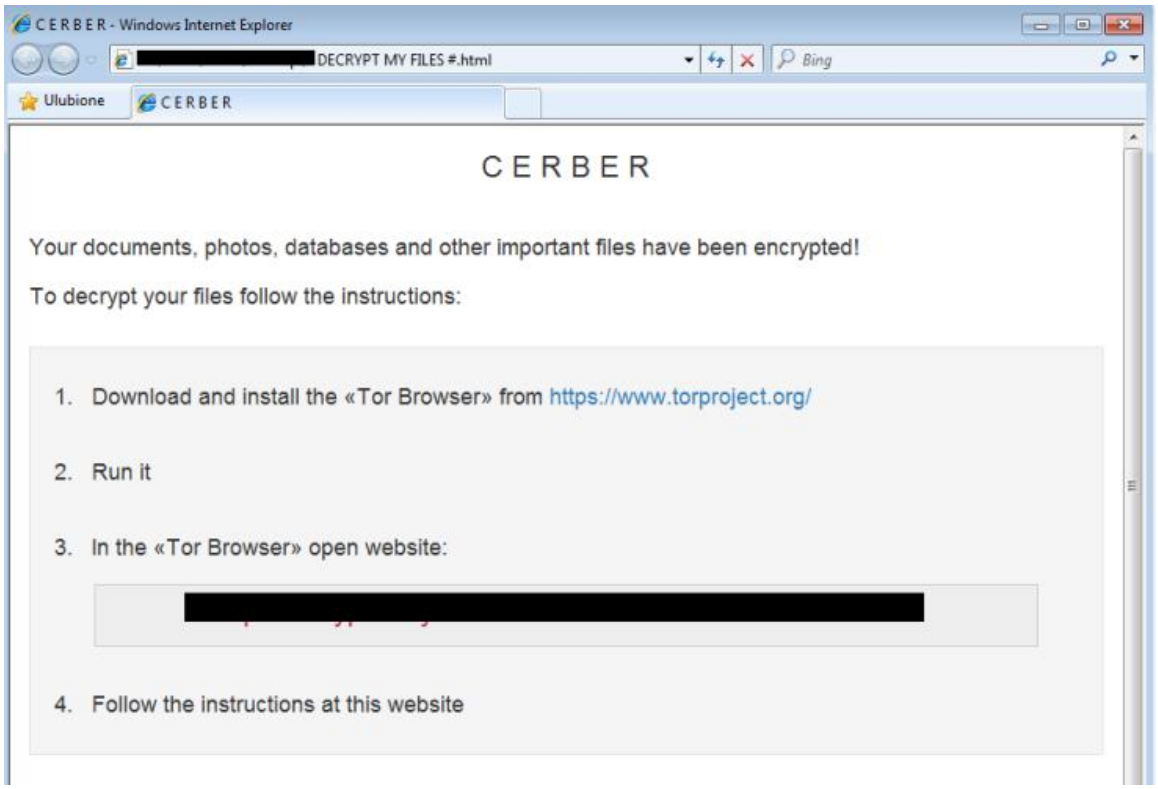
1. de_crypt_readme.bmp
2. de_crypt_readme.txt
3. de_crypt_readme.html

CryptXXX takes over your desktop image and displays a note with instructions on how to make a ransom payment. The CryptXXX attackers constantly update versions of this malware, making it difficult for tech professionals to come up with a decryptor. Hence, CryptXXX attackers are able to demand high fees from you to release your data.



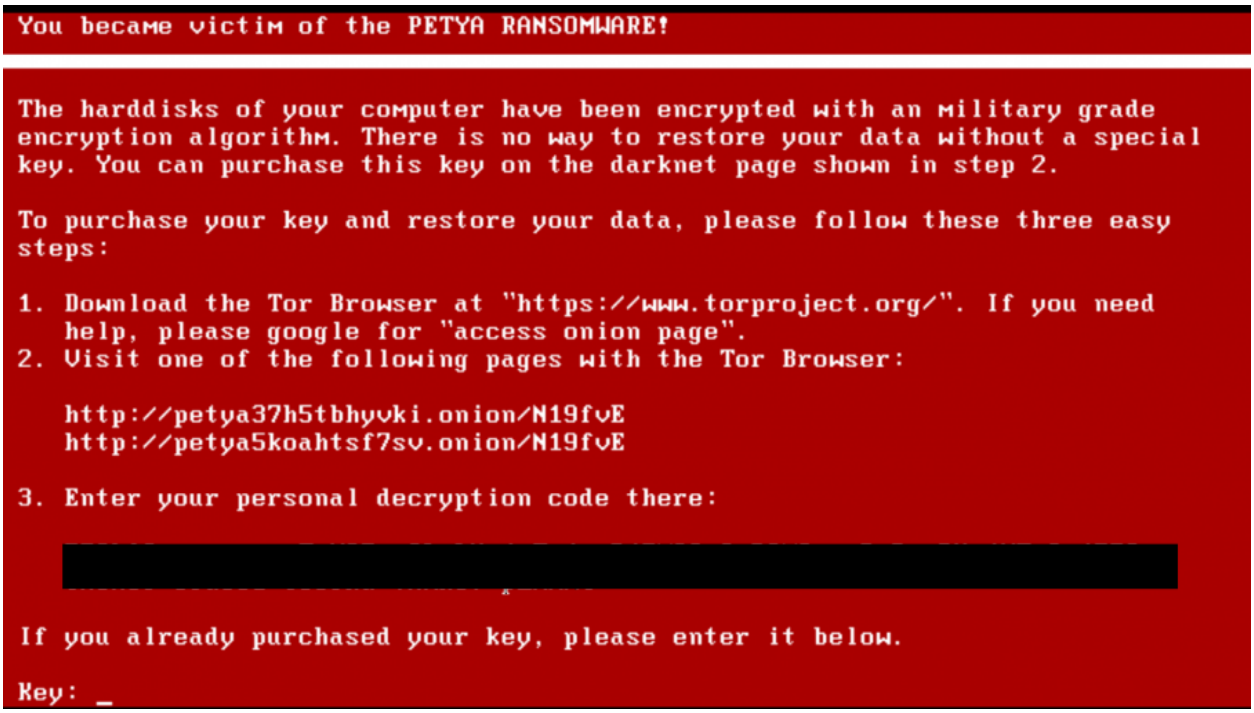
Cerber: Cerber is another new form of ransomware that appeared in 2016. It's different from other types of ransomware in that it comes with a script that enables your computer to talk to you. It also allows anyone to distribute it in exchange for a 40 percent share of the paid ransom. Attackers made over $2.3 million dollars from Cerber in 2016. It's also a favorite for attackers as it has the ability to delete databases by encrypting files. To date,

there are no decryption tools for the newer versions of Cerber, making it especially dangerous.

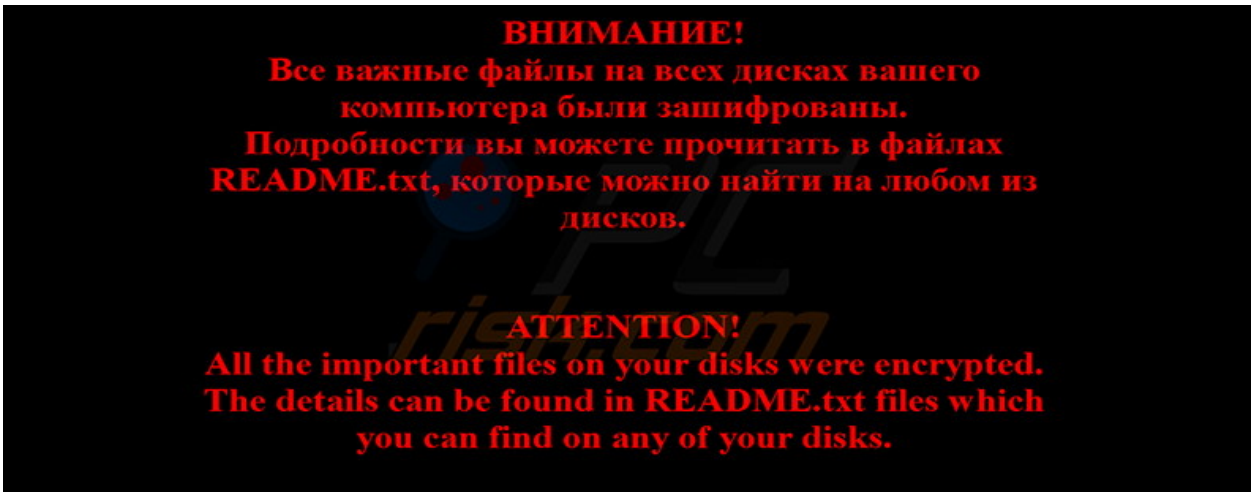


Petya: Petya ransomware uses two new tactics that ransomware attackers haven't used in the past. Posing as a job applicant, the attacker sends you a professional-looking email with a Dropbox link to a supposed resume. When you try to open the link, the infection begins.

Unlike other forms of ransomware, Petya then begins to overwrite the boot files your computer needs to load Windows. Your computer gets locked and a red boot screen appears demanding a ransom to unlock it. In the meantime it starts encrypting your files. Because this is such a new type of infection, there are no updated tools to remove Petya ransomware or decrypt your files.



Shade: Shade not only encrypts your files and demands a ransom but it uses your encrypted data to make even more money. Prior to encrypting your files, Shade goes through your files looking for banking or accounting activity. Once discovered, it installs remote-control malware that allows the attacker to can gain access to your finances. Even if you're able to get the decryptor tool to recover your files, the damage has already been done. Attackers now have the ability to retrieve your financial information.



Virlock: Virlock is a very dangerous ransomware that not only infects your computer but

your cloud files as well. It's the first self-replicating form of ransomware, functioning like a parasitic virus that infects both your computer and cloud files while creating new versions of itself. This makes it very difficult to detect and block Virlock. All it takes is for you or another user to open an infected file on your shared folder. Virlock then spreads through cloud storage and shared applications, enabling one infected user to inadvertently spread the file-locking malware across your enterprise network.

It's important to know what to do if you experience a ransomware attack.

If you believe a ransomware attack is occurring and your files are being encrypted, power off your machine immediately. You can simply unplug the power cord if you can't do this with the power button. Tell all users to do the same.

Contact your IT professional immediately to:

- Identify the source of the attack and any damage that may have occurred.
- Scan, clean and protect affected machines.
- Re-install software that no longer works correctly, and restore data if needed.

The best way to protect your organization from ransomware is to prevent it from landing on your computers in the first place.

If you experienced a ransomware attack this means that it got through all your anti-virus software and security on your machine(s). Unfortunately, because ransomware performs multi-layers attacks there is no security feature today that can protect against every threat. However, your IT professional can provide advice on the most current and effective protection.

The best security software is made up of layers that protect specific areas, and where each layer communicates with another for the best protection possible. The first layer of protection is for your email where spam typically enters. Securing your email with the right program allows you to scan every email for malicious files before you or other users open them. Your IT professional can also offer a compatible sandboxing program so you can open attachments in a secure environment where they can be analyzed for ransomware.

Always backup your data so your IT professional can restore it in the event of an attack.

To protect yourself and your business from ransomware attacks you must perform secure backups. This requires backups that occur in realtime, daily and weekly. These backups must be isolated from your network to ensure they can't be compromised by a ransomware attack. Your IT professional will need these backup files to restore your data. In most cases he or she can erase the hard drive, reinstall the operating system and restore your machine with the backup copy.

Don't forget to educate your staff about the threats and prevention of ransomware attacks. Ask your IT professional if they can train you and your personnel with simulation tools to help them recognize malicious IT threats of any kind. By doing this you'll reduce the odds of falling victim to a ransomware attack.