CUSTOMER ADVISORY

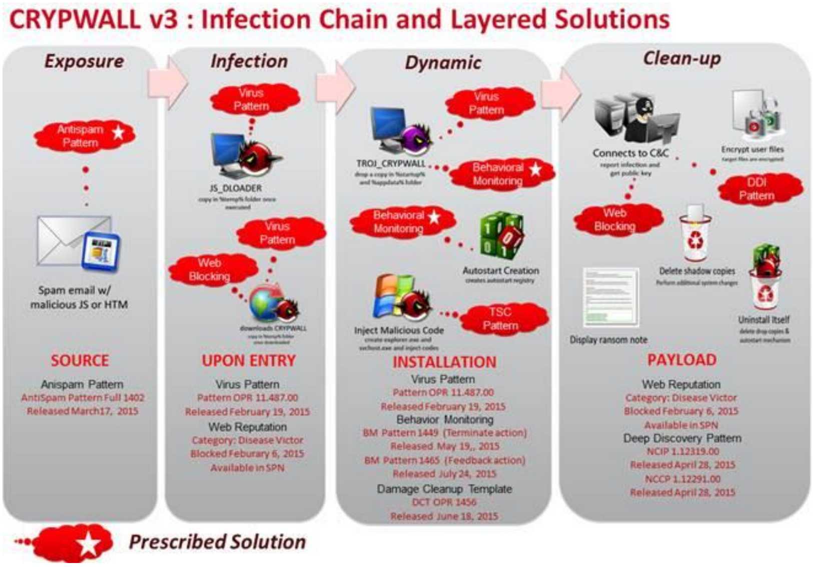
Ransomware: Trend Micro Solutions, Best Practice Configuration and Prevention

Date: August 18, 2015

Overview

Trend Micro has seen a dramatic rise of ransomware related issues, especially ones dealing with sophisticated Crypto-Ransomware, which has both home and commercial users alike concerned. Like many other cyber threats, ransomware has become increasingly complex and advanced over time – making prevention and protection more challenging.

Ransomware can enter an organization through many vectors; including via email spam, phishing attacks, or malicious web downloads. Like other high sophisticated threats, organizations are recommended to employ multiple layers of protection on the endpoint, gateway and mail servers for the highest level of protection against ransomware. More detailed information about a typical ransomware infection chain can be found here (including this small graphic below).



The purpose of this advisory is to share information about some of Trend Micro's recommended configuration best practices on various products, as well as to share some details on some important software updates that are available to better protect against and combat ransomware.

Trend Micro Solutions and Best Practice Configuration

Trend Micro has several solutions that leverage the Trend Micro™ Smart Protection Network™ to help administrators block ransomware threats from possible points of infection. The latest versions of each of these, including important service packs and critical patches can be downloaded from the Trend Micro Download Center.

Endpoint Protection Layer

Trend Micro OfficeScan and *Worry-Free Business Security*

- Both of Trend Micro's corporate endpoint protection products contain key technologies that are highly recommended to be enabled to protect against ransomware: *Web Reputation Services* and *Behavior Monitoring.* Information on enabling and configuring these options can be found in the following Knowledge Base (KB) articles:
  - OfficeScan Best Practice Configuration
  - Worry-Free Business Security (including Services) Best Practice Configuration

- Beginning with *OfficeScan version 11 SP1* and *Worry-Free Business Security 9.0 SP2*, two new *Ransomware Protection* features have been added with advanced behavior monitoring. Information on enabling these features can be found in Trend Micro's Knowledge Base here: OfficeScan 11 SP1 and Worry-Free 9.0 SP2.

- In order to better alert customers to potential ransomware behavior or attacks, Trend Micro has released some hotfixes that enable some new notification and protection features. The following links contain both information and download instructions for the various products:
  - OfficeScan 11 SP1 B3071
  - Worry-Free Business Security 9.0 SP2 B3205

Trend Micro Endpoint Application Control

- Administrators who wish to have an additional layer of protection on endpoints, including preventing unwanted and unknown applications (like ransomware and 0-day malware) from executing, may deploy policies to block untrusted EXE files. Customers who have purchased one of *Trend Micro Complete User Protection* suites may already have the license for this protection, but have not yet implemented it. More information on how to install and configure policies can be found here.

Email and Gateway Protection Layers

- Since email is a popular vector for attackers to deliver ransomware, effective blocking of certain non-essential file types such as JS or HTM files is also recommended. Administrators may block these file types by true file type (recommended) or by specific extension names. More specific information on how to block email attachments using Trend Micro Messaging and Gateway products, including *ScanMail for Microsoft Exchange, Hosted Email Security, and InterScan Messaging* can be found here.

- *Trend Micro Email Reputation Services* users are strongly encouraged to enable the Quick Information List (QIL) filtering level for IP reputation and set the level to at least **Level 2**. Information on enabling and configuring this option can be found here.

Prevention

Victims who have been affected by ransomware can generally attest to the pain and complexity of trying to recover after such an attack. Because of this, increased user awareness and vigilance can save a potential victim time and money in the unfortunate event of an attack. Preventing the attack in the first place is still the most effective way of dealing with this threat.

The following is a list of some preventative measures that users and administrators can employ as a matter of best practice:

- Regular backups of critical data in case of any sort of loss (not just ransomware)
- Timely application of software patches from OS and 3rd party vendors
- Exercise good email and website safety practices – downloading attachments, clicking URLs or executing programs only from trusted sources
- Encourage users to alert IT Security team of potentially suspicious emails and files
- Ensure your security products are updated regularly and perform periodic scans
- Implement application whitelisting on your endpoints to block all unknown and unwanted applications
- Regular user education around the dangers and signals of social engineering

Trend Micro continues to devote countless hours of research into new ways of combating these threats and will continue to update our users with the latest information and recommendations through our Security Intelligence Blog and in additional updates to this article in Trend Micro's Knowledge Base.

In addition, your authorized Trend Micro support representative is available for any questions regarding the configuration options mentioned in this advisory to combat ransomware.