I. J. Computer Network and Information Security, **2019, 1, 26-39**
Published Online January 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.01.03

Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures

Aaron Zimba
Mulungushi University/Department of Computer Science & Information Technology, Kabwe, 10101, Zambia
E-mail: gvsfif@gmail.com

Mumbi Chishimba
National Institute of Public Administration/Information & Communications Technology, Lusaka, 10101, Zambia
E-mail: Chishimba.mumbi@gmail.com

Received: 23 June 2018; Accepted: 14 November 2018; Published: 08 January 2019

***Abstract*—**The devasting effects of ransomware have continued to grow over the past two decades which have seen ransomware shift from just being opportunistic attacks to carefully orchestrated attacks. Individuals and business organizations alike have continued to fall prey to ransomware where victims have been forced to pay cybercriminals even up to $1 million in a single attack whilst others have incurred losses in hundreds of millions of dollars. Clearly, ransomware is an emerging cyber threat to enterprise systems that can no longer be ignored. In this paper, we address the evolution of the ransomware and the associated paradigm shifts in attack structures narrowing down to the technical and economic impacts. We formulate an attack model applicable to cascaded network design structures common in enterprise systems. We model the security state of the ransomware attack process as transitions of a finite state machine where state transitions depict breaches of confidentiality, integrity, and availability. We propose a ransomware categorization framework that classifies the virulence of a given ransomware based on a proposed classification algorithm that is based on data deletion and file encryption attack structures. The categories that increase in severity from CAT1 to CAT5 classify the technical prowess and the overall effectiveness of potential ways of retaining the data without paying the ransom demand. We evaluate our modeling approach with a WannaCry attack use case and suggest mitigation strategies and recommend best practices based on these models.

***Index Terms*—**Ransomware, encryption, attack structure, bitcoin, enterprise security.

I. Introduction

Ransomware has risen in the past two decades as a virulent infamous malware to reckon with which has posed a lot of challenges. In its early years, ransomware attacks were opportunistic which leveraged spam emails as the major infection vector [1]. Furthermore, it targeted individual users and the attacker generally did not have any prior information about the would-be victims. Additionally, the employed attack structures were based on primitive techniques which were easy to mitigate [2]. As such, earlier calls by academics and scientists stressing the potentially devastating effects of ransomware and preventative measures thereof went answered [3]. But today, ransomware is a destructive billion dollar [4] and game-changer industry in the malware landscape that can no longer be ignored. It has grown to target enterprises businesses and extort millions of dollars in a single attack instance [5]. The success of ransomware can be attributed to many factors but generally, it has evolved from primitive attack structures to techniques that employ industry-standard encryption and protocols, effective infection vectors and targeting enterprises among other things. These factors have seen ransomware attacks eschew indiscriminate single victims and turn to target enterprise systems where the turnover for a successful attack is expectedly high [6]. This shift of focus by cybercriminals from targeting single users to targeting organizations and businesses is echoed by the Interest Over Time (IOT) correlating to major ransomware attacks events on businesses. Enterprise security in most business organizations is focused on confidentiality, i.e. protection of intellectual property, user data, client data etc. Confidentiality in most cases is achieved through the implementation of encryption policies that leverage state-of-the-art protocols based on resilient and robust symmetric and asymmetric cryptosystems such as AES and RSA respectively [7]. Conversely, ransomware has utilized the same robust encryption techniques to effectuate a very robust denial of resource (DoR) attacks [8]. Figure 1 illustrates the IOT of major ransomware attacks on businesses and organizations in 2017 and 2018. The first peak in Figure 1, 14th -20th May 2017, signifies the major turning point of the paradigm shift towards attacking businesses and organizations on a large scale pioneered by the WannaCry crypto ransomware [9]. The second peak corresponds to a variation of the NotPetya ransomware which targeted Ukrainian businesses and government institutions [10]. It is worth noting that although this particular ransomware was discovered in 2016, the initial ransomware did not target enterprises thus not drawing significant IOT. The third peak corresponds to Bad Rabbit ransomware which equally spread via enterprise network structures [11]. The fourth peak corresponds to IOT activities of the SamSam ransomware which typically targets healthcare and government institutions [12].

Unlike other security attacks which leave some parts of the functional, ransomware attacks pose a great security threat to enterprise information systems because they are capable of incapacitating the core business functions of a system. This has forced some victims to part away with millions of dollars [13] and thousands of dollars [14] in form of ransoms, as was with the case of the Nayana Internet Company which paid $1.01 million and the Hancock Health Hospital which paid $55,000.00. Apart from targeting enterprise systems and using robust cryptosystems, the latest variants of ransomware exhibit worm-like features to enable them to propagate and attack various target networks in a short space of time without any human intervention, as was evidenced with WannaCry [16]. Furthermore, newer strains do not embedded encryption keys in the malware payload as was with the case of earlier variants [17]. Instead, they communicate with the command and control (C2) servers upon infection to download resilient hybrid encryption keys. Notwithstanding the aforementioned, newer variants prevent recovery by employing effective data deletion attack structures as later elaborated in this paper. As such, there’s a need to comprehensively understand the paradigm shifts in the ransomware landscape in order to combat the associated challenges.

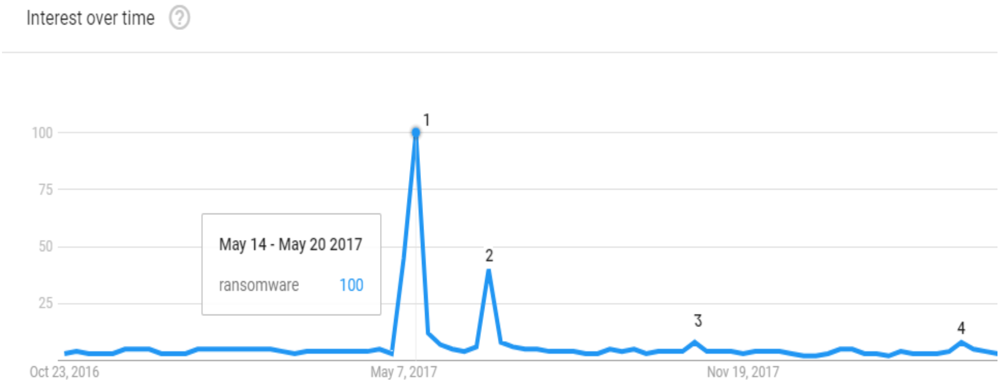


Fig.1. Interest over Time (IOT) Correlating to Ransomware Attacks on Various Businesses and Organizations [15]

In this paper, we seek to address the paradigm shifts in ransomware attack structures to enterprises and other factors that have made the effective such the bitcoin cryptocurrency. We formulate attack models representative of the ransomware attack process from which we devise a ransomware categorization framework by on a classification algorithm. We elaborate on the economic significance of the various categories of the ransomware information systems and recommend mitigation strategies and best practices based on the uncovered attack structures and proposed attack models.

The remainder of the paper is structured as follows: Section II introduces the paradigm shifts in ransomware attack structures and the evolution thereof. Section III discusses the attack and threat models whilst the attack structure classification is presented in Section IV. Section V presents the use case scenario of a ransomware attack whilst the associated illustrative results and the analyses thereof are presented in Section VI. Section VII discusses the mitigation strategies and best practices. Related works are discussed in Section VIII and the conclusion is drawn in Section IX.

II. Paradigm Shift in Attack Structures

There are many components that characterize the overall attack process of ransomware. Newer ransomware strains have sought to exploit the execution of such components to produce resilient ransomware attacks. We focus on four aspects: 1) encryption 2) recovery-prevention techniques 3) C2 communication 4) target audience.

A. Encryption

At the core of the ransomware business model lies encryption. Earlier versions of ransomware did not include encryption. Basically, they were a form of locker-ware which would only lock most parts of the system leaving only essential devices such as the keyboard to enable the victim to pay the ransom [18]. The victim would be intimidated into paying the ransom through various intimidation tactics. However, such ransomware was easy to mitigate. As such, ransomware evolved to include encryption. This implied that all other parts of the system would be left functional, only user files were encrypted and thus inaccessible. At first, ransomware would embed a symmetric encryption key that would subsequently be used to encrypt user data. This fallacy in implementation meant that the key could be extracted via reverse engineering. Newer strains started to use hybrid encryption where a public key embedded in the ransomware payload would be used to encrypt the victim’s data. The advantage was that the data could not be decrypted without the corresponding private key, which resided with the attacker. The difficulty in this attack methodology once a victim was provided with the symmetric key after paying the ransom, the same key could be shared and subsequently used to decrypt any other victim data in different attacks. As such, the latest ransomware uses hybrid cryptosystems where the malware generates sub symmetric and symmetric keys of the host such as AES and RSA, then use the AES keys to encrypt the data. The sub RSA key is used to encrypt the AES keys and the embedded key is used to encrypt the sub RSA key.

B. *Recovery-prevention Techniques*

Despite data being encrypted in any of the above-mentioned approaches, some data would still be recovered via system volume shadow copies or via third party software. As such, upon successfully completing the aforementioned encryption, the newer ransomware strains proceed to delete the remnant files and the volume shadow copies. The volume shadow copies are usually deleted via vssadmin.exe while the remnant files are either deleted primitively by erasing directories structures and meta-data information of the files. The other way of deleting the files is by overwriting it with random data which corrupts the file and make it unreadable. If the files are deleted via meta-data information and directories structures, they are easily recoverable via third-party software and utilities. On the other hand, overwriting the target file with random data makes recovery very difficult. Therefore, newer ransomware strains have evolved to include deletion techniques that delete volume shadow copies and prevent data recovery by overwriting the original target files after encryption.

C. *C2 Communication*

Ransomware has evolved to include C2 communications for various purposes. The C2 infrastructure usually houses the malware and the associated encryption and decryption keys. The C2 is also used to handle ransom payments usually via the bitcoin system. The C2 infrastructure can be owned by the attacker but it is usually a botnet of compromised hosts residing behind some anonymity network [19]. Furthermore, some newer ransomware strains propagated by scripts do not contain the actual payload. Instead, upon infection, the script contacts the C2 server to download the payload and associated keys. In so doing, detection of the ransomware becomes difficult in the early stages when only the script is running. Additionally, some ransomware payloads such as Cryptowall [20] cannot start with first contacting the C2 server for further instructions. As such, the latest ransomware variants have evolved to include C2 communications as an integral component.

D. *Target Audience*

Cybercriminals using ransomware have shifted from targeting arbitrary Internet users to targeting business organizations which turn out lucrative to cybercriminals. Recent trends have seen a shift towards attacking enterprise systems where attackers leverage exploit kits and exploit weakness and vulnerabilities in Internet-facing remote access services such as RDP. Furthermore, newer ransomware strains, like WannaCry, SamSam, Erebus etc, exhibit worm-like characteristics which enable them to traverse the entire network structure of an information system subsequently infecting any discovered vulnerable host. This leads to attack on online backup systems. Contrast the average demand ransom of $300 in opportunistic attacks to $55,000 in targeted attacks. And depending on the value of the data, cybercriminals have even extorted over $1 million in a single ransomware attack. This has seen the rise of destructive ransomware such as Erebus, SamSam, NotPetya etc, all targeted at enterprises. Furthermore, the new strains have worm-like capabilities which enable them to propagate throughout the entire enterprise network with further human intervention. As such, the attack vectors used in such attacks have not been the classical spam emails but spear-phishing and vulnerability exploitation.

III. Attack and Threat Models

Using the information thus far, we now turn to formulate the threat and attack models. It can be deduced that the first generation of ransomware did not include encryption and neither did it employ any data recovery-prevention techniques.

A. *Attack Model*

The second generation introduced the use of encryption but the keys were recoverable due to poor implementation strategies. The third generation saw the inclusion of robust encryption techniques and communication with the C2 servers. The diagram in Figure 2 shows the timeline of this evolution.

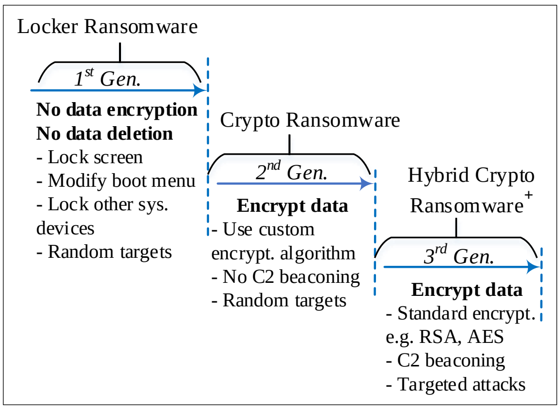


Fig.2. Evolution of Ransomware Attack Structures

It is clear from Figure 2 that 3^{rd} generation ransomware includes improved attack structures of the previous generations. As such, to capture all the attack structures associated with the latest ransomware, we develop an attack model based on the characteristics of 3rd generation ransomware. The diagram in Figure 3 depicts our attack model which encompasses all the characteristics exhibited in 3rd generation ransomware.

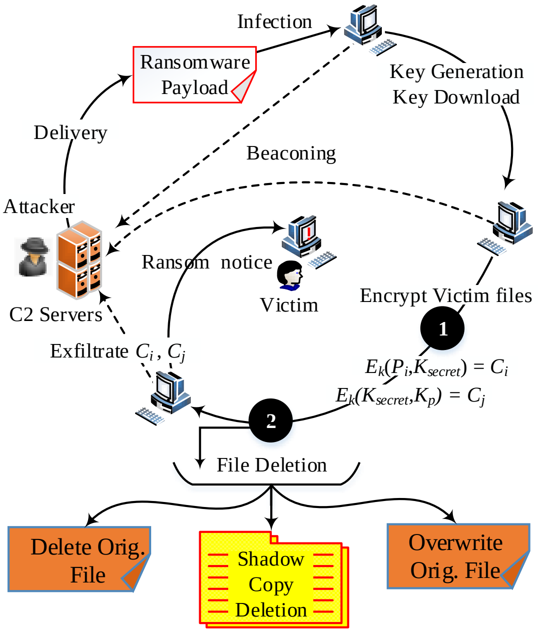


Fig.3. 3rd generation-based Attack Model

To effectuate an effective ransomware attack in 3rd generation ransomware, the ransomware carries out two major tasks; (1) encrypt the target files and (2) delete the original files after encryption. Encryption of the target files is denoted by $E_k(P_i, K_{secret}) = C_i$. Some attack structures generate a symmetric key using the victim's operating system *CryptoAPI* [21]. After this key completes encrypting the target files, it is further encrypted by the embedded public key which is denoted by $E_k(K_{secret}, K_p) = C_j$. The resultant ciphertext C_j is exfiltrated to the C2 server. In the case of single key attack model, the encryption process is denoted as:

$$\{m_i(target\_payload)\}_{K_{pub}} \to C_i \tag{1}$$

$$\{m_i(target\_payload)\}_{K_{secret}} \to C_i \tag{2}$$

Equation (1) is an implementation of an asymmetric cryptosystem whilst Equation (2) a symmetric cryptosystem. It is worth noting that such an attack structure is valid for a single key cryptosystem where the encryption key is K_{pub} in an asymmetric cryptosystem and K_{secret} in a symmetric cryptosystem. In the case of a hybrid key attack model, the encryption attack process is denoted as:

$$\{m_i(data_1)\}_{K_{sym}} \to C_i \tag{3}$$

$$\{K_{secret}(data_2)\}_{K_{pub}} \to C_j \tag{4}$$

Equation (3) denotes the first stage of the encryption process where m_i is the plaintext message (targeted files) $data_1$ and C_i is the resultant ciphertext. Equation (4) is the second stage of the encryption process where $data_2$ is the symmetric key K_{secret} used in Equation (3) and K_{pub} is the public key while C_j is the resultant ciphertext.

B. Threat Model

The evolution of ransomware from 1st to 3rd generation has not only seen the integration of the aforementioned robust and resilient encryption methodologies but also a shift towards attacking enterprise information systems. As such, we formulate a threat model applicable to cascaded network design structures common in enterprise systems. The diagram in Figure 4 shows the resultant threat model.

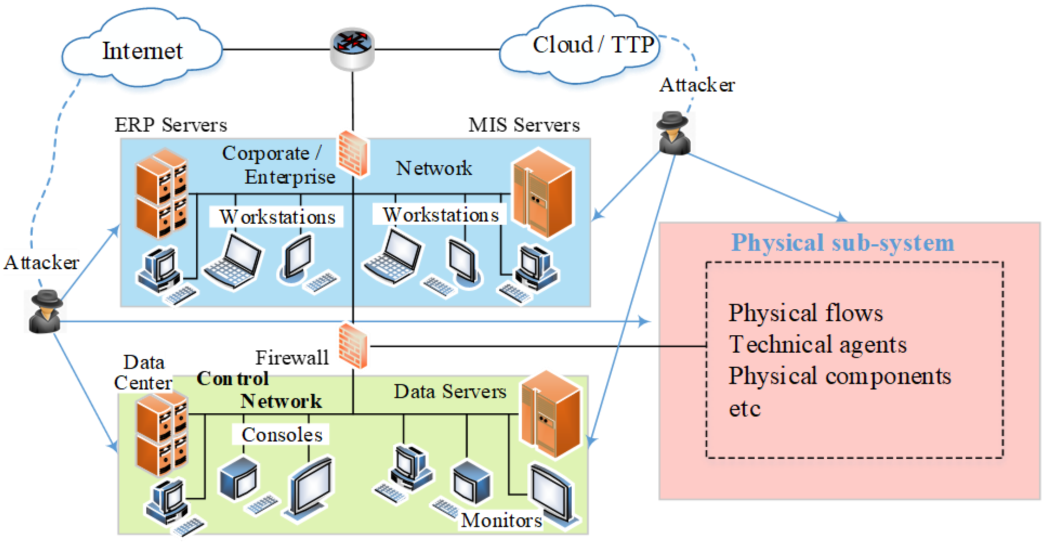


Fig.4. Generic Enterprise System Network Structure

The conventional network design structure in enterprise networks presents multiple entry points as infection vectors for ransomware, unlike independent Internet users where the main infection vector is spam emails. This increases the attack surface which in itself is an attractive feature to ransomware cybercriminals. The threat model in Figure 4 shows the various susceptible entry points into EISs. Most network structures implement the Purdue Model [22] where the enterprise network is separated from the control and physical network via a cascaded design. Few poorly designed network patterns combine any two of the three network segments into one broadcast domain which poses even a higher threat. Regardless of the network design pattern, enterprise networks present three major entry point into the network. The first entry point is the corporate network that is directly connected to the Internet via some firewall or router. Any lapses or vulnerability in the Internet-facing device will act as an entry point of the malware. This is a feature which the SamSam ransomware exploited, unlike the common spam email infection vector. The same is true of any Internet-facing device in the control network or physical sub-system which are two other entry points. Vulnerabilities of such devices are easily found on Internet devices public search engines such as Shodan [23]. In the event that the enterprise outsources ICT solutions, trust relationships with third-party or vendors can foster ransomware infection as the vendor will act as a conduit through which the malware will traverse the network. Trusted third-party providers (TTP) or vendors could also be cloud providers or remote technical solutions providers who might have remote access permissions to the three segments of the network structure. Ransomware propagation is also known to take advantage of such RDP connections which even empowers them with a persistent presence [24]. Apart from all these potential infection vectors, there is also the common infection vector that exploits the ignorant user via spam email, phishing and watering hole attacks. All these infection vectors to an enterprise network make them a lucrative target of ransomware attacks.

It is evident that the end goal of a ransomware attack is to make user data inaccessible. Essentially, ransomware breaches the Availability security principle in the CIA (Confidentiality, Integrity, and Availability) triad. However, as seen from the attack model in Figure 3, the ransomware has to access and modify target file before encrypting them. As such, access to the prohibited user files is an act of breaching confidentiality. Ransomware usually targets certain file extensions such as .docx, .pdf, .jpeg, .mp3 etc. Therefore, the ransomware will seek to first access such types of files which is a breach of confidentiality. Afterward, the ransomware will delete the delete the original file or overwrite it with random data to make recovery impossible. This file modification, together with deleting the system volume shadow copies is, in essence, a breach of integrity. In view of this, the principles of the CIA triad are breached in the following order:

$$Confidentiality \rightarrow Integrity \rightarrow Availability$$

This order of attack events is particularly important in the formulation of effective mitigation strategies. As such, we employ a finite state machine to depict the CIA security breaches that a target system undergoes in a typical 3rd generation ransomware attack.

Using binary encoding, we define four security states S_n (henceforth referred to as states) namely:

$$f(\alpha,\beta,\gamma), where\ \alpha,\beta,\gamma\ \in\ \mathbb{N}_2 \tag{5}$$

Equation (5) characterizes the state of the system at any instance during the ransomware attack. In any given state, any or all or a combination of CIA principles can be breached. Since $\alpha,\beta,\gamma\ \in \{0,1\}$, it follows that these variables have complement values henceforth denoted as $\bar{\alpha},\bar{\beta}\ and\ \bar{\gamma}$ respectively. We now seek to deduce state functions representative of these states which are valid in as far as the attack model is concerned. We use canonical Sum of Products (SOP) and K-maps to derive the equations representative of the four states. Thus, the state function representative of the first state $\boldsymbol{S_{00}}$ is defined as:

$$f(S_{00}) = \bar{\alpha}\cdot\bar{\beta}\cdot\bar{\gamma}\ \ where\ \alpha,\beta,\gamma\ \in\ \mathbb{N}_2 \tag{6}$$

Since $f(S_{00})$ is a Boolean function which only holds true when all the three binary variables are equal, we can use the Kronecker discrete delta function to represent this secure state where $\alpha,\beta,\gamma\ \in [i,j,\ldots]$:

$$\delta_{i,j}(\boldsymbol{S_{00}}) \equiv \begin{cases} 1\ for\ i=j, \\ 0\ for\ i\ \neq\ j. \end{cases} \tag{7}$$

Intuitively, the last state $\boldsymbol{S_{11}}$ can also be expressed Kronecker discrete delta function since it only holds true when all the variables are equal, i.e. a full breach of all the CIA principles. As such, the state function is expressed as:

$$\delta_{i,j}(\boldsymbol{S_{11}}) \equiv \begin{cases} 1\ for\ i=j, \\ 0\ for\ i\ \neq\ j. \end{cases} \tag{8}$$

The state of the system when only one tenet on the CIA principles is breached is denoted as:

$$f(S_{01}) =\ \alpha\cdot\bar{\beta}\cdot\bar{\gamma}\ +\ \bar{\alpha}\,(\beta\ \oplus\ \gamma) \tag{9}$$

Owing to the XOR operation, Equation (9) is a system of three equations. According to the attack model in Figure 3, the ransomware first needs to read the file extensions before deleting or encrypting any files. As such, this is representative of a confidentiality breach. Therefore, Equation (9) further reduces to:

$$f(S_{01}) =\ \alpha\cdot\bar{\beta}\cdot\bar{\gamma},\ where\ \alpha,\beta,\gamma\ \in\ \mathbb{N}_2 \tag{10}$$

In the same way, the state function representative of an instance when two tenets of the CIA principles have been breached is denoted as:

$$f(S_{10}) = \alpha \cdot \beta \cdot \bar{\gamma} + \gamma\,(\alpha \oplus \beta) \tag{11}$$

Owing to the XOR operation, Equation (11) is a system of three equations. According to the attack model in Figure 3, the ransomware first needs to read the file extensions then deletes volume shadow copies and then encrypts the files. As such, this is representative of a confidentiality and integrity breach. Therefore, Equation (11) further reduces to:

$$f(S_{10}) = \alpha \cdot \beta \cdot \bar{\gamma}, \quad where\ \alpha, \beta, \gamma \in \mathbb{N}_2 \tag{12}$$

Using the four state equations depicting the various states of a 3rd generation ransomware attack, we construct the corresponding finite state machine as shown in Figure 5.

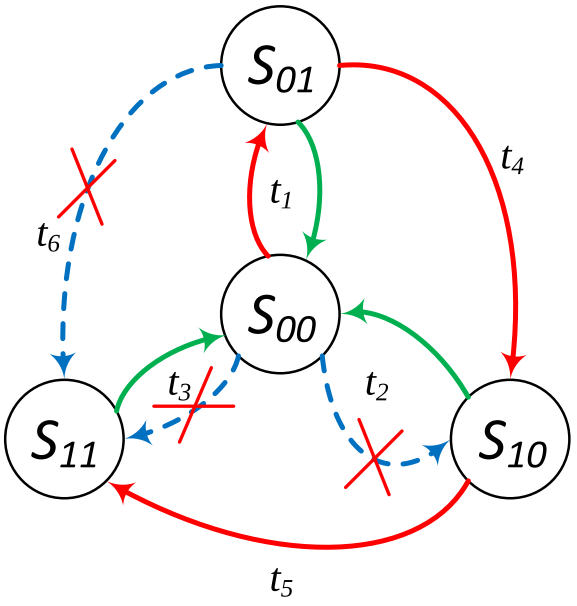


Fig.5. State Transition Diagram of CIA Breaches

From the state diagram in Figure 5, the nodes are denoted by states $\boldsymbol{S_{00}}$, $\boldsymbol{S_{01}}$, $\boldsymbol{S_{10}}$ and $\boldsymbol{S_{11}}$ while attack actions are denoted by directed red edges and directed green edges denote actions that thwart these attacks. The blue dotted edges denote infeasible transitions. This valid considering the logical occurrence of the CIA attack events. To deduce which node is the isthmus of the graph and consequently to be prioritized during mitigation, we deduce the corresponding connectivity matrix which denotes the adjacency matrix.

$$CM = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{13}$$

We see from the connectivity matrix in Equation (12) that even node $\boldsymbol{S_{10}}$ has the highest vertex degree, node $\boldsymbol{S_{01}}$ represents a cardinal node and the source of the isthmus of the graph $\boldsymbol{t_1}$. Without the isthmus edge $\boldsymbol{t_1}$ which essentially results into a breach of confidentiality, other attack actions $\boldsymbol{t_4}: \{\boldsymbol{S_{01}} \rightarrow \boldsymbol{S_{10}}\}$ and $\boldsymbol{t_5}: \{\boldsymbol{S_{10}} \rightarrow \boldsymbol{S_{11}}\}$ which corresponding to breaches of integrity and availability respectively do not materialize. As such, turning this vertex into a failure node should be prioritized as it can be seen that there is no further graph traversal in the absence of node $\boldsymbol{S_{10}}$ and transition $\boldsymbol{t_1}$. The blue transition $\boldsymbol{t_2}: \{\boldsymbol{S_{00}} \rightarrow \boldsymbol{S_{10}}\}$ denotes an infeasible attack action where an integrity breach supersedes a confidentiality. Such a condition forbidden by the attack model as attested by Equation (11). In the same manner, the blue transition $\boldsymbol{t_3}: \{\boldsymbol{S_{00}} \rightarrow \boldsymbol{S_{11}}\}$ denotes an infeasible attack action where an availability attack supersedes a confidentiality and integrity breach. Likewise, such an attack action is forbidden as constrained by the attack model. The attack action denoted by the blue edge $\boldsymbol{t_6}: \{\boldsymbol{S_{01}} \rightarrow \boldsymbol{S_{11}}\}$ represents an attack action which was common in earlier variants of ransomware where there was no actual encryption or deletion of files.

IV. Attack Structure Classification Framework

We now present a framework that classifies any given ransomware attack of the 1st, 2nd or 3rd generation. The framework is based on the evolution of the various ransomware attack structure characteristics presented in Figure 2. Table 1 shows the various characteristics spread across the three generations of ransomware. We use this categorization framework to formulate a classification algorithm that classifies a ransomware given its attack structures. Algorithm 1 depicts our classification algorithm. Our framework expresses the severity of a ransomware in terms of file encryption and file deletion. As such, it shows how challenging and time consuming it will be to mitigate a given ransomware attack using the classical methods of static and dynamic analysis. The virulence depicted in the framework is flexible, i.e. a ransomware can move up or down the category list depending on newly discovered properties.

Since the framework categorizes the ransomware in ascending order, it is clear that ransomware CAT1, which is a typical 1st generation ransomware, is easier to mitigate than CAT5 which is 3rd generation ransomware. As such, CAT5 is the most virulent whilst CAT1 is the least virulent where recovery of data does not require any decryption keys. Since the first sub-category of CAT1 does not implement resilient attack structures as depicted in Figure 2, the severity is negligent and it's thus categorized as Scareware/Locker-ware. Examples of such malware include AnonPop [25]. CAT2 ransomware employs only the file encryption attack structures. The key can be download from the C2 or it can come embedded in the payload. This is an example of a poorly implemented ransomware as was the case with Bad Rabbit [26] despite using robust cryptosystems. Since there's no deletion of volume shadow copies, data can be recovered via system restore utilities or third-party software.

Table 1. Ransomware Classification Framework

CATEGORY (Severity)	**ENCRYPTION ATTACK MODEL**						**DELETION ATTACK MODEL**	
	Hybrid cryptosystem			*Single Key Cryptosystem*			*Delete Volume Shadow Copies*	*Overwrite & Delete Original File*
	C2 download	*Payload embedded*	*Local key Generation*	*C2 download*	*Payload embedded*	*Local key Generation*		
CAT1	✗	✗	✗	✗	✗	✗	*NO*	*NO*
	✗	✗	✗	✗	✗	✗	*YES*	*NO*
	✗	✗	✗	✗	✗	✗	*NO*	*YES*
	✗	✗	✗	✗	✗	✗	*YES*	*YES*
CAT2	✓‖ ✓‖ ✓			✗			*NO*	*NO*
	✗			✓‖ ✓‖ ✓			*NO*	*NO*
CAT3	✗	✗	✗	✓*($K_{enc} = K_{sym}$)*			*YES*	*YES*
CAT4	✗	✗	✗	✓‖ ✓‖ ✓			*YES*	*YES*
CAT5	✓‖ ✓‖ ✓			✗	✗	✗	*YES*	*YES*

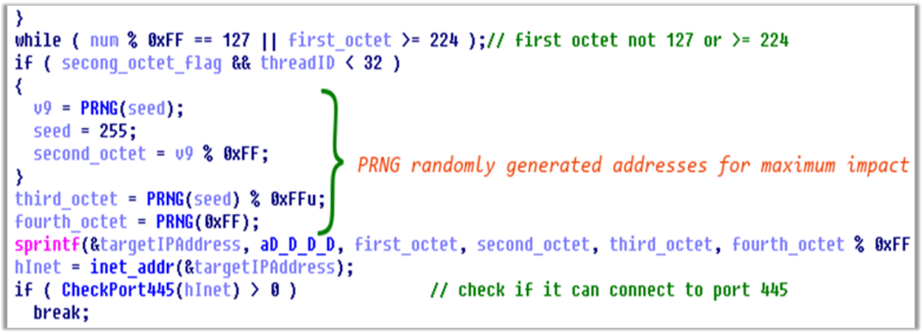
CAT3 represents earlier and uncommon types of ransomware that are based on single key attack structures. In this category, the ransomware comes with an embedded symmetric key in the payload. The key can be simply retrieved using reverse engineering. In the event that the key is deleted from the payload, data deletion recovery techniques discussed in the preceding categories can be used to recover the key. However, if the embedded key is a public key from an asymmetric cryptosystem, it is of no value to extract the public key since it cannot decrypt the data. This is representative of CAT4. Another instance of CAT4 is where the key is downloaded from the C2 server. The key can be symmetric or asymmetric as was with the case of CryptoWall. In the case of the latter, it is very difficult to mitigate the attack since there are no residual encryption essentials on the victim. CAT5 represents the current generation of ransomware. The attack structures implement all the deletion techniques and use hybrid cryptosystems.

Algorithm 1: Attack structure classification algorithm

```
Input: Encryption & deletion attack structures
Output: Ransomware category
if SKc2emb=SKPemb=SKlocalgen=
      HKc2emb=HKPemb=HKlocalgen=no then
     malware ← CAT1
 else
    if delShdCpy=ovrFile=no then
       malware ← CAT2
    else
       if SKc2emb=SKPemb=SKlocalgen=no then
          malware ← CAT5
       else
          if SKc2embsym = SKPembsym =
              SKlocalgensym = yes then
             malware ← CAT3
        else
          malware ← CAT4
        end if
     end if
  end if
 end if=0
```

Wannacry is a typical CAT5 3rd generation ransomware which deletes not only the volume shadow copies but the remnant files as well. Further, it comes with an embedded master RSA public key and uses the operating system's CryptoAPI to generate an RSA sub-key pair and AES keys. Each of the unique AES keys is used to encrypt a unique target file. The embedded RSA master public key is used to encrypt the private key from the generated RSA sub-key pair. The public key of the generated RSA sub-key pair is used to encrypt the unique AES keys. As such, to decrypt the data, the victim needs the AES which is encrypted by the private key of the generated RSA sub-key pair. This can only be decrypted by the corresponding generated RSA private sub-key pair, but then, it has been encrypted by the embedded RSA master public key. What the RSA master key has encrypted can only be decrypted by the corresponding RSA master private key which is in the domain of the attacker. The attacker thus demands a ransom to release the decryption key.

Furthermore, new ransomware strains not only attack the targeted host in a given network but also scans the entire network for vulnerable hosts. This worm-like capability was observed in WannaCry which propagated throughout the entire network on port 445 running vulnerable SMBv1 file-sharing services. This means that all online backups likewise would be encrypted. The ransomware also scans for vulnerable hosts in the neighboring networks, both private and public IP scopes. The diagram in Figure 6 shows an extract of ransomware code with directives to scan neighboring subnets in the enterprise network after successfully infecting the target network. The ransomware uses a PRNG and a corresponding seed to generate IP address scopes to scan both in the local network scope as well as the Internet. This implies that the ransomware would spread to other parts of the cascaded enterprise networks as shown in Figure 4. The worm-like capabilities are a new feature of 3rd generation ransomware targeting large networks.



```
}
while ( num % 0xFF == 127 || first_octet >= 224 );// first octet not 127 or >= 224
if ( secong_octet_flag && threadID < 32 )
{
  v9 = PRNG(seed);
  seed = 255;
  second_octet = v9 % 0xFF;
}
third_octet = PRNG(seed) % 0xFFu;
fourth_octet = PRNG(0xFF);
sprintf(&targetIPAddress, aD_D_D_D, first_octet, second_octet, third_octet, fourth_octet % 0xFF
hInet = inet_addr(&targetIPAddress);
if ( CheckPort445(hInet) > 0 )                // check if it can connect to port 445
  break;
```

PRNG randomly generated addresses for maximum impact

Fig.6. Directives to Scan both Private and Public Neighboring Networks

V. A Use Case Scenario: WannaCry Ransomware

To illustrate the capabilities of CAT 5 3rd generation ransomware depicted in Table 1, which include unsupervised attacks on neighboring networks, we employ a use case of Wannacry ransomware attack. We choose to use WannaCry owing not only to its worldwide attacks and media coverage but also because it was the ransomware in the 3rd generation that exhibited self-propagation worm features which enable it to attack large networks.

Since the *Access Vector* for the CVE-2017-0144 (exploited by WannaCry) is *Network*, the attack is feasible from within and outside the targeted cloud subnet. Therefore, we partition two attack scenarios generating two different attack paths:

(1) when the attacker resides within the internal subnet
(2) when the attacker resides in an external subnet and thus requires to reach the target network across OSI layer 3 boundaries before launching the attack.

We simulate these two attack scenarios (1 and 2) on VMs in a virtualized sandbox environment as illustrated in Figure 7 using hypervisor type II.

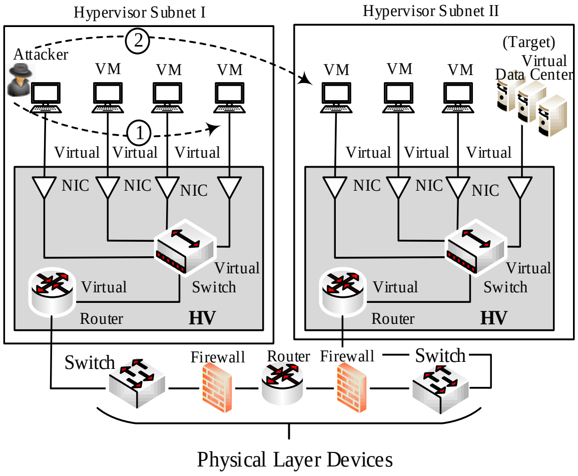


Fig.7. Attack Scenarios from two Different Subnets

A. Internal Subnet

Upon infection on a local subnet, WannaCry spawns two threads which scan the local and external subnets. The first thread uses the $GetAdapterInfo()$ function to retrieve local subnet details such as subnet mask and network range. Local subnet scan is multithreaded and limited to 10 IP addresses per scan. The thread seeks to establish a connection on port 445 to exploit CVE-2017-0143 if the SMB vulnerability is present on any host in the scanned IP addresses. In our use case, we infect a vulnerable host in the subnet with RDP backdoor vulnerability [27]. Based on the CVE values, we deduce $\lambda = 0.430$ and $k = 2$ using the base score, where k is the attack steps and λ the attack complexity. We later use these values to generate characteristic density functions.

B. External Subnet

In the second attack scenario where the target resides in a different subnet, the second thread generates a list of external IP addresses ranges to be scanned and probes for a connection on port 445. Based on the CVE values, we deduce $\lambda = 0.348$ and $k = 3$ using the base score.

Another attack scenario utilizing a path identical to the above seeks to reach the target by exploiting another SMB vulnerability CVE-2017-0148. Using this particular CVE, the corresponding values of the attack complexity and attack steps are $\lambda = 0.400$ and $k = 3$ respectively.

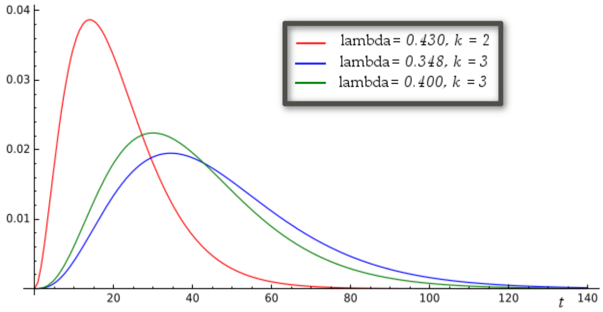


Fig.8. Density curves for the 3 Attack Instances

We use the above evaluated characteristic values together with the Erlang functions to generate density functions representative of the attack scenarios. The result density curves are shown in Figure 8. All the three density curves are positively skewed denoting intensified attack activities in the early stages of the attack. This is a typical feature of the WannaCry ransomware as earlier explained. The first attack scenario corresponds to the red curve where the mean and median of the distribution lie after the mode. As such, we can infer the characteristics of the attack scenarios from the generated density functions and use them for prioritizing which attack paths need attention in the mitigation process.

In this case, nodes and edges in the shortest attack paths should be given first priority when designating failure nodes for mitigation purposes.

VI. Illustrative Results and Analyses

We analyzed the attack structures of 20 different ransomware samples. The classification both in terms of virulence and generation categories are shown in Table 2.

Table 2. Classifications of Ransomware Attack Structures

Name	Gen.	CAT.	Year	Paid Ransoms	Platform
AIDS	2nd Gen.	*CAT2*	1989	-	Windows
CryptoDefense	3rd Gen.	*CAT4*	2014	> $65,000	Windows
CryptoLocker	3rd Gen.	*CAT4*	2014	>$ 3 million	Windows
CryptoWall	3rd Gen.	*CAT4*	2015	$18 million	Windows
DMA-Locker	3rd Gen.	*CAT4*	2015	> $180,000	Windows
Linux.Encoder	3rd Gen.	*CAT3*	2015	-	Linux
TeslaCrypt	3rd Gen.	*CAT4*	2015	> $80,000	Windows
AnonPop	1st Gen.	*CAT1*	2016	-	Windows
Cerber	3rd Gen.	*CAT5*	2016	> $500,000	Windows
Jigsaw	3rd Gen.	*CAT3*	2016	> $2,000	Windows
KeRanger	3rd Gen.	*CAT4*	2016	> $5,000	Mac OS
Locky	3rd Gen.	*CAT4*	2016	>$ 1 million	Windows
Petya	3rd Gen.	*CAT5*	2016	> $30,000	Windows
VenusLocker	3rd Gen.	*CAT5*	2016	> $6,500	Windows
ZCryptor	3rd Gen.	*CAT5*	2016	-	Windows
Bad Rabbit	2nd Gen.	*CAT2*	2017	-	Windows
Erebus	3rd Gen.	*CAT5*	2017	> $1 million	Linux
NotPetya	3rd Gen.	*CAT3*	2017	> $10,000	Windows
WannaCry	3rd Gen.	*CAT5*	2017	> $140,000	Windows
SamSam	3rd Gen.	*CAT5*	2018	> $850,000	Windows

The Name column denotes the name of the ransomware. We maintain the initial name associated with the malware when it first appeared as depicted in the Year column. The Gen. column denotes the generation under which the ransomware falls whilst the CAT column denotes the category under which the ransomware categorized by the classification algorithm. The Paid Ransoms column denotes the monetary value associated with the corresponding ransomware attack campaign. Null entries reflect unavailable or unverified data whereas the Platform column denotes the target operating system. It is clear from the table that the Windows operating system is the primary target across all categories and generations. Despite being a billion-dollar industry today, ransomware attacks came to prominence just this decade (at the time of writing). Most of the ransomware for this era fall in the 3rd generation and mostly fall under CAT4 and CAT5. Even though the encryption methodologies used in current ransomware have been available for some time, their widespread adoption has not been until the appearance of 3rd generation ransomware. The monetary value attached to this generation is exceptionally high when compared to other generation. It is worth noting that 3rd generation ransomware is mostly not necessarily new ransomware strains but are rather enhanced variants of earlier generations with new attack structure characteristics. As such, it is important to note the generation to which a ransomware variant belongs because mitigation strategies applicable to an earlier variant of the ransomware will not be effective in countering the new variant. As such, a ransomware variant can go up the generation and category classification with time when attackers include new attack structures to the existent ransomware. It is clear from Table 2 that 3rd generation and CAT4/CAT5 have been persistent as they are difficult to mitigate owing to the many incorporated attack structures. The evolution of ransomware from 1st generation to 3rd generation has seen an increment in the emergence of resilient ransomware variants mostly falling in CAT5 as depicted in ransomware-attack statistics in Figure 9 [28]. The surge in ransomware attacks represents a 229% increment most of which are CAT4 and CAT5 ransomware in the 3rd generation.

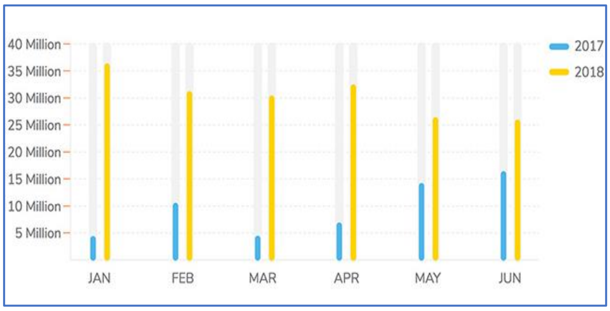


Fig.9. 2017/2018 Global Ransomware Attack Statistics

Poorly designed ransomware have been neglected over the years as was the case with CAT2 ransomware which appears only in 2017 and not prior or after. This is a common characteristic erroneously or poorly implemented ransomware variants. Modifications of such variants are not uncommon and the result is usually a state-of-the-art ransomware, i.e. 3rd generation and CAT5.

Figure 10 shows the overall statistics of the various generations of ransomware and their associated categories. The years 2014 – 2016 see a steady appearance of CAT4 ransomware which is followed by a steady appearance of CAT5 ransomware from 2016 – 2018. Other ransomwares are resilient and span several years. This is the case with CAT3 ransomware except for the AIDS ransomware of 1989. By volume, it is evident from Figure 10 that CAT4 and CAT5 are the most common which are essentially 3rd generation ransomware, followed by CAT3. CAT3 and CAT4 ransomware can be mitigated effectively via reverse engineering (static analysis) provided the key used is symmetric. CAT5 can be mitigated if the encryption attack structure uses hybrid encryption essentials from the victim.

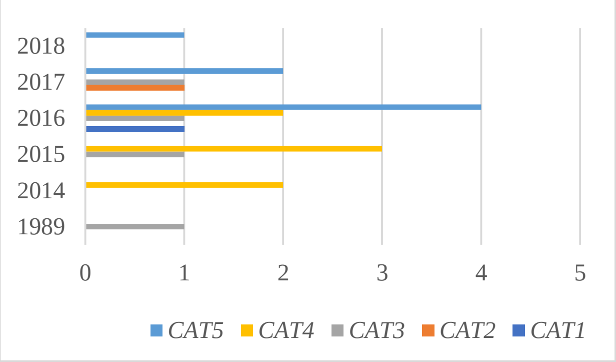


Fig.10. Distributions of Ransomware Categories

Table 3. Notable Disclosed Paid Ransoms

Campaign Name	CAT	Gen.	Victim	Ransom Paid	Time
Erebus	CAT5	3rd Gen.	Nayana	$1.01 million	June 2017
SamSam	CAT5	3rd Gen.	Hancock Health	$55,000	Jan. 2018
Undisclosed	-	-	Los Angeles Community College District	$28,000	Jan. 2017
Undisclosed	-	-	University of Calgary	$28,000	June 2016
Locky	CAT5	3rd Gen.	Hollywood Presbyterian Medical Center	$17,000	Feb. 2016

The adverse effects of ransomware attacks, especially 3rd generation CAT4 and CAT5, have been felt across all sectors of the economy. The ransomware business model is a fast-growing billion-dollar industry whose global damage costs are extrapolated to reach $11.5 billion by 2019. Ransomware costs come in two forms; (1) money paid via ransoms, (2) and loss of production and money spent on recovery efforts in the event the victim does not pay, or when they pay but the attacker does not keep his end of the bargain, or when decryption fails due to implementation errors. In the former, costs range from hundreds of dollars to thousands of dollars, except the Nayana attack which is the only reported ransom payment to reach millions of dollars. In the latter, costs range from thousands to millions of dollars in terms of loss of production and recovery efforts. In our scope, we concentrate on losses incurred by business organizations or government institutions and not individuals. Table 3 shows some of the most notable paid ransoms in the past 3 years at the time of writing this paper. It shows that 3rd generation CAT4 and CAT5 ransomware are not uncommon and due to the difficulty in retaining the data, such attacks tend to cost more. One major hindrance to statistics on ransomware attacks is that some incidents go unreported due to various reasons such as legal implications and fear of loss of credibility. As can be seen, most financial losses are in the range of thousands of dollars apart from the Nayana entry which is an outlier.

Apart from losses in paid ransoms, business organizations incur financial losses in form of recovery efforts when they do not have backups and they are unable to meet the ransom demand for one reason or another. In other instances, they would have met the ransom demand but they are unable to decrypt their encrypted data for a reason or two. The recovery processes can last from a couple of days to even years. Table 4 shows the losses incurred in the form of recovery efforts in the aftermath of 3rd generation CAT5 ransomware attacks.

Table 4. Estimated Losses after 3rd Gen, CAT5 Ransomware Attacks

Attack Name	Gen.	CAT	Victim	Ransom Demand	Estimated Loss	Year
Sam Sam	3r Gen.	CAT5	City of Atlanta	$50,000	$3 million	Mar 2018
Not Petya	3r Gen.	CAT5	Merck	$50,000	$310 million	June 2017
Sam Sam	3r Gen.	CAT5	Colorado Transp. Dept.	$51,000	$1.5 million	Feb. 2018
Not Petya	3r Gen.	CAT8	Maersk	$51,000	$300 million	June 2017
Not Petya	3r Gen.	CAT5	FedEx	$51,000	$300 million	June 2017
Not Petya	3r Gen.	CAT5	Nuance Communication	$50,000	$92 million	June 2017

It is worth noting that loss of production begins the moment the attack strikes whether the victim is willing to honor the ransom or not. For an enterprise, this implies that it is very difficult to mitigate a ransomware attack without incurring any form of loss. As can be seen in Table 4, 3rd generation CAT5 ransomware attacks cost millions of dollars due to loss of production and recovery efforts. It further shows that the value of the demanded ransom is way less than losses incurred in recovery efforts. Additionally, there are usually unaccounted for financial losses even in the aftermath of paying a ransom since it's illogical not to upgrade the security of the system after an attack. The attack fallouts that need mitigation in the recovery process includes restoration and redistribution of thousands of affected computers, email communication blackout, complete rebuilding of affected servers, free service to affected customers and percentage discount in perpetuity (Nayana attack aftermath), free service in perpetuity for clients whose data is unredeemable, establishment and or strengthening security infrastructure such as firewalls, IDS, filters, user awareness training programmes, security consultancy etc. This results in huge financial losses as depicted in Table 4. Furthermore, it is clear that the affected business organizations are those with massive information system, hence the huge loss. This shifting towards attacking enterprise systems is a characteristic feature of 3rd generations ransomware variants. The discussed financial proceeds of the ransomware attack thus far relate to singular payments made by specific organizations.

Another perspective of evaluating the economic impacts of the various ransomware generations and categories is by tracking the actual payments made to a specific bitcoin address. Cybercriminals usually have bitcoin addresses where ransom payments are directed to. The cumulative payments made to these bitcoin addresses over specific periods of time are shown in Table 5. However, one important thing to note is that Bitcoin addresses associated with criminal activities might receive a number of different payments other than for the sole purpose of ransom payments. One way to capture ransom payments is to consider the age of the bitcoin address and the value of each incoming payment to verify whether such parameters correspond to the period of the ransomware attack campaign and the demanded ransom respectively. As seen from Table 5, WannaCry a 3rd generation CAT5 ransomware, despite having made world headlines and taking the media by storm, did not accrue substantial cyber-crime revenue when compared to others. This was due to poor implementation and an embedded kill-switch which was used to stop the attack.

Table 5. Cumulative Payments to specific Bitcoin Addresses

Name	Gen.	CAT	Cumulative Value	Period
CryptoWall	3rd Gen.	CAT 5	$2.2 million	Jan 2014 – Jan 2018
Erebus	3rd Gen.	CAT5	$1.01 million	June 2017
CryptoLocker	3rd Gen.	CAT5	$450,000	Sep. 2013 - Feb.2014
DMA Locker	3rd Gen.	CAT5	$179,000	Dec. 2015 – Sep. 2016
WannaCry	3rd Gen.	CAT5	$140,000	May – Aug. 2017

From all the ransomware campaigns that have been running for the past 6 years as shown in Table 5, CryptoWall has accrued the highest proceeds. This is despite the fact that the ransomware does not operate successfully in the absence of the Internet as it requires communication with the C2 in order to complete the encryption process. As such, this particular ransomware lies that the border of 2nd and 3rd generation ransomware because it exhibits some but not all of the characteristic of 3rd generation ransomware. The average grace period for paying the ransom is typically 72 hours (3 days). However, this time might not be enough to make a decision and follow through the process of converting fiat money to bitcoins. In light of this, some companies are reported to be keeping Bitcoins in reserve just in case ransomware strikes unexpectedly should they decide to pay. From the categorization framework, we can see that data recovery in a ransomware attack can be implemented against data deletion or cryptographic encryption. In the former, the use of standard tools like volume shadow copies or third-party recovery tools can be used based on the deletion attack structure. In the latter, data recovery can be attained using the decryption key.

Depending on the attack structure, this can be achieved by extraction of encryption key parameters from memory analysis if some facets of the encryption essentials are generated on the host. Most attack structures implementing hybrid cryptosystems involve some form of key generation on the host which can be exploited for building the decryption key. Therefore, rushing to consider paying a ransom after a ransomware attack should not be the first option.

VII. Mitigation Strategies and best Practices

The common saying that "prevention is better than cure" is more applicable to ransomware. This is evidenced by the huge financial costs associated with recovery efforts as depicted in Table 4. The reason why it is best to prevent ransomware than seek to mitigate the after effects is that unlike other attacks, getting rid of the ransomware malware does not restore the data once encryption is complete. Therefore, ransomware is better kept away from information systems right at the entry point, i.e. infection vectors. There are two main strategies through which ransomware enters the victim's environment; (1) through third-party pivots like emails, EKs, malvertising, watering-hole, social engineering etc (2) direct attack via vulnerability exploitation.

A. Third-party Pivots

Communication, whether internal or external, is a core functionality of any business organization. As such, most enterprises use emails for such communications. Attackers, therefore, seek to leverage email as a medium to deliver ransomware payload to victims and employ social engineering such as spear-phishing to trick the benign victim into running the ransomware. Figure 11 shows the various mediums through which ransomware enters information systems with emails topping the list with a cumulative total of 59%.

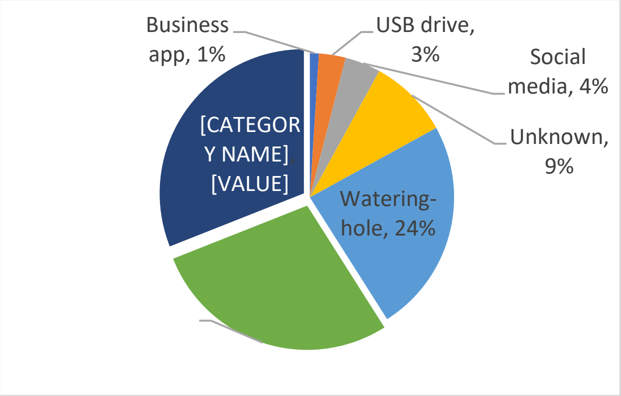


Fig.11. Ransomware Infection Vectors

As can be seen from the graph, emails are a major source of ransomware. One of the most effective ways of securing this entry point is strong spam email filters and intelligent-based intrusion detection systems. These should be configured on two levels; host level and network level. Spam filters are more applicable to the network level domain while intelligent IDS capable of discovering ransomware activities can be employed at host-level. Such filters should not only sick to filter certain ransomware payloads as identified according to the digital signature but also dirty links that might point to external sources housing the ransomware. The intelligent IDS can also act as a feed-source for spam filter policies. However, no one system is fool-proof. No matter the security controls, ransomware might slip through the system and as such, user training and awareness is very vital. Employees ought to be trained on the ways through which ransomware spreads, and not only that but how it also relies on their action to actually effectuate the attack. Ransomware hiding in an attachment or “dirty” link will remain inactive so long no one clicks on it. Therefore, user actions in as far as email infection vectors are concerned are of utmost importance, hence user awareness.

B. Vulnerability Exploitation

The presence of intrusion detection and prevention systems in form of anti-spam has forced attackers to look for other ways of infiltrating corporate networks. This is also echoed in 3rd generation ransomware which is not only spread via emails. As witnessed in the Erebus and SamSam ransomware campaigns, targeted attacks on enterprises do seldom user emails as infection vectors. Rather, attackers look for loopholes into the targeted system via exploitations of system vulnerabilities and weaknesses on remote access services such as RDP. Therefore, the only plausible way of thwarting infections via these vectors is addressing these vulnerabilities. Such vulnerabilities are exhibited in unpatched software and misconfigurations. This calls for a recurring thorough system vulnerability assessment and penetration testing. Security patches should always be applied to avoid ransomware like WannaCry that exploits unpatched systems. The security updates should not only be limited to network peripheral devices but to user workstations as well.

C. Offline Backups

Backups are the only sure way of mitigating ransomware attacks. Inasmuch as there can be intensive user training and awareness, strong security around the network perimeter etc, ransomware might again slip through the security perimeter via zero-days. With offline backups in place, a victimized enterprise can effectuate a full system restoration in a specified time. We stress offline because newer generations of ransomware strains exhibit worm-like characteristics whereby they traverse the network to infect any discovered network device, even backup systems. As such, a network attached backup such as NAS or SAN should be properly segmented from the network depicted in threat model in Figure 4 so as to prevent access of 3rd generation ransomware such as WannaCry which attacked network devices. A quick and resilient backup system is of paramount importance since studies show that each day that passes without access to encrypted enterprise data can typically result in lost business and damages from $5,000 to $20,000 due to downtime. As such, a poorly configured and implemented backup strategy might even be costlier than the ransom demand itself despite having readily available in backup all the data encrypted by the ransomware. Then there’s the question of whether to pay or not to pay in the unfortunate event of a successful attack, this is a grey area for different victims depending on the nature of the business.

VIII. Related Works

Research on the characteristics of ransomware has drawn interests from both the security industry and academia. In [29], authors present a comprehensive taxonomy of ransomware and the associated research directions. In [30], authors address ransomware attacks from a data resilience perspective and introduce the concept of attack structures. However, unlike our work, authors in [29, 30] do not address the evolution of ransomware nor the classifications of the attacks based on attack structures and the underlying cryptosystems. In [31], authors employ the use of support vector machines which is one of the supervised machine learning algorithms to detect ransomware. The detection methodology is based on API calls history. In [32], authors address ransomware characteristics by exploring the transition from early ransomware attacks to the current ones. They consider the general characteristics of different ransomware families from 2001 to 2017. In [33], authors present the results of a long-term study of different types of ransomware attacks observed between 2006 and 2014. They look at the various encryption, deletion, and communication techniques employed by the respective ransomware. Our work, however, addresses the categorization of the different ransomware families in the past decade using a classification algorithm based on encryption and deletion attack structures. Furthermore, our work details how paradigm shifts in attack structures are targeting enterprise systems. The related works do not correlate them with economic perspectives like ours.

IX. Conclusion

In this paper, we have evaluated the evolution of ransomware from an attack structure point of view. We have presented how ransomware has evolved from primitive attacks that did not really include encryption, to resilient and robust attack structures that leverage industry-standard encryption and deletion methodologies. We have shown how new generations of ransomware attacks seek to incapacitate data recovery via data deletion and cryptographic attack structures. We formulated an attack model applicable to cascaded network design structures common in enterprise systems detailing the various susceptible entry points. We presented an elaborate ransomware infection process and the corresponding attack methodologies using various cryptosystems. We have modeled the security state of ransomware attack process as transitions of a finite state machine where state transitions depict breaches of confidentiality, integrity, and availability. We have proposed a ransomware categorization framework that classifies the virulence of a given ransomware based on a proposed classification algorithm that is based on data deletion and file encryption attack structures. The categories that increase in severity from CAT1 to CAT5 classify the technical prowess and the overall effectiveness of potential ways of retaining the data without paying the ransom demand. As such, the framework provides an avenue for a deeper comprehension of potential inadequacies and flaws in a given ransomware attack campaign. We have shown how recent trends from 1st through to 3rd generation ransomware have depicted a shift towards attacking enterprise systems where attackers leverage exploit kits and exploit weakness and vulnerabilities in Internet-facing remote access services such as RDP. Third generation ransomware exhibit worm-like capabilities which enable them to traverse the entire network structure of an information system subsequently infecting any discovered vulnerable host. This leads to attack on online backup systems. With the rise of ransomware targeting enterprise systems capable of traversing different network segments for maximum impact, backup strategies should be offline since poorly orchestrated backup and recovery mechanisms can cost much more than the actual ransomware attack itself.

References

[1] Palisse A, Le Bouder H, Lanet JL, Le Guernic C, Legay A. Ransomware and the legacy crypto API. In International Conference on *Risks and Security of Internet and Systems* 2016 Sep 5 (pp. 11-28). Springer, Cham.

[2] Thomas J, Galligher G. Improving backup system evaluations in information security risk assessments to combat ransomware. 2017

[3] Young AL, Yung M. On Ransomware and Envisioning the Enemy of Tomorrow. IEEE Computer Vol.50(11):82-5. 2017.

[4] Srinivasan CR. Hobby hackers to billion-dollar industry: the evolution of ransomware. Computer Fraud & Security. 2017 Nov 30;2017(11):7-9. 2017.

[5] Baek S, Jung Y, Mohaisen A, Lee S, Nyang D. SSD-Insider: Internal Defense of Solid-State Drive against Ransomware with Perfect Data Recovery. In 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) Jul 2 (pp. 875-884). IEEE.2018.

[6] Kim, W., Jeong, O.R., Kim, C. and So, J. The dark side of the Internet: Attacks, costs, and responses. Information systems, 36(3), pp.675-705. 2011.

[7] Mather, T., Kumaraswamy, S. and Latif, S. Cloud security and privacy: an enterprise perspective on risks and compliance. O'Reilly Media, 2009.

[8] Al-rimy, B.A.S., Maarof, M.A. and Shaid, S.Z.M. A 0-day aware crypto-ransomware early behavioral detection framework. In International Conference of Reliable Information and Communication Technology (pp. 758-766). 2017.

[9] Ehrenfeld, J.M. Wannacry, cybersecurity and health information technology: A time to act. Journal of medical systems, 41(7), p.104. 2017.

[10] Fayi, S.Y.A. What Petya/NotPetya Ransomware Is and What Its Remediations Are. In Information Technology-New Generations (pp. 93-100). Springer, 2018.

[11] Chen J. Effectively Exercising Deterrence in the Cyber Domain. In ICCWS 2018 13th Int. Conf. on Cyber Warfare and Security (p. 120). Academic Conferences and publishing. 2018.

[12] Wirth, A. The Times They Are a-Changin': Part One. Biomedical instrumentation & technology, 52(2), pp.148-152. 2018.

[13] Cohen A, Nissim N. Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory. Expert Systems with Applications. Vol.15; 102: pp. 158-78. 2018.

[14] Roberts, N., 2018. Ransomware: An Evolving Threat (Doctoral dissertation, Utica College).

[15] Google Trends. (2018). [Online] Available: https://trends.google.com/trends/explore?date=2016-10-18%202018-07-18&geo=US&q=ransomware.

[16] Kao DY, Hsiao SC. The dynamic analysis of WannaCry ransomware. In Advanced Communication Technology (ICACT), 2018 20th International Conference on 2018 Feb 11 (pp. 159-166). IEEE.

[17] Bajpai P, Sood AK, Enbody R. A key-management-based taxonomy for ransomware. In APWG Symposium on Electronic Crime Research (eCrime) 2018 May 15 (pp. 1-12). IEEE.

[18] Bhardwaj A. Ransomware: A rising threat of new age digital extortion. In Online Banking Security Measures and Data Protection 2017 (pp. 189-221). IGI Global.

[19] Cabaj K, Mazurczyk W. Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Network. 2016 Nov; 30(6):14-20.

[20] Cabaj K, Gawkowski P, Grochowski K, Osojca D. Network activity analysis of CryptoWall ransomware. Przeglad Elektrotechniczny. 2015; 91(11):201-4.

[21] Palisse A, Le Bouder H, Lanet JL, Le Guernic C, Legay A. Ransomware and the legacy crypto API. In International Conference on Risks and Security of Internet and Systems Sep 5 (pp. 11-28). 2016.

[22] Williams, T.J., 1994. The Purdue enterprise reference architecture. Computers in industry, 24(2-3), pp.141-158.

[23] Bodenheim, R., Butts, J., Dunlap, S. and Mullins, B. Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices. International Journal of Critical Infrastructure Protection, 7(2), pp.114-123. 2014.

[24] Wang, Z., Wu, X., Liu, C., Liu, Q. and Zhang, J., 2018, June. RansomTracer: Exploiting Cyber Deception for Ransomware Tracing. In 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). IEEE.

[25] Newman I.H. 2018. Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare. [Online] Available: https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

[26] Bad Rabbit: A new ransomware epidemic is on the rise. 2017. [Online] Available

https://www.kaspersky.com/blog/bad-rabbit-ransomware/19887/.

[27] Zimba A, Wang Z. Malware-Free Intrusions: Exploitation of Built-in Pre-Authentication Services for APT Attack Vectors. International Journal of Computer Network and Information Security. Vol 9(7). 2017.

[28] Ransomware back in a big way, 181.5 million attacks since January. (July 13, 2018). [Online] Available: http://vinransomware.com/latest-news/ransomware-back-in-big-way-181-5-million-attacks-since-january.

[29] Al-rimy BA, Maarof MA, Shaid SZ. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security. 2018 Jan 10.

[30] Zimba A, Wang Z, Simukonda L. Towards Data Resilience: The Analytical Case of Crypto Ransomware Data Recovery Techniques. International Journal of Information Technology & Computer Science 10 (1), 40-51.

[31] Takeuchi Y, Sakai K, Fukumoto S. Detecting Ransomware using Support Vector Machines. In Proceedings of the 47th International Conference on Parallel Processing Companion 2018 Aug 13 (p. 1). ACM.

[32] O'Kane P, Sezer S, Carlin D. Evolution of ransomware. IET Networks. 2018 May 17; 7(5):321-7.

[33] Kharraz A, Robertson W, Balzarotti D, Bilge L, Kirda E. Cutting the Gordian knot: A look under the hood of ransomware attacks. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment 2015 Jul 9 (pp. 3-24). Springer, Cham.

Authors' Profiles

Aaron Zimba is a lecturer at Mulungushi University and he is currently pursuing PhD studies at the University of Science and Technology Beijing in the Department of Computer Science and Technology. He received his Master and Bachelor of Science degrees from the St. Petersburg Electrotechnical University in St. Petersburg in 2009 and 2007 respectively. He is also a member of the IEEE. His main research interests include Network and Information Security, Big Data Analytics, Network Security Models, Cloud Computing Security, and Malware Analysis.

Mumbi Chishimba holds a Master's and Bachelor's Degree in Computer Science from Mulungushi University in the department of Computer Science and Information Technology. Currently, he is with the National Institute of Public Administration (NIPA) where is he is serving as the information systems analyst and developer. His research interests are information systems management, software algorithm development, and information and network security.

How to cite this paper: Aaron Zimba, Mumbi Chishimba,"Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.1, pp.26-39, 2019.DOI: 10.5815/ijcnis.2019.01.03