The Emergence of Ransomware

Babu Nath Giri
babu@avertlabs.com

Nitin Jyoti
nitin@avertlabs.com

McAfee AVERT
Bangalore
India

ABSTRACT

Computer crimes in one way or another have modeled themselves on biological organisms (such as viruses and worms) or on real-life actions or incidents (Trojan horses) to carry out their tasks. Some of these methods have been used consistently and improved upon over time and others have languished, only to return when their potential was rediscovered.

We define "ransomware" as a Trojan that encrypts or holds a computer or system resources—files, data, etc.—in its control for a ransom (commercial benefits or information) in exchange for releasing the seized resources.

The behavior of this family of malware is analogous to real-life incidents of holding up valuable assets and demanding payment for its release.

Efficiently used first in late 1989 as the "PC CYBORG/AIDS information Trojan," this malware demonstrated the threat it posed. Yet this implementation of ransomware did not gain much popularity among the bad guys. Seemingly abandoned for 15 years, ransomware was reborn in 2005 as malware authors recognized the potential of ransomware in this era of widespread Internet usage and e-commerce.

With malware authors getting better at social engineering and other techniques to get malware to the users, everyone with access to Internet is a potential victim. Ransomware poses a greater threat to the corporate world because data is regarded as a valuable resource. Home users, however, are not immune to these attacks, as their security measures are minimally enforced.

This paper will look at the emergence of ransomware by briefly describing the different ransomware attacks and their increasing complexity. We shall explore the possibility of other malware blending with ransomware to become a more effective threat, essentially giving this new breed of malware an edge by continuing to exist and carrying on its activities even after detection. We shall also look at a new avenue of online shopping adapted by one form of ransomware to extort users.

Introduction

The days when computer malware was written for fame are long gone. Money is what causes the adrenaline rush in cyber criminals these days. With virus writers and their adversaries involved in a cat-and-mouse game, every day we see innovations on both sides to defeat each other.

With the increasing Internet user population and e-commerce, there are a number of opportunities for malware authors to seize. For malware authors to cash in upon these opportunities efficiently, they need to satisfy a few important prerequisites. Survival is one of the key elements.

Hiding from users or having stealthy behavior is one of the most crucial characteristics of any malware to survive at its host. By doing so, malware evades users and—more important—their antivirus programs. Malware authors are constantly trying to perfect the art of concealment.

Ransomware on the other hand, announces its existence to the user and that the fate of some of the victim's system resources depends on the malware's survival. Having achieved this goal, the ransomware can then order the user to act according to the malware author's instructions (assuming a perfect implementation of ransomware). Ransomware is similar to other malware types in its delivery. It can use all the existing methods to reach users.

The Abductors so Far

In the following section we shall describe some of the most popular ransomware that we have seen over the years.

PC CYBORG/AIDS Trojan–1989: The first ransomware

The PC CYBORG/AIDS Information Trojan was one of the first in this new line of malware. This ransomware not only demonstrated the concept but also integrated with some of the well-known techniques used by malware authors these days. This Trojan was mailed in a socially engineered package containing a floppy disk to deceive the recipients. At a time when public Internet usage was nonexistent, the author mass-mailed the package through surface mail, addressing it to a mailing list to which the author subscribed. The developer of this malware was arrested on charges of blackmail.

Activities

Once installed on the system from the floppy disk, this program replaces *autoexec.bat* file with one that counts the number of times the system reboots. Once the number reaches 90, the Trojan hides directories and encrypts all file names in the system's root directory. At this point the Trojan displays a message asking the user to pay $378 for renewing license and to recover the lost files and directories. The money was to be mailed to an address in Panama. [1, 2]

GPCoder–May 2005

After a lull in ransomware of 15 years, a new form, GPCoder, emerged to extort users again. By the time GPCoder was released the Internet was in wide use, which helped the author deliver this malware to computer systems. There have been many variants of GPCoder in the wild, with the most recent released in June 2006. The variants of GPCoder have improved their method of encryption, ranging from the author's own algorithm in the first version to a much more complex RSA encryption in the latest version.

Activities

Entering the system through e-mail spam, this Trojan searches and encrypts many files of predetermined extensions. It then places a ransom note in each directory that it encrypts, asking users to e-mail to a particular address in order to get the corresponding decoder. Eventually, users are instructed to transfer the ransom to an online bank account. [3]

CryZip–March 2006

About a year after GPCoder appeared, CryZip joined the fray. CryZip did not operate very differently than GPCoder. But unlike GPCoder CryZip does not use custom encryption. Instead it uses a commercial zip library to store files in password-protected zip files.

Activities

This Trojan comes in the form of a DLL file. Attaching itself to all running processes after its installation, it searches for files and stores them in a password-protected zip file while deleting the original file, and then drops a ransom note with instructions on how to get back the files. To transfer the ransom, CryZip adds an E-Gold account number randomly picked up from a list. [4]

MayArchive–May 2006

Now the ransomware trend seems to be catching on [5, 6]. The next notable malware was MayArchive, which seized files and dropped a ransom note as the others did.

But MayArchive differentiates itself from the others in the ransom note that it drops. The note states "WE DO

NOT ASK YOU FOR ANY MONEY! We only want to do business with you. You can even EARN extra money with us." This was a paradigm shift in the way malware authors planned their extortion. We will look at this type of extortion in detail, with MayArchive as our example, later in this paper.

Activities

MayArchive searches the system for files with different extensions and then it adds them to its archive and deletes the original file. This archive file is password protected, but the files inside the archive are not encrypted. MayArchive drops a ransom note on how to acquire the password in order to extract the files. This also drops a demo archive to demonstrate how the archive works. [7]

Getting to Extortion

Ransomware, as its name suggests, demands ransom. The ransom could be in any form: system resources, personal information, or money, among other possibilities.

In most reported cases the ransom has been money. In most implementations the author would demand the money as early as possible, before users could reclaim their systems or resources. The process of getting a user to pay a ransom depends on many factors. Here are three:

- User Education: Well-educated users would never succumb to such a threat. They could be well prepared for such malware attacks—by having a good backup policy or by using good system-restore options. In these cases the transaction would never happen. This scenario is outside of the author's control.

- Complexity Level of Malware: This determines the extent of damages the malware may cause to a system and the chances for a user or for a repair tool to recover the sabotaged resources. Depending on the complexity, a user might find it impossible to recover compromised resources without contacting the malware author. Sometimes the system becomes dependent on the malware for its functioning [8].

- Urgency of Recovering the Seized Resource: Ransomware might not be very successful unless the resources it seizes are important enough for a user to recover. For trivial resources, a user might well decide to ignore the incident.

These criteria are some of those that might inspire users to pay a ransom, but these are not the only ones.

For an author of ransomware the process of getting a user to pay the ransom is just half the work. There also has to be a payoff. An unsecure transaction might expose the author's identity, so ransomware authors must create transaction in a way that would lead only to a wild goose chase. In the following section, we'll talk about some of the ways that have been or could be used to transact a ransom payment.

Escaping the "Follow the money" Trail

The method of paying off a ransom is a key element in implementing successful ransomware. This, after all, is one of the potential trails that could lead to the author. Ever since the AIDS Trojan in 1989, most ransomware attacks have demanded money. With the advent and wide use of the Internet, the ways of transacting have also evolved considerably. The preferred method of transacting ransom has been by online payment methods such as PayPal [9] or E-Gold [10].

However, these methods do not fully hide the identity of an extortionist. Here are some of the problems these pose for a ransomware author:

- Not all users who are infected will have a PayPal, E-Gold, or similar account; they would need to create one.

- Since the terrorist attacks of September 11, 2001, there is a greater realization that organized crime and cyber crime are beginning to overlap [11]. The account facilitators have taken many precautions to enhance the security of these online payment accounts so that criminals are not able to use them for illegal purposes such as money laundering and funding.

- This increased security awareness has led to number of measures to track funds and to the identity attached to these accounts.

Online payments are getting secured as more and more countries are entering into mutual agreements on these issues and are making an effort to stop these kinds of criminal activities. Thus there is hope that digital accounts will no longer be exploitable for illegal activities. But criminals are always on the lookout for ways to evade detection by trying different things.

Money Laundering

Money laundering is one of the most effective tricks used by criminals involved in illegal activities to escape the trail

of illegal money. Money laundering covers the source of illegal money and the final recipient by making a complex chain of financial transactions. Widespread use of the Internet, the absence of strict global cyber laws, and the ease of trading are some of the reasons that attract ransomware authors to use money laundering over the internet.

There are many ways to launder transactions; irregular funding is one of them. Irregular funding is a method of routing illegal money through legitimate business and having the ransom amount deposited into a separate account while paying a certain amount for this service. Irregular funding fits perfectly in the framework of online shopping, which can be used for transacting ransom. We'll explain in the next section.

Online 'shopping'

MayArchive [7] created a paradigm shift in the way it demanded ransom. It used online shopping as a mode of transacting ransom, and "suggested" victims purchase goods from specific web sites. There are several reasons why this could be an easier and efficient way of transacting ransom:

- Most online shopping web sites accept credit cards. Online shopping also offers more payment methods, including credit cards and online accounts such as PayPal or others.

- From the social engineering perspective, this is a better way of demanding ransom. As approached by MayArchive, the program states it wants to do business and does not want money. This sounds better than just demanding payment. But in no way is this legal; it still qualifies as a criminal act.

- "Shopping" online to pay a ransom can still work through a legal business. The recipient of this transaction would be a legitimate company. On the other hand, moving the ransom to a personal online account belonging to the malware author could look suspicious.

Attributing a purchase as a ransom transaction could be easier for the ransomware author by using tracking techniques. The most common method is using query string parameters and cookies [12]. A ransomware author could make money off the commission that gets paid to him for facilitating those purchases.

So far we have looked at ransomware, different attacks, how they have evolved, and different methods of extortion. The attacks we have specified so far are direct attacks, i.e., a Trojan gets installed in a system and seizes resources, ultimately demanding some kind of ransom. But Ransomware can be used as part of or in conjunction with other classes of malware as well.

In the next section we shall discuss how some implementations can use ransomware's inherent property of demanding things to complete their tasks or for surviving on their host machines.

The Show Must Go On

Getting malware onto a user's system becomes easier day by day. Depending on the type of malware, the infection vectors can be different. Self-replicating malware can use file infection or mass mailing to spread. Ransomware falls in the category of Trojans that are non-self-replicating malware and that use different methods for transmitting themselves. Our colleague Dmitry Gryaznov describes some of these in his publication *Malware in Popular Networks* [13]. But getting into a system is just half the job. The more important task is surviving and being efficient. Once malware enters the system, users must identify an infection either by themselves or by using an antivirus scanner; the choice of living with or getting rid of the malware is their onus. The survivability of malware depends on the users making (or not making) those choices. The effectiveness of some malware also depends on human interaction at some level in their life cycles. Automating this human link is a difficult task. In the following paragraphs we shall discuss the ways some classes of malware could utilize ransomware techniques to coerce a user into making (or not making) those choices.

Adware and Affiliates

Adware has added a new dimension to the malware field. The security industry has even created a new type of classification—"Potentially Unwanted Program" [14]—to identify these threats that are often more annoying than dangerous to users.

As the name suggests, their main behavior is to display ads to users; the ads are sometimes targeted based on the surfing habits of the user. Clicking on these ads or banners usually takes the user to a sponsor's site. With the use of botnets and spam mail, adware companies have been very successful in delivering adware to users. These popup and banner ads and spam mails are successful only in displaying ads; the choice of clicking on these ads and ultimately visiting these sites depends solely on the user. A well-educated user or a user with prior experience with adware would never click on these ads.

The adware business thrives on affiliate networks. This

business and its financial aspects have been well explained in the paper "Adware and Spyware: Unraveling the Financial web" [12]. This paper explains how affiliates are paid by affiliators in many various program types.

One of the affiliate program types is "pay per profile." In this program, each affiliate is paid different amounts depending on the user's action, which can vary from submitting e-mail addresses to filling in bulk forms.

The choice of taking the actions that adware requests remains with the user. It might be possible for adware to use techniques employed by ransomware to coerce a user to make these choices. We can imagine this happening with the adware either threatening users for not taking action or by asking victims to take actions as a payout for their relief from the malware.

Botnets

A botnet is a software robot network; botnets have swarmed like an army on the Internet for several years. Usually every botnet has thousands of bots, or compromised systems, spread across the globe, ready to spring into action with a command or two. The number of bots in a botnet can increase and decrease every day, and the numbers mainly depend on their survivability on their host machines.

Any malware survives on its host until the user of the system notices its existence and erases it, or until an antivirus program detects and deletes the malware. Antivirus programs are the most common enemy that threatens malware's survival. Systems controlled by botnets are no exception.

As with other forms of infection, delivering bots to vulnerable machines is becoming faster over time. SANS Internet Storm Center reported that computer survival time is shrinking [15]; another study suggests it could get as low as 20 minutes [16]. One of the several reasons for a shorter vulnerability window is the fact that more and more vulnerabilities are now becoming zero-day exploits [17]. Survivability is still a challenge for these bots because antivirus software vendors sometimes release updates as frequently as every hour. We can imagine a botnet controller using some of the techniques employed by ransomware to increase the survivability of bot programs.

Here are two scenarios that we might see:

- Seize them at the start. A ransomware technique could be exploited from the time a bot is installed on a machine. This will guarantee a fixed population for the bots at any time.
- Seize them as the need arises. A bot master could later send ransomware from the botnet command and control center to manipulate the propagation rate of the botnet.

Dagon et al. have described in their publication [16] that the propagation rate for a botnet varies as users switch off their computer systems over night. A bot master could effectively use ransomware techniques to make sure there aren't any significant changes in the population on a botnet, thus guaranteeing a consistent propagation rate. Victims could be threatened using these techniques to leave their computers turned on over night or for other periods. In the first scenario above, however, bot programs are more vulnerable to detection and cleaning by antivirus software if users are informed in the beginning by a ransom note.

Conclusion

Combining different attack modes to deliver a variety of payloads to a user's machine has been the natural evolution for any class of malware. It is not uncommon to see malware using a zero-day exploit to drop adware payloads for better distribution and increased revenue. We have yet to see ransomware being used in combination with other malware threats to increase the efficacy and survivability of each other, but the danger remains. The best way of keeping these malware attacks in check is through behavioral detection, and that's what leading security industry vendors are striving for.

We encourage users to not submit to the demands of malware authors. An alternative to recover from such damages is to roll back one's machine to an earlier backed-up state. Increased awareness and better user training will go a long way to help negate these attacks. Given the stir ransomware has caused with its limited appearance and subdued implementation thus far, we predict an increase in the ransomware trend and in the scenarios where malware authors might end up using techniques commonly used by ransomware.

References

1. Solomon, A., Nielson, B., and Meldrum, S., AIDS Technical Information, June 2000, The Center for Education and Research in Information Assurance and Security, September 2006, http://ftp.cerias.purdue.edu/pub/doc/general/aids.tech.info

2. Computer Incident Advisory Capability, *Infor-*

mation about the PC CYBORG (AIDS) Trojan horse, December 1989, U.S. Dept. of Energy, September 2006, http://ciac.llnl.gov/ciac/bulletins/a-10.shtml

3. McAfee Virus Information Library, *GPcoder,* June 2006, McAfee Inc., September 2006, http://vil.nai.com/vil/content/v_133901.htm

4. McAfee Virus Information Library, *CryZip,* March 2006, McAfee Inc., September 2006, http://vil.nai.com/vil/content/v_138886.htm

5. Krebs, B., *Ransomware Rising,* May 2006, The Washington Post, September 2006, http://blog.washingtonpost.com/securityfix/2006/05/ransomware_rising_1.html

6. Espiner, T., *Beware of ransomware, firm warn*s, July 2006, CNET News.com, September 2006, http://news.com.com/Beware+of+ransomware,+firm+warns/2100-7349_3-6097741.html

7. McAfee Virus Information Library, *MayArchive,* May 2006, McAfee Inc., September 2006, http://vil.nai.com/vil/content/v_139543.htm

8. Young, A, and Yung, M, "Cryptovirology: Extortion-Based Security Threats and Countermeasures," *Proceeding from the IEEE Symposium on Security and Privacy,* 1996

9. *About us,* PayPal, September 2006, http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside

10. *What is e-gold*, e-gold, September 2006, http://www.e-gold.com/unsecure/qanda.html

11. Williams, P., "Organized Crime and Cyber-Crime: Implications for Business," *Global issues electronic journal of U.S. Dept. of State on Arresting Transactional Crime*, August 2001

12. McAfee Avert Labs Technical White Papers, *Adware and Spyware: Unraveling the Financial Web,* July 2006, McAfee Inc., September 2006, http://www.mcafee.com/us/threat_center/white_paper.html

13. Gryaznov, D., "Malware in Popular Networks," *Proceedings of the 15th virus bulletin international conference,* 2005

14. *Anti-Spyware Coalition Definitions Document,* June 2006, Anti-Spyware Coalition, September 2006, http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm

15. Internet Storm Center, Survival Time History, http://isc.sans.org/survivalhistory.php

16. Dagon, D., Zou, C., Lee, W., Modeling Botnet Propagation Using Time Zones, *Proceedings of the 13th Annual Network and Distributed System Security Symposium,* 2006

17. Thomas, V., *Internet browsers and cyber-crime,* September 2006, McAfee Inc., September 2006, http://www.avertlabs.com/research/blog/?p=91