RANSOMWARE

Tactical | Strategic | Diplomatic

Tools of Warfare

Alok Vijayant
Dr J S Sodhi

Introduction

RANSOMWARE are cleverly crafted application executables that the victims are tricked to click and the executable embed certain pieces of codes and instruction to the computer to act in a way determined by the white collared criminals for super normal advantages of different forms.

While the earliest forms of such Malware targeted primarily the known targets as a response to some bad engagements with the target. The payloads of such malware were focused on creating disturbances to the intended target system or even for gleaning sensitive information from the target for its exploitation accordingly. However with the increased levels of sophistication the quality of the malware also began to be more robust, stealth and resilient. Also, the intention of such attacks also took several forms.

Literature Review

A number of literature are available regarding Ransomware, where most of them identify the evolution of the ransomware family, its reach, exploitation mechanism and the detection and mitigation methodologies.

Modern ransomware emerged around 2005 and quickly became a viable business strategy for attackers (Richardson, North, 2017, Wilner, Jeffery, Lalor, Matthews, Robinson, Rosolska, Yorgoro, 2019).

This is a way of democratising crime, giving ordinary people and smaller players an easier way into the criminal market (Jaishankar, 2008; Naylor, 2000), while reducing the risk of exposure for the ones on top of the value chain.

Economic incentives from developing and distributing ransomware are high, simply because the revenue is high, whereas the costs of resources and probability of apprehension are low. Hernandez-Castro et al. (2017) put forth an economic model based on the victim's willingness to pay.

Currently, the relationships between organised crime and the Internet is under-investigated (Lavorgna, 2015).

This research gap can be narrowed down by looking at the motivations and incentives of the people involved, and Waldrop (2016) suggests that this can be accomplished by embracing behavioural science and economics as part of the research.

In the current paper, we would explore the changing behavior, intent and mechanics of operating the RANSOMWARE that is now beginning to make its headway into the critical information infrastructure and targeting state based infrastructure rather than the standalone systems of the past. While a number of studies have been done on the ransomware and its methodology of operations, this paper would primarily focus on the behavioural analysis, motivational factors, generation of funds and strategy for economic warfare and diplomatic underpinnings

The conceptual paper would also explore the next levels of complications that the RANSOMWARE are likely to pose, its mitigation techniques as well as the need for a global eco system to prevent accidental or otherwise damages to the life critical information infrastructure.

General Concepts

Darknet and Dark Web - .The hidden portion of the Internet is commonly known as the dark Web or the DarkNet. Information from the same is obtained using a special browser known as the TOR Browsers. The non-indexed content on the Dark Web ensures its anonymity on the Internet.

Dark Web Marketplace and Forums - Dark Web market places are places where tools, techniques, knowledge, exploits are traded/sold. Forums also help in collaborating with complementary partners while carrying out any activity. Forum members also provide global services for pivoting from one systems to other for achieving greater anonymity.

Cryptovirology- Cryptovirology is a term used for employment of Cryptography for the development of virus. In terms of Wikipedia, it refers to the use of cryptography to devise particularly powerful malware, such as ransomware and asymmetric backdoors.
Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users, . cryptovirology employs a twist on cryptography, showing that it can also be used offensively. It can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents.

Historical Imperatives of Ransomware

The first generation malware played around with the indexing of files wherein the payloads were such designed that the index of all the files maintained with the operating system were deleted or altered which resulted into non-accessibility of the files by the intended application. These malwares were very rudimentary and could be easily recovered using the snapshot of the index files on the system.

Next came a generation of malware coded with an intention to create disturbances to some targeted people with whom the attacker had to settle some scores.

Therefore, this generation of malware was characterized by its ability to penetrate into the system, taking a random number, using the existing hashing algorithms, identifying the document folders and recursively encrypt the documents in the folder. This kind of malwares had an ability to lock the documents and make it non-readable by the normal applications. However, generation of random key value could easily decrypt the documents and bring the system up and running.

Then was the era of malwares that crypted the documents with a real time salt generation method that took into account the different ambient parameters of the system in real time scenarios. This made generation of salt value during decryption process very difficult to achieve.

Therefore, the functional parameters were characterized by disruption/denial of the information system and the target was primarily a known target in majority of the cases.

Over the last decade, the erstwhile malwares that were used for encrypting the files and make it unusable by the target went through a series of metamorphosis and thus came the concept of Ransomware where in the intended target was communicated with through anonymous messaging system who in turn desired for stuffs in kind or cash in return for giving out the salt value and defining a mode of decryption of the locked documents. Ransom for Malware or in short RANSOMWARE was thus born with ill-intention to get somethings in return for the salt or the decryption key. Anonymous payment systems therefore got devised soon and one of the fundamental features of such payment systems was its ability to stay anonymous.

Over the last 2-3 years, the global systems have seen that the anonymous financial system with reduced number of intermediaries have gained significance over the traditional banking systems with a number of intermediaries who could track such transactions down. More and more non-intermediary based financial transaction using non-repudiable Block Chain Technologies and digital crypto coins are now in offing and several

Digital Currencies are now in operations that can be transacted anonymously over the dark and the deep webs. This development coupled with the sophistication of the Ransomware and non-detectible payloads began to pave way for a new era of anonymous payments for the random attack vector using Ransomware. The typical trend of a targeted attack using Ransomware was now a new method of generating value from all and sundry who got caught in the fish hook.

The functional parameters now were characterized not by disruption and denial but to engaging with the target and extracting value from the target depending upon the depth of ones pocket. Methods were devised to provide remote support using the Dark web and the deep web once the value has been extracted from the target systems. Dark Web and the anonymous payment systems therefore have started being a catalyst to such method of generating easy money using the Ransomware.

Current Trend

Current trends of the Ransomware in the recent past show definite patterns wherein the target is carefully selected so that the ransom can be duly demanded. The reputation of an organization is also factored in while sending out the attack thread (fish-hook) to the intended target.

A weak link in the organizational chain is carefully selected who has adequate authorization within the organization and is amenable to social engineering. While, it is assumed that the IT Systems of large organizations would be duly designed, the mailing systems normally remain a neglected area wherein individual mail boxes act as the storage point for the malwares that are to hit the surface of the organization.

Features of worming that are now getting embedded into most of the latest malware are absolutely lethal and spread of its own through devices and air connects. The self-identifying malwares that auto-generate themselves and propagate through the available networks have the potential to spread at a very fast pace within the organization thereby making many a systems available for exploitation.

Through a careful mining of the processes from these machines, the malware automatically select the most critical nodes and start activating the payload thereby designed with intentions.

Normally, when the systems are locked, a parallel chat mode opens up on the compromised system that remains out of the ambit of the locked files which enable the attacker to communicate remotely through hopped chains of proxies within the dark web. When the communication begins, the attacker entices the target to pay ransom as per the need of the target systems to restore - the greater the need and criticality of the system, greater is the demand for ransom.

The attacker then communicates to the target system regarding the Crypto Walet address where the desired ransom is to be paid and waits for the money transfer to happen. Such money is then broken into several small crypto coins and distributed to several other crypto walets and hops through walet to walet to land at a desired location of the attacker.

Most Notable Ransomware Family *

Cryptolocker	Discovered in September 2013 and used RSA Key Pair to encrypt the data on victims system
CryptoWall	Discovered in 2014, it infiltrated networks first by gaining access through browser plugins and downloading the payload and then encrypting the files . The delivery mechanism was through email campaigns
Fusob	Discovered in 2015, it was a mobile ransomware that locked and encrypted data and then communicated with the victim t o pay ransom. It was the first region restricting ransomware and was written to spread to Eastern European Countries only
WannaCry	Discovered in May 2017, it was the largest attack vector till date. It exploited the Microsoft's SMB protocol to infiltrate

*** source : https://www.cybergrx.com/resources/7-ransomware-last-decade**

Work Flow of the RANSOMWARE

RANSOMWARE from the stage of development to the extraction of value from the targeted system goes through a very systematic full proof system by the attacker. We would diagnose the process as a block diagram to demystify the complexity attached with Ransomware

The first step in the life cycle of a Ransomware Process is the development of the Payload. Payload is the pieces of codes/instruction set provided to the computer to perform some act while extracting value from the target system. Some of the features that the payload must have are - persistent connection to the command and control system of the attacker, worming abilities to spread to the adjacent networks and systems, stealth, virtual space for the desired codes, non-reversing codes, chatting protocol enabled, system information back propagation etc.
After the Payload is coded and tested for its performance, the next step is to identify the latest vulnerability that needs to be exploited through an exploit. Vulnerabilities are issues with the systems that render it available to the attacker to inject and execute ones codes. When the exploits are prepared, the payloads are loaded on top of it as the activity that should be performed on the target system after it reaches the intended system. This includes activities like keylogging, rootkit, controls, scanning or locking the system.

The next step is to enumerate systems that are prone to such attacks and are important from the perspective of a milky cow. Such systems are either identified through a reconnaissance exercise through the open source channels or even identified through open search mechanism. The quality of target and its compromise decides as to what would be the return on investment of time and energy of the attacker.

Then, comes the requirement to hide your back and leave no traces. The Dark Web provides an excellent framework for anonymity and the attacker uses all the methods to create proxy chains to pivot from one dark web system to other to finally reach the intended target. Social Engineering is an important method to entice important and selected target .

After the systems are infected, the payload embedded with the exploit begins to work and carries out all the instruction set coded by the attacker sequentially or parallelly, resulting into denial of the computer system to the legitimate user. The ransomware usually creates a key by calling a cryptographic API on the user's operating system (Zimba et al., 2019)

The communication channel created by the attacker hopping through multiple systems and proxies enables a regular communication between the target and the attacker. This is where the attacker passes certain information and demands for the ransom. He also specifies the dead drop (a place where to drop the ransom as demanded). In the current days, this is one of the mule crypto wallets which are just used to park funds temporarily and thereafter the funds are broken into multiple smaller denominations and transferred to multiple mule wallets ultimately to land at the attackers wallet through the route of Dark Web.

After the receipt of the funds and the ransom, the attacker may choose to provide the random key for unlocking the computer system or may choose to disappear from the scene. He may also choose to unlock it remotely through a systematic chain of command.

Ransomware - a tactical or a strategic weapon

In the earlier days of the malware and ransomware they were normally seen as a tactical method to glean immediate returns, however the potential of Ransomware is beyond the initial returns. We would evaluate certain situations where such malware could turn into strategic and sometime even weapon for diplomatic underpinnings.

Ransomware for Revenge

Ransomwares as a weapon in the hands of insiders who are disgruntled within an organization are asymmetrically lethal and have the potential to completely destroy the IT Systems. Such attempts are characterized by less number of failed attempts during exploitation process as the system would be well known to the insider and therefore there would be extra-ordinarily low hit and trials

Ransomware for Money

Ransomware for money and gains are very common and therefore most of the Ransomware attacks that take place today are in this category. The need for an isolated Crypto Wallet and access to several mule wallets is mandatory for the attacker so that the possibility of a traceback is reduced to a minimum. The value of the ransom in these cases is normally decided on the appetites' of the target system. It is also to be decided as to the ransom demanded is proportionate in value to the cost of restoration.

Ransomware for Warfare

Ransomware for Information Warfare has yet not found its way into the system, however in the futuristic virtual wars against nations and to create psychological pressures, this would find a place in strategic weaponization. Also, in order to win wars without firing a bullet, Ransomware are sure to play a major role in future wherein systems of the target nation would be locked up for ransom at a large scale and as and when the critical systems of the target country begin to cripple, a third country negotiation shall begin to fund some of the activities and let the target country bleed economically.

Ransomware for Political Funding

Yet another innovative method to use Ransomware for generation of fund would be in politics. Knowing it well that the tracing of the funds pivoting through several continents through the dark streets of the dark web, it is almost impossible to get to the root of the crime and therefore it would be a best candidate to generate funds from within the governments of the world.
These are the following acts that the attackers need to protect against and as we would see that all these acts are generally coverable by the Government of the day.

(a) Attack Vector - Attacker is dependent normally on the weakness of the system and his success depends upon the mistake committed by one of the person in the network. Now, this aspect can be almost assured by the Governments of the day to ensure that the infection does take place.

(b) Crippling of System and Mayhem - When the systems get compromised by the agents of the Government of the day, Government purposefully would go slow on the investigation and let the situation boil so that a demand for the negotiation can be justified.

(b) Crippling of System and Mayhem - When the systems get compromised by the agents of the Government of the day, Government purposefully would go slow on the investigation and let the situation boil so that a demand for the negotiation can be justified.

(c) Media Pressure - Media Pressure would thereafter be created to restore the system to normalcy and reports of a mayhem would be propagated. Such Mayhem would bring in an artificially created pressure on them to direct the affected organization to take any measure that is desired to restore normalcy. Investigative postures would be pretended to be speeded up. However, the intention would be to ensure that the investigations are carried out by non-professionals so that even the remotest chance of detection of the attack thread is messed up with.

(d) Negotiation as a means of restoration - While the investigation would go on, the negotiation teams would be formed who would negotiate with the attackers on the virtual platform and ultimately land up paying the ransom at the negotiated price.

(e) Post restoration - After the systems are restored, once again there would be brownie points collected by the sympathizers both in the media as well as the investigators. A few low hanging heads would roll temporarily to get a good berth on a later day.
Media would once again start playing the role of pressure builder and start advertising products that would have helped delimit such instances in future.

Conclusion

The stealth and the lethality of Ransomware are sure to hit the Cyber Security Space in a big way in the future dynamics of wars in the world - be it for the purpose of tactical gains or for nation -state game plays or even for raising funds for the political parties.

Reducing the human vulnerability, setting in accountability in systems, collaborative investigative postures, DR and BCP, Third Party Audit and accountability,International conventions as well as creation of a Cyber Red Cross would be the apt strategy to follow among all other cyber security measures that are in vogue today.

RANSOMWARE WORKFLOW

FEATURES

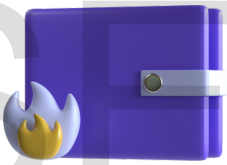
- Floating Command and Control
- Recursive Codes
- Encrypt with random generated salt
- Registry Updates
- Worming Codes - Virtual Space
- Payload Features
- Wireless Enumeration
- Propagation
- Chat Sockets
- Information Dumping
- Backup Overwrite
- Block Re-Boot

Programs Malware

Exploitable Vulnerability

Payload

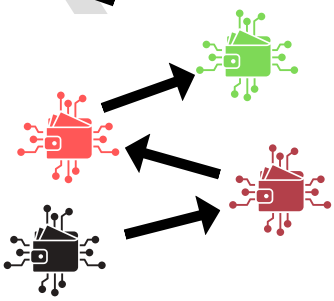
Exploits Design

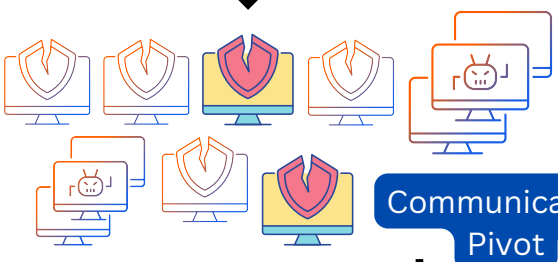


Fund Transfer
Attackers Wallet

Attacker Anonymity
(Dark Web)

Exploitation





Communication
Pivot

Proxy Crypto
Wallet

Scans for Vulnerable
High Value
SystemsDesign

Commands

Ransomware Planted

Fund
Transfer

Alok Vijayant

References

1. Young, A.; Yung, M. (2004). Malicious Cryptography: Exposing Cryptovirology. Wiley. ISBN 978-0-7645-4975-5.
2. R. Richardson, M. North - Ransomware: evolution, mitigation and prevention International Management Review, 13 (1) (2017), pp. 10-21
3. A. Zimba, Z. Wang, H. Chen, M. Mulenga - Recent advances in cryptovirology: state-of-the-art crypto mining and crypto ransomware attacks KSII Trans. Internet Inf. Syst., 13 (2019), pp. 3258-3279 doi:10.3837/tiis.2019.06.027
4. Jaishankar K, 2008. Space transition theory of cyber crimes - Schmalleger, F., Pittaro, M.(Eds.), Crimes of the Internet, Pearson, pp. 283-301
5. Hernandez-Castro, J., Cartwright, E., & Stepanova, A. (2017). Economic analysis of ransomware. arXiv:1703.06660v1.
6. A. Lavorgna - crime goes online: realities and challenges, J. Money Launder. Control, 18 (2) (2015), pp. 153-168