Fallstudie: Deaktivierung von Endpoint-Protection-Software auf nicht autorisierte Weise

Wie man die Passwort-basierte Authentifizierung für das Entladen von Trend Micro OfficeScan *umgeht*

Dipl.-Inform. Matthias Deeg
Dipl.-Inform. Sebastian Schreiber

SySS GmbH

18. Juni 2012

1 Einleitung

Endpoint-Protection-Software wie Antiviren- oder Firewall-Software bieten Benutzern oftmals die Funktion, den angebotenen Schutz durch die Eingabe eines Passworts zu deaktivieren. In manchen Fällen kann dabei die Schutzfunktion nur temporär für wenige Minuten abgeschaltet werden, in anderen Fällen bis zu einer erneuten manuellen Aktivierung oder einem Neustart des Systems.

Diese Funktion kann in gewissen Situation für den IT-Support hilfreich sein.

Aber ist die Passwort-basierte Authentifizierung nicht sicher umgesetzt, so können Angreifer oder Schadsoftware die Schutzfunktion auf nicht autorisierte Weise deaktivieren ohne das korrekte Passwort zu kennen, wodurch die Endpoint-Protection-Software nicht ihren Zweck erfüllt.

In dieser Fallstudie demonstriert die SySS GmbH dieses Sicherheitsproblem am Beispiel der Antivirensoftware Trend Micro OfficeScan.

2 Sicherheitsanalyse

In manchen Konfigurationen bietet die Antivirensoftware Trend Micro OfficeScan nicht-administrativen, eingeschränkten Windows-Benutzern die Möglichkeit, die Antivirensoftware mit einem *Unload*-Passwort zu deaktivieren, wie Abbildung 1 mit der Darstellung des entsprechenden Menüpunktes zeigt.

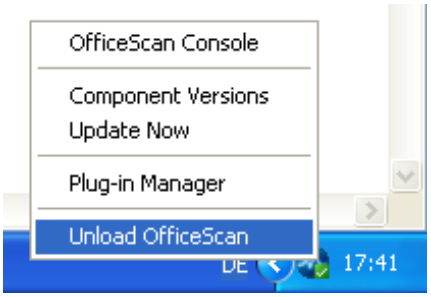

Abbildung 1: Option um Trend Micro OfficeScan zu deaktivieren

Um Trend Micro OfficeScan zu deaktivieren, muss der Benutzer das korrekte *Unload*-Passwort in einem entsprechenden Dialogfenster eingeben, welches in Abbildung 2 dargestellt wird.

Abbildung 2: Passworteingabe um Trend Micro OfficeScan zu deaktivieren

Wird dabei ein falsches Passwort eingegeben, so wird die in Abbildung 3 gezeigte Fehlermeldung ausgegeben.

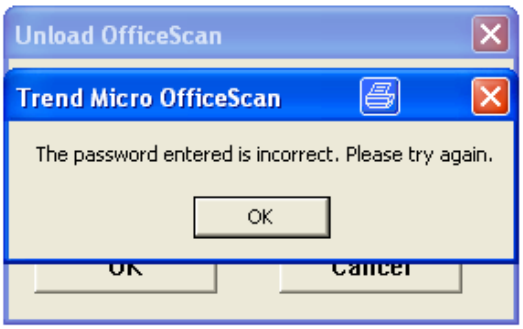

Abbildung 3: Fehlermeldung bei der Eingabe eines falschen Passworts

Bei der Analyse der Passwort-basierten Authentifizierung für die Deaktivierung von Trend Micro OfficeScan stellte die SySS GmbH fest, dass der Passwortvergleich innerhalb des Prozesses `pccntmon.exe` stattfindet, der im Kontext des aktuellen Windows-Benutzers ausgeführt wird. Bei dem Benutzer kann es sich dabei auch um einen Standardbenutzer mit eingeschränkten Benutzerberechtigungen handeln.

Diese Tatsache erlaubt eine weitere Analyse und – was noch viel interessanter ist – die Manipulation des Passwortvergleichs zur Laufzeit ohne administrative Berechtigungen, da jeder Benutzer in der Lage ist diejenigen Prozesse zu debuggen und zu manipulieren, die mit seinen Benutzerberechtigungen laufen.

Abbildung 4 zeigt den entsprechenden Code für den Vergleich des MD5-Hash-Werts des eingegebenen Benutzerpassworts mit dem MD5-Hash-Wert des korrekten *Unload-*

Passworts für eine 32-Bit-Softwareversion von TrendMicro OfficeScan im Windows-Debugger OllyDbg[1].

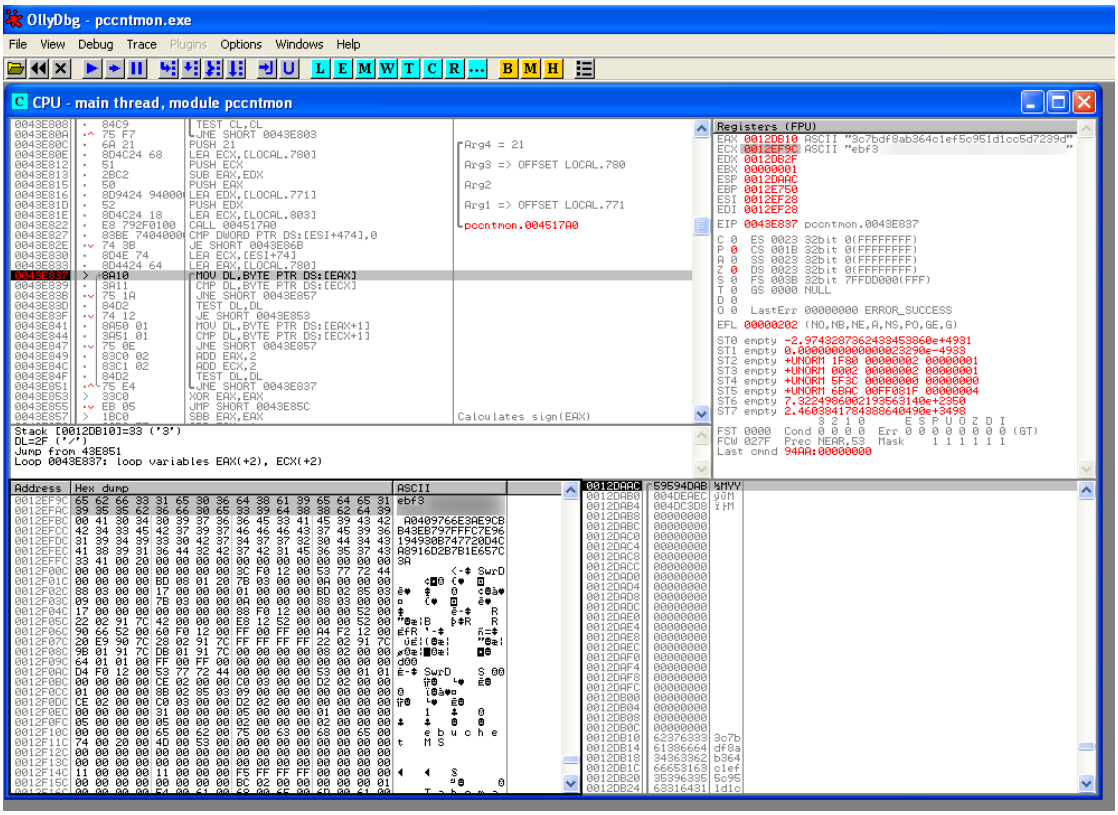

Abbildung 4: Vergleich von MD5-Hash-Werten

Um diese Passwort-basierte Authentifizierung zu umgehen, muss ein Angreifer lediglich diesen Passwortvergleich modifizieren, sodass er immer erfolgreich ist, beispielsweise indem das korrekte *Unload*-Passwort mit sich selbst verglichen wird.

Darüber hinaus besteht die Möglichkeit, den MD5-Hash-Wert des korrekten *Unload*-Passworts zu extrahieren, um das entsprechende Passwort mit Hilfe eines *Password Recovery*-Tools, wie beispielsweise John the Ripper[2], wiederherzustellen.

Die notwendigen Schritte, um die Antivirensoftware Trend Micro OfficeScan zu deaktivieren, können auch vollständig automatisiert durchgeführt werden, sodass diese Sicherheitsschwäche auch von Schadsoftware ausgenutzt werden kann.

[1] `http://www.ollydbg.de/`
[2] `http://www.openwall.com/john/`

3 Empfehlung

Die SySS GmbH empfiehlt, den Passwortvergleich nicht innerhalb des Prozesses `pccntmon.exe` durchzuführen, der im Kontext das aktuellen Benutzers mit dessen Berechtigungen läuft, sondern innerhalb eines Dienstprozesses von Trend Micro OfficeScan, der mit höheren Berechtigungen ausgeführt wird, wie etwa `SYSTEM`-Rechten.

In diesem Fall kann ein Windows-Benutzer mit eingeschränkten Rechten oder Schadsoftware, die in seinem Kontext zur Ausführung kommt, nicht den Passwortvergleich von Trend Micro OfficeScan zur Laufzeit manipulieren, um die Antivirensoftware auf nicht autorisierte Weise zu deaktivieren.

Die SySS GmbH informierte den Hersteller Trend Micro am 26. April 2012 über diese Schwachstelle.

Nach Informationen von Trend Micro wurde die demonstrierte Schwachstelle, die eine Deaktivierung von Trend Micro OfficeScan auf eine nicht autorisierte Weise ermöglicht, mit dem kürzlich veröffentlichten *Service Pack* für die Antivirensoftware Trend Micro OfficeScan behoben.