White Paper

Prevent Ransomware Attacks

Identify and respond to malware and URL threats, at scale.

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Introduction

Ransomware is a major threat to every business. Every single day, organizations around the world are having to pause operations due to inaccessible encrypted files, and they have to decide whether they let the attackers win and pay a large ransom to resume their work. However, as common as these attacks are, many businesses do not have a plan in place to prevent them.

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Contents

What is Ransomware 4

Breaking Down a Ransomware Attack 4

How Does a Ransomware Attack Work 5

Types of Ransomware Attacks 6

Examples of Ransomware in the Real World 7

How To Prevent Ransomware 8

IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

What is Ransomware

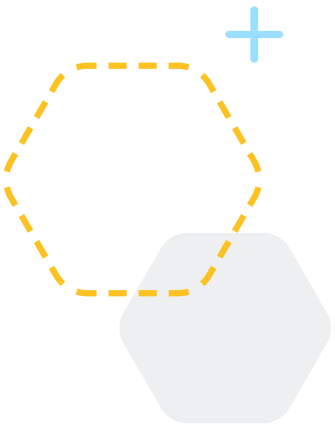
Ransomware is a type of malware that encrypts files on a device and demands some form of payment from the victim (almost always in crypto currency) in order to decrypt and release the hostage files. Like many other forms of malware, ransomware is often introduced as the payload of a phishing campaign, where the attacker tries to get unsuspecting victims to download a file in the form of an email attachment or on a malicious website.

Ransomware is particularly pernicious due to the fact that encrypted files typically cannot be decrypted without the attacker's private encryption key. Even if a victim is able to remove the malware from her device, she will still be unable to access her files without the attacker decrypting them.

In addition to the cost of the ransom, businesses incur large additional operational expenses. In fact, it's estimated that it costs over $84,000 for organizations to recover from a single attack.

Therefore, it's important to attack ransomware at the source before it lands in the inbox or to get it out of email mailboxes before it can detonate.

Breaking Down a Ransomware Attack



IRONSCALES
SAFER TOGRTHER

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

How Does a Ransomware Attack Work

Before implementing a system to prevent these ransomware attacks, it's important to understand how the different parts of the attack work:

Target

- Victim downloads the file
- For example, a user may download a file attachment from what seems to be a known source such as a business partner or friend

Execution and Encryption

- Program begins executing
- The ransomware detects the files it wants to attack
- Files are encrypted using the attacker's remote private encryption key

"Ransom" Demanded

- User is prompted with a message about the attack, letting them know that their files are encrypted and they'll need to pay to get them decrypted
- The attacker provides a method of payment such as a bitcoin address

User Response

- User decides whether or not they want to pay the ransom
- If the payment is not made, the files will remain encrypted
- The user can potentially remove the malware with antivirus software, but this will not decrypt the files

Resolution

- If the user paid the attacker, the attacker will likely—but not guaranteed—decrypt the files and move on

Types of Ransomware Attacks

There are three major subtypes of ransomware:

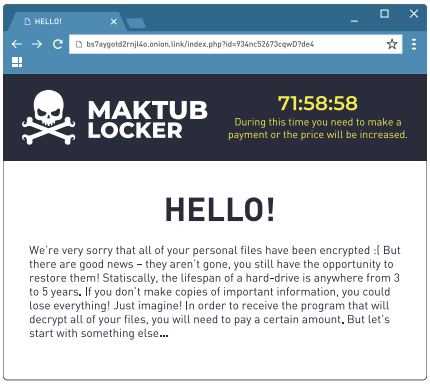
Scareware

Scareware is a type of malware where the attacker tries to scare or threaten the victim into performing some action. When used within a ransomware attack, scareware will involve aggressive language about what will happen to the encrypted files if the victim does not pay in a short window of time. The attacker may even pretend to be another organization such as a Federal agency demanding payment for a fine.

Crypto Ransomware

Crypto ransomware is when the ransomware attack demands payment in a cryptocurrency such as bitcoin. Unlike a traditional payment using a credit card or ACH network, a bitcoin payment cannot be reversed so the attacker can be confident that they'll keep the payment after they decrypt the files. Furthermore, attackers can create numerous different bitcoin wallet addresses so that law enforcement cannot easily track their attacks or determine the true identity of the attacker.

Locker Ransomware



Locker ransomware is when the victim is locked out of their device completely rather than simply having files encrypted. In addition to being unable to access their files, this limits victims' abilities to run anti-virus software to remove the malicious software from the device. This effectively makes the device unusable until the ransom payment is made.

Examples of Ransomware in the Real World

Now that we have a good understanding of how ransomware works and the different types, let's look at a few real-world examples of major attacks:

CryptoLocker, 2013

CryptoLocker was an email based ransomware attack that sent infected email attachments through a large Russian botnet. It was targeted at Windows users and encrypted numerous types of files when activated. The program demanded either bitcoin or pre-paid cash vouchers before a deadline when the private key used to initiate the attack would be deleted.

Fortunately, a security firm eventually was able to obtain a database of many of the private keys, but the attackers were still able to collect around $3m dollars from businesses and users around the world.

WannaCry, 2017

WannaCry was a sophisticated ransomware attack that exploited a network vulnerability in older Windows operating systems that allowed it to propagate itself across computers in a network automatically.

The program demanded between $300-600 USD in bitcoin to be paid to the attackers. Due to the automatic propagation technique, it was able to spread to over 300,000 computers in only four days. It's estimated that the economic toll may have been up to $4 billion in the form of ransom payments, business losses, and operational expenses.

AIDS Trojan Horse, 1989

One of the first known ransomware attacks, known as the AIDS Trojan Horse, was a malicious file that was sent on floppy disks to people on a mailing list in Europe. The attack claimed that users owed a license fee for running the program and demanded payment be sent in the form of international money order to a PO box in Panama.

The author was eventually arrested. He claims the money was being raised to fund AIDS research.

How To Prevent Ransomware

To prevent a ransomware attack, you must understand where the current threats and attack vectors lie within your organization, implement advanced software systems to detect and remove them, and develop a sophisticated incident response program to help resolve ongoing attacks and make plans to prevent future ones.

Assess Preparation For Potential Threats

Organizations must understand where their current vulnerabilities are and what types of attack vectors exist. Since ransomware typically comes from phishing attacks, it's particularly vital to gauge the strength of your email email security stack as well as the savvy of your employees.

Phishing simulations can help proactively detect weaknesses in employee understanding of attack types. In addition to running simulations to train employees, phishing emulation can be performed to test the adaptability of the technical defenses.

Defend Against Future Attacks

Organizations must have a Security Operations (SecOps) team in place that is able to quickly triage, investigate, and respond to potential phishing attacks in real time. Further, they must have automated incident response systems in place so that resolution can be done quickly and without anything slipping through the cracks.

Implement Advanced Protection Tools

In an evolving phishing, malware, and ransomware landscape, you need real-time tools that analyze and remove the most advanced threats instantly.

Traditional protection tools often fail against modern attacks. Firewalls, URL filters, and anti-spam software certainly have a place, but they will not protect you, your employees, and your company from today's sophisticated attacks.

Advanced malware and URL protection and visual learning tools are some examples of technologies that can be deployed to help detect and prevent evolving threats much faster than manual analysis and keep organizations ahead of the attacks.

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

www.srccybersolutions.com
+91 120 232 0960 / 1
sales@srccybersolutions.com