CryptoLocker and the Rise of Cryptographic Ransomware

Michael Tran

December 11, 2014

Abstract

This paper examines the recent history of ransomware and its methods of distribution and prevention. Ransomware is a type of malware which forces victims to pay large sums of moneys. Some forms imitate law enforcement and convince victims to pay fines, whereas others encrypt the victims' files and ask for a payment for their decryption. This paper mainly focuses on cyptographic ransomware. Specifically, it will focus on the inner-workings of Cryptolocker, which was widely considered the first effective cryptographic ransomware. Understanding Cryptolocker will provide a foundation to more recent derivatives like Cryptowall. I will review the GameOver ZeuS botnet and the principles of cryptocurrencies to provide some background to why and how ransomwares have become such a major risk to not only personal computers, but mobile devices as well. Further, this paper will go over the effectiveness of prevention and recovery techniques. Understanding and being aware of ransomware is important as the demonstrated effectiveness and profitability of Cryptolocker has inspired a wide variety of new dangerous ransomwares. This new breed of profitable organized malware has already proven to be a major risk to not only home users, but also private and government agencies. This paper will provide background on this class of malware and, more importantly, methods to prevent its spread.

Contents

1 Introduction

Cryptographic ransomware, though first envisioned by Moti Yung and Adam Young in 1996, has only recently been fully realized and developed [1]. Over the past few years, ransomware attacks have become much more complex, effective, and frequent. Factors such as anonymous payment processing and new sophisticated encryption methods, have contributed to the rapid growth of cryptographic ransomware this year.

Crpytographic ransomware for the most part was unseen in the wild until 2005. By 2006 there were a large variety of worms and trojans such as PGPCoder, Krotten, Cryzip, and Reveton, that though were largely unsophisticated, were successfully implemented and distributed [2]. Though, these malwares were generally ineffective given broken symmetric encryption methods and relatively easy retrieval of keys, they represent an important proof of concept for this type of extortionary malware. As progress is made in network anyonyminity and encryption algorithms, cryptographic ransomware has burgeoned into one of the most lucrative fields for malware authors.

CryptoLocker a recent and widely publicized implementation of the concept was a devastating malware which successfully extorted millions of dollars and likely caused the loss of billions of files. CryptoLocker used advanced encryption methods and a state-of-the-art botnet to infect and encrypt millions of users. Though CryptoLocker's author, Evgeniy Bogachev, is now on the FBI's most wanted list, and CryptoLocker has been taken down, it has spawned countless copycats and the security community is likely to see many more derivatives over the next few years [3].

2 Functionality

2.1 Encryption and Decryption

CryptoLocker is largely effective because of its method of encryption. Most modern cryptographic ransomware variations use both asymmetric and symmetric key algorithms in com-

bination to increase the robustness of the malware. CryptoLocker, in particular, uses both the AES-256 symmetric and the RSA-2048 asymmetric key algorithms. Cryptolocker generates many 256-bit AES keys which are used to encrypt all of the targeted files. Each of the victims files are first encrypted with a specific and unique AES key. These keys are then further encrypted using a uniquely generated RSA-2048 public key which is sent from the author's server [4]. The malware then writes the RSA encrypted key to the AES encrypted file. This pairs each of the files with its newly encrypted AES key for decryption later. CryptoLocker's double encryption ensures that the private key is never transferred over the network and that victims have no feasible method of decryption without the associated private key.

Both these cryptographic algorithms are extremely secure and decryption without the private key is all but impossible. The AES-256 algorithm is essentially overkill and is so effective that the National Security Agency has approved the algorithm for top-secret data. This algorithm yields 2^{256} different possible key combinations and has proven virtually impossible to brute force in any reasonable amount of time. To decrypt RSA based keys, factorization is usually used. Even without brute force, breaking the RSA-2048 keys requires the factorization of extremely large prime numbers. It has been estimated that given the computing power of a standard desktop computer, an RSA key based certificate would take upwards of 15 million desktop computers roughly a year to decrypt [5]. Cryptographic ransomware effectiveness relies on these types of advanced cryptographic algorithms and their robustness.

2.2 Method Of Delivery

The author of CryptoLocker relied on the botnet GameOver ZeuS to distribute and function as the Command and Control server [6]. Botnets in the simplest definition, are systems of machines connected by a network which can as a whole be controlled by a single entity. Botnets have a variety of purposes and have functions. The early historical examples of botnets mainly used the Internet Relay Chat protocol, because it was is relatively simple way to maintain a communication network. Because of this, IRC botnets were extremely useful before the days of instant messaging. They were used to maintain, IRC channels by keeping them open and managing the privileges of each user in the channel.

Since then, botnets have been appropriated for a variety of other uses. Today, botnets are more regularly associated with the spread of malware and distributed denial of service (DDOS) attacks. They are naturally useful in malicious activity as botnets are generally easy to build and can infect users quickly and remotely. Machines on the botnet receive and send information to and from the command and control server. The command and control server of the botnet has the ability to access and use the machines of unaware users to further spread malware, grow the botnet, and access their sensitive information.

In this case, GameOver ZeuS was used to spread CryptoLocker and store the RSA key pairs it generated. GameOver ZeuS is a peer-to-peer (P2P) variant of the well known ZeuS botnet, which mainly deals with stealing bank and login credentials. Botnets, such as GameOver ZeuS, can be loaned or rented by malware authors for other criminal purposes. In this case, GameOver ZeuS allowed CryptoLocker's author to distribute the malware and generate/store all the 2048-bit RSA key pairs.

2.3 Payment

The rise of cryptocurrencies and the anonymity that they allow has allowed cryptographic ransomware to advance greatly over the past few years. CryptoLocker accepted two forms of ransom payments, Moneypak and Bitcoin. The malware authors preferred Bitcoin payments and understandably adjusted the ransom to discourage Moneypak payments. By encouraging Bitcoin payments, Bogachev was able to protect his identity and secure the large sums of money much more simply and quietly. Even today, an estimate of how much ransom Bogachev received is uncertain. Bitcoin and cryptocurrencies in general have already been greatly publicized for being an anonymous and effective way payment method for criminal activity, as these currencies grow and become more widely used tracking extortionary malware will become more common as well.

3 Defenses

The danger of CryptoLocker and its variants come from the fact that there is little chance of recovery from these malwares once they have encrypted the victims files. Because of this, the most reliable protection is regular physical backups of sensitive and important data. After having their data encrypted, victims are either forced to pay the ransom, restore from a backup, or lose the data. Though CryptoLocker was eventually taken down by a team of researchers, many users do not have the option to wait quietly delaying their work schedule in hopes of an eventual fix. Though users have few options once their files are encrypted, the security community has worked together to improve the state of defense against cryptographic ransom wares.

As a community there are ways to combat specific variants of this malware. Specifically, in the case of CryptoLocker, though it took just over under 10 months to do so, CryptoLocker was eventually isolated by the joint international collaborative effort of Operation Tovar. Though Operation Tovar was able to find GameOver's C&C servers and restrict the communication and propogation of CryptoLocker, it took another month before an actual fix was found for those already infected. In August 2014, 13 months after CryptoLocker was first spotted, FireEye Security along with Fox-It released a web app which was able to provide a fix to many, but not all, victims of CryptoLocker. The website, called DecryptCryptoLocker, allows victims to upload one of their encrypted files along with their emails [7]. The application then searches through all the keys available to it, checking for a match. If a match is found the victim is then emailed the private key necessary to unencrypt their files. Though this did not provide a perfect fix for all victim, it was a major breakthrough and the first real solution to a sophisticated cryptographic ransomware implementation. Since then, many security firms have been developing more preemptive fixes to the oncoming scourge of cryptographic ransomwares.

Examples of such a software are CryptoPrevent and CryptoGuard. CryptoPrevent is a free anti-malware windows utility which, as the name implies, attempts to prevent any unwanted encryption from occurring. The software does so by using definition based protection against executables and protecting against fake file extensions e.g. note.pdf.exe [8]. On the other hand, CryptoGuard, developed by the security firm HitmanPro, hopes to prevent ransomwares

from encrypting your files encryption is happening. [9] CryptoGuard decided that recognizing malware signatures is impossible given the creativity of malware authors and their ability to use polymorphic engines, instead Cryptoguard monitors file system behavior and alerts the user when any suspicious encryption occurs.

4 To the Community

Cryptographic ransomware is quickly becoming one of the, if not already, the single greatest threat to data security. CryptoLocker has proven to be an extremely lucrative malware, generating an estimated $27 million USD through bitcoin and moneypak transactions. CryptoLocker alone infected over 250,000 machines [10]. Variants are becoming widespread, malware authors are finding that this cryptographic ransomware is easy to implement given advances in both the methods of payments and encryption. The anonymizing nature of cryptocurrencies allows for an easy and secure method of extortion. To defend against such a threat, precautions should be taken in backing up and securing any data users find important. Malware authors are no longer just targeting obviously valuable data such as credit numbers or banking information, but are also targeting the work of everyday users. Cryptographic ransomware has the ability to target files that many users thought worthless to others. Indeed, it easy to imagine that significant revenue could be generated by simply encrypting things like vacation photos or small business spreadsheets and extorting their owners for bitcoins. Such examples represent the more private effects of cryptographic ransomware is, and how important data security and widespread backups are, even for every day users.

The variant CryptoWall demonstrated just how effective CryptoLocker derivatives can be and has, in many ways, proven itself more devastating than its predecessor. By embedding itself into ads on commonly used websites such as Yahoo! and Match.com, CryptoWall has infected over 800,000 users and has encrypted well over 5 billion files [10]. It's authors have also just recently released a CryptoWall 2.0 which is a more effective TOR based version. CryptoWall is proof that, though CryptoLocker was eventually taken down, the global effort to stop cryptographic ransomware and the likes was not enough to prevent malware developers

from adapting ransomware into more effective forms. Certainly, success and news recognition of these ransomwares will only encourage malware developers to produce their own variation. As variants become more and more common defenses against ransomware must advance as well.

5 Conclusion

In conclusion, cryptographic ransomware has become a very real and serious problem. The security community should be aware of this new type of malware and its rapid growth. If enough exposure is given to the topic, the scourge of cryptographic ransomware will likely be mitigated quickly. As of now, malware developers can use a model similar to CryptoLocker and extort users on a variety of platforms. The network anonyminity that cryptocurrencies allow has made it much more difficult for malware developers to be caught. Even in the case of CryptoLocker, it is unlikely that its author, Bogachev, would have been identified if he did not use notorious botnet GameOver ZeuS as his command-and-control server. This is a serious problem, CryptoWall currently uses a TOR based command-and-control server and it is unlikely that it will be taken down soon; especially given that there currently is not a global movement, like Operation Tovar, to prevent its spread.

References

[1] A. Young and M. Yung. Cryptovirology: extortion-based security threats and countermeasures. pages 129–140, May 1996.

[2] Blackhat USA 2014 - the new scourge of ransomware.

[3] EVGENIY MIKHAILOVICH BOGACHEV.

[4] CryptoLocker a new ransomware variant.

[5] Just how strong is 2048-bit SSL certificate encryption?

[6] Krebs on Security. Your locker of information for CryptoLocker decryption executive perspective | FireEye inc.

[7] Your locker of information for CryptoLocker decryption executive perspective | FireEye inc.

[8] Foolish IT LLC. CryptoPrevent.

[9] HitmanPro.alert CryptoGuard - SurfRight.

[10] CryptoLocker's crimewave: A trail of millions in laundered bitcoin.