Chapter 17
Ransomware:
A Rising Threat of New Age Digital Extortion

Akashdeep Bhardwaj
UPES Dehradun, India

ABSTRACT

Compared to the last five to six years, the massive scale by which innocent users are being subjected to a new age threat in form of digital extortion has never been seen before. With the rise of Internet, use of personal computers and devices has mushroomed to immense scale, with cyber criminals subjecting innocent users to extortion using malware. The primary victim to be hit the most has been online banking, impacting the security and reputation of banking and financial transactions along with social interactions. Online security revolves around three critical aspects – starting with the use of digital data and files, next with the use of computer systems and finally the internet as an unsecure medium. This is where Ransomware has become one of the most malicious form of malware for digital extortion threats to home and corporate user alike.

INTRODUCTION TO RANSOMWARE

With the recent explosion of internet and use of personal computers, has led to cyber criminals' subject internet users to widespread and damaging threats leading to extortion focused on making profits at such a massive scale that has never been seen before. Apart from facing virus, worms, spyware, phishing, Ransomware has now become the new form of malware threat entering the user systems from various infection aiding vectors like browser exploit kits, drive-by freeware apps, malicious email attachments, links offering free software or advertisements offering free cash and incentives through a downloaded file or an unpatched vulnerability in the operating system with a malicious program running a payload that compromises and encrypts the user data files or even hijacking the system itself forcing the innocent user into paying up to the ransom demands before having the data files and system restored and released.

DOI: 10.4018/978-1-5225-6201-6.ch017

According to NIST, "Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim."

The malware injects a malicious code into the user system that installs randomly in the system location as an executable. This code then takes the user system hostage by preventing users from accessing their computer systems normally, stopping certain applications or input devices from running or encrypting user data files and using scare tactics like asking the user to either do something like pay a ransom amount in form of Bitcoin or fill in surveys before releasing the system or data. Ransomware uses different psychological, social-engineering, coercing, behavior-economic techniques to convince the users to pay the ransom to regain control of their systems.

Malware is an umbrella term that represents malicious software whose sole purpose is intentionally malicious in nature operating with different actions and concealment technologies for attacking end users. Some of the common malware are virus, worms, Trojans, backdoors, rootkits, bots and spyware as

- Virus one of the most commonly available globally, represents multiple subcategories of the malware versions. This malware is parasitic in nature, unable to survive alone and generally found replicating itself by copying onto other application programs.
- Worm comprise of malicious code causing maximum damage to data and user information. It has the capability of replicating itself via networks, using inbuilt email or scan engines to identify and spread to other hosts. Worms tend to exploit OS vulnerabilities, executing other malware as payload.
- Backdoors are standalone alternative entrance to user systems bypassing the existing security mechanisms built into OS and application systems. Usually created by programmers and accidently left behind when testing specific code functionality at the last moment, however, these are planted and utilized by attackers in order to enjoy continued privileged access of an application or the server system.
- Trojans are programs that resemble a legitimate code or application, however have some malicious code inbuilt. These are based on Homer's Iliad on the concept of the Trojan horse and are non-replicating parasitic in nature, requiring a legitimate application program to hide and execute.
- Spyware are the most popular tools used for Identity thefts, comprising of malicious code to spy on victim's activities and system and then for stealing sensitive information. Identity theft has become a major risk for users accessing their data from unsecured or public systems.
- Rootkits are a set of programs to alter the standard functionality of operating systems in order to hide any malicious activity done by it. These replace common operating utilities like kernel, net stat, ls, ps with their own set of programs with the intention of any malicious activity gets filtered before displaying results on screen.
- Bot is a program that performs action based on instructions received from the master controller system. These are mostly autonomous programs residing on unsuspecting end user systems, used majorly in the 'dark community' to accomplish malicious tasks as dictated by the controllers. A network of such bots is called a botnet. IRC is an example of bot that is used to communicate with other botnets.

Ransomware started with misleading applications and free software programs around 2005 as the use and acceptance of Internet grew (Savage, Coogan, & Lau, 2015). These free and fake applications came