RANSOMWARE: A GROWING THREAT TO SMES

Qinyu Liao

The University of Texas at Brownsville and Texas Southmost College, Brownsville, TX 78521

Tel: 956-882-5825 Fax: 956-882-5805

Email: Qinyu.liao@utb.edu

ABSTRACT

This article attempts to discover the surreptitious features of ransomware and to address it in information systems security research. It intends to elicit attention with regard to ransomware, a newly emerged cyber threat using such encryption technology as RSA, and to help both academic researchers and IT practitioners understand the technological characteristics of ransomware, along with its severity analysis. As ransomware infections continue to rise and attacks employing refined algorithm become increasingly sophisticated, data protection faces serious challenges. The article discusses future trends and research directions related to ransomware, and provides prevention strategies for SMEs.

INTRODUCTION AND BACKGROUND

As online presence and business transactions are considered as a necessary profit-driven avenue and not a luxury for large corporations only, today's SMEs are facing keen peer competitions in business society as well as increasingly sophisticated information security threat in cyber world. The consequences of inadequate security measures are as catastrophic for SMEs as they are for large enterprises. According to a recent survey, most SME respondents still consider spam the number one security risk to their business. While spam is a nuisance, threats such as spyware, phishing and crimeware can pose a greater threat to a firm's livelihood.

SMEs world wide spent about $11.4 billion on IT security during 2006, according to a report issued in summer of 2006 by analyst firm AMI-Partners. The expenditure represented a 23 percent increase from 2005, when SMEs shelled out an estimated $9.3 billion on security products. And the trend shows no sign of slowing: AMI-Partners projects double-digit annual increases in security spending by SMEs for the next several years (Coggrave, 2006).

Past information systems security research has investigated such malware programs as Trojan horse, worms, and spyware from a plethora of scientific perspectives (Warkentin, Luo and Templeton, 2005), and relevant strategies and tactics have been proposed to alleviate and eradicate the cyber threats (Luo, 2006).Young and Yung (2004) indicated that future attacks will result from combining strong cryptography with malware to attack information systems. Very recently, the emergence of a new form of malware in the cyberspace, known as ransomware or cryptovirus, starts to draw attention among information systems security practitioners and

researchers. Imposing serious threats to information assets protection, ransomware victimizes Internet users by hijacking user files, encrypting them and then demanding payment in exchange for the decryption key. Seeking system vulnerabilities, ransomeware invariably tries to seize control over the victim's files or computer until the victim agrees to the attacker's demands, usually by transferring funds to the designated online currency accounts such as eGold or Webmoney or by purchasing a certain amount of pharmaceutical drugs from the attacker's designated online pharmacy stores. The most recent ransomware attack was trying to hijack web email accounts for ransom.

This article attempts to discover the surreptitious features of ransomware and to address it in information systems security research. In an effort to cater to both security practitioners and researchers, the rest of this article is organized by three parts. Part 1 addresses ransomware's underpinning structures; recent statistics and attack methodologies of ransomware infection are also offered; part 2 will discuss the future trend of ransomware in terms of technological sophistication level; part 3 will propose the recommendations for anti-ransomeware by SMEs.

HOW RANSOMWARE WORKS?

In the cyber world, computer users have faced certain types of threat such as worms, spyware, phishing, viruses and other malware. Ransomeware is an extortion scheme whereby attackers hijack and encrypt the victim's computer files and then demand a ransom from the victim for these files in original condition. Kaspersky, one of the global leading anti-virus companies, warned that ransomeware is a serious threat because there is no way to recover the effected data.

We thereby define ransomware as a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt all his/her files; then the attacker keeps the files locked unless the victim agrees to pay a ransom. In a typical ransomware attack, the attacker reaches into a compromised computer by seeking the exposed system vulnerabilities. If this system was victimized earlier by a worm or Trojan, the attacker can easily enter the weakly configured system. He then searches for various types of important files with such extension names as .txt, .doc, .rft, .ppt, .chm, .cpp, .asm, .db, .db1, .dbx, .cgi, .dsw, .gzip, .zip, .jpg, .key, .mdb, .pgp .pdf. Knowing these files are of possible crucial importance to the victims, he then encrypts these files, making them impossible for the victim or owner to access them. Later, the attacker sends the victim an email ransom or pop-up window demanding for the encryption key that unlocks the frozen files.

Once the attacker locates these files, there are several processing strategies that he might implement. First, he can compress all the located files into a password-protected zip package, then he removes the entire original files; secondly, he can individually encrypt each located file, and then removes the original files. For example, if the original file is "DissertationFinalVersion.doc", ransomware will create a file such as "Encrypted_DissertationFinalVersion.doc" in order to label the original file; thirdly, the attacker might create a hidden folder and move all the located files to this folder, producing a pseudophase to deceive the victim. The third strategy, of course, carries the slightest damage and is comparatively feasible for victim to retrieve all the "lost" files.

Furthermore, when ransomware attacks successfully take control of an enterprise's data, the attacker encrypts the data using sophisticated algorithm. The password to the encryption is only released if ransom is paid to the attackers carrying out the attack. The attacker usually notifies the victim by means of a striking message, which carries specific instructions as to how the victim reacts to retrieve the lost files. A text file or a pop-up window message is generally created in the same folder where files are encrypted. The text file or message box clearly indicates that all the important files are already encrypted and informs the victim of specific money remittance methods. Table 1 lists all the methodologies used by recent ransomware attacks and ransom methodologies as to what attacker demands for.

Name	**Time**	**Attack Methodologies**	**Ransom Methodologies**
Trojan.Pluder.a	6-14-2006	Copy different types of file to hidden folders	Remit $10 to designated Chinese Industrial and Commercial Bank
Arhiveus	5-5-2006	Link all the files in folder "My Documents" to a single file named EncryptedFiles.als, and delete all the original files. Create a text file named "INSTRUCTIONS HOW TO GET YOUR FILES BACK.txt" in the folder, directing how users can receive the decrypt key, which exists in the malicious codes	Ask victims to purchase $75 pharmaceutical products from certain Russian websites. Once victims make the purchase and email the order ID to the attacker, the ID will be confirmed by the attack, who will email the decryption key back to the victims if the ID is validated.
Trojan.Randsom.A	5-1-2006	A notification window always shows above other windows to distract victims. This bluffs that a file is deleted every 30 minutes, but no files are indeed deleted	Remit $10.99 through Western Union
Trojan.Cryzip Trojan.Cryzip Variant	3-11-2006 3-22-2006	Compress document files (txt, doc, rft, etc.), data base files, and multimedia files into a password-protected ZIP file. The decryption key used for the ZIP file is stored in file Cryzip. The decryption key can be dynamically downloaded for Cryzip's new version	Notify victims to remit $300 to a designated E-Gold account. Specific instructions are given.

Trojan.PGPCode	5-23-2005	Encrypts all files using RSA algorithm	Notify victims to remit $200 to a designated E-Gold account.

Table 1: Comparison of ransomware attack methedologies

FUTURE TRENDS

It is argued that we will probably get to the point where we are not able to reverse the encryption, as the length of ransomware encryption keys are pushing the boundaries of modern cryptography. For example, if add a rootkit to hide the installer of the ransomare so that if we break its password it then randomly encrypts the files again, or after say 5 failed logins, it scrambles every thing. In this way it can hold us to total ransom. But so far no fancy rootkits like this has been reported. Overall, Trojans which archive data tend to present a threat to Western users; Russian virus writers are more likely to use data encryption for blackmail purposes.

Despite the keen efforts that enterprises have contributed towards information security hardening, we, however, deem that the occurrences of ransomware will continue to rise. More importantly, the encryption algorithms used by ransomware writers will become increasingly complicated. As more technologically sophisticated encryption technologies are employed for cybercrime, an encryption war between the malicious perpetrators and the security professionals seems inevitable and increasingly intense. This scenario, again, mirrors what we have witnessed in a cat-and-mouse battle between virus producers and antivirus companies in computer virology. As such, security professionals endeavor to crack the encrypted code and attackers, in turn, promptly respond back with more complex methodologies. By the same token, simple encryption codes being cracked by security professionals will trigger the birth of further complicated encryption seeking ransom. Very recently, complex incarnations RSA encryption embarks and ransomware writers will continue to seek for increasingly sophisticated methods of password-protecting and hiding corrupted files.

Social engineering is now also involved in the spreading of ransomware, as the attackers tend to exploit such popular websites as online recruitment to victimize unwary users. Furthermore, RSA algorithm or any other similar algorithm which uses a public key will continue to generate far more complicated digital keys in terms of bit unit. The initial 50-bit key which did not pose any difficulties for security professionals has enabled attackers to rethink the attacking approach and to birth 260-bit key, which has been extended a 330-bit key. In addition, the recent emergence of Gpcode ransom virus featured a 660-bit key, which could take security professionals about 30 years to break using a 2.2 GHz computer.

Based on Kaspersky's research, it is argued that the encryption methods are reaching the limits of modern cryptography. As such, future incarnations could be theoretically unbreakable, thereby forcing the IT community to face a dilemma in that those infected may have no choice but unwillingly to pay the ransoms in order to unlock their important files. Even though the documented ransomware attacks have been fare, the use of asymmetric encryption in malicious programs may continue to evolve to exploit computer user for the gain of profit. According to Alexander Gostev, a senior virus analyst, it's only a matter of time before ransomware hackers

have the upper hand. As the criminals turn to every-more-elaborate encryption, they may be able to outpace and outwit antivirus vendor researchers. With a longer key would appear at any time in a new creation, IT security businesses may fail to win the war, even if maximum computing power were to be applied to decrypting the key. Ransomware will undoubtedly remain a major headache for the security industry. Figure 1 categorizes different types of ransomware, based on the degree to which threat severity varies.

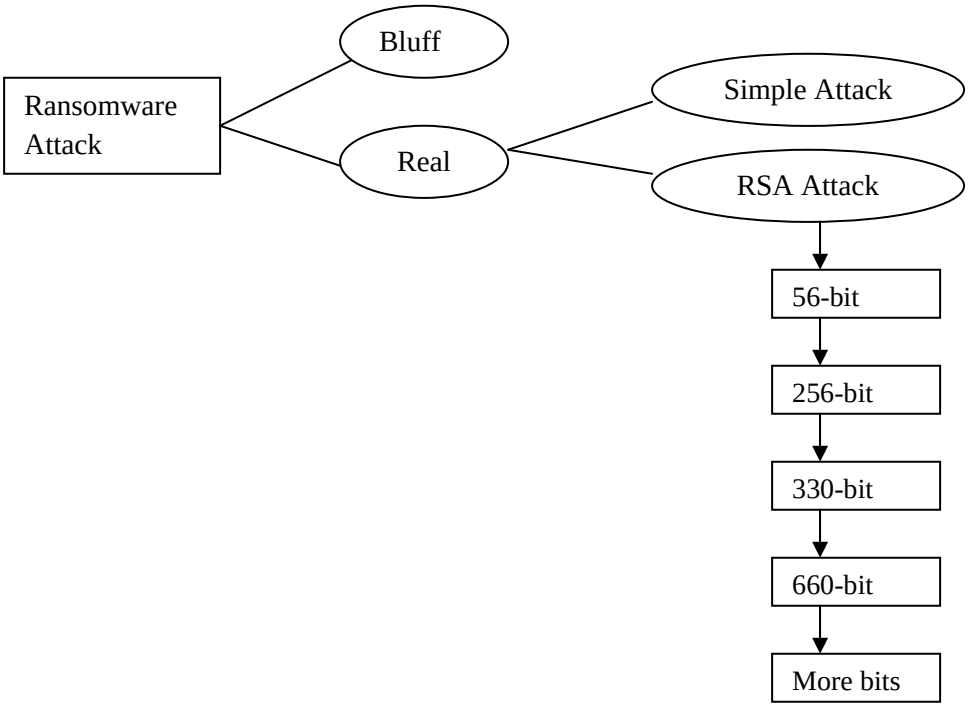

Figure 1: Ransomware Categorization on Threat Severity

RECOMMENDATION FOR RANSOMWARE PREVENTION BY SMES

Since most large companies have devices at the perimeter that constantly monitor for malicious activity and take steps when signs of malicious activity occur (Mueller, 2006), ransomware is being viewed as a more serious problem for SMEs. SMEs suffer similar consequences to larger organizations when it comes to security and should have appropriate protection in place around the clock. There are several reasons. First, most SMEs are reactive and ad hoc in their approach to security and are consequently an easy target for threats such as ransomware. This is caused by the clear disparity between perceptions and reality towards security among SMEs. Second, most IT security companies has not targeted SMEs and they need to step into this field and provide true business value to the SME customers. The third reason is the small amount of monetary lost related to ransomware invasion. The authorities are not interested because the value of the individual crime is too low and it crosses one or more jurisdictions. Since there is no panacea to the eradication of ransomware, preventive measures such as awareness education, regular file

back-up, and system hardening with multiple layers of security are the most effective and efficient ways to fight ransomware invasion.

The key of awareness education is to show SME employees and owners the direct impact of ransomware induced by a security lap could have on them and their company. The employees and owners of SMEs should be reminded not to install their own software on company computers or connect to unauthorized devices into the company computer. Some ransomware outbreaks have been linked to user visits to game, gambling and social-networking web sites. They could loose important customers or the company could be shut down. When people understand how their behavior can play a major role in safeguarding the business's data assets, they are more likely to take steps to comply with the security procedure.

Although when the data reaches into the partial-TB size (spread across multiple machines), backup systems for SMEs can be frighteningly expensive, backups of critical user files on media that isn't located on Internet-exposed platforms are the most effective approach to prevent ransomware attack. These files should be updated as often as possible.

To harden the system or computer, SMEs should deploy up-to-date antivirus software, update operating systems and browsers, have a firewall that controls what information people can access on your computer, and keep up-to-date with the security patches, and use a pop-up blocker. The challenge for security companies is to make security simple for the SME since they don't have much in-house security resources and need a 'set and forget' solution that provides peace of mind and allows them to concentrate on what they do best.

Paying ransom is never an acceptable reaction because there is no assurance that the hacker will actually deliver the decryption key. If the good business practice were followed, companies will have a recent backup of the affected files readily available. If not, a security specialist may be able to help recover some or all of the maliciously encrypted data. But the task will be time-consuming and the ultimate financial cost may be quite steep.

CONCLUSION

With occurrences of ransomware are on the rise, the encryption algorithms employed are becoming increasingly sophisticated. Ransomware will undoubtedly continue to be a serious challenge for both information systems security professionals and researchers, as future incarnations could be unbreakable and the encryption methods, powered by social engineering, are reaching the limits of modern cryptography. SMEs should take preventative measures to regularly back up important data and continuously harden their systems from different layers. The key is to proactively deter ransomware attacks through awareness at the management eand user level. We hope our recommendations can guide SMEs to more effectively cope with the increasingly sophisticated threats of ransomware.

REFERENCES

Coggrave, F. (2006). SME security gets set to grow. Computer Reseller News 42.

Mueller, L. (2006). Webjacking, and how to boot it out. Network Security 2006(6), 15-18.

Warkentin, M., Luo, X., and Templeton, G.F. (2005) A Framework for Spyware Assessment. Communications of the ACM 48(8), 79-84.

Young, A. and Yung, M. (2004). Malicious Cryptography: Exposing Cryptovirology, Wiley Publication Inc.