On the Current State of Ransomware

Daniel Kim

December 15, 2015

Abstract

In general, ransomware is a type of malware which, once it infects a system, will restrict access to that system, either locking the entire system or certain parts. The ransomware will attempt to then trick the victim into paying a certain sum of money in order to regain access. The most typical tricks include pretending to be a legitimate security program and offering to remove detected malware (i.e. itself) for a fee, impersonating police/FBI and threatening legal repercussions if a fee is not paid, and simpler intimidation where the attacker threatens to render the system useless if a ransom is not paid. Some of the most typical ways to end up with ransomware include visiting malicious websites and unknowingly downloading ransomware with seemingly legitimate files. This paper will delve into the current state of ransomware, including the many ways in which an attacker can inflict it and how to defend against today's ransomware.

Introduction

The first documented example of ransomware was the AIDS Trojan in 1989 [1]. Also known as the PC Cyborg Virus, it was created by Joseph Popp, a biologist. Popp simply handed out 20,000 disks infected with the AIDS Trojan at the WHO's AIDS Conference of that year. After an infected computer booted 90 times from the start of the infection, the ransomware would then hide all the directories on the computer and either encrypt or lock the names of all the files. The ransomware instructed the user to send $189 to PC Cyborg Corporation somewhere in Panama. Though this was the first ransomware, it was not particularly strong or well made; it used symmetric cryptography, and the proper decryption tools soon became available not long after this ransomware was released [1].

While Popp's ransomware ultimately was rather mild, today's ransomware varies from being about as mild as Popp's to being highly debilitating. The weakest form of ransomware today can be labeled as "scareware." Some ransomware of this form does not even lock your computer in any way but merely pesters the victim with popups and notifications. In general, "scareware" pretends to be an anti-virus service of some sort (almost always phony; never something a user has knowingly installed) and tells the victim to pay a certain sum of money in order to remove the viruses and malware on the infected computer [2]. Stronger ransomware actually blocks the victim from using their computer in any way at all; these typically impersonate some organization like the FBI and try to scare or intimidate the user into immediately paying a fee to remove the ransomware. The strongest ransomware uses asymmetric encryption to totally encrypt and lock a victim's files. In this scenario, little can be done to remove the ransomware.

To the Community

Ransomware is still a serious issue that continues to affect millions of users worldwide. According to the FBI, $18 million in total was lost to the CryptoWall ransomware alone, from April 2014 to June 2015 [3]. The most common victims are the average personal computer user and businesses. Many continue to unwittingly download ransomware; it is in fact surprisingly easy to have one's personal machine infected with it. Many victims will download and install software without checking to see what other things the software wants to install onto their computers. Still, the average computer user is most definitely not the only victim–even large companies, police departments [4], and government organizations suffer from ransomware. Since ransomware continues to be such a widespread problem, it is important for anyone who uses a computer on a daily basis to be aware of the risks and dangers of getting ransomware as well as how to deal with a ransomware infection on one's computer. Indeed, the problem is only spreading and growing; there are new forms of ransomware that even affect cloud storage and mobile devices.

How Ransomware Works

Infection methods

Different forms of ransomware each work in different ways. The most common methods of infection are compromised/malicious websites, spam email with malicious attachments or links to malicious websites, and fake software that seems legitimate and safe to download [5]. Some ransomware will even infect users across peer-to-peer file sharing. When a user visits a compromised/malicious site, the ransomware is silently downloaded and installed onto the victim's computer. Ransomware can also be spread via social engineering. Joseph Popp's original ransomware is one such example; he gave out the infected disks under the pretense that they were informational disks about AIDS. Something similar can still happen today with more modern pieces of technology, like USB flash drives.

Threats and Effects

Most ransomware that exists today typically tries to impersonate a legitimate entity or organization. Ransomware of this sort commonly tries to impersonate either some authority organization (i.e. a local police department or the FBI itself) or an existing software company. Impersonation of an authority organization typically involves threatening legal repercussions for not paying a fine within a certain short time window. The pretext of the "notice" is that illicit materials were found on the victim's computer [5]. Payment of such "fines" typically involves an untraceable method of money transfer, like "Ukash" or "MoneyPak". Impersonation of a software company also involves trying to make the victim panic and feel some sense of urgency; this ransomware usually notifies the victim that their software is not valid and that the user needs to pay for a valid license for their software [5]. Some forms of ransomware do not attempt such impersonation and simply demand money in exchange for the release of the infected computer.

There are many different ways in which different forms of ransomware will inhibit the use of an infected computer. One of the most common ways is a lock screen [2] which can be difficult for a normal computer user to get past without paying the ransom. Lock screens aim to block the victim from doing anything on the infected machine other than paying the ransom fee. Other variants will actually disable peripherals like the keyboard and mouse, only leaving the keyboard's

number keys working so that the victim can enter an unlock code once the ransom is paid [5]. Some ransomware will hijack control of an attached camera and take photos as means of coercion to pay the fee. However, none of these effects are quite as debilitating as a full encryption of the infected machine's files. While older forms of ransomware used weaker symmetric encryption, today's encrypted ransomware uses strong asymmetric 1024 bit encryption, which is completely infeasible to break [5]. CryptoWall, one of the forms of ransomware that uses strong asymmetric encryption, exploits CVE-2013-3660 to gain the privileges to be able to encrypt the infected system [8].

Defenses

The same basic methods of defense against viruses and malware in general are methods that are useful to protect against getting ransomware. Such methods include popup blockers, firewalls, and anti-virus software. It is also always important to simply be skeptical of certain sites, emails, or other things and to know what looks suspicious and untrustworthy. However, these basic defenses are only useful for preventing ransomware from reaching one's computer. In particular, anti-virus software is not particularly useful for actually removing ransomware; even the weaker forms of ransomware that merely pester a victim with popups and notifications are hard to remove with normal anti-virus. Even acclaimed anti-virus software like MalwareBytes and ComboFix can fail to do anything about ransomware. When it comes to a user taking matters into his/her own hands and trying to remove ransomware, finding the right anti-virus that is able to handle a particular ransomware can simply be a matter of guess and check.

Once a computer is infected with ransomware, not much can usually be done to remove it. One option is to combine an anti-malware service with Windows safe mode to remove the ransomware; this option is only feasible for particularly weak varieties of ransomware. Another option is to use Windows System Restore in order to attempt to bring the infected machine back to a state before the ransomware infected the computer. However, this option is by no means a guarantee of removal and can end up completely ineffectual for even a weak ransomware infection. As long as the ransomware is not of the asymmetric encryption variety, another possible option to remove the ransomware is using a bootable scanner [2]. This involves loading a virus scanner, like Bitdefender or Avast, from a bootable disc or USB stick. Essentially, the general approach to removing ransomware from a personal computer is to try various anti-malware remedies until something eventually works. The only way to be sure of recovering from ransomware is to do regular backups of one's machine, remembering to keep at least one backup offline and safely away from possible infection. Otherwise, the FBI actually recommends payment of the ransom as a possible option [6]. Still, one should not immediately choose this as an option; the FBI still recommends contacting them first if the compromised machine/system has truly important data that needs to be recovered and the files are strongly encrypted. Additionally, it is not usually possible to catch the ransomware attacker afterward; attackers are usually untraceable behind Tor-hidden Bitcoin payment domains or other untraceable services [3].

One new defense against ransomware that has had success in protecting businesses from powerful ransomware like CryptoWall is SentinelOne [7]. The company's main protection software is its Endpoint Protection Platform (EPP). The company claims that its EPP is able to protect businesses against both known ransomware threats and zero day threats. SentinelOne EPP can immediately respond to ransomware and other attacks as soon as it is detected, and also can detect an attack as soon as it occurs. It can “automatically remove an endpoint from the network, terminate a

malicious process, quarantine malware, and delete malicious code altogether to prevent it from infecting other devices" [7]. The EPP can additionally roll back an infected system to precisely before the infection occurred as well as pinpoint what parts of a system were affected. According to CEO Tomer Weingarten, SentinelOne EPP also dynamically adapts to any previously unseen polymorphic malware, allowing systems that are under SentinelOne's protection to be safe against virtually any ransomware and other threats. Since more and more companies are becoming victims of ransomware, it is important for a company like SentinelOne to always be on top of current security threats and be able to respond to attacks swiftly and thoroughly.

Conclusion

Despite constant research and development of responses to and defenses against various forms of ransomware, ransomware continues to be a problem affecting many thousands of computer users worldwide and is only becoming a bigger and bigger issue. Indeed, in the past year, the number of organizations targeted for ransomware increased significantly [7]. Whereas typical consumers were the main target for many years, both commercial and government organizations are starting to get targeted more, presumably because such organizations are often able to pay much larger ransoms. However, organizations are also better able to acquire reliable defenses like SentinelOne EPP to both prevent ransomware and disinfect a system with ransomware on it; the average consumer does not typically have such solutions as easily available. The best an average computer user can do is to simply follow good habits that generally prevent malware infection, like avoiding malicious sites, spam email, and other suspicious things, as well as keeping one's operating system and antivirus up to date. Unfortunately, these habits can only accomplish so much, and once a system is infected, the only way to recover if antivirus doesn't work is to load an uninfected backup. Like numerous other security threats, ransomware continues to be a problem after having existed for so many years and does not look like it will be a solved problem any time soon. Since this problem is only growing larger as the years pass, even beginning to affect more than just the average personal computer, it is becoming increasingly important for computer users to be up to date on the current state of ransomware and what to do about it.

Supporting Material

The supporting material is an analysis of the Hidden Tear software, a ransomware-like crypter kit that uses symmetric encryption. The analysis is a separate pdf in this folder.

References

1. "AIDS Trojan or PC Cyborg Ransomware". *KnowBe4*. Retrieved November 2, 2015 from `https://www.knowbe4.com/aids-trojan`
2. Geier, Eric. "How to rescue your PC from ransomware". *PCWorld*. January 13, 2014. `http://www.pcworld.com/article/2084002/how-to-rescue-your-pc-from-ransomware.html`
3. FBI Public Service Announcement Alert Number I-062315-PSA. *Internet Crime Complaint Center*. June 23, 2015. `http://www.ic3.gov/media/2015/150623.aspx`

4. Newcomb, Alyssa. "Ransomware: How Hackers Are Shaking Down Police Departments". *ABC News*. April 13, 2015.

   http://abcnews.go.com/Technology/hackers-shaking-police-departments-ransom/story?id=30278202

5. Power, John-Paul. "Security Response: Trojan.Ransomlock". *Symantec*. April 15, 2009. Updated August 6, 2015.

   http://www.symantec.com/security_response/writeup.jsp?docid=2009-041513-1400-99&tabid=2

6. Zorabedian, John. "Did the FBI really say 'pay up' for ransomware? Heres what to do...". *Sophos*. October 28, 2015.

   https://nakedsecurity.sophos.com/2015/10/28/did-the-fbi-really-say-pay-up-for-ransomware-

7. Gendron, Marc. "SentinelOne Frees Enterprises from Ransomware". *Business Wire*. November 18, 2015.

   http://www.businesswire.com/news/home/20151118005485/en/

8. Kovacs, Eduard. "CryptoWall 2.0 Ransomware Capable of Executing 64-Bit Code: Cisco". *Security Week*. January 7, 2015.

   http://www.securityweek.com/cryptowall-20-ransomware-capable-executing-64-bit-code-cisco