CENTER FOR INTERNET SECURITY®

INTEGRATED INTELLIGENCE CENTER

TECHNICAL WHITE PAPER

William F. Pelgrin, CIS President and CEO

Private and Public Key Cryptography and Ransomware

December 2014

Authored by:Ted Fischer
Center for Internet Security (CIS)
Security Operations Center (SOC) Analyst

INTRODUCTION

Cryptography is a method used to encrypt, or scramble, the contents of a file in such a way that only those with the knowledge of how to decrypt, or unscramble, the contents can read them. Ransomware, a type of malware that holds a computer or files for ransom, continues to highlight the malicious use of cryptography. CryptoLocker and CryptoWall are two of the most currently reported types of ransomware. Both encrypt the files on an infected system and demand payment for the ability to decrypt the files. This paper provides an explanation of cryptographic methods and describes how ransomware uses modern cryptographic methods.

CRYPTOGRAPHY

Cryptography requires two things: a process for encryption, known as the cryptographic algorithm[1], and a way to manipulate the process, known as the key. There are two main types of cryptography in use today: private key or symmetric cryptography and public key or asymmetric cryptography. The primary difference between the two methods is how many keys are used, as private key cryptography uses one key to both encrypt and decrypt the data, and public key cryptography uses two keys, with one key encrypting the data and a different, but mathematically-related key decrypting the data.

Prior to the development of sophisticated, computer-generated algorithms, the most common type of cryptography was private key cryptography. Substitution algorithms are an early example of private key cryptography, because the same key that was used to encrypt the plaintext must be used in reverse to decrypt the encrypted text.

An early substitution algorithm is the "Caesar Cipher," since Julius Caesar is one of the first known users of the technique. Substitution ciphers work by substituting one letter for another and the key tells the user what substitution technique to use. In a Caesar Cipher the key indicates how much of a shift should be applied and in which direction.

For example, one might indicate that the key (the substitution) and the algorithm (the method) calls for shifting the alphabet four characters to the right. The encryption would then look like this:

[1] Algorithm – a procedure for solving a mathematical problem (Merriam---Webster).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

The unencrypted data is known as "plaintext" and the encrypted data is "ciphertext." By using this algorithm (a Caesar Cipher letter substitution), and key (four character shift right), one would perform the following encryption:

Plaintext: *the quick brown fox jumps over the lazy red dogs back*
Ciphertext: *wkh txlfn eurzq ira mxpsv ryhu wkh odcb uhg grjv edfn*

In order to further obfuscate the ciphertext in a substitution cipher, it is typically grouped into blocks of "n" number of characters. This prevents someone from guessing that "wkh," which is repeated twice in the above sentence, is the common three-letter word "the," and thereby guessing the key. Grouping the above ciphertext into five character blocks would yield:

wkhtx lfneu rzqir amxps vryhu wkhod cbuhq grjve dfnlr

Two random characters, "lr" in this example, are added to the end of the string to maintain the five character grouping and further obfuscate the ciphertext.

MODERN CRYPTOGRAPHIC ALGORITHMS

In modern cryptography, private key algorithms are incorporated in complex computer programs instead of simple substitution schemes, and keys are expressed in bit lengths instead of, for example, number of character shifts. Technology has also led to the development of public key cryptography.

There are several private key (symmetric) algorithms in use. One of the most common, which is also the U.S. federal government standard, is the Advanced Encryption Algorithm (AES). It is also known as the Rijndael Algorithm (after its developers, Vincent Rijmen and Joan Daemen). Most U.S. government agencies are required to use the AES algorithm to encrypt data up to Secret (128, 192, or 256-bit key lengths) and Top Secret (192 or 256 bit key lengths).[2]

Other private key algorithms include Blowfish, Data Encryption Standard (DES), and Triple DES. DES, the previous U.S. federal government standard, is no longer authorized for use by U.S. federal government agencies[3], as it was proved breakable through brute force techniques[4] in 1999. Triple DES is a variation of DES, where the data is encrypted, decrypted, and re-encrypted. Although there are no known instances

[2] Committee on National Security Systems (CNSS) Policy No. 15

[3] FIPS 46---3

[4] Brute force in cryptography is the process of deriving the plaintext from the ciphertext without knowledge of the key by trying every key until a solution is derived.

of Triple DES being broken, the inherent weakness of the DES algorithm makes it a poor choice to use in contemporary applications.

Well known public key (asymmetric) algorithms include Diffie-Hellman (D-H), the Digital Signature Algorithm (DSA), and the Rivest, Shamir, Adleman (RSA) algorithm. Whitfield Diffie and Martin Hellman developed D-H, one of the earliest published public key algorithms, in 1976. (An earlier public key algorithm was developed in the United Kingdom, but was kept secret by the British Government until 1997.) Recently, the D-H algorithm has been adapted to use a type of math known as elliptic curve, which has had the effect of reducing the key sizes that are necessary. The classic D-H algorithm requires key sizes from 1024 to 4096 bits, while Elliptic Curve D-H (ECDH) only requires key sizes from 160 to 512 bits.[5]

DSA is, as the name implies, for use in the creation of digital signatures. RSA was developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977.

STRENGTHS AND WEAKNESSES

The difference between private key and public key algorithms is the speed of encryption vs. ease of key distribution.

Private key algorithms are very efficient at encrypting large amounts of bulk data. The weakness of private key algorithms is the logistics of key distribution. For example, if Bob decides to exchange encrypted data with Alice using a private key algorithm, then they must both be in possession of the key that is used to encrypt the data, since it will be required to decrypt the data. This means that Bob and Alice must set up a secure method for transmitting the key; emailing the key will not suffice. If the emailed key is intercepted, that interceptor (or anyone who possess the private key) will be able to decrypt any data the key was used to encrypt. This issue is compounded when the key must be shared among multiple people, as everyone will have access to the same key, increasing the opportunity for key theft.

Public key algorithms are not as efficient at encrypting large amounts of bulk data, however, they do solve the key distribution issue. In public key cryptography, data encrypted by one key can only be decrypted by the mathematically related other key. Therefore, if Bob and Alice want to exchange encrypted data, and they do not have a secure method of getting a key to each other, they can opt to use a public key algorithm. In this example, Bob and Alice would each generate a "public/private key pair" with the algorithm they choose.

The terms "public" and "private" are arbitrary as far as the individual keys are concerned, but they serve as a reminder of what to do with them. The public key can be made publicly available, allowing Bob and Alice to email their respective public keys to each other, or even post them online. The private key is kept private. When Bob wants to

[5] NIST Special Publication 800---57 "Recommendation for Key Management – Part 1: General (Revision 3)"

send encrypted data to Alice, he encrypts it with Alice's public key. Bob can now safely email that encrypted data to Alice. It will not matter if anyone intercepts the data, or if anyone else has Alice's public key, because only Alice's private key (the one she kept private to herself) can decrypt the data.

Public Key Cryptography

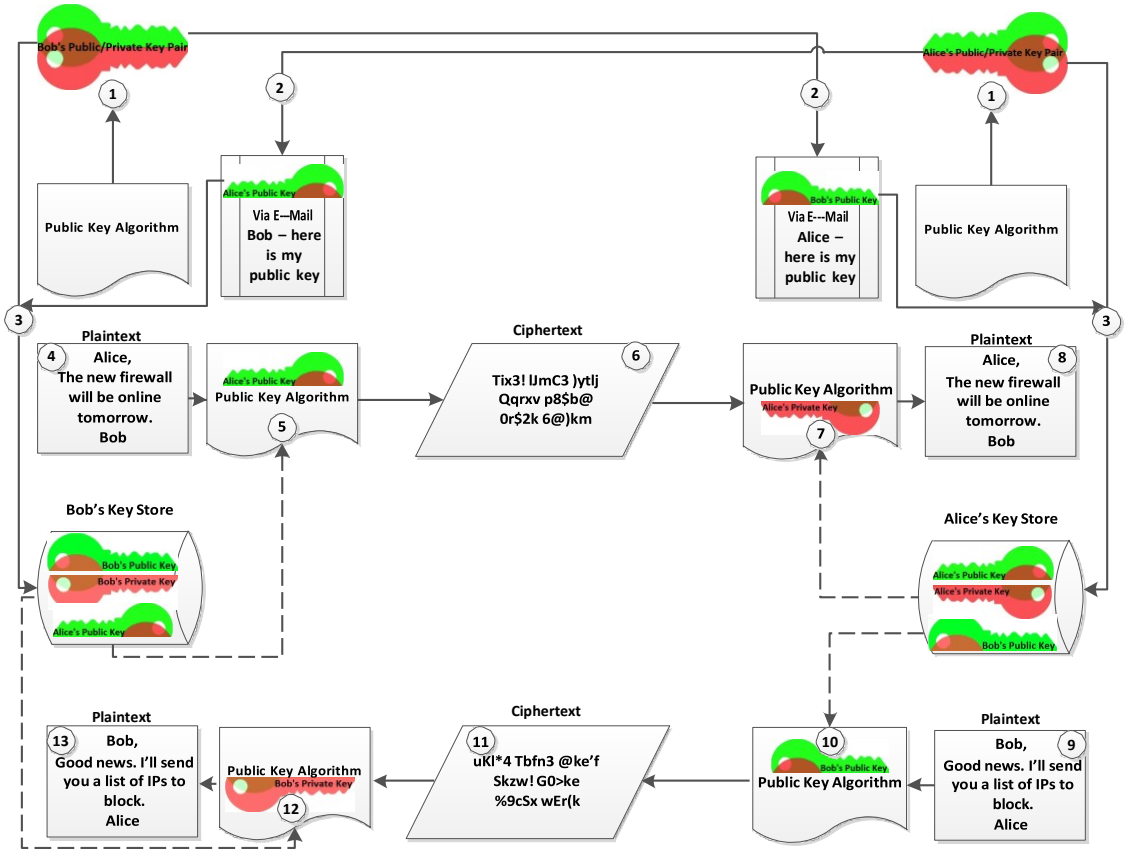


Image Source: Ted Fischer, Center for Internet Security

① Bob and Alice generate a public/private key pair from their cryptographic algorithm;
② Bob and Alice email their respective public keys to each other;
③ Bob and Alice place their own public and private keys in their local "key store" (a repository of cryptographic keys);
④ Bob creates a message for Alice;
⑤ Bob's plaintext message is encrypted to ciphertext using the cryptographic algorithm and Alice's public key;
⑥ Bob's ciphertext is sent to Alice;
⑦ Alice decrypts Bob's ciphertext using the cryptographic algorithm and Alice's private key;
⑧ Alice now has a copy Bob's plaintext message;
⑨ Alice creates a message for Bob;
⑩ Alice's plaintext is encrypted to ciphertext using the cryptographic algorithm and Bob's public key;
⑪ Alice's ciphertext is sent to Bob;
⑫ Alice's ciphertext is decrypted using the cryptographic algorithm and Bob's private key;
⑬ Bob now has a copy of Alice's plaintext message.

CRYPTOLOCKER

Cryptolocker is financially motivated ransomware that encrypts user files and demands payment in Bitcoin or Moneypak payment cards. It is propagated through spam emails purporting to come from shipping companies or regarding business processes, can be dropped by other malware, disseminated through thumb drives, or transmitted through Yahoo! Messenger.

CryptoLocker exploits features of public key (key distribution) and private key (efficient encryption of large amounts of data) cryptography as part of its ransom scheme.

When CryptoLocker infects a computer, it attempts to connect with one of several pre-configured malicious websites (generically known as a Command and Control (C2) server). The C2 server generates an RSA public/private key pair, and passes the public key to the CryptoLocker malware on the infected computer.

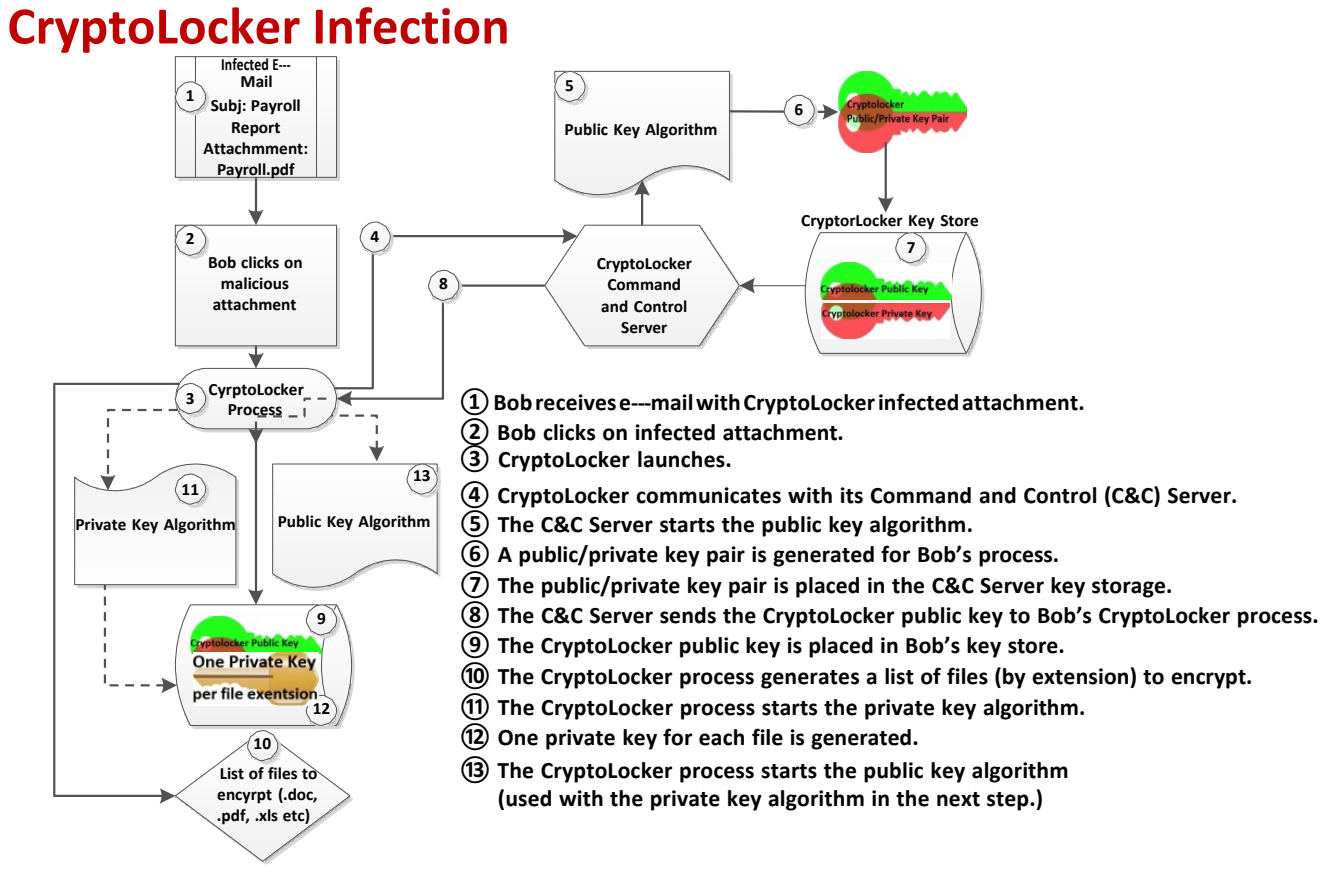
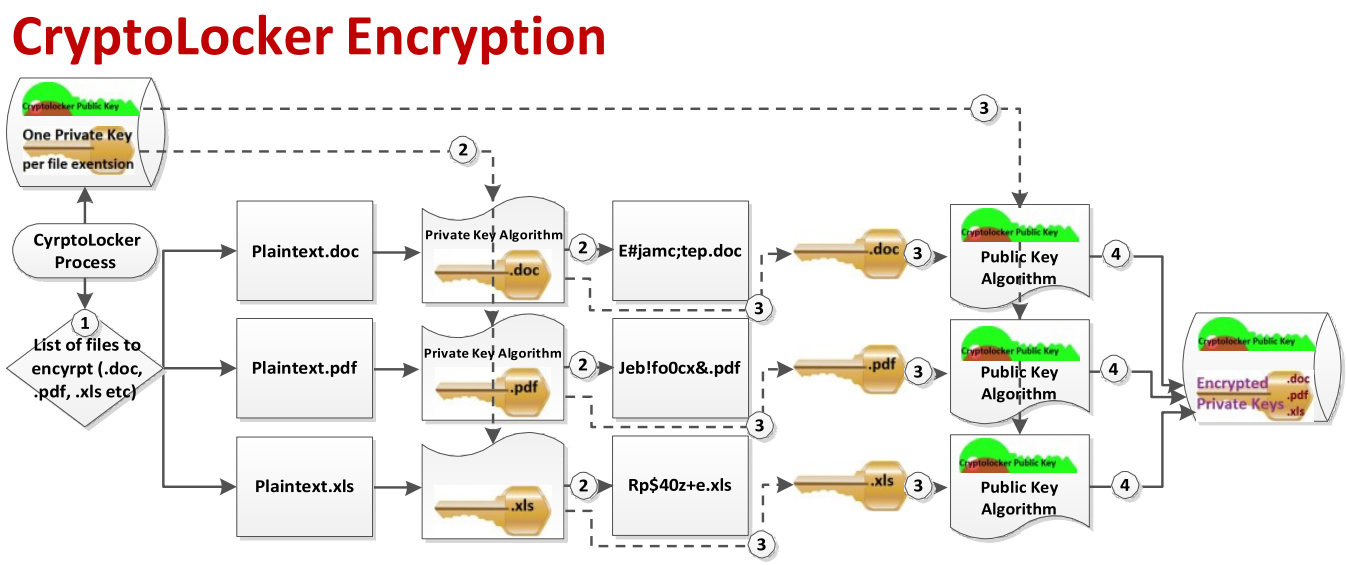


Image Source: Ted Fischer, Center for Internet Security

CryptoLocker then generates the AES private key algorithm to encrypt files on the target computer, targeting specific, common extensions (e.g. .exe, .doc, .jpg, .pdf, etc.), and generating a different 256-bit private key for each group of files per file extension. After

each group of files is encrypted, CryptoLocker uses the RSA public key it received from the C2 server to encrypt the AES private key that was used to encrypt the files.



① The files to be encrypted are identified by extension.
② Each file is encrypted using the private key algorithm and the private key for the specified extension.
③ After all of the files are encrypted, each extension's private key is encrypted using the public key algorithm and the CryptoLocker C&C public key.
④ The encrypted keys are stored in the local key store.

Image Source: Ted Fischer, Center for Internet Security

In this manner, CryptoLocker uses the key distribution strength of public key cryptography to deliver a public key to the infected computer, and the efficiency of private key cryptography to encrypt the files. The public key is not used to actually encrypt the files; CryptoLocker uses the more efficient private key algorithm for that purpose. The public key, however, is used to encrypt the private keys that were responsible for the actual encryption of the files. Efficiency is not a factor for encrypting those keys, since the public key is only encrypting a short string (the private keys).

Image source: http://www.bleepingcomputer.com/virus---removal/cryptolocker---ransomware---information

When all of the files have been encrypted, the ransomware generates a page to be displayed to the victim that indicates the price, method, and time period for payment to be made.

If the ransom is made within the indicated time, the victim will be presented with a download screen that links to the RSA private key that will be used to decrypt the AES private keys encrypted by the RSA public key. The decrypted private keys will then be used to decrypt the associated files.

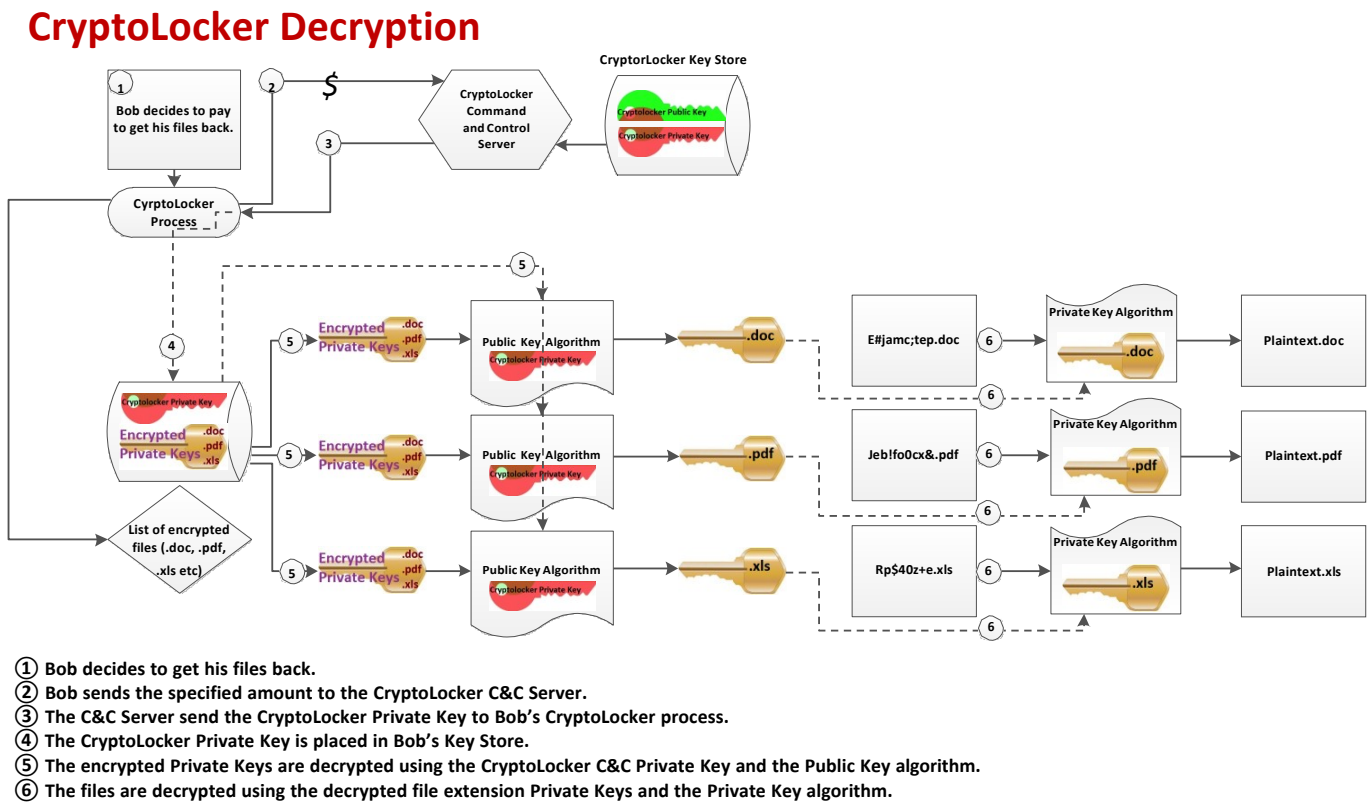


Image Source: Ted Fischer, Center for Internet Security

RANSOMWARE CRYPTOGRAPHIC ALGORITHMS

CryptoLocker is uses the RSA public key algorithm, with a 4096-bit key, and the AES private key algorithm with a 256-bit key.

Other recent ransomware variants include:

a. Powerlocker. Powerlocker uses a 2048-bit RSA key, and the Blowfish private key algorithm (default key size is 128-bits)
b. Cryptowall. Cryptowall uses a 2048-bit RSA key to directly encrypt files.
c. Onion Ransomware. The Onion Ransomware, so called because it uses the TOR Network (the "Onion" router) for anonymity, uses the ECDH with a 256-bit key, and AES with a 256-bit key.

There are no known successful brute force attacks against RSA, ECDH, Blowfish, or AES-encrypted data. Therefore, in the absence of a current backup of your data, paying the ransom is the only potential way to decrypt the compromised files. However, open

source intelligence suggests paying the fee does not always result in the restoration of files. (CIS does not opine as to whether victims should or should not pay the ransom.)

RECOMMENDATIONS

CIS recommends the following actions:

- Educate users to verify the legitimacy of an email, since the emails used in ransomware scams originate from spoofed email accounts,
- Block traffic to known ransomware C&C server IP addresses at your network perimeter devices.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Remind users to be cautious when clicking on links in emails coming from trusted sources.
- Ensure anti-virus software is installed and definitions are up to date.
- If infected with ransomware, remediate the infection via antivirus. Following the remediation, restore any encrypted files from backup or system restore points and volume shadow copies.
- Have regular system backup routines in place.
- Disconnect any drives that are used for backup storage after the backups are made, as ransomware will attempt to find and encrypt files on mapped drives.

REFERENCES

[1] http://msisac.cisecurity.org/daily---tips/cryptowall---indicators.cfm

[2] https://blogs.cisco.com/security/rig---exploit---kit---strikes---oil.

[3] http://www.bleepingcomputer.com/virus---removal/cryptolocker---ransomware---information

[4] http://blog.emsisoft.com/2013/09/10/cryptolocker---a---new---ransomware---variant/

[5] https://www.schneier.com/blog/archives/2014/01/powerlocker_use.html

[6] http://pastebin.com/Dnhh0MWd (PowerLocker Announcement)

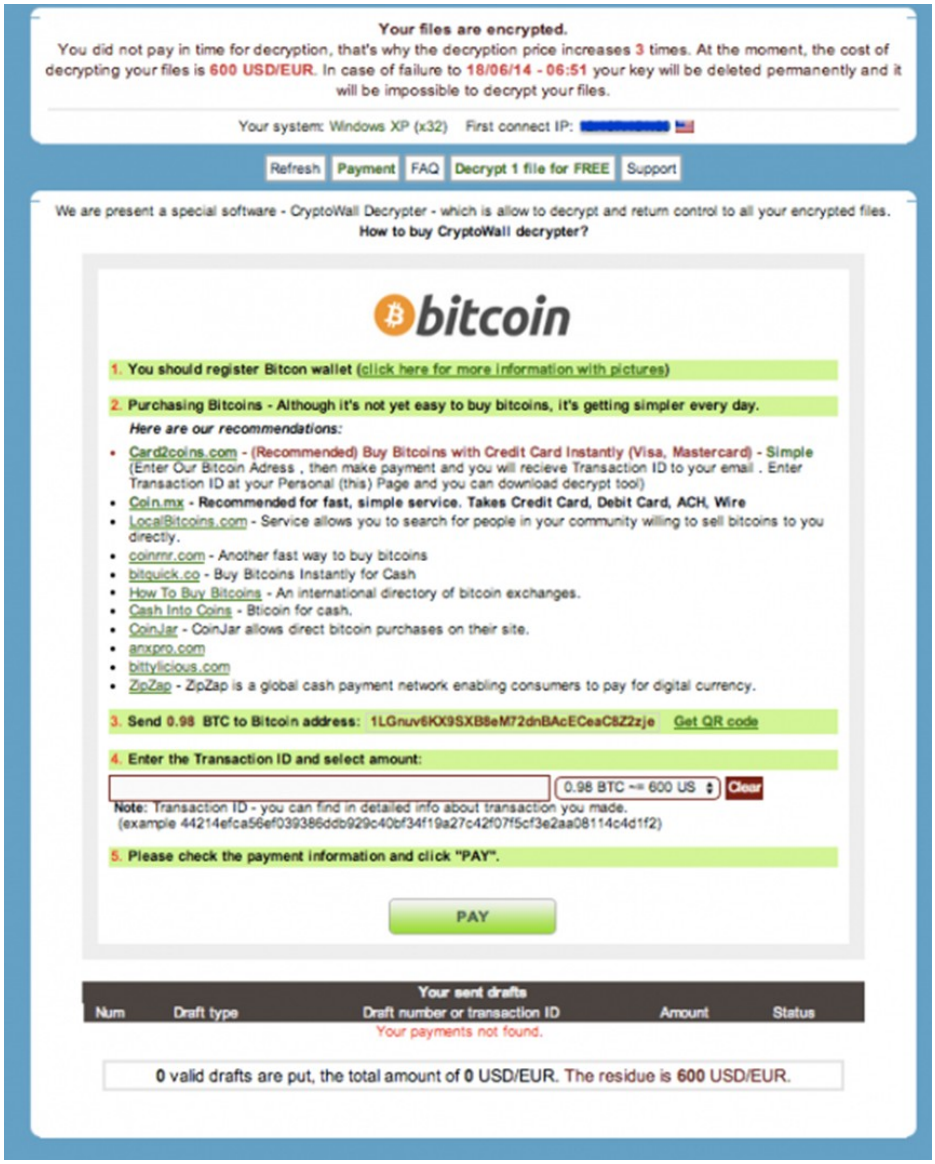
[7] http://www.technibble.com/cryptolocker---update/

[8]http://www.tripwire.com/state---of---security/vulnerability---management/new---cryptolocker--- variant---spread---yahoo---messenger/

[7] https://securelist.com/analysis/publications/64608/a---new---generation---of---ransomware/

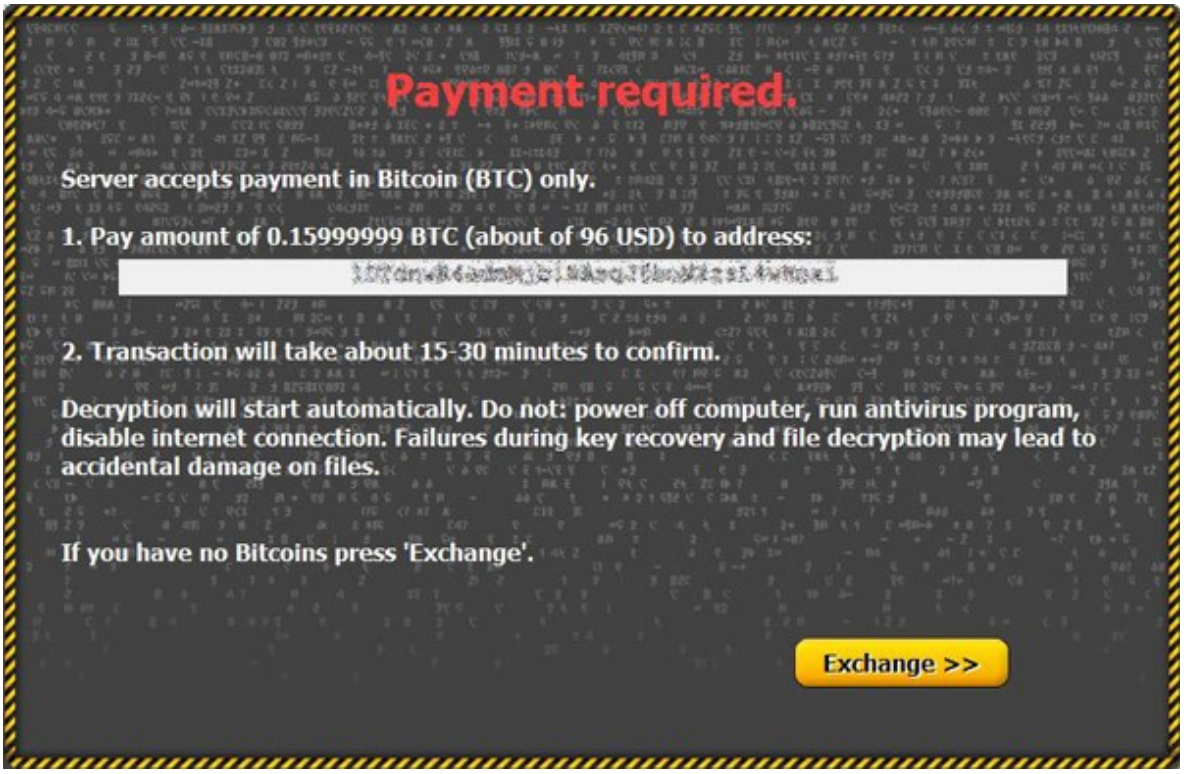
APPENDIX A: Sample Ransomware Generated Pages

CryptoWall Image source: https://blogs.cisco.com/security/rig---exploit---kit---strikes---oil



Onion Ransomware (Trojan---Ransom.Win32.Onion) Image Source: https://securelist.com/analysis/publications/64608/a---new---generation---of---ransomware/

Window informing the victim that files on the computer have been encrypted



The cybercriminals' demands

Image set as desktop wallpaper