Evidential Study of Ransomware

Cryptoviral Infections and Countermeasures

Ransomware infections are rising exponentially. Attackers are motivated to extort money from individuals and organizations by infecting the systems with malicious code and altering the state of data for ransom.

Ransomware is a class of malware (malicious software) that encrypts user data and demands payment in return for the decryption key. Cryptoviral extortion campaigns have been steadily rising since 2005.[1] Financially motivated cybercriminals are naturally attracted to ransomware[2] and rely on the anonymity provided by cryptocurrencies[3] to collect the ransom. In recent news, variants such as WannaCry[4] and NotPetya[5] have made a significant impact and helped familiarize the general public with the growing threat of ransomware. WannaCry demonstrated that attackers are now exploring other attack vectors that go beyond traditional phishing[6] and that organizations need regular patch management and other security assessments. For instance, targeted ransomware attacks such as SamSam are exploiting weakly secured remote services.[7] As cybercriminals generate income following a ransomware campaign, a part of this income is allocated toward research and development for the next ransomware project. This investment includes improving the cryptosystem, offering victims more services to ease the payment process, advertising and organizing Ransomware as a Service (RaaS) in the underground markets, exploring new attack vectors, and more.

A key-based management taxonomy has been proposed[8] that classifies ransomware variants into different categories based on their inherent cryptosystems. A holistic picture of the threat of cryptoviral extortion campaigns is provided by exploring various characteristics of modern ransomware via empirical analysis of real-world ransomware samples. A number of ransomware families are investigated to unearth the inherent design and behavioral characteristics of modern ransomware. In addition, preventative and corrective countermeasures can facilitate effective action against the menace of ransomware.

Aditya K. Sood, Ph.D.,
Is a security researcher and consultant. Sood has research interests in cloud security, malware secure software design and cybersecurity. He has authored several papers for IEEE, Elsevier, CrossTalk, ISACA®, Virus Bulletin and others. His work has been featured in several media outlets including AP, Fox News, The Register, Guardian, CBC and others. He has been an active speaker at industry conferences and presented at BlackHat, DEFCON, HITB, RSA, Virus Bulletin, OWASP and many others. Sood is also an author of *Targeted Cyber Attacks*, a book published by Syngress.

Pranshu Bajpai
Is a security researcher working toward his Ph.D. in computer science and engineering at Michigan State University (USA). His research interests lie in computer and network security, malware analysis, digital forensics and cybercrimes. In the past, he worked as a penetration tester. He has authored several papers in security magazines and journals and has served as a technical reviewer for books within the security domain. He has been an active speaker at industry and academic conferences and has spoken at IEEE APWG eCrime conference, Bsides, GrrCon and others.

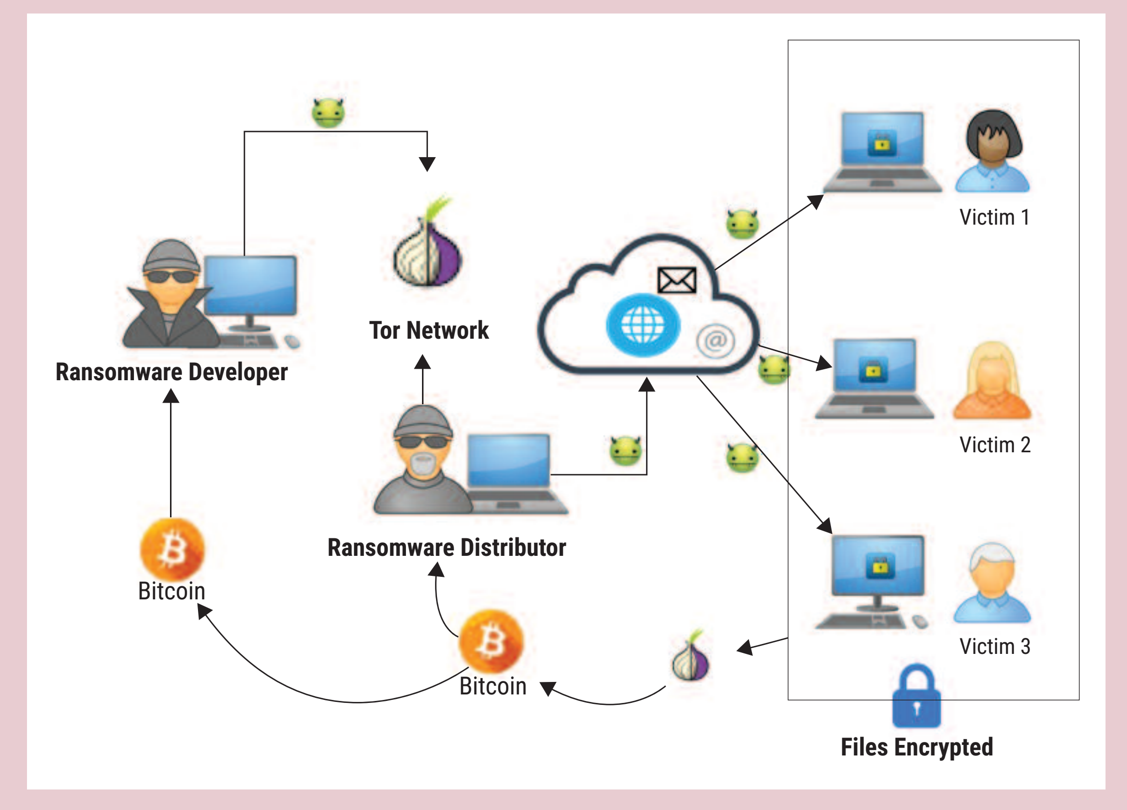
Richard Enbody
Has been a professor at Michigan State University since 1987 in the department of computer science and engineering in the College of Engineering. His current research is in cybersecurity, especially how hackers hack and how to defend against them, with particular interest in ransomware, cryptojacking and automotive vulnerabilities. He also studies how students learn to program. He has authored several papers for IEEE, ACM, Elsevier, CrossTalk, ISACA, Virus Bulletin and others. Enbody is also an author of *Targeted Cyber Attacks*, a book published by Syngress.

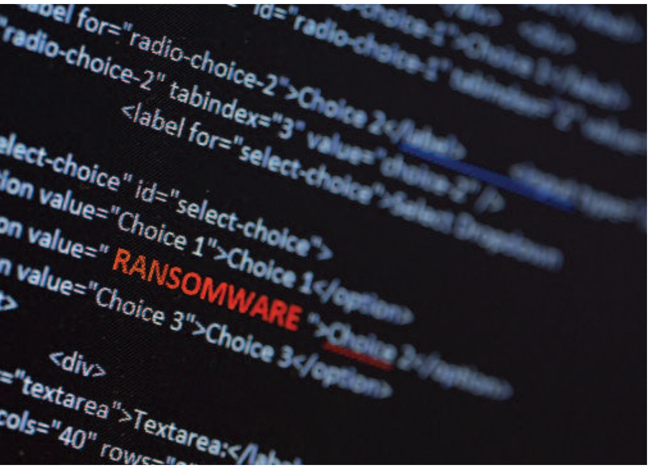
Ransomware Infection Model

With RaaS on the rise, many effective ransomware strains are created by professional malware developers. These developers provide their ransomware to buyers in the underground markets for either a fixed one-time amount or through an affiliate program. An affiliate program ensures that developers earn an agreed-upon percentage of the ransom collected during each campaign carried out by the operators. These operators act as soldiers for the ransomware developers, spreading the infection through a variety of attack vectors as described in the distribution mechanisms list. A basic ransomware life cycle model is presented in **figure 1**. This ransomware operation model works using the following steps:

1. **Infiltrate host**—The ransomware binary needs to execute on the victim's computer to start the encryption process. Ransomware developers have traditionally deployed phishing attacks to deliver the malware. However, they are now expanding the attack surface by exploiting critical security vulnerabilities and brute-force attacking a Remote Desktop Protocol (RDP).
2. **Acquire encryption key**—Once the ransomware binary has infiltrated the host machine, it seeks to acquire a data encryption key. This data encryption key is usually a symmetric key, since symmetric encryption provides fast encryption. The encryption key can be acquired in the following ways:
   - Embedded in the ransomware (making it susceptible to recovery via reverse engineering)
   - Generated on the host system by exploiting resident crypto application programing interfaces (APIs)
   - Acquired from a command and control (C&C) server over the network
3. **File encryption**—Once the data encryption key is acquired, the ransomware commences the data encryption procedure. This process performs a file search that seeks specific file types, such as

Figure 1—Working Model: Ransomware Life Cycle





bel for="radio-choice-2"
radio-choice-2" tabindex="3" value="choice-2" />
<label for="select-choice">
elect-choice" id="select-choice">
ion value="Choice 1">Choice 1</option>
on value=" RANSOMWARE ">Choice 2</option>
n value="Choice 3">Choice 3</option>
<div>
="textarea">Textarea:</label>
cols="40" rows=

.docx, .xlsx, .pdf and .jpg. The purpose is to encrypt only user files and leave the system files unaltered so that the host machine is still usable. This process aligns with effective biological viruses that do not kill or debilitate the host promptly. Once the scan concludes, the ransomware then goes through the list and performs file encryption one file at a time using the symmetric key. After file encryption is complete, the symmetric key is destroyed on the host to prevent key recovery by the victim. Once the symmetric key is wiped from the host system, the attacker becomes the sole possessor of the key, which provides the needed leverage over the victim.

4. **Display ransom note and collect payment**—A ransom note is then made available to the victim in plain sight explaining what has happened and how the files can be recovered. Recovery involves sending the ransom payment, usually using cryptocurrencies, over a secure, anonymous channel such as The Onion Router (Tor). In the ideal scenario, attackers provide the symmetric key to the victim after receiving payment. However, in practice, successful payment to an attacker does not guarantee file recovery.[9]

Ransomware Characteristics

Ransomware characteristics include how the ransomware is distributed, the three levels of extortion tiers observed, master boot record (MBR) manipulation, common cryptosystems deployed, payment methods, the rise of RaaS and ransomware support services.

Distribution Mechanisms

The distribution mechanism refers to the techniques selected by attackers to distribute ransomware. A number of tactics have been used, and the leading ones include:

- **Drive-by download attacks**—Drive-by download attacks[10] refer to the attacks that constitute coercing a user to visit a domain that is serving malicious code in a stealthy manner. When the browser renders the webpage, the unauthorized code is executed, which then downloads malware in the form of a payload. A direct drive-by attack refers to the downloading of ransomware directly from the malicious domain without any exploitation of a vulnerability. Indirect drive-by refers to a stealthier way of downloading the ransomware by exploiting an inherent vulnerability in a browser or system component. Drive-by downloads are generally implemented using exploit kits.
- **Phishing attacks**—These attacks are prevalent and involve social engineering tactics to trick the user to either open an attachment or entice them to click an embedded URL to fetch the content. In both cases, the downloaded attachment can execute malicious code to download the ransomware either by exploiting a vulnerability in a system component or abusing the functionality of operating system (OS) components. In both scenarios, a successful execution results in downloading ransomware onto the system. Phishing and drive-by download attacks are often used together. The phishing email directs a user to an infected site.
- **Malvertisements via a rogue online portal and websites**—The attackers can also deploy malicious code on a rogue online portal or website that includes content delivery networks (CDNs), compromised websites, domains registered for malicious use and others. The malicious code can be deployed in the form of malicious advertisements[11] that are displayed to the end user in the browser but trigger unauthorized activities in the backend. Using a rogue online portal or website both aim to download ransomware through different channels and sources.

- **Online social networks (OSNs)**—Ransomware can also be downloaded via OSNs. Generally, unvalidated and malicious links are shared between users' profiles. If the user clicks the shared link (or graphic video), the browser is redirected to the malicious domain, which results in the downloading of ransomware onto the end-user machine. To be precise, OSNs can be used as launchpads[12] for conducting drive-by download attacks.
- **Cloud storage apps**—Ransomware can be easily distributed by cloud storage applications (apps).[13] Attackers abuse the cloud storage apps to host the ransomware and share the links publicly with users via phishing emails. Users are tricked into believing that a file is stored in a legitimate cloud storage app, where it should be secure. In fact, accessing the link results in the downloading of ransomware.
- **Critical vulnerabilities**—Ransomware developers are making their malware more efficient by targeting unpatched code execution vulnerabilities in the OS. This way, they do not have to rely on user gullibility. A prime example of this is the EternalBlue exploit used by WannaCry and Petya.[14]
- **Brute-force attacking passwords**—Remote services such as Secure Shell (SSH) and RDP secured with weak passwords are brute-force attacked to deliver malware content.[15]

Extortion Tiers

The extortion tiers define the level of extortion performed by the ransomware in the system. The extortion levels are categorized based on the data encryption and stealing mechanisms used. The three tiers are:

- Tier 1 extortion is the process of only encrypting data in the system and extorting money. The ransomware operator decrypts the data once the ransom is paid and has no control of the data later.
- Tier 2 extortion not only includes data encryption but also data stealing. That is, once the ransom is paid, the data are unencrypted so control of the data is partially returned to the victim, but the ransomware steals the copy of data to still retain some control.
- Tier 3 extortion is a process in which ransomware does not decrypt the data even after obtaining the ransom from the user. It means that ransomware permanently encrypts data, which is effectively a denial of control over the data.

MBR Manipulation

A master boot record (MBR) code is used to store information about the booting of the operating system (OS), which involves logical partition type and size, filesystem layout, presence of executable code, etc. Tampering with the MBR code can have a considerable impact on the state of the OS that is loaded in the memory. Generally, an MBR contains an executable loader code that loads the OS. Internet of Things (IoT) bots manipulate the MBR code either by tampering with the code or by rewriting the record to perform nefarious operations once the OS is loaded in the memory. For example, some IoT bots rewrite the MBR in the compromised device with a malicious boot record. When the OS is loaded, the malicious boot record hijacks the system process and displays the ransom note while freezing the OS resources. Other adverse impacts of MBR manipulation include forceful rebooting, device bricking, custom code execution and others. It is important to dissect IoT bots to understand the risk and impact on the compromised devices.

> “MODERN RANSOMWARE USES A COMBINATION OF SYMMETRIC AND ASYMMETRIC CRYPTOGRAPHY TO ACHIEVE ITS OBJECTIVE.”

File Encryption and Cryptography

Modern ransomware uses a combination of symmetric and asymmetric cryptography to achieve its objective. An advanced encryption standard (AES) symmetric key is used to encrypt the victim's files. This key is then encrypted using the attacker's public key and either stored on the system or delivered to the attacker's C&C server. The unencrypted symmetric key is then removed from the host to ensure that the victim cannot decrypt the files without paying the ransom. In some cases, such as Petya and PetrWrap, elliptic key cryptography is deployed in place of Rivest-Shamir-Adleman (RSA) as the public key scheme.

The pseudocode presented in **figure 2** shows the process of file encryption as performed by common ransomware that deploys a hybrid encryption methodology on a Windows host. The symmetric AES key is generated on the host system using the CryptoAPI on the host, and then files are encrypted using this key. The key is then securely stored on the host by encrypting it using an asymmetric RSA public key that shipped with the ransomware. The unencrypted key is destroyed. A ransom note is then displayed for the user with payment instructions.

Payment Mechanism

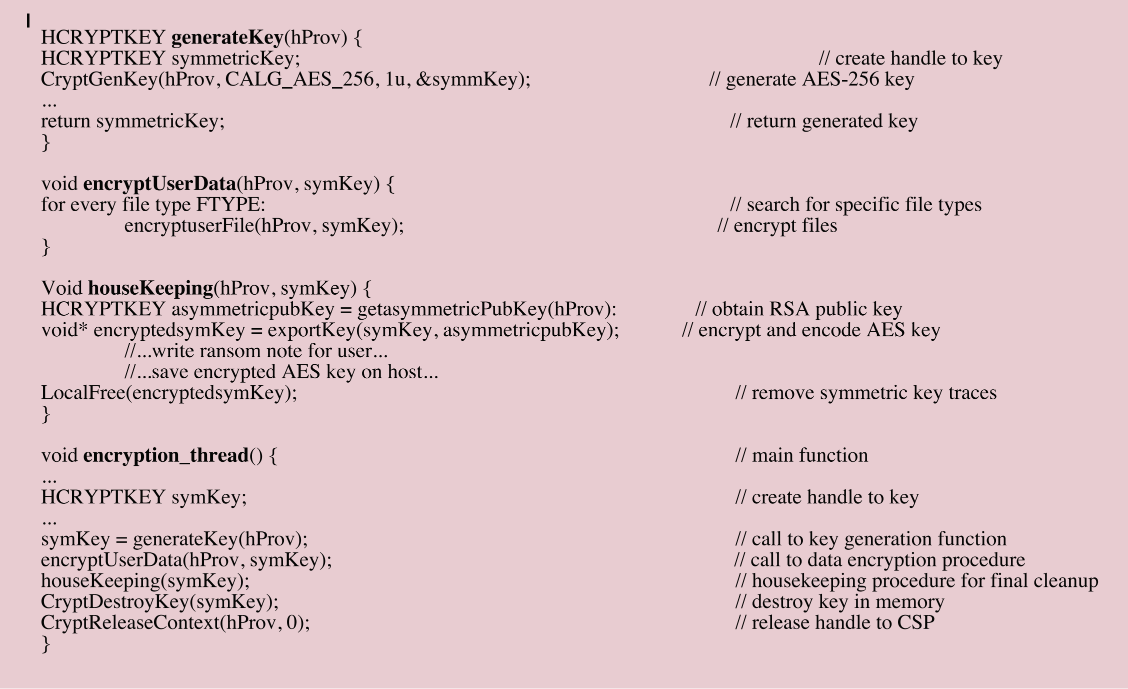
A payment mechanism is needed by attackers to obtain ransom from the victims whose systems have been compromised and infected with ransomware. The attackers have multiple options to obtain payments. Once the ransom is paid, the attacker provides the key for decrypting the data.

Some of the payment mechanisms include:

- The attackers can provide an account number to the end user so that money in the form of eCurrency such as Bitcoin or MoneyPak can be submitted as ransom. This option expects the user to create a Bitcoin or similar account and follow the deposit instructions accordingly. Using anonymous cryptocurrency removes the need for further anonymization.
- The attackers can also force the end users to download Tor client on their machine and ask them to initiate an encrypted and anonymized communication channel via a Tor browser. This process harnesses the power of Tor communication to enable anonymous payments.
- The attacker can ask for payment in any e-currency. The end user has to provide the identity number provided by the ransomware after installation as a part of a notification process to obtain the secret to decrypt the data.

In this way, no transactions are performed directly with regulated and federated banks. The money is exchanged using e-currency.

Figure 2—Pseudocode for File Encryption



```
HCRYPTKEY generateKey(hProv) {
HCRYPTKEY symmetricKey;                                          // create handle to key
CryptGenKey(hProv, CALG_AES_256, 1u, &symmKey);          // generate AES-256 key
...
return symmetricKey;                                       // return generated key
}

void encryptUserData(hProv, symKey) {
for every file type FTYPE:                                 // search for specific file types
        encryptuserFile(hProv, symKey);                   // encrypt files
}

Void houseKeeping(hProv, symKey) {
HCRYPTKEY asymmetricpubKey = getasymmetricPubKey(hProv):         // obtain RSA public key
void* encryptedsymKey = exportKey(symKey, asymmetricpubKey);   // encrypt and encode AES key
        //...write ransom note for user...
        //...save encrypted AES key on host...
LocalFree(encryptedsymKey);                                 // remove symmetric key traces
}

void encryption_thread() {                                  // main function
...
HCRYPTKEY symKey;                                           // create handle to key
...
symKey = generateKey(hProv);                                // call to key generation function
encryptUserData(hProv, symKey);                             // call to data encryption procedure
houseKeeping(symKey);                                       // housekeeping procedure for final cleanup
CryptDestroyKey(symKey);                                    // destroy key in memory
CryptReleaseContext(hProv, 0);                              // release handle to CSP
}
```

Figure 3 shows the payment mechanism details displayed by the ransomware.

RaaS

RaaS is defined as a service model in which malware developers (cybercriminals) charge other cybercriminals (buyers) for access to existing infrastructure so the buyers can distribute ransomware across the Internet. As discussed previously, the buyers do not have to deal with the management of infrastructure and building binaries. These tasks are available as part of the RaaS. Generally, the developers rent the infrastructure, which they control, to the buyers so that the buyers can operate the infrastructure. The buyers are provided with specific operational functionalities that they can use to meet their requirements. A number of characteristics of RaaS are:

- Buyers are provided with infrastructure that is managed by the developers. The infrastructure may be built out of compromised data centers.
- Buyers can request developers to customize the ransomware (binary).
- Buyers can request developers to distribute ransomware (binary).

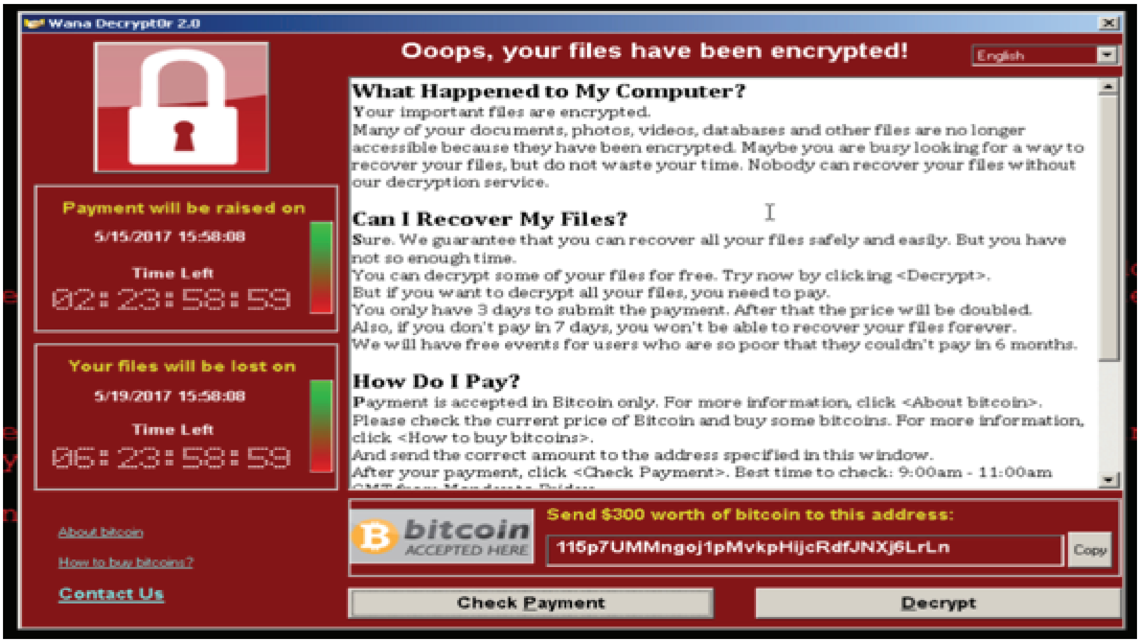
Generally, in this case, the malware developers are not directly involved with the ransom process; rather, they are interested in making money by providing ransom infrastructure as a service.

Ransomware Support Service

Ransomware support is a service that is provided by the developers to the end users to better understand what steps are required to be performed to retrieve data. It is basically a manual shipped with the ransomware or shared later. Developers can select various ways to present this content to the end users. A few of them include, but are not limited to:

- **Embedded static pages**—The details about the ransomware and payment expectations are written explicitly in the software by embedding a static component. The details are highlighted using the static component once the ransomware is installed in the system.
- **Dynamic queries**—In this process, end users are asked directly to join developer-controlled chat sessions or messaging rooms and all the related discussions about payment and others are discussed there. This system is more of an interactive approach and is similar to what online business do.

Figure 3—Payment Notifications Displayed by Ransomware



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

- **Hybrid service**—In this service mode, the developers can provide details using embedded static pages and the provision of chat rooms. The end user can select a suitable choice of data exchange with the attackers.

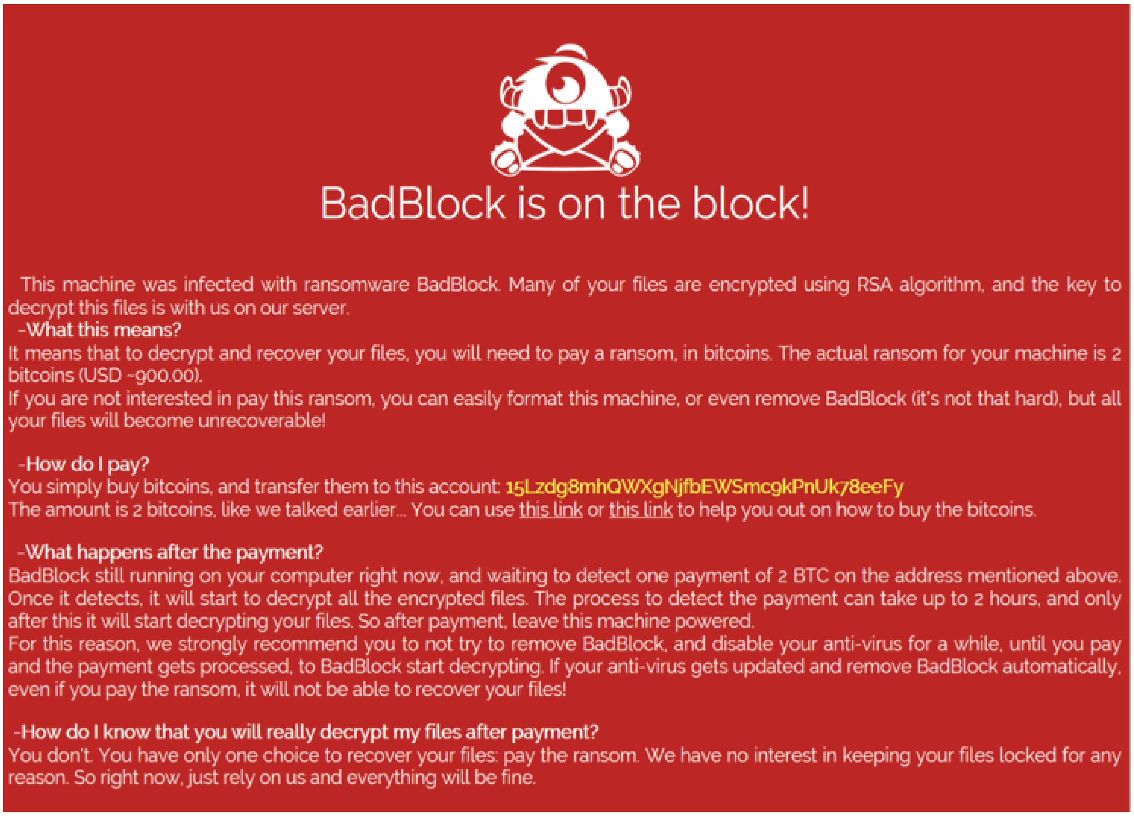
Ransomware support service is a critical service, as it can provide clear instructions for payment and enlighten users about the compromised systems and how they will retrieve or recover the data. **Figure 4** shows how the details are communicated to the end users on an infected system as a part of ransomware support service.

Experimental Analysis

Based on the characteristics discussed earlier, a number of ransomware variants were analyzed to determine the existing state of ransomware. **Figure 5** highlights the analysis of the different ransomware families. A number of observations were made:

- Phishing attacks are the most widely used technique for distributing ransomware, followed by exploitation of vulnerabilities and password-cracking attacks.
- Some families of ransomware analyzed manipulate the MBR; others do not. For example, RedEye, Petya and NotPetya rewrite the MBR code, whereas Locky, Cerber, WannaCry, Chimera and SamSam do not.
- The majority of ransomware encrypts the files available on the compromised system to be used in lieu of ransom. AES 128 and AES 256 are the most widely used encryption algorithms to encrypt files.
- Ransomware uses Tor to obtain payments via Bitcoin. This means that the victims need to access the Tor network to pay the ransom. Tor networks are used to maintain the anonymity and privacy of the ransomware operator. Some ransomware use direct web links for ransomware payment in Bitcoin.
- Considering the extortion mechanism, the majority of the ransomware follow the tier 1 strategy in which files are decrypted after obtaining ransomware. However, there was a deviation here in which two ransomware families, WannaCry and Chimera, follow the tier 3 strategy, in which data are either stolen or destroyed even after the ransom is paid.

Figure 4—Support Service Details Displayed by Ransomware



BadBlock is on the block!

This machine was infected with ransomware BadBlock. Many of your files are encrypted using RSA algorithm, and the key to decrypt this files is with us on our server.

-What this means?

It means that to decrypt and recover your files, you will need to pay a ransom, in bitcoins. The actual ransom for your machine is 2 bitcoins (USD ~900.00).

If you are not interested in pay this ransom, you can easily format this machine, or even remove BadBlock (it's not that hard), but all your files will become unrecoverable!

-How do I pay?

You simply buy bitcoins, and transfer them to this account: 15Lzdg8mhQWXgNjfbEWSmcgkPnUk78eeFy

The amount is 2 bitcoins, like we talked earlier... You can use this link or this link to help you out on how to buy the bitcoins.

-What happens after the payment?

BadBlock still running on your computer right now, and waiting to detect one payment of 2 BTC on the address mentioned above. Once it detects, it will start to decrypt all the encrypted files. The process to detect the payment can take up to 2 hours, and only after this it will start decrypting your files. So after payment, leave this machine powered.

For this reason, we strongly recommend you to not try to remove BadBlock, and disable your anti-virus for a while, until you pay and the payment gets processed, to BadBlock start decrypting. If your anti-virus gets updated and remove BadBlock automatically, even if you pay the ransom, it will not be able to recover your files!

-How do I know that you will really decrypt my files after payment?

You don't. You have only one choice to recover your files: pay the ransom. We have no interest in keeping your files locked for any reason. So right now, just rely on us and everything will be fine.

Figure 5—Characteristics Analysis of Ransomware Variants

No.	Characteristics	WannaCry	Petya	Cerber	Locky	NotPetya	Chimera	SamSam	RedEye
1	**Distribution mechanism**	Critical vulnerabilities	Critical vulnerabilities	Phishing attacks	Phishing attacks	Critical vulnerabilities	Phishing attacks	Brute-forcing passwords	Phishing and spam emails
2	**MBR manipulation**	No	Yes	No	No	Yes	No	No	Yes
3	**File encryption and cryptography**	Yes, AES-256	No	Yes, RC4	Yes, AES-128	Yes, AES-128	Yes, AES-256 (local implementation)	Yes, RSA-2048 or Rijndael	Yes, AES 256
4	**Payment mechanism**	Unique Bitcoin payment address	Onion Network:Tor browser links	Onion Network: Tor browser links	Normal web links and Onion Network: Tor browser links	Bitcoin payment address	Bitcoin payment address	Normal web links and Onion Network:Tor browser links	Onion Network: Tor browser links
5	**Extortion tier**	Tier 3	Tier 3	Tier 1	Tier 1	Tier 1	Tier 3	Tier 1	Tier 1
6	**RaaS**	No	Yes	Yes	No	Yes	Yes	No	No
7	**Ransom support services**	Embedded static pages	Embedded static pages	Embedded static pages	Embedded static pages	Hybrid service	Hybrid service	Hybrid service	Embedded static pages

- The RaaS model has been adopted by malware developers to provide infrastructure to buyers to operate the ransomware. Ransomware families such as Petya, Cerber, NotPetya and Chimera are sold in the underground cybercommunity as RaaS.
- The support services were also analyzed by dissecting the ransomware to check how the ransom notifications are provided to end users once the systems are compromised. The majority of ransomware use static web pages or components to display payment instructions and notifications to the victims. A few ransomware variations also provide notifications to victims to start chat sessions with the attacker.

Overall, this analysis helps professionals comprehend the inherent characteristics of the ransomware families.

Countermeasures and Recommendations

Ransomware is a promising underground industry that is steadily growing. Defense against this formidable threat is a necessity. Based on empirical analysis, recommendations toward strategies and methodologies that should be deployed into security solutions against ransomware may include:

- **System backups**—The first and the most effective corrective action against ransomware is to restore from backups. Backups should be regular and complete, otherwise they are ineffective. Backups are known to fail, so having multiple backups of critical data is necessary. With proper backups, ransomware is reduced to a mere annoyance since a system can be cleaned of the infection and data restored from a backup. Having cloud backups is better than maintaining local copies since ransomware is known to explicitly search for and remove or encrypt backups on the host and the network. If data

> “WITH PROPER BACKUPS, RANSOMWARE IS REDUCED TO A MERE ANNOYANCE SINCE A SYSTEM CAN BE CLEANED OF THE INFECTION AND DATA RESTORED FROM A BACKUP.”

cannot be backed up on a third-party cloud service (e.g., due to privacy concerns), the backups must be isolated and not mapped as a network drive on the host because some ransomware find and destroy attached backups.

- **System updates**—Ransomware such as WannaCry and Petya are known to exploit known vulnerabilities in the operating system (e.g., EternalBlue) to infect hosts. Installing regular updates and patches prevents such ransomware from gaining access to a host. Postponing updates leaves systems vulnerable to a wide array of security threats. Furthermore, it is crucial to update all programs (e.g., Flash Player, Java, browsers) since vulnerabilities in software are also targeted by attackers.
- **Employee training and awareness**—For organizations, it is critical to train employees in safe computing practices. For example, downloading and executing luring attachments, such as "invoice" and "resume," should be avoided unless they are from a trusted source.
- **Antivirus and firewalls**—Antivirus programs protect against a wide array of malware, including ransomware. An updated antivirus program will scan all suspicious files and perform signature-based and/or heuristics-based analysis to determine if the file is safe and will stop most ransomware before the malicious activities can commence. Firewalls can prevent malicious traffic such as a ransomware communication to the C&C server. In some cases, this will prevent the ransomware from acquiring an encryption key and render the ransomware ineffective.
- **Disabling unnecessary Windows utilities**—Ransomware is known to delete Visio Stencil (VSS) files on Windows to prevent victims from restoring from VSS backups. Protect VSS files by renaming vssadmin.exe since this is the Windows utility that ransomware uses to remove VSS files. Similarly, Windows Script Host (WSH) has been abused by JavaScript-based ransomware and should be disabled. In addition, execution of PowerShell scripts should be disabled as well.
- **Strong passwords**—Ransomware such as WYSIWYE and SamSam are known to brute force RDP logins. As a protection, all remote access services such as RDP and SSH can be protected with strong passwords and proper firewall policies enforced to block all unauthorized traffic.

Conclusion

A characteristic study of ransomware botnets has been presented. The study resulted in obtaining information related to distribution mechanism, cryptography, extortion mechanism, service models, payment (ransom) handling and others. Dissecting the inherent characteristics to perform analysis across a number of ransomware families helps to gather intelligence about their behavior. The obtained information can be used to build automated solutions to detect and prevent ransomware. In the end, there are a number of countermeasures that can be chosen to combat ransomware infections.

Endnotes

1 Johnson, B.; "Ransomware on the Rise: A Brief History and Timeline," *Carbon Black*, 14 September 2016, *https://www.carbonblack.com/2016/09/14/ransomware-rise-brief-history-timeline/*

2 Zetter, K.; "What Is Ransomware? A Guide to the Global Cyberattack's Cary Method," *Wired*, 14 May 2017, *https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/*

3 Eitzman, R.; K. Goody; J. Valdez; "How the Rise of Cryptocurrencies Is Shaping the Cyber Crime Landscape: Blockchain Infrastructure Use," *FireEye*, 18 April 2018, *https://www.fireeye.com/blog/threat-research/2018/04/cryptocurrencies-cyber-crime-blockchain-infrastructure-use.html*

4 Greenburg, A.; "The WannaCry Ransomware Hackers Made Some Real Amateur Mistakes," *Wired*, 15 May 2017, *https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/*

5 Newman, L. H.; "Petya Ransomware Hackers Didn't Make WannaCry's Mistakes," *Wired*, 27 June 2017, *https://www.wired.com/story/petya-ransomware-wannacry-mistakes/*

6 Olenick, D.; "WannaCry and NotPetya: Who, What, When and Why?" *SC Magazine*, 2 October 2017, *https://www.scmagazine.com/wannacry-and-notpetya-who-what-when-and-why/article/696198/*

7 Boyd, C.; "SamSam Ransomware: What You Need to Know," *Malwarebytes Labs*, 1 May 2018, *https://blog.malwarebytes.com/cybercrime/2018/05/samsam-ransomware-need-know/*

8 Bajpai, P.; A. K. Sood; R. Enbody; "A Key-Management-Based Taxonomy for Ransomware," *2018 APWG Symposium on Electronic Crime Research (eCrime)*, San Diego, California, USA, 2018, p. 1-12, *https://ieeexplore.ieee.org/document/8376213/*

9 Everett, C.; "Ransomware: To Pay or Not to Pay?" *Computer Fraud & Security*, vol. 4, 2016, p. 8-12, *https://www.sciencedirect.com/science/article/pii/S1361372316300367*

10 Sood, A. K.; S. Zeadally; "Drive-By Download Attacks: A Comparative Study," *IT Professional*, vol. 18, no. 5, 2016, p. 18-25, *http://ieeexplore.ieee.org/document/7579103/*

11 Sood, A. K.; R. Enbody; "Malvertising—Exploiting Web Advertising," *Computer Fraud & Security*, iss. 4, April 2011, p. 11-16, *https://www.sciencedirect.com/science/article/pii/S1361372311700410*

12 Sood, A. K.; S. Zeadally; R. Bansal; "Exploiting Trust: Stealthy Attacks Through Socioware and Insider Threats," *IEEE Systems Journal*, vol. 11, no. 2, June 2017, p. 415-426, *http://ieeexplore.ieee.org/document/7042925/citations*

13 Sood, A.; "Cloud Storage Apps as Malware Delivery Platforms (MDP): Dissecting Petya Ransomware Distribution via Dropbox," *Symantec*, 30 March 2016, *https://www.symantec.com/connect/blogs/cloud-storage-apps-malware-delivery-platforms-mdp-dissecting-petya-ransomware-distribution-dro*

14 *Op cit* Olenick

15 *Op Cit* Boyd