SecLab

Praktikum IT-Sicherheit

- Versuchshandbuch -

Aufgaben

Trojaner

Als Trojaner wird eine Art von Malware bezeichnet, bei der es sich um scheinbar nützliche Software handelt, die aber neben ihrer sichtbaren Tätigkeit im Hintergrund unbemerkt schädliche Funktionen ausführt. Zur Klasse der Trojaner gehören auch die Remote Administration Tools. Auf das bekannte Remote Administration Tool „DarkComet" wird in diesem Versuch näher eingegangen.

B.Sc. AI, WI
M.Sc. AI
M.Sc. EB

IT-Sicherheit

Einleitung

In diesem Versuch wird der Einsatz des Remote Administration Tools „*DarkComet*" behandelt, um das Angriffspotenzial eines Trojaner besser nachvollziehen zu können. Bei Remote Administration Tools (RAT) handelt es sich um Malware, die Client-Server-Funktionen nutzt. DarkComet und viele weitere Remote Administration Tools stellen ganze Baukästen dar, mit denen man Trojaner nach den eigenen Wünschen erstellen und aus der Ferne steuern kann.

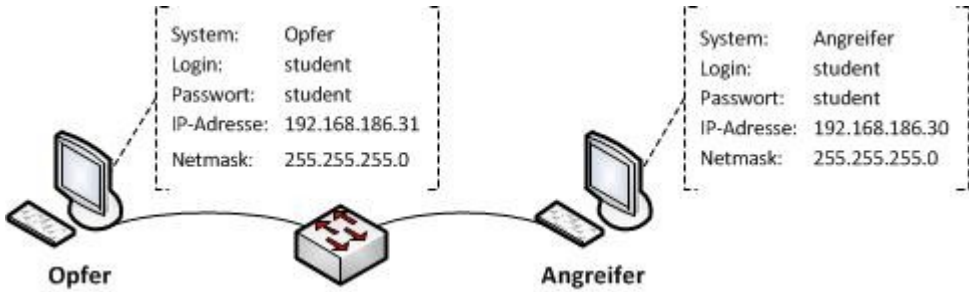
Der Versuch sieht die Infiltration eines Opfer-PCs vor, der letztlich vollständig durch den Angreifer gesteuert werden soll. Dazu werden zunächst ein DarkComet-Server und ein versteckter DarkComet-Server erstellt und auf den PC des Opfers übertragen. Nach der Infektion des PCs werden einfache Möglichkeiten der Fernsteuerung, aber auch der Einsatz eines Keyloggers demonstriert.

Da Remote Administration Tools auf Grund ihrer großen Verbreitung auch Anti-Malware-Herstellern bekannt sind und von den meisten Malware-Scannern erkannt werden, wird im folgenden Versuch auch auf eine Technik zur Verschleierung der Signaturen von Malware eingegangen.

Zugangsdaten

- Systeme: Windows XP
- Benutzername: student
- Passwort: student

Netzwerkplan



Aufgabe 1: Erstellen eines DarkComet-Server (Trojaner)

Zunächst wird ein DarkComet-Server erstellt. Gehen Sie dazu wie folgt vor.

1. Begeben Sie sich auf die VM „Angreifer".
2. Öffnen Sie den Ordner „DarkComet", der sich auf dem Desktop befindet.
3. Starten Sie die Anwendung „Client.exe"
4. Wählen Sie unter dem Reiter „Edit Server" die Option „Server module" aus und treffen Sie folgende Einstellungen:
    1. „Main Settings" können beibehalten werden
    2. Unter „Network Settings" klicken Sie neben der IP-Adresse auf den grünen Pfeil und wählen „Get LAN IP" aus.
       Merken Sie sich hier noch den Port 1604 für die spätere Analyse.
    3. Aktivieren Sie unter „Module Startup" die Funktion „Enable module server startup (fwb++).
    4. Unter „Module Shield" aktivieren Sie die Optionen „Disable Task Manager" und „Disable Registry".
    5. Im Punkt „Choose Icon" können Sie sich ein beliebiges Icon aussuchen.
    6. Begeben Sie sich nun zum Punkt „Build Module" und klicken auf die Schaltfläche „Build Server", wo Sie als Pfad den Ordner „Transfer" auf dem Desktop angeben. Geben Sie dem Trojaner nun noch einen passenden Namen.
5. Nach erfolgreichem Abschluss haben Sie Ihren ersten Trojaner erstellt.
6. Wechseln Sie auf die VM „Opfer".
7. Öffnen Sie den Ordner „Transfer Angreifer" und führen Sie über einen Rechtsklick auf die erstellte Datei eine Virensuche mit dem Programm *avast!* durch. Führen Sie die Datei jedoch noch NICHT aus, sondern löschen Sie sie nach der Malwaresuche.

a) Wird bei der Malwaresuche durch *avast!* eine Bedrohung erkannt? Falls ja, um welche Art von Bedrohung handelt es sich? Wie erklären Sie sich das Verhalten von avast!?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 2:

Erstellen Sie nun nach der folgenden Anleitung einen verborgenen DarkComet-Server.

1. Begeben Sie sich in die VM „Angreifer" und wiederholen Sie die Schritte 1-5 der Aufgabe 1.
2. WICHTIG: Bevor Sie den Trojaner im Ordner „Transfer" sichern, schließen Sie den Ordner in der VM „Opfer".
3. Nachdem sich der neue Trojaner im Ordner „Transfer" befindet, öffnen Sie das Programm „Themida" aus dem gleichnamigen Ordner.
4. INFO: Bei „Themida" handelt es sich um ein Programm, das ein Binärprogramm vor einer Dekompilierung schützen soll. „Themida" verändert durch diesen Vorgang die Signatur des Trojaners in der Art und Weise, dass es nicht mehr von allen Anti-Malware-Scannern als Trojaner erkannt wird.
5. Treffen Sie im Programm „Themida" folgende Einstellungen:
    1. Wählen Sie unter „Application Information" im Punkt „Input Filename" den erstellten Trojaner aus.
    2. Unter „Advanced Options" aktivieren Sie noch „Protect DLL plugin"
6. Nachdem die Einstellungen getroffen wurden, betätigen Sie die Schaltfläche „Protect" und klicken im neuen Fenster erneut auf „Protect".
7. WICHTIG: Klicken Sie NICHT auf die Schaltfläche „Test Protected File". Dies würde sonst zur Infektion des Angreifer-PCs führen.
8. Schließen Sie nun das Programm „Themida".
9. Begeben Sie sich nun auf den Opfer-PC und öffnen erneut den Ordner „Transfer Angreifer". Führen Sie nun erneut eine Virensuche mit avast! auf der erstellten Datei durch.

a) Erkennt *avast!* eine Bedrohung durch die erstellte Datei? Wie erklären Sie sich die Reaktion von *avast!*?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 3: Infektion des Opfers

Nun soll der PC des Opfers durch den erstellten Trojaner infiziert werden. Gehen Sie wie folgt vor.

1. Kopieren Sie den Trojaner auf den Desktop der VM „Opfer" und öffnen Sie ihn.
2. Wählen Sie ggf. beim Erscheinen eines *avast!*-Informationsfensters die Option „Normal öffnen" im Aktionsmenü aus.

   INFO: Da es sich bei dem Programm „Themida" um eine kostenlose Demoversion handelt, erscheint beim Öffnen des Trojaners zweimal ein Werbebanner, der durch einfaches Daraufklicken verschwindet.
3. Ob die Infektion erfolgreich war, überprüfen Sie über das Kommandozeilentool „netstat".

a) Interpretieren Sie die Ausgabe von „netstat". Gehen Sie dabei besonders auf den Bereich der Remoteadresse und den Status ein.

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 4: Einfache Fernsteuerung der VM „Opfer"

Nach der nun erfolgreich durchgeführten Infektion der VM „Opfer" durch den Trojaner begeben Sie sich wieder auf die VM „Angreifer".

1. Öffnen Sie wieder das Programm „Client.exe" aus dem Ordner „DarkComet" und bestätigen Sie über den Reiter „Listen" den bereits angegebenen Port.

   INFO: Beim Erscheinen einer Sicherheitswarnung durch Windows, wählen Sie „Nicht mehr blocken" aus.
2. In der Liste der infizierten PCs müsste nach wenigen Sekunden ein Eintrag über die VM „Opfer" erscheinen, der die grundlegenden Systeminformationen anzeigt.
3. Öffnen Sie die Fernsteuerung durch einen Doppelklick auf den PC-Eintrag.
4. Eine einfache Demonstration der Fernsteuerung ist unter der Option „Fun Funktions" im Punkt „Fun Manager" anzutreffen.
5. Klicken Sie unter diesem Punkt auf die Schaltfläche „Hide Clock".
6. Wechseln Sie zur VM „Opfer" und überprüfen Sie, ob die Uhr noch sichtbar ist.
7. Aktivieren Sie die Uhr nun wieder.

Aufgabe 5: Erweiterte Fernsteuerung der VM „Opfer"

1. Begeben Sie sich in der Fernsteuerungskonsole zu dem Menüpunkt „System Functions" und rufen Sie die Option „Remote Shell" auf.
2. Wechseln Sie sich nun in das Verzeichnis C:\WINDOWS\system32\drivers\etc

a) Welche Aufgabe hat die Datei „hosts" in diesem Verzeichnis?

.....

.....

.....

.....

b) Führen Sie nun im aktuellen Verzeichnis den folgenden Befehl aus:
echo 192.168.186.30 www.google.de >> hosts

Was könnte durch diesen Befehl in der VM „Opfer" erreicht werden?

.....

.....

.....

.....

c) Überprüfen Sie über den Menüpunkt „Hosts File" und durch das Klicken auf die Schaltfläche „Get hosts content", ob der Befehl erfolgreich angewandt wurde.
HINWEIS: Die Schaltfläche „Update hosts file" funktioniert in dieser „DarkComet Version" nicht wie gewünscht, sondern löscht stattdessen den gesamten Inhalt der Datei.

Aufgabe 6: Keylogger

1. Begeben Sie sich in der Fernsteuerungskonsole zum Menüpunkt „Spy Functions" und wählen Sie die Funktion Keylogger aus.
2. In dem geöffneten Fenster klicken Sie auf die Schaltfläche „Active Keylogger" und „Online Keylogging".

a) Erklären Sie die Aufgabe eines Keyloggers.

.....

.....

.....

.....

.....

.....

b) Begeben Sie sich in die VM „Opfer" und öffnen Sie den Windows Editor. Schreiben Sie einen beliebigen Satz in das Editorfenster. Begeben Sie sich danach wieder zurück auf die VM „Angreifer" und überprüfen Sie die Ausgabe im Keyloggerfenster.

c) Stimmt die Ausgabe mit Ihrer Editor-Eingabe überein?

.....

.....

.....

.....

d) Welche Informationen erhalten Sie zusätzlich vom Keylogger?

.....

.....

.....

.....

Aufgabe 7: Trojaner entfernen

1. Begeben Sie sich in die VM „Opfer".
2. Der Trojaner wurde von Ihnen so konfiguriert, dass er bei jedem Neustart erneut aktiv wird.
3. Machen Sie einen Rechtsklick auf die Taskleiste.

a) Was fällt Ihnen auf?

.....

.....

.....

.....

4. Geben Sie nun den Befehl „regedit" unter „Start-> Ausführen" ein, um die Registry zu öffnen und um den Autostart des Trojaners zu entfernen.

b) Was fällt Ihnen dabei auf? (Hinweis: Sie arbeiten mit administrativen Rechten).

.....

.....

.....

.....

5. Öffnen Sie nun das Programm „autoruns" im gleichnamigen Ordner, der sich auf dem Desktop befindet.
6. Unter dem Reiter „Everything" finden Sie den merkwürdigen Eintrag „C:\\Windupdt\winupdate.exe" eines Windows-Updatesystems, dass sich direkt unter C: befinden soll.
7. Führen Sie einen Rechtsklick auf den Eintrag durch und wählen Sie „Delete" aus.
8. Sie haben nun den Autostart des Trojaners erfolgreich gelöscht.
9. Um nun auch die unter Punkt 3 und 4 erkannten Probleme zu beheben, steht das Programm „Malwarebytes" zur Verfügung, das sich auf dem Desktop befindet. Öffnen Sie das Programm und bestätigen die „Testphase starten".
10. Führen Sie einen „Quick-Scan" durch, indem Sie auf die Schaltfläche „Scannen" klicken.
11. Es werden nun die Veränderungen der Registry aufgelistet.

c) Wird die Datei „C:\\Windupdt\winupdate.exe" von „Malwarebytes" erkannt?

……

……

……

……

12. Betätigen Sie nun die Schaltfläche „Entferne Auswahl", um die gefundenen Probleme zu beseitigen.
13. Führen Sie anschließend einen Neustart durch.

d) Können Sie nach dem Neustart den „Task-Manager" und die Registry aufrufen?

……

……

……

e) Ist der Trojaner-Eintrag unter „netstat" noch enthalten?

……

……

……