Ransomware has rapidly emerged as a significant threat to businesses and organizations of all sizes. Effective defense against this type of cyber crime begins with a combination of advanced global threat intelligence, technical solutions properly configured according to best practices, and strong end-user education and training can help prevent ransomware attacks in the first place. In addition, a secure backup solution (ideally cloud-based backup) is a necessity.

**THREAT BACKGROUND**

Ransomware is a type of malware that locks, encrypts, or otherwise prevents data and systems from being accessed by their owners, and which requires victims to pay a ransom to the criminal responsible for the attack in order to regain access.

Ransomware is primarily distributed via spam and phishing emails that are sent to large numbers of email addresses. When a recipient opens a malicious attachment or clicks a compromised link, the malware is loaded onto the user’s system. It then searches the hard drive and the associated network for predefined types of files and databases. Some variants also search for connected backup solutions, in order to lock or encrypt both live files and any backup archives that it can identify.

The cyber criminals behind the attack will usually give you a short window of time in which to pay—miss the deadline and the data will be erased. For small businesses or others with limited IT resources or expertise, this can create extra pressure to pay the ransom.

The number of ransomware attacks is increasing, reflecting the fact that they are all too often successful. While these attacks may result in a profit of only a few hundred dollars—far less than the potential returns from a major data breach—they are relatively easy to carry out, and do not require the criminal to monetize stolen data on the black market or elsewhere.
Ransomware Defense Strategies

Strategies that can help ensure that ransomware (along with other types of attack) is unable to get ahold of your important data in the first place:

1. Carefully designed policies that strictly limit the number of people and systems with access privileges for shared data stores
2. Advanced monitoring of incoming email and other traffic that uses real-time threat intelligence to identify malicious emails, compromised URLs and C&C hosts, and contaminated file attachments
3. Comprehensive monitoring of network traffic using advanced heuristic, sandbox, and emulation analysis to identify suspicious behavior by attacks both at and within the network perimeter
4. Next generation endpoint technologies such as advanced anti-malware which can detect and stop ransomware. In addition, application whitelisting technology can be configured to automatically block any unknown applications/malware/ransomware from executing on your endpoints by only allowing known, good applications (and their associated updates)
5. End-user training to minimize the effectiveness of malicious spam and phishing attacks that can infiltrate ransomware into the network

In addition to these preventive strategies, it is also critically important for you to use a secure backup solution. If, despite your best defensive efforts, you fall victim to ransomware, the ability to rapidly restore your hijacked data from a recent backup file will mean that you don’t have to pay the ransom. Indeed, if everyone were to use a secure, automated backup system that is independent of local storage and systems—ideally a cloud-based solution—then ransomware would cease to be profitable, and would probably disappear.

Access Control

When ransomware infects a particular system, it can access whatever data that particular system and its user can access. So, even if someone in your organization clicks the wrong link or opens the wrong file and allows ransomware into their system, as long as that individual does not have access to sensitive or business-critical data, there is little damage that the ransomware can do.

Organizations that enforce strong policies that strictly limit the number of people who have access to business-critical data are therefore far less vulnerable to ransomware attacks than those that permit unrestricted access.

CryptoLocker is a common family of ransomware that locks up affected systems and encrypts key files found on the system’s hard drive. Upon payment of the ransom, the encrypted files are unlocked and decrypted.

Since its first appearance in late 2013, CryptoLocker and its variants have been used in a large number of ransomware attacks. Critroni, or CTB-Locker, is a newer variant that uses Tor to mask its command-and-control (C&C) communications.
The Trend Micro Smart Protection Network

The Trend Micro™ Smart Protection Network™ is a real-time threat intelligence system that gathers global input from millions of collection points and uses big-data analytics to produce up-to-the-minute information about the latest threats. All of Trend Micro’s security solutions are constantly updated with the latest intelligence to enable them to identify malicious IP addresses, web addresses, C&C hosts, malicious code hidden in files, and the latest zero-day malware and exploits.

The Trend Micro Custom Defense

Trend Micro™ Deep Discovery provides network-wide monitoring of both internal and cross-perimeter traffic, using custom sandbox analysis, advanced heuristics, and dynamic analytic engines to identify malicious behavior at all stages of an attack, both at the perimeter and within your network.

In addition, it shares analytic capabilities and intelligence with Trend Micro and third-party email and web gateway solutions, creating a custom defense that identifies ransomware and other attacks, whether known or unknown, before they can find and compromise critical data and systems.

* CONSUMER EPP COMPARATIVE ANALYSIS: Socially Engineered Malware. NSS Labs, 2014.
Trend Micro Complete User Protection

A robust, multi-layered endpoint solution can help detect ransomware if it gets past other layers of protection. With an interconnected suite of security capabilities, you can protect against threats like ransomware—no matter where your users are going or what they are doing. Trend Micro Smart Protection Suites protect your users at multiple layers: endpoint security, email and collaboration security, web security and mobile security. Plus, the suites feature web reputation, file reputation, and behavior monitoring to help detect ransomware files during download or execution. In addition, Smart Protection Suites give you the broadest range of advanced threat protection for anti-malware, packer variant protection, encryption, device control, data loss prevention, vulnerability shielding, command and control blocking, browser exploit protection, application whitelisting, web threat protection, social engineering attack protection, Census data and more.

Trend Micro Support Services

Once you deploy advanced technical solutions, it is still critical to ensure that they are configured to provide optimal protection. In addition, you must institute a robust training program to ensure that all employees within your organization are equipped to recognize spear-phishing attacks and other attempts to penetrate your network. Trend Micro support services are available to help you adopt best-practice configurations to optimize your Trend Micro solutions to identify and block attempts to penetrate your network with ransomware and other malware.

In addition, we are available to help you design a training program that can enlist your workforce in supporting your security strategy with essential email hygiene habits. This is important because of how often ransomware is delivered through spam phishing email. The most important habit is to be suspicious of all emails that contain attachments or links. When you receive a suspicious email like the example at left:

• Do NOT click on the link in the email
• Do NOT open an attachment in the email
• Do NOT enter a CAPTCHA if requested
• Confirm the validity of the email by contacting the sender using independent means—preferably by phone, or using an address that you already have, or find separately, rather than anything within the email
• If the email appears to come from a company or organization, use a search engine to find the correct URL for that organization's site, then visit the site and contact the organization using information there

Sample of Crypto Ransomware spam

TAKING THE FIRST STEP

Whether you are already protected by Trend Micro solutions, or are in the early stages of selecting a way to protect your organization against ransomware and other threats, now is the time to contact us for expert assistance. We can help you to ensure your existing solutions are optimally configured to protect you from today’s advanced threats. And we can craft customized recommendations for an employee training program that makes your organization less vulnerable to the most common attack vectors.