



The Truth is Out There

How Trend Micro CAN really protect you.



Topics

Configuration Strategies and Best Practices for OSCE 8.0

- Scan Configuration, Scan Actions
- OSCE Real-time Scan Configuration and Intellitrap
- Heuristic/Generic Pattern
- GeneriClean
- Service Pack 3

Features and Mitigation Strategies

- Web Reputation Service (WRS)
- Outbreak Prevention Policy (OPP)

Incident Assistance

- How to submit a virus to Shea or TM
- How to submit a TM ticket

OfficeScan 8.0

Configuration Strategies and Best Practices



Service Packs and Patches

- Service Packs and Patches

<http://www.trendmicro.com/download/product.asp?productid=5>

- Service Pack 1
- Patch 3- Build 3243 (3/25/09)



Scan Configurations

- Scan Configurations
 - Manual Scan
 - All Scanable Files
 - Use Specific Actions
 - Real-Time Scan
 - Created/Modified and Retrieved
 - Intelliscan
 - [Intellitrap](#)
 - Use Specific Action
 - Scheduled Scan
 - All Scanable Files
 - Enable Intellitrap, scan boot area
 - Medium CPU usage
 - Specific Scan Action



Scan Actions

- Generic and Heuristic Scan
 - Can identify by name
 - Possible_
 - Cryp_
 - Xxxx_xxxxx.gen
 - Xxx_generic
 - Default Action=NoNothing
 - After 2 weeks, loaded into the engine and it becomes detected.
 - **Recommendation-** Enable a Scan Action (see Best Practices Document)



Scan Actions

- GeneriClean Technology
 - Referential cleaning –Automatically removes malicious files and restores system modifications
 - Removes or cleans registry entries
 - 90% malware samples received were cleaned by Genericlean
 - Requirement OSCE 8.0 SP1
- Please refer to the Best Practices for details on registry keys
- Every time GeneriClean is triggered, it will automatically modify these registry keys and set the value. If you do not want the keys to be modified, set the value to 0.



Service Pack 3

- Scheduled Scan Enhancements
 - Postpone Scheduled Scan
 - Skip and Stop Scheduled Scan
 - Resume Scheduled Scan
 - Scan Reminder
- Product Enhancements
 - %i variable in alert messages (IP)
 - Different update schedules for online and offline clients
- Lots and Lots of 'issues' resolved refer to readme

OfficeScan 8.0

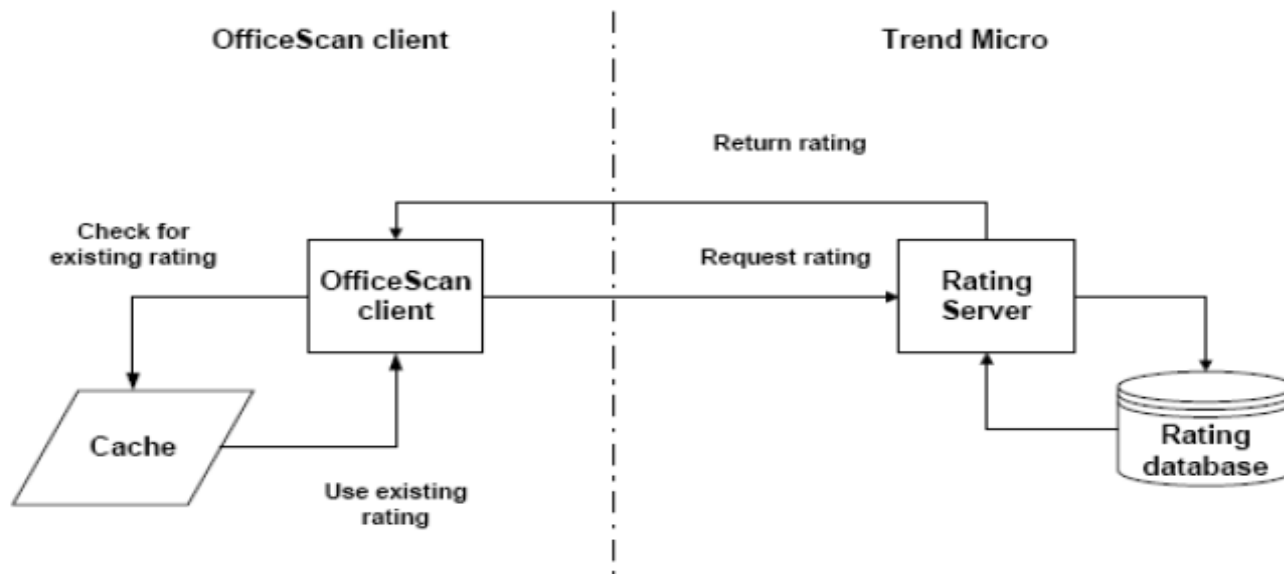
Features and Mitigation Strategies



Web Reputation Services

- Stops web-based threats based on the URL
- Access to a URL is allowed or denied based on TM global web reputation database
- Does not discriminate based on content. Focus is exclusively on scoring URLs according to their threat potential

Web Reputation



Uses in memory cache if an existing rating exists.

If new site OfficeScan queries rating server by sending request to `osce80-en.url.trendmicro.com`

Web Reputation

- Security Level
 - High
 - Threshold-80
 - Medium
 - Threshold-70
 - Default in external policy
 - Medium-Low
 - Threshold-60
 - Default internal policy
 - Low
 - Threshold-50

Score	Description
81	Safe sites
71	Unrated
51	Suspicious
49	Known malicious sites



Web Reputation

- Approved list
 - URLs listed will not go through server lookup
 - Maximum URLs: 50
- Client Alert Messages
 - Customize alert messages
- WR Logs
 - Can enable so that list of block sites is created in OfcUrlf.log.



Outbreak Prevention

- Proactively prevents and contains outbreaks
- Can
 - Limit/Deny Access to shared folders
 - Block Ports
 - Deny Write access to files and folders
- Specify time frame and notification message

OfficeScan 8.0

Incident Assistance



How to Submit Virus

- Run SICTool
 - <http://www.trendmicro.com/download/sic.asp>
- Send SICLOG and SUSPECT.ZIP to Shea McGrew or Harvard Townsend. Password protect the file.

How to submit ticket

- **Trend Micro technical support**
- **Phone:** (888) 608-1009
Hours: Mon-Fri, 5 a.m.-5 p.m., U.S. Pacific Time
(except on holidays)

To submit a case:

<http://kb.trendmicro.com/solutions/Srf/questionEntry.aspx>
<http://esupport.trendmicro.com/support/viewxml.do?ContentID=EN-121922&id=EN-121922>

****You will need the OfficeScan activation code to complete a ticket that code is:**

Thanks!!!



IntelliTrap

Product : OSCE 8.0

- Pattern used – tmlblack and tmwhite
- Intellitrap is capable of detecting packed files
- It **only** scans these 2 folders
 - * IE Temp Folder
C:\Documents and Settings\%LoginUserID%\Local Settings\Temporary Internet Files\
 - * Outlook temp folder (Outlook 2000, XP, 2003 and 2007)
C:\Documents and Settings\%LoginUserID%\Local Settings\Temporary Internet Files\%OLKB5%*.*
- Can it be configured to scan a different directory (i.e. c:\, c:\windows or d:\) = NO
- Detected as trend as PAK_Generic.001