OIC-CERT Journal of Cyber Security
Volume 5, Issue 1 (July 2024)
19 – 22

Study on Ransomware Threat and Anti-Ransomware

Zhiqiang Lou[1]
[1]Affiliation: Huawei Technologies Co.,Ltd., Shenzhen, China
Louis.lou@huawei.com

ARTICLE INFO

Article History
Received 6 Jun 2023
Received in revised form 31 Jan 2024
Accepted 31 Jan 2024

Keywords:
Ransomware; anti-ransomware; Air Gap; file system WORM; data recovery; APT attack

ABSTRACT

Ransomware has become a major global cyber threat. Six trends in ransomware attacks are noticed in the industry. After listing the ransomware damages, countermeasures and three attack phases, the article analyzes five key technologies of anti-ransomware. Efforts are called to enhance security awareness and management and build a multi-layer defense system for ransomware protection.

I. RANSOMWARE HAS BECOME A MAJOR GLOBAL CYBER THREAT

Ransomware is a type of malware that hackers tend to use to steal and encrypt data, and make the system inaccessible. Then it can ask you to pay a ransom to decrypt the system. These threats include the publishing of stolen data or the self-destruction of data if the ransom is not paid.

Ransomware attacks have been more and more common, increasing by 350% in recent years, and ransomware variants have been up by 46% in just the past year. It's become clear that traditional antivirus software is not equipped to handle all new threats.

According to the World Economic Forum's Global Cybersecurity Outlook 2022, ransomware is one of the most alarming threats in the view of today's cyber leaders. Ransomware attacks target enterprise users, individual users, and operating systems like Windows, and Linux, Mac. They have caused enormous losses to enterprises across a wide range of industries.

Ransomware is stealthy by nature, and very good at disguising itself. There are many ways that it may attack your system. These include zero-day vulnerabilities, storage media, and phishing emails, which are difficult to detect and defend against.

II. SIX TRENDS IN RANSOMWARE ATTACKS

There are six trends for recent ransomware attacks. Firstly, attackers focus on large enterprises and infrastructure. Previous ransomware attacks cast a wide net. That changed in 2020, when professional ransomware organizations made large enterprises and infrastructure their main targets. The research and intrusion that hackers need to undertake started to become more difficult and time-consuming. Sometimes, it takes weeks or even months. But the potential payoff makes it worthwhile, in their view. Ransomware attackers tend to use Bitcoin for ransom payments. And darknet makes these payments difficult to trace. Strong encryption algorithms, Bitcoin and darknet together form an "iron triangle" for ransomware attackers.

ISSN 2636-9680
eISSN 2682-9266

Next, there's Ransomware as a Service. Ransomware operators now sell ransomware-related services to other attackers through customized solutions, memberships, or subscriptions. This lowers the barrier to entry for launching ransomware attacks and has led to explosive growth in the prevalence of ransomware.
Double extortion is becoming more frequent as well, leading to an increased risk of data breaches. Ransomware is not limited to the encryption of data and demand for a ransom. Attackers also steal data, and threaten to leak it. Such attacks can put the victim in a vulnerable position after their data is exposed.

Fourth, the supply chain has become the point of entry for extortion attacks. In June 2017, the server for a Ukrainian software company was attacked by ransomware, an attack that spread to several other large enterprises around the world. In July 2021, the US software developer Kaseya was attacked as well. Suppliers have become a quick entry point for ransomware attacks.

Worse yet, ransomware attacks are becoming increasingly common. The rapid development of network and information technologies, the widespread application of big data, cloud computing, and mobile Internet, and the continued popularity of crypto digital currencies have created the right conditions for cyber ransomware to take hold.

The last of the trends is that ransomware attacks have APT-like capabilities. Advanced Persistent Threat (or APT) is a complex and continuous network attack that consists of three elements: advanced, long-term, and threatening. Advanced means that APT attacks require higher customization and complexity than traditional attacks. Such attacks are also time and resource-intensive, as they require that the attacker researches and identifies vulnerabilities in the system. Long-term indicates that the attackers will monitor the target and obtain and reserve long-term access permissions to achieve their objectives during the attack. Threatening means that man-made attacks target high-value organizations. Once successful, attacks can lead to enormous economic loss, political implications, and devastating reputational blows to the target. Ransomware first came onto the scene in 2013, when it was widely spread, purposeless, and limited in scope. In 2017, the famous WannaCry ransomware started to sweep the globe, and in 2018 to 2019, ransomware attacks began to evolve from casting a wide net to spreading through methods like phishing emails and Brute-forcing RDP. In 2020, attacks began to be customized by high-level teams for the purpose of extorting targeted victims. The attack capabilities and threats are similar to APTs.

III. RANSOMWARE DAMAGES

Ransoms are also not the only problem organizations face: ransomware damages brand reputations, causes long service interruptions, and exposes enterprises to legal liability. Such collateral damage can be enormous: as much as 23 times the value of the actual ransom payment.

In 2021, ransomware halted all of the operations of an oil pipeline giant in the US. The company paid a ransom of US$4.4 million and experienced huge losses. The president declared a national emergency, and fuel shortages even caused some panicked residents to fill plastic bags with fuel. The State Department even offered a $10 million bounty on key members of the ransomware attack group. The loss caused by extortion attacks is huge. Therefore, building a complete ransomware protection line for data security is an urgent priority.

IV. RANSOMWARE COUNTERMEASURES

Ransomware incidents occur on an all-too-frequent basis, and ransomware groups continued to be active in 2021. Governments are taking ransomware seriously and passing legislation to guide businesses as they attempt to safeguard their data against ransomware.

The United States has the Sheltered Harbor Data and the NIST Cybersecurity Framework. Chinese Mainland also published cybersecurity laws, data security laws, and ransomware prevention guidelines. The Hong Kong Association of Banks (HKAB) has issued Secure Tertiary Data Backup (STDB) Guideline to restore critical data.

V. THREE ATTACK PHASES

Ransom attacks can be divided into three phases. In the first phase, attackers attack enterprise servers through network or management vulnerabilities. After illegally obtaining server permissions, attackers implant ransomware viruses and spread the ransomware viruses on the enterprise network to infect as many servers as possible, for the purpose of obtaining valuable enterprise data. During the second stage, the attackers initiate ransomware to encrypt the user's valuable data. In the third phase, the attackers delete unencrypted data and backup data, before extorting the enterprise.

VI. KEY TECHNOLOGIES OF ANTI-RANSOMWARE

1) E2E Data Encryption

Ransomware attacks have evolved from "pay the ransom and get your data back" to "pay the ransom or we expose your data." Data encryption and protection against leakage are basic requirements for ransomware protection.

2) Air Gap Replication

Isolated storage of backup copies is the best way to defend against ransomware because it directly reduces the possibility of attacks

3) File System WORM and Secure Snapshot

Ransomware infiltrates the backup system and deletes the backup data before encrypting production data and using that to demand ransom. Without backup data available, users have to pay the ransom to get their data back. Therefore, anti-tampering of backup data is particularly important in defense against ransomware attacks.

4) Detection and Analysis

Ransomware attacks are unavoidable. Both the ransomware file or production data encrypted by the ransomware can be backed up to the backup system. Security breach may occur again when infected copies are used. Therefore, detection and analysis need to be performed on both production data and backup copies to ensure that all data is "clean" and safe to use.

5) Instant Recovery of Data

Hardware:

a) Efficient all-flash storage media
b) Intra-node multi-controller A-A architecture

Software:

a) Full-stripe write and intelligent prefetch greatly improve service performance.

VII. SUMMARY: ENHANCE SECURITY AWARENESS AND MANAGEMENT AND BUILD A MULTI-LAYER DEFENSE SYSTEM FOR RANSOMWARE PROTECTION

Ransomware protection requires both technology and individual efforts. This means people are also important in protecting against ransomware. Regular security trainings are a must as they equip staff with the necessary knowledge to prevent phishing attacks.

The network and host layers intercept most ransomware before they launch further actions on the storage. You don't want to neglect these two layers when controlling the impact of viruses.

Storage is the last line of defense for data security because the network and host layers cannot always successfully intercept ransomware attacks. This is when storage should step in to retain the last copy of clean data for quick data recovery, reducing the loss caused by system downtime.

ISSN 2636-9680
eISSN 2682-9266