A Technical Analysis of RedAlert Ransomware - Targeting Virtual Machine Files

Tangila Islam Tanni
University of Central Florida
Orlando, USA
tanni@knights.ucf.edu

Noah Heikes
University of Central Florida
Orlando, USA
noah.heikes@knights.ucf.edu

Khan Shaikhul Hadi
University of Central Florida
Orlando, USA
shaikhulhadi@knights.ucf.edu

ACM Reference Format:
Tangila Islam Tanni, Noah Heikes, and Khan Shaikhul Hadi. 2022. A Technical Analysis of RedAlert Ransomware - Targeting Virtual Machine Files. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Abstract

Ransomware is one of the biggest malware threats that companies and organizations face. Successful malware attacks can disrupt services, or in the worst case, shut them down completely. Our study focuses on Ransomware called RedAlert, which encrypts Virtual Machine files. Our main goal is to break down how RedAlert works, and find out what its characteristics are. We first used several static and dynamic analysis tools to break apart a sample of the malware, as well as compiled several outside articles. Our study shows that RedAlert needs to run in a Virtual Machine's host in order to encrypt files, as well as the fact that there is no way to recover the encrypted files without purchasing a key.

2 Introduction

Malware has developed over the course of the last few decades in terms of the sophisticated obfuscation of malicious software and the variety of attack methods [14]. Ransomware is one of the greatest and most rapidly growing threats to the digital world. Ransomware is a type of malware that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid. Figure 1 shows the global ransomware attack volumes in the past three years. Nearly 188 million ransomware infections occurred worldwide in 2019. The next year, in 2020, ransomware threats rapidly increased and surpassed the 300 million mark. However, the quantity of ransomware attacks observed in 2021 far exceeds that of either year. The number of attacks increased to 623 million ransomware strikes. In 2021, there were roughly 20 ransomware attempts every second. Moreover, 421.5 million ransomware threats were made against the US, far more than any other nation [22].

The emergence of malware creation tools has made the development of new ransomware variants easier [6]. Ransomware may simply change its capacity for rapid spread. The hacking tools are stored on the dark web. To carry out ransomware assaults, which only cost a few hundred dollars, attackers can reach the dark web by installing the TOR (The Onion Router) browser [10]. The difficulty of launching a cyberattack is made easier by attackers having easy access to hacking tools. The circular chain of hacking weapons now includes any newly produced hacking tool used in a hacking campaign or malware epidemic [10]. Once ransomware is activated on a user's computer, it encrypts all essential data and files in the victim's computer system using a public and private key pair. It is a type of infection that, once spread, is difficult to remove. The data owner can only access the files when the ransom is paid. Threat actors typically demand cryptocurrency payments such as Bitcoin because this payment method protects the anonymity of the destination address linked to the ransom demand [29]. Once infected, there are only two options left for the victim: either pay the ransom, which does not ensure that the victim will be able to unencrypt their file, or format the computer and switch off the Internet [19]. Therefore, first responders must quickly analyze and act immediately when confronted with security breaches. Following the collection of ransomware samples, malware analysis is used to provide a broad overview of the attack and identify key indicators and signatures that can be used to prevent future attacks [6]. To summarize, ransomware is a major target for financial exploits, an effective tool for cyberattacks, and incorporates multiple layers of security concepts (i.e. phishing attack, cryptography, compromising kernel level permission, and securely sending information to the adversary).

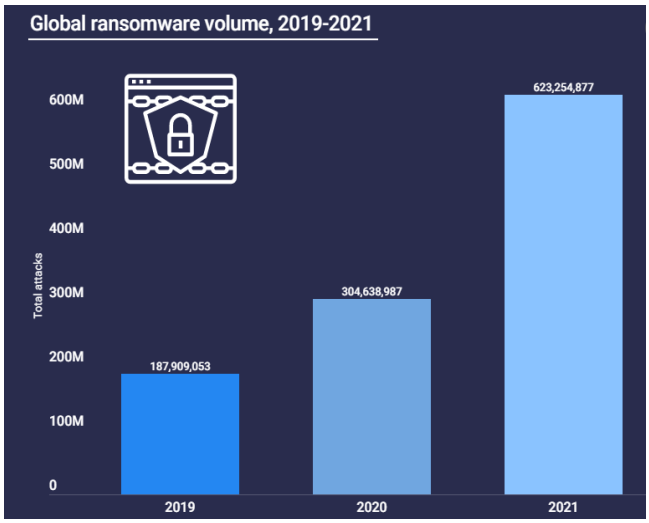


Figure 1: Global Ransomware Volume, 2019-2021 [22]

While looking for a suitable ransomware for study purposes, we wanted a ransomware that is recent and could cause trouble for a large number of people. RedAlert is a recent ransomware attack first exposed by MalwareHunterTeam [18] that targeted VMware ESXi servers running on Windows and Linux platforms. This ransomware is a cross-platform program; RedAlert is the name of the Windows version, and N13V is the name of the Linux version that targets VMware ESXi servers [25]. For the rest of the paper,

we only use the name RedAlert to address this malware. As our life highly dependent on cloud services, RedAlert could affect a large group of people if it could infect popular cloud services like AWS. There is already more than one victim of this ransomware. This made RedAlert a suitable candidate for our study. The goal of this paper is to outline a technical analysis of the RedAlert ransomware and to produce useful information for future researchers.

3 Related Work

This section discusses the characteristics of ransomware and presents an overview of several stages associated with ransomware-based attacks.

3.1 Ransomware

Any type of malware classified as ransomware aims to have users pay a ransom in exchange for full access to their machine. Ransomware is divided into three basic categories: locker, crypto, and scareware [12, 15]. Scareware may employ pop-up advertisements to trick users into believing they must download specific software, utilizing coercion to spread malware. Instead of locking the device or encrypting any data, cybercriminals use scareware to prey on people's fears [5]. The victim's machine is not usually harmed by this type of ransomware. Locker ransomware attempts to utilize basic or sophisticated processes to lock the user's computer, preventing the user from regaining access. Next, they frequently display a message on the screen that requests money. Only after the ransom is paid is access restored. Crypto ransomware encrypts the user's private files but does not affect standard computer operations. The majority of the time, crypto-ransomware doesn't encrypt the entire hard drive; instead, it looks for files with specific extensions, such as .doc, .jpg, and .pdf [23]. These files frequently contain text documents, presentations, and images, all of which typically contain valuable and private user data and would cause the most harm to users if lost. Crypto ransomware, in contrast to locker ransomware, is often irreversible because modern encryption algorithms (such as AES and RSA) are nearly impossible to reverse if implemented properly [12, 20, 23].

3.1.1 Ransomware Encryption One of three encryption techniques — symmetric, asymmetric, or hybrid—can be used by crypto ransomware [9]. A completely symmetric technique is troublesome as the encryption key must be included in the malware [11]. Because of this, this strategy is susceptible to reverse engineering. Asymmetric encryption is the second strategy. Asymmetric encryption is slower than symmetric encryption, which makes it difficult to encrypt larger files, which is the problem with this method [7]. Hybrid encryption, which employs both symmetric and asymmetric encryption, is the most efficient method (and hence the most difficult to decrypt). Typically, the ransomware calls a cryptographic API on the user's operating system to generate this key [30]. As the ransomware moves across the file system, the symmetric key encrypts the victim's files. A public-private key pair is established by a command and control (C&C) server that the ransomware connects to after all files have been encrypted. The symmetric key is encrypted using the public key that is sent to the ransomware, while the C&C server holds the private key. Once the victim pays the ransom, they will receive the key to decrypt their files. For each new ransomware infection, a distinct public-private key pair is often generated; this stops victims from exchanging private keys with other victims so they can recover the symmetric key [8].

3.2 Recent advances in ransomware attack

Strong data encryption methods, attributable to improvements in computer power and memory technology/affordability, together with improvements in payment methods and cryptocurrencies, have sped up ransomware progress between 2007 and 2016 [21]. In today's digitally connected world, it is simple for an adversary to hide their identity and make money by spreading ransomware viruses across billions of Internet-connected devices. The ransomware variant CTB-Locker (Curve, TOR, Bitcoin) is thought to be the first to successfully combine three essential characteristics necessary to achieve a high degree of success in infection, namely the anonymity capabilities of the TOR routing protocol to conceal adversary location, the anonymous payment capabilities of Bitcoin to keep payment path untraceable, and strong encryption based on Elliptic Curve Cryptography with sufficient key lengths to resist attestation [13]. The first temporary spike in ransomware evolution occurred in 2006–2007 [17], primarily as a result of the emergence of the GPCode variants. Particularly the GPCode.ak variation was known to delete the user's unencrypted user files while writing the encrypted file contents to a new spot in the user's disk. Application of the "undeletion utility" allowed for partial user data recovery without the need to pay the adversary's ransom. Stronger encryption methods and longer encryption keys (1024 or 2048) were employed in more recent iterations of GPCode, thus complicating the user's attempts to recover the victim's data from the system.

A detailed examination of the development of multiple ransomware releases showed that the majority of their code was simply copied and pasted from earlier iterations. As a result, many of the shortcomings of one version transferred over to another. Several ransomware strains also functioned in unusual ways. For instance, it was discovered that the 2015 Reveton ransomware [13] only locked the operating system's boot process without encrypting user data. Because retrieving user data without having to pay the ransom was discovered to be possible, the ransomware activity was restricted to disrupting operations.

3.3 Flow of a Typical Ransomware Attack

The ransomware's procedural requirement to get in touch with a central Command-and-Control (C2C) Server once the victim's computer has been infected and before encrypting the data is another recently noticed aspect of ransomware. Usually, the cryptographic key needed to unlock the victim's encrypted data is stored on the C2C Server. The following is a summary of the four stages of a ransomware-based attack:

- Infection: When a gullible victim clicks an attachment that comes with spam mail, the ransomware software gets installed on their computer. Alternatively, accessing a compromised website might potentially cause the victim's computer to become infected [13].
- Data encryption: Cryptographic keys using the Public Key Infrastructure (PKI) are produced either on the infected computer or the C&C server once the victim's computer has

been infected with ransomware. The user's files or device are then locked down by the malware. One of two activities is typically carried out as a result of ransomware-specific definitions: either the data/files on the victim's machine are attacked file by file, or crucial file system structures, such as the Windows Master File Table, are changed. In all situations, the original files or data are encrypted using host-specific cryptographic keys before being removed [13].

- Demand: The victim sees a message from the ransomware program requesting payment of a particular sum in order to unlock the locked data/files [13].
- Outcome: The victim's actions could result in any of the following outcomes: (a) data is restored by removing the ransomware's traits from the victim's computer without having to pay the demanded ransom. (b) payments are processed through private channels like BitCoin/MoneyPak or DarkCoin, or (c) unless a backup is established, the victim's data and files are permanently lost if payments are not provided and the ransomware characteristic is not removed. [13, 23].

4 Approach

In order to better understand how RedAlert worked, we broke our research up into two parts:

4.1 Outside Research

First, we looked into what research had already been done. By looking into already published articles and other online entries, we were able to get a better understanding of how the ransomware worked. We were also able to alleviate some of the risks of running a live virus on our machines.

4.2 Independent Analysis

Using the sample ransomware from MalwareBazaar Database [2], we performed an independent analysis of our own. The source website has two options for sample malware: a. *.exe and a *.bat file. We decided to use the .exe sample since it's the more common file extension. Our independent analysis is divided into two parts.

- Static Analysis
- Dynamic Analysis

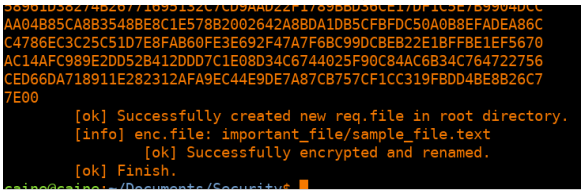
4.2.1 *Static Analysis*

Static analysis is performed in a sandbox environment to isolate it from the rest of the system for security reasons. Our main reverse engineering tool was the Ghidra SRE suit. Once loaded into Ghidra, we were able to see that the sample was written in C and unstripped of any debugging symbols, which gave us access to method names.

4.2.2 *Dynamic Analysis*

For dynamic analysis, we tried to test the malware in a more protected environment than a sandbox environment. We used a Live OS (OS directly run from a Flash drive or CD in protected mode. Any modification made in the system will be lost after each reboot) where we ran the malware. Also, we ensured that the OS was disconnected from the physical hard disk so that the physical device did not get compromised.

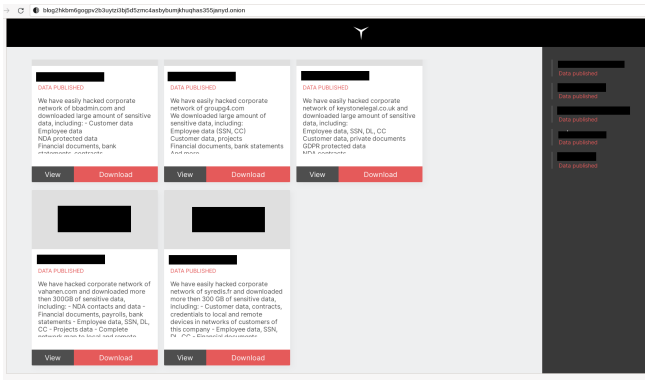
(a) Initiation of execution with target file TestFile.text



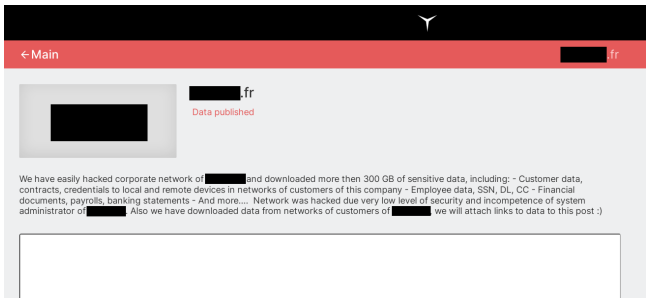
(b) Encryption success message

Figure 2: Successful execution of RedAlert malware on LiveOS to corrupt sample test file

Figure 2a shows the successful execution of the malware in our environment [1].



(a) Board of Shame main page



(b) Description of data that attacker leaked for a particular victim

Figure 3: Board of Shame web-page for RedAlert malware attack

[1] Due to page limitation, we only show a screen-shot of the beginning and the ending message of the message RedAlert show in the terminal.

5 Evaluation

5.1 Threat Model

In this paper, we assume that the adversary's objective is to deny a user or organization access to files on their computers by encrypting essential files and demanding a ransom payment for the decryption key. In our threat model setting, we assume the following steps for executing a successful ransomware attack:

(1) Phishing attacks to convince a user to download the ransomware or get access to the user account.
(2) Ransomware scans the whole system for the potential target file.
(3) Executes the ransomware (we assume that either RedAlert ransomware could take over root permission or the attacker must acquire it first) to encrypt files.
(4) Sends data to the attacker over the internet.
(5) Notifies the victim that his/her files are encrypted and need to pay to get the decryptor key (4 and 5 may be interchanged).

5.2 Evaluation Metrics

Before starting our proposed analysis, we considered different types of matrices to measure the quality of our analysis. These metrics led us to conduct both static and dynamic analyses. In this project, we mainly focused on the accuracy and usefulness of our findings, information coverage, time to conduct the experiment (speed), and safety of our data and system while conducting the analysis. First, we wanted to gather as much information as possible regarding the RedAlert ransomware. Therefore, we carried out a simple static analysis, which is quick and easy to perform. The analysis consists of examining the executable file without viewing the actual instructions to confirm whether a file is malicious and provide information about its functionality. Furthermore, the static method of malware analysis is the most secure because the malware can not infect the test system this way. However, static analysis can be ineffective against sophisticated malware, and it can miss essential behaviors. To better understand how ransomware behaves after infecting a potential target system and confirm the static analysis findings, we also decided to run a dynamic analysis. Furthermore, we also wanted to observe network traffic during the execution of ransomware, which is only possible for dynamic analysis. These factors led us to conduct static and dynamic analysis for this project.

5.3 Outside Research

5.3.1 Ransom website

Adversary hosts a ransom website that they use as a way to instruct the victim and leak secret information about the victim if they refuse to pay the ransom. The ransom site can be divided into two sections:

(1) Instruction for the Victim
(2) Board of Shame

Instruction for Victim

After successfully compromising any machine, the attacker directs the victim to an onion site for detailed information on purchasing a decrypter and communicating with their support. Ironically, they also let the victim decrypt a file for free. The attacker only accepts Monero as cryptocurrency [2]. We extracted the URL for the onion site from our sample malware binary, but that website was disabled soon after we accessed it.

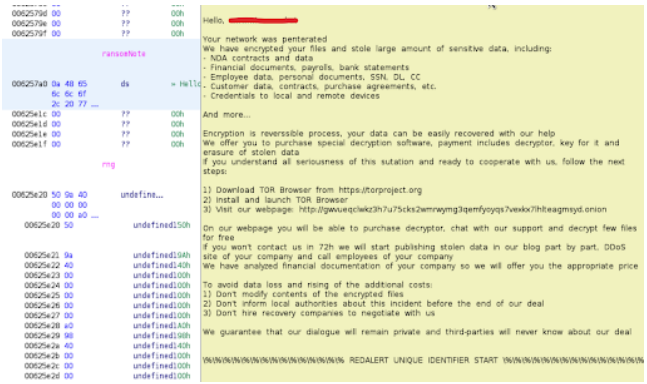


Figure 4: Ransom Note

Board of Shame

This is a .onion site that releases collected information of the victims who refused to pay the ransom. There are five victims listed whose collected data were made public as shown in figure 3[3]. Figure 3a shows the main page which contains the names of the victims who refuse to pay the ransom. From figure 3b, we could see that attackers were able to collect sensitive data like Customer data, contracts, and credentials to local and remote devices along with employee data, SSN, DL, CC, and more. [4]

5.4 Static Analysis

In our research, we found that RedAlert specifically targets VMWare ESXi server files. The ransomware can be run on both Windows and Linux platforms.

RedAlert contains three main portions of code: launch arguments, file scanning, and encryption.

5.4.1 Launch Arguments

Unlike other malware, RedAlert was not designed to be as barebones as possible. Besides not stripping their code of debugging symbols, the authors included several launch options to give the malware more versatility. These include:

- -w Run command to stop all running VMs
- -p Path to encrypt (by default encrypt only files in the directory, not include subdirectories)
- -f File for encrypt
- -r Recursive. used only with -p (search and encryption will include subdirectories)

[2] Our last access to this URL did not contain information regarding cryptocurrency anymore. Thus our Figure 3a does not contain a section regarding cryptocurrency for payment
[3] To prevent the spread of the names of the victims, names and icons are darkened in the image
[4] Our latest attempt to enter the "board of shame" URL did not work. This link may be broken now. Either attacker changed the address to prevent detection or shut down their operation as RedAlert ransomware activity is exposed now.

- -t Check encryption time (only encryption, without key-gen, memory allocates ...)
- -n Search without file encryption (show files and folders with some info)
- -x Asymmetric cryptography performance tests. DEBUG TESTS
- -h Show this message [4]

The Linux encryptor will shut down every active VMware ESXi virtual machine when the ransomware is launched with the '-w' argument [4]. By leveraging the following esxcli command, the actors performed the action:
esxcli –formatter=csv –format-param=fields=="WorldID,DisplayName" vm process list | tail -n +2 | awk -F $',' 'system("esxcli vm process kill –type=force –world-id=" $1)'

5.4.2 File Scanning

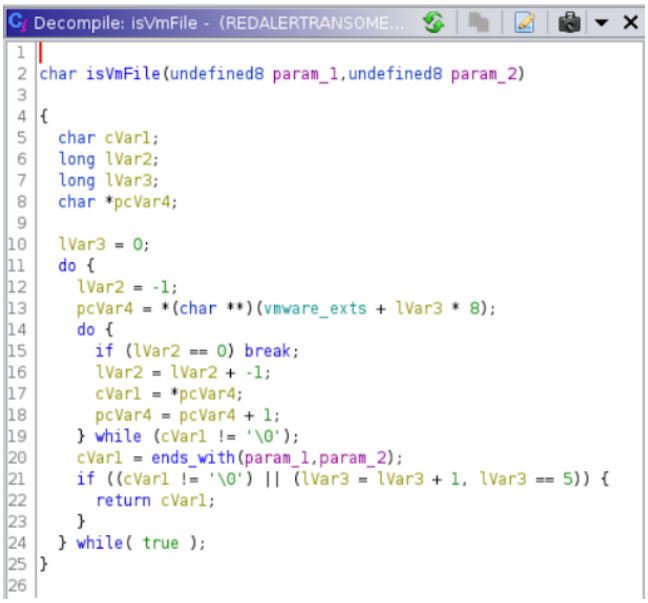


Figure 5: Decomplied File Checking Function

Once the ransomware has been launched, it will scan through the file system looking for any virtual machine files to encrypt. Specifically, it looks for files with the extension of:

- .log
- .vmdk
- .vmem
- .vswp
- .vmsn [4]

5.4.3 NTRUEncrypt Public-Key Encryption

After a suitable file has been found, the ransomware will use the NTRUEncrypt public-key encryption scheme to encrypt the file. Files encrypted will have the extension ".crypt" appended to their name along with a number. [4].

Key Generation

Before starting the encryption process, the attackers start by generating public and private key pairs. The key generation process starts by choosing the general parameters N, p, and q. The attacker selects two random polynomials, f, and g, with integer coefficients between [-1; 1] with a degree of no more than N-1 (which means the coefficients are the numbers -1, 0, or 1). $-x^3-x^2+x-1$ is a prime example of such a polynomial. The extra prerequisite that the polynomial f has inverses under modulus p and q must be met. After that, the attacker calculates the inverses f_p of f (mod p) and f_q of f mod q.
f * f_p = 1 (mod p)
f * f_q = 1 (mod q)
Next, the public key, h, is calculated using the following formula:
h = p * f_q * g (mod q)
In contrast, (f, f_p, g) is used as their private key by keeping them secure and private from the outside world. Figure 6 presents the key generation process.

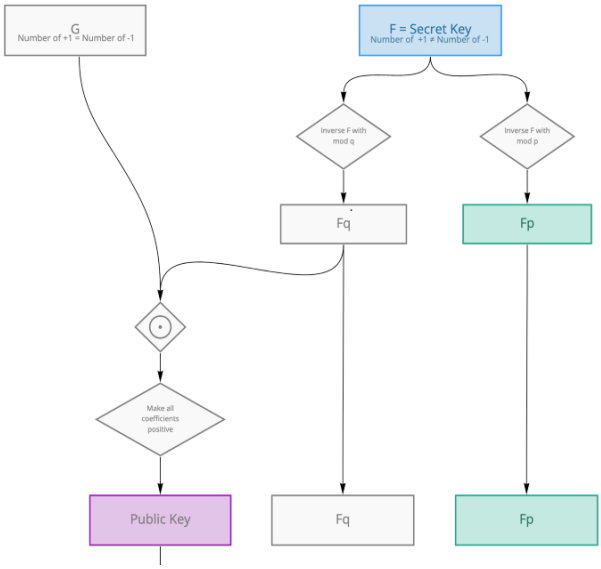
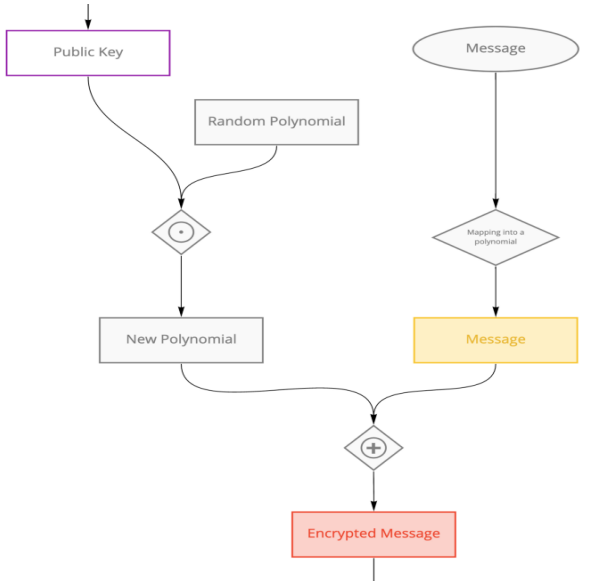


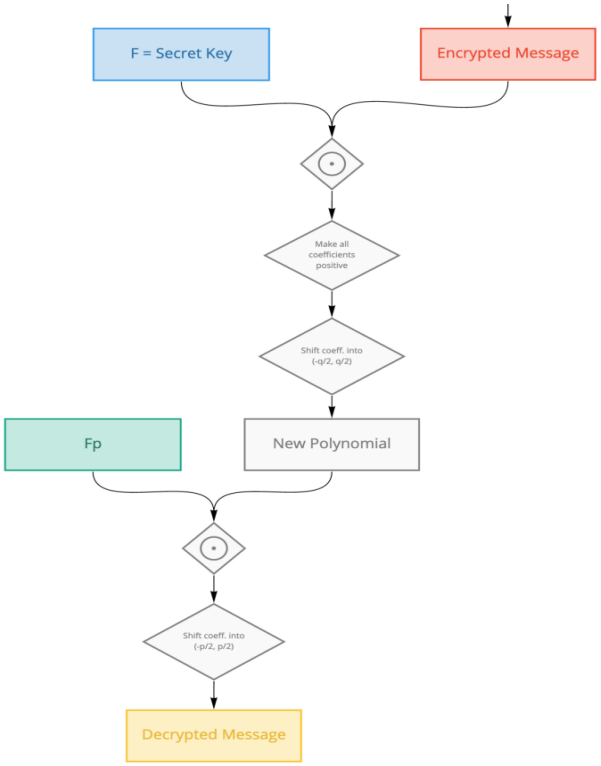
Figure 6: Key Generation [24]

Encryption Algorithm

At first, the file is converted into a polynomial to be encoded and encrypted. For NTRU, it requires a polynomial with coefficients between -1 and 1. By converting the message into binary, it is possible to create a polynomial. For example, if the message is 13, which can be represented as 1101 and its equivalent polynomial can be written as $1*x^3+1*x^2+0*x+1 = x^3+x^2+1$. Once the message is converted into a polynomial m, it is ready to be encrypted using the public key, h. Next, the attacker chooses a blinding value, which is a random polynomial r. This is the key point in the encryption process because the polynomial m is hidden by the arbitrary and unknown polynomial, making it difficult to decrypt without the private key. The ciphertext, e is calculated using the following formula:



(a) NTRU Encryption [24]



(b) NTRU Decryption [24]

Figure 7: Encryption and decryption algorithm for NTRU

e = r * h + m (mod q)
Figure 7a presents the encryption process.

Decryption

The decryption phase can be divided into three unique steps. At first, upon receiving the ciphertext, e, the receiver uses his private key to uncover the plaintext. The decryption process starts by calculating a polynomial, using the following formula:
a = f * e (mod q)
To prevent decryption issues, the coefficients of a are chosen to be between -q/2 and q/2; in general, they should lie in an interval of length q. In the next step, the receiver calculates a polynomial, b such that, b = a (mod p)
Finally, the message m is retrieved by the receiver using his secret polynomial f_p.
m = f_p * b (mod p)
Figure 7b presents the decryption process.

5.5 Dynamic Analysis

Our dynamic analysis consists of three parts as follows:

(1) Create a secure environment to analyze malware with minimal risk
(2) Make a test file to be a victim of the malware
(3) Analyze activity in the environment to understand the impact of the virus

5.5.1 *Secure Environment*

We ransomware by definition attempts to take control from the host and cause harm to the system, it is important to ensure that the execution environment is as isolated as possible and does not contain any private or sensitive information. We ensure that our main hardware is disconnected from the operating system (OS) so that any malware that could take over the operating system could not access the hardware. To ensure that, we used a live operating system run directly from a Flash drive or CD with restricted write permission. This way one could remove the requirement for hardware to boot OS. We used CAINE 12 [1] OS for this purpose which is based on Ubuntu 20.04.3 LTS.

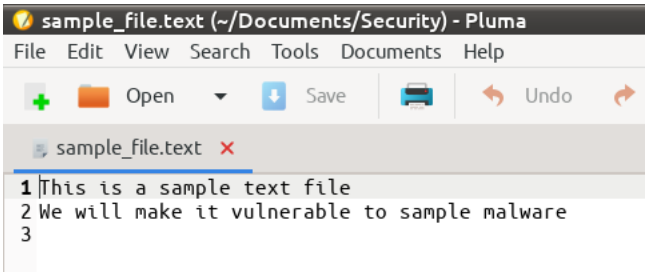
5.5.2 *Sample File Encryption*

Our sample malware is not active (i.e. it does not automatically scan the system and try to encrypt files). It requires a command line argument to perform encryption. We were able to corrupt a sample text file using our sample malware as shown in figure 8. When RedAlert completes its operation, it shows information regarding the success of the operation as shown in Figure 2. Also, we observe that after encryption was complete, it renamed the file as **.crypt658* file-type.

As we saw in Figure 3b, the attacker collects a good amount of data from the victim. Thus we assume that there would be other underlying activity in the system when we encrypt a file using RedAlert.

5.5.3 *Activity Analysis*

Based on our outside research 5.3.1, we knew that besides encrypting victim files the ransomware must be performing additional activity (i.e. internet communication). To capture those activities we used Wireshark [28] network analysis tool. We observe a broadcast is sent which we were able to capture as shown in figure 9. The broadcast packet does not contain any destination IP address, which is why attackers used this method to hide their IP address to establish communication with the victim. This is a 32-byte packet.



(a) Content of sample_text.txt file

(b) Encrypted data for sample_text.txt file

Figure 8: RedAlert ransomware encrypts a sample text file

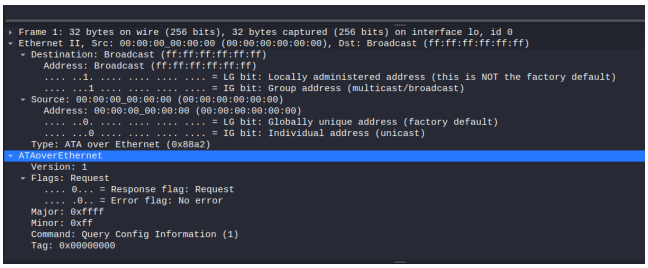


Figure 9: Network packet from sample RedAlert malware

Instead of IP protocol, it uses AoE (ATA over Ethernet) protocol whose primary use is simple, high-performance access of block storage devices over Ethernet networks [27]. Unfortunately, this packet does not contain any sensitive information that it's trying to send over the internet. We assume, as this sample ransomware is provided for study purposes only, malwarebazzar [2] has modified some portion of the code to prevent anyone from becoming a victim of this ransomware. This particular sample is modified to prevent sending any information over the internet as it may result in leaking important information of the user.

6 Discussion

The paper focuses on providing insights into RedAlert ransomware by analyzing samples of selected ransomware variants from existing RedAlert ransomware families. We also conducted a static analysis to gather as much information about this ransomware as possible. The majority of findings from the dynamic analysis matched the information, which was collected through the static analysis. Surprisingly, the virus sample we used seemed to have Rijndael as its encryption algorithm (based on its function names). In the end, we decided to go with NTRU for the paper since multiple sources from static analysis confirmed the usage of NTRU public encryption system for RedAlert ransomware [3, 16, 18, 26]. Moreover, we also suspect that our sample may have been an outlier or obfuscated. During the dynamic analysis, we also noticed that our sample malware does not automatically scan and encrypt the critical files in the host machine as it should do based on our outside research. We suspect that this sample malware underwent a significant modification by the provider of sample malware to make it harmless. Furthermore, upon analyzing the malware-generated internet packet, we found an empty packet that did not leak any information, supporting our assumption. We presume they made it harmless and inactive so that anyone could use it for educational/learning purposes without becoming a victim of the ransomware. Furthermore, it also prevented using the malware with malicious intent.

One of the primary purposes of ransomware attacks is financial gain. So, attackers lock the system and encrypt important files so that the data owner can no longer access the resources until payment is made. The practical reason for using fundamental encryption algorithms is that today's encryption algorithms are tough to crack. These attackers mostly use public encryption systems to encrypt these files, which is very difficult to break, considering limited computational power and adversarial capabilities. With technological advancements, our encryption mechanism has also improved. Attackers know that if the data owner has no backup, the organization/corporation can't break the encryption and recover their data. Therefore, the only way is to pay the ransom and get the decryption key to recover their data. However, it indicates how a powerful tool like encryption can be misused by bad people, which is scary and alarming at the same time.

A mix of reliable monitoring tools, regular file backups, anti-malware software, and user education are necessary for effective ransomware avoidance. Regular backup operations should be carried out. Backups must be kept offline since many ransomware variations try to locate and erase any accessible backups. Maintaining offline backups is essential because victims won't have to pay a ransom for data that is easily accessible. A basic cyber incident response strategy and a communications plan that includes response and notification processes for a ransomware event are also helpful in these situations. Although no cyber-defense can eliminate danger, it can significantly lessen the likelihood that an attack would succeed.

7 Work Distribution

7.0.1 *Tangila*

- Wrote the Introduction, Background, NTRU Key Generation, Encryption and Decryption section, and Discussion.

7.0.2 *Shaikhul*

- Search for online portals that attackers use to publish data or communicate with the victim. Seems like the attacker minimized this footprint. We were able to find the board of shame, which was found broken one day later.
- Analyze malware from the user's point of view (ongoing) within necessary safety.
- Capture and analyze network packets

7.0.3 *Noah*

- Static analysis of the virus and general research
- Wrote the Methods section and parts of How Does RedAlert Work, as well as general proofreading and document structure

8 Conclusion

Our study of RedAlert has shown how the malware works, what kind of encryption it uses, and how it performs when run. Through outside research and our own static and dynamic analysis, we were able to dissect RedAlert and see how it runs. Our study has shown three things. First, RedAlert does not run from within a virtual machine, only outside it. Malicious actors will need to infect the host of the VM to run RedAlert. Second, not all malware is obfuscated. Sometimes versatility is better for malware users than the secrecy of their program. In this case, RedAlert prioritized utility functions and ease of coding, rather than trying to minimize the amount of space it took up. Finally, RedAlert uses the AoE protocol when it communicates back to the malware host. By scanning to see if this packet is being transmitted over the network, an antivirus may be able to detect RedAlert before it has finished encrypting.

References

[1] [n.d.]. CAINE Computer Forensic Linux Live Distro. https://www.caine-live.net. [Accessed 04-Dec-2022].

[2] [n.d.]. MalwareBazaar | Browse Checking your browser — bazaar.abuse.ch. https://bazaar.abuse.ch/browse.php?search=tag%3Aredalert. [Accessed 03-Dec-2022].

[3] Lawrence Abrams. [n.d.]. New RedAlert Ransomware targets Windows, Linux VMware ESXi servers. https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/. [Accessed 23-Oct-2022].

[4] Lawrence Abrams. 2022. *New RedAlert Ransomware targets Windows, Linux VMware ESXi servers.* https://www.bleepingcomputer.com/news/security/new-redalert-ransomware-targets-windows-linux-vmware-esxi-servers/.

[5] Nicoló Andronio, Stefano Zanero, and Federico Maggi. 2015. Heldroid: Dissecting and detecting mobile ransomware. In *international symposium on recent advances in intrusion detection*. Springer, 382–404.

[6] Rima Asmar Awad and Kirk D Sayre. 2016. Automatic clustering of malware variants. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. IEEE, 298–303.

[7] Pranshu Bajpai, Aditya K Sood, and Richard Enbody. 2018. A key-management-based taxonomy for ransomware. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–12.

[8] Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security* 111 (2021), 102490.

[9] Fabrizio Cicala and Elisa Bertino. 2020. Analysis of encryption key generation in modern crypto ransomware. *IEEE Transactions on Dependable and Secure Computing* (2020).

[10] KAO Da-Yu, Shou-Ching Hsiao, and TSO Raylin. 2019. Analyzing WannaCry ransomware considering the weapons and exploits. In *2019 21st International Conference on Advanced Communication Technology (ICACT)*. IEEE, 1098–1107.

[11] Tooska Dargahi, Ali Dehghantanha, Pooneh Nikkhah Bahrami, Mauro Conti, Giuseppe Bianchi, and Loris Benedetto. 2019. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques* 15, 4 (2019), 277–305.

[12] José Antonio Gómez-Hernández, L Álvarez-González, and Pedro García-Teodoro. 2018. R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security* 73 (2018), 389–398.

[13] Nikolai Hampton and Zubair A Baig. 2015. Ransomware: Emergence of the cyber-extortion menace. (2015).

[14] Steven Strandlund Hansen, Thor Mark Tampus Larsen, Matija Stevanovic, and Jens Myrup Pedersen. 2016. An approach for detection and family classification of malware based on behavioral analysis. In *2016 International conference on computing, networking and communications (ICNC)*. IEEE, 1–5.

[15] SH Kok, Azween Abdullah, NZ Jhanjhi, and Mahadevan Supramaniam. 2019. Prevention of crypto-ransomware using a pre-encryption detection algorithm. *Computers* 8, 4 (2019), 79.

[16] Cyware Labs. [n.d.]. RedAlert: A Ransomware that Targets Multiple OS Platforms | Cyware Hacker News. https://cyware.com/news/redalert-a-ransomware-that-targets-multiple-os-platforms-47b4d715. [Accessed 23-Oct-2022].

[17] Xin Luo and Qinyu Liao. 2009. Ransomware: A new cyber hijacking threat to enterprises. In *Handbook of research on information security and assurance*. IGI global, 1–6.

[18] MalwareHunterTeam. 2022. A look at RedAlert ransomware gang's leak site, titled "Board of shame". https://twitter.com/malwrhunterteam/status/1544387107577335813. [Accessed 04-Dec-2022].

[19] Savita Mohurle and Manisha Patil. 2017. A brief study of wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science* 8, 5 (2017), 1938–1940.

[20] Ibrahim Nadir and Taimur Bakhshi. 2018. Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques. In *2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. IEEE, 1–7.

[21] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton University Press.

[22] William S. 2022. *Ransomware volume doubles in 2021, surpassing 600 million.*

[23] Daniele Sgandurra, Luis Muñoz-González, Rabih Mohsen, and Emil C Lupu. 2016. Automated dynamic analysis of ransomware: Benefits, limitations and use for detection. *arXiv preprint arXiv:1609.03020* (2016).

[24] Vihren Stoev. 2019. *The Essence of NTRU: Key Generation, Encryption, Decryption.* https://medium.com/autobahnnetwork/the-essence-of-ntru-key-generation-encryption-decryption-7c0540ef8441.

[25] PIOTR TARNAWSKI. 2022. *New ransomware is targeting Windows and Linux VMware ESXi servers – RedAlert/N13V.* https://angrysysops.com/2022/07/13/new-ransomware-is-targeting-windows-and-linux-vmware-esxi-servers-redalert-n13v/.

[26] DORA TUDOR. [n.d.]. New Strain of Ransomware Discovered.

[27] wikipedia.org. [n.d.]. ATA over Ethernet - Wikipedia. https://en.wikipedia.org/wiki/ATA_over_Ethernet. [Accessed 04-Dec-2022].

[28] wireshark.org. [n.d.]. Wireshark Go Deep. — wireshark.org. https://www.wireshark.org. [Accessed 04-Dec-2022].

[29] Pavol Zavarsky, Dale Lindskog, et al. 2016. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science* 94 (2016), 465–472.

[30] Aaron Zimba, Zhaoshun Wang, Hongsong Chen, and Mwenge Mulenga. 2019. Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. *KSII Transactions on Internet and Information Systems (TIIS)* 13, 6 (2019), 3258–3279.