Trend Micro Deep Security: Ransomware Detection and Prevention

Trend Micro Deep Security can protect servers from the effects of ransomware in multiple ways.

Trend Micro Deep Security has protection capabilities which generically defend servers against malicious software, including ransomware. Deep Security includes:

- ***Anti-Malware*** scanning, leveraging data from the Smart Protection Network, to stop malicious software from attacking a server
- Network security, including ***intrusion prevention (IPS)*** which stops vulnerabilities from being exploited and the resulting potential installation of malicious software (including ransomware)
- System security, including ***integrity monitoring*** which can provide visibility of system changes that represent malicious software activity
- ***Web Reputation***, which blocks outbound communication to known bad domains

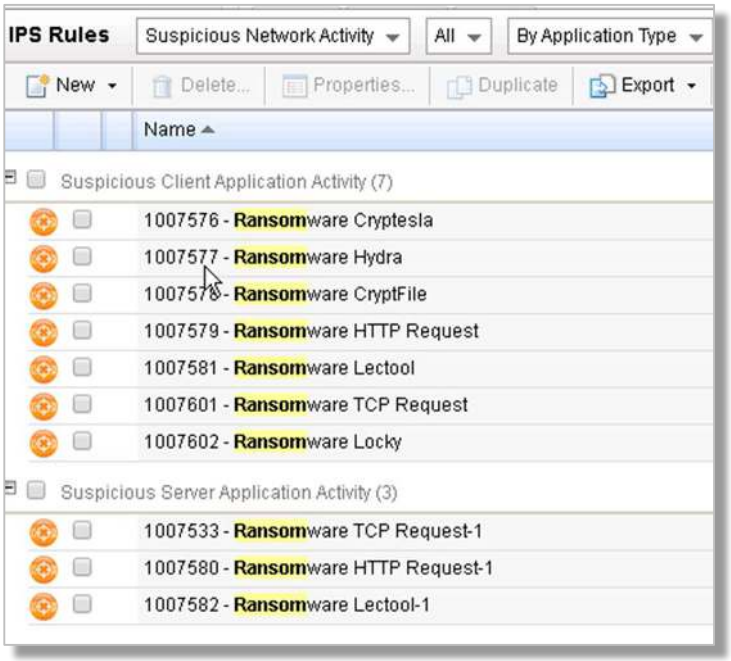
Trend Micro Deep Security protection modules also contain ransomware-specific defense capabilities, which are listed below.

Note: This list is current as of document publishing. Trend Micro's threat team is constantly looking for ways to enhance the protection that Deep Security can provide and the list will grow over time.

Intrusion Prevention (IPS): Suspicious Network Activity

Ransomware Command and Control Communication:

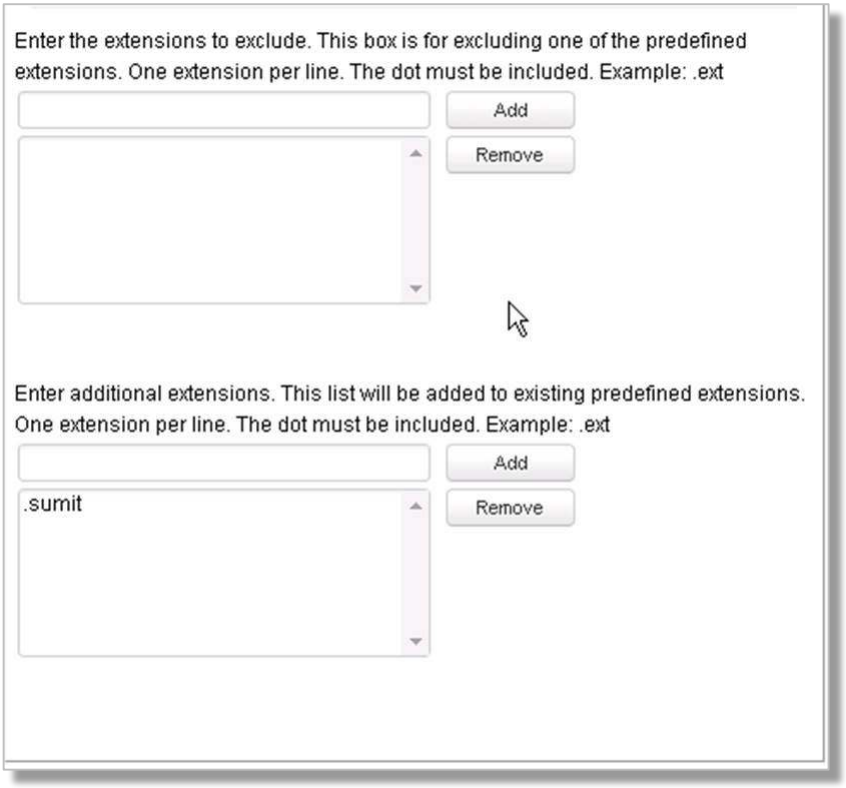
Deep Security detects and prevents ransomware command and control (C&C) activity over the network. Instead of focussing on domains and IP addresses, these rules scan network traffic for known communication techniques used by ransomware.



Network File Share Protection

Trend Micro Deep Security provides the following Intrusion Prevention rules which specifically address the ransomware technique of encrypting files on mounted shares (Windows or Linux – Samba).

1. Rule name: **1007596 - Identified Suspicious File Extension Rename Activity Over Network Share**
   This rule provides visibility into ransomware activity but in most cases does not prevent ransomware encryption activity. This rules monitors for known techniques that ransomware uses in changing file extensions (e.g. .zzz, .encryptedRSA, .crypt etc.). There's a check for ~50 file extensions in the rule. The rule also provides an option to exclude and include certain file extensions to maximize the benefits of this rule



   a. Default settings for the rule are
      i. Detect-only
      ii. Recommended on windows computers.

2. Rule Name: **1007598 - Identified Suspicious Rename Activity Over Network Share**
   This rule can be used to protect a server from clients infected with ransomware. This rule monitors and limits file change activity over the network. More specifically, this rule prevents the number of file renames in a specific period of time (N renames in T1 seconds results in limiting any rename activity *for* T2 seconds from the malicious source IP Address).

a. Default settings for the rule are
    i. Detect-only
    ii. Not recommended by default. The rule must be manually assigned.
    iii. N=0, T1=0, T2=0 (no action by default)