

**Dear Valued Trend Micro Customer:**

On December 31, 2009, two (2) legacy anti-spyware pattern files, TMAPTN and DA5, will reach end-of-service (EOS) status. After this date, Trend Micro will no longer add new signature updates to these anti-spyware patterns.

Customers who are utilizing products with either of these technologies should upgrade to a current version that supports the newer technology or apply the necessary software patch (if applicable).

Details on the list of products affected by this EOS announcement, as well as the availability of product patches may visit the following Knowledge Base articles:

**TMAPTN:** <http://esupport.trendmicro.com/0/End-of-Service-EOS-for-the-TMAPTN-VSAPI-Anti-Spyware-pattern.aspx>

**DA5:** <http://esupport.trendmicro.com/9/End-of-Service-EOS-for-Anti-Spyware-Engine-SSAPI-5x-DA5-pattern-file.aspx>

If you have any questions or concerns, please refer to the attached FAQ guide for more information or feel free to contact your authorized Trend Micro technical support services provider in your region for further assistance with any migration questions or technical issues you may have.

Sincerely,

Trend Micro

## **Introduction**

### **Overview**

This document is intended to communicate key information for the End-of-Service of the legacy anti-spyware patterns used by some older Trend Micro products and solutions.

### **Audience**

This document is intended solely for the use of Trend Micro Customers and Partners.

### **Clarification**

*Please note that this document covers the EOS for legacy anti-spyware patterns only. Conventional VSAPI pattern files (the main pattern file) that contain the bulk of the malware signatures are unaffected by this announcement.*

*The TMAPTN spyware pattern is updated with roughly **10-50** signatures **PER WEEK**. In comparison, the main VSAPI pattern file is updated with approximately **800-1200** new signatures **PER HOUR**.*

*Even though there may be minor impact for customers who are having difficulty moving to the latest technology, Trend Micro still encourages migration and/or upgrading to the latest versions as soon as possible to enjoy the benefits and expanded protection of the technology.*

Also, this article does not apply to and is not relevant to any product that has already reached its own EOL/EOS status.

## **TMAPTN Anti-spyware Pattern**

### **What is TMAPTN?**

TMAPTN is a pattern that exists in legacy Trend Micro products. In the past, it has been used to deliver anti-spyware protection to customers. Currently, TMAPTN is used by the VSAPI anti-malware engine to implement anti-spyware protection either during scheduled, manual or real-time scans.

### **Why is TMAPTN being decommissioned?**

The protection provided by the TMAPTN pattern is inferior to its successor pattern – SSAPTN which includes many more signature updates and offers the customer better protection.

### **What supersedes TMAPTN and when was the successor pattern released?**

TMAPTN has been superseded by the SSAPTN pattern, which provides better anti-spyware protection to customers with significantly more signatures being added on a daily basis. SSAPTN was released in July, 2005.

### **Which products still use TMAPTN and what are their upgrade paths?**

As of the date of the EOS notice, most Trend Micro products have already decommissioned the use of TMAPTN either via:

- Product level End of Service (EOS) or
- A patch that upgrades the product to use the newer SSAPTN pattern

A list of products using TMAPTN and their upgrade paths can be found at:

<http://esupport.trendmicro.com/0/End-of-Service-EOS-for-the-TMAPTN-VSAPI-Anti-Spyware-pattern.aspx>

### **What are the benefits of using the newer SSAPTN pattern?**

Customers who use the newer SSAPTN anti-spyware pattern will benefit from the following:

- Uninterrupted spyware protection
- Improved spyware detection capabilities

### **What is the impact if I DO NOT upgrade to the newer SSAPTN pattern?**

Customers who continue to use TMAPTN based products past their EOS date will lose approximately **10 to 50** signature updates **per week**.

In comparison, the current primary malware patterns – LPT\$VPN and iCRC\$xxxx receive approximately **800-1200** new signature updates **per hour**.

Customers should not experience any warning messages or other issues, but spyware detection will decrease over time.

## **DA5 Anti-spyware Pattern**

### **What is DA5?**

DA5 (the successor to DA3) is a pattern that exists in legacy Trend Micro products. In the past, it has been used to deliver anti-spyware protection to customers. Currently, DA5 is used by the SSAPI anti-spyware engine to implement anti-spyware protection to desktop products only and is typically used during a scheduled or manual scan only. It is not used in real-time scan.

### **Why is DA5 being decommissioned?**

As with TMAPTN, the protection provided by the DA5 pattern is inferior to its successor pattern – DA6 which receives many more signature updates and offers the customer better protection.

### **What supersedes DA5 and when was the successor pattern released?**

The DA5 pattern has been superseded by the DA6 pattern, which provides better anti-spyware protection to customers with significantly more signatures being added on a daily basis. DA6 was released in 2007.

### **Which products still use DA5 and what are their upgrade paths?**

At the date of the EOS notice, most Trend Micro products have already decommissioned the use of DA5 either via:

- Product level End of Service (EOS) or
- A patch that upgrades the product to use the newer DA6 pattern

A list of products using DA5 and their upgrade paths can be found at:

<http://esupport.trendmicro.com/9/End-of-Service-EOS-for-Anti-Spyware-Engine-SSAPI-5x-DA5-pattern-file.aspx>

### **What are the benefits of using the newer DA6 pattern?**

Customers who use the newer DA6 anti-spyware pattern will benefit from the following:

- Uninterrupted spyware protection
- Improved spyware detection and cleanup
- Lower memory consumption
- Better application performance
- More efficient file scanning

**What is the impact if I DO NOT upgrade to the newer DA6 pattern?**

Customers who continue to use DA5 based products past their EOS date will lose approximately **100 to 200** signature updates **per week**.

In comparison, the current primary malware patterns – LPT\$VPN and iCRC\$xxxx receive approximately **800-1200** new signature updates **per hour**.