Malware: intelligente Schadsoftware als virtueller Trickbetrüger

Allgemeines

Das klassische Virus, das noch vor Jahren Bootsektoren infizierte und sich schneller ausbreitete als der Fortpflanzungszyklus von Ratten, ist kaum noch von Bedeutung. Intelligente Schadsoftware, die für kriminelle Zwecke entwickelt wird, um das wirtschaftliche Potential von vernetzten Computern auszunutzen, hat nicht zuletzt wegen der Naivität und Nachlässigkeit der Anwender erhebliche Erfolge zu verzeichnen. Internetwürmer wie **Blaster** und **Sasser** nutzten vor einigen Jahren eine Schwachstelle im Betriebssystem Windows aus, die sog. **DCOM**- Schnittstelle. Während diese Gesellen für erhebliches Aufsehen sorgten, weil sie sich rasend schnell über Netzwerkverbindungen verbreiten und wiederum die Nachlässigkeit der User ausnutzen konnten, weil diese in großer Anzahl die Notwendigkeit von Updates anscheinend nicht erkennen wollten, war ihr Schadpotential hingegen verhältnismäßig gering. Sehr eindrucksvoll wurde ein Shutdown ausgelöst, der innerhalb von vorgegebenen 60 Sekunden das System unweigerlich zur Abschaltung zwang. Viel heimtückischer gehen die sog. **Trojaner** vor. Der Name wurde treffend aus der griechischen Mythologie übernommen, weil diese Schadprogramme sich in manigfaltigerweise tarnen, um ihre Entdeckung möglichst lange hinauszuzögern. Wie auch schon bei Odysseus und seinen Gefährten ist das **Trojanische Pferd** auch erst der Anfang vom Ende. Kann sich das kleine Programm erfolgreich auf dem System einnisten, versucht es weiteren Schadcode aus dem Internet nachzuladen. Haben diese Aktivitäten erst einmal begonnen, ist es nahezu unmöglich, die Schädlinge in ihrer Gesamtheit guten Gewissens zu entfernen. **Backdoor**- Programme versuchen den Datenfluß an eingesetzter Security Software unbemerkt vorbeizuschleusen. **Keylogger** protokollieren die Tastatureingaben, um an Passwörter oder andere sensible Daten heranzukommen und andere Routinen sorgen dafür, daß Firewalls und Antivirenprogramme zu gefügigen Placebos gezähmt werden. Eigene **SMTP- Engines** (Simple Mail Tranfer Protocol) sorgen dafür, dass vom infizierten System SPAM- Mails in alle Welt versendet werden oder der **Cracker** (wenn man diese Bezeichnung akzeptieren kann) übernimmt gleich die Kontrolle über den PC. Der Phantasie sind quasi keine Grenzen gesetzt und der so gekaperte PC ist zu einer Zombie- Maschine mutiert. Dann gäbe es da noch die nervigen **Browser Hijacker**, die dem Internetsurfer die Auswahl seiner Ziele abnimmt und gleich auch gerne eine neue Startseite bestimmt und dann noch die gerne als harmlos eingestufte **Adware**, die in regelmäßigen Abständen Werbeeinblendungen generiert. Allesamt werden diese lästigen virtuellen Zeitgenossen auch schon mal als **Spyware** bezeichnet, weil eine Eigenschaft dieser Programme es ist, Daten des Users auszuspionieren und an entsprechende Stellen zu versenden.

Wie kommt Malware auf den Computer ?

Ideenreichtum ist für Trickbetrüger ein hilfreiches Werkzeug, um ihr Ziel zu verfolgen. In der virtuellen Welt ist das nicht anders. Ausschlaggebend ist jedoch immer das Verhalten der Opfer. Unachtsamkeit, Leichtgläubigkeit, Nachlässigkeit, Neugier und Naivität sind nur einige Zutaten, die den Erfolg von Malware täglich aufs Neue garantieren. Darüber wurde schon ausreichend geschrieben, diskutiert und philosophiert - und deshalb möchte ich die Sache aus einer anderen Perspektive beleuchten. Das Öffnen von virusbehafteten Emailanhängen könnte man inzwischen als alten Hut bezeichnen, aber immer wieder fallen Leute darauf herein. Dennoch sehe ich die Hauptursache für Malwarebefall an anderer Stelle. Präparierte Websites führen Schadcode direkt aus, sobald man die entsprechende Website mit dem Browser öffnet. Besteht ein lückenhaftes Sicherheitskonzept, ist eine Infizierung beinahe garantiert. Auch hierüber gibt es unzählige Grundsatzdiskussionen, die gerne in sog. Glaubenskriegen gipfeln. Das habe ich aber bereits in meiner Abhandlung **Sinn und Unsinn von Personalfirewalls** abgehandelt und möchte mich daher nicht wiederholen. In einschlägigen Foren findet man täglich Hilferufe von Usern, die sich einen Virus bzw. eine Malware "eingefangen" haben. Nur ganz selten wird dabei der Weg der Infektion dargestellt, in der Regel geht es dann nur noch um die Rettung der Daten und das Entfernen des Schädlings vom System. Daß so wenig über die Herkunft der Malware berichtet wird, hat einen interessenten Grund, wie ich denke: Der User hat es selbst bewußt verschuldet und möchte nun ungern seine Dummheit eingestehen. Damit meine ich, der User hat sich eine unseriöse Software aus dem Internet gedownloadet und installiert, ein vermeintlich kostenloses Angebot wahrgenommen, schmuddelige Internetseiten besucht oder mit Hilfe eines sog. **Crack**- Programmes die legale Nutzung einer kostenpflichtigen Software umgehen wollen. Oft glauben die Anwender, daß sie durch Installation von Security Software und der eigenen Selbstüberschätzung den Schritt auf gefährliches Terrain unbeschadet wagen könnten. Das ist leichtsinnig bis fahrlässig und auf jeden Fall dumm! Da ich nun mal kein Freund von theoretischem Geplänkel und spekulativen geistigen Ergüssen bin, habe ich einen Test durchgeführt, der mich selbst wieder überraschen konnte.

Der Test

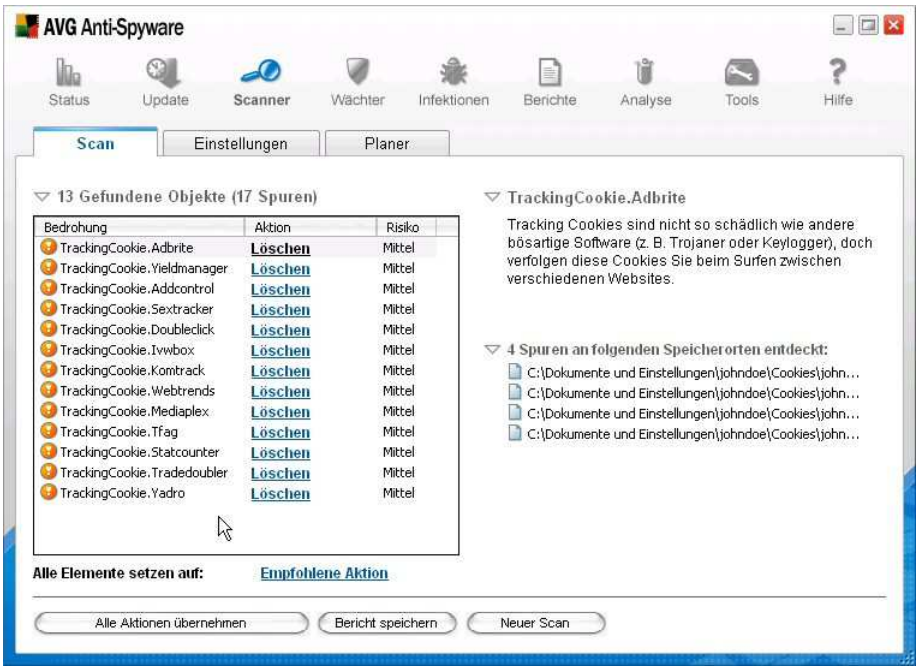
Ich habe also wieder einen Testrechner vorbereitet und Windows XP SP2 installiert. Aktueller Patchlevel versteht sich von selbst und eher zufällig folgende Security- Produkte installiert: **AVG- Antimalware Free**, **AdAware SE** und die Trial- Version von **Norton Internet Security 2008**. Alle Programme habe ich auf den aktuellen Updatestand gebracht und wie sooft üblich mit "administrativem Benutzerkonto" den Versuch gestartet. Ich denke, daß genau so, viele Anwender im Glauben einer scheinbaren Sicherheit und mit viel Selbstvertrauen bewußt gefährliches Internet- Territorium beschreiten...

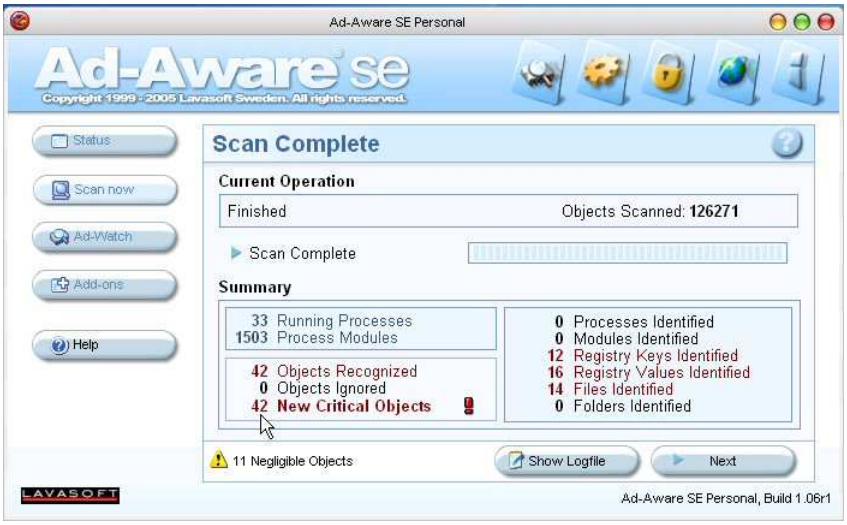
Natürlich braucht man eine Zielvorgabe. Ich habe hierfür aus dem Bauch raus die Software **StyleXP** ausgewählt, die unter vielen Usern Beliebheit genießt, weil man damit sehr komfortabel das Outfit von Windows verändern kann. Nun ist der kostenlose Download selbst zwar völlig harmlos und auch das Installieren der Software sollte in der Regel keine sicherheitsrelevanten Probleme bereiten, doch manche User möchten natürlich auch die Vorzüge der Vollversion nutzen können. Warum kaufen, wenn's doch einen Crack dafür im Internet gibt, denken nicht wenige und das Schicksal nimmt seinen Lauf, wenn der User nun diesen Weg beschreitet...

Es ist nicht schwer, per Suchmaschine Internetpräsenzen zu finden, die derartige **Cracks** anbieten. Diese Internetseiten besitzen dann wiederum eigene Suchmechanismen, die den User zum gewünschten **Crack** führen sollen. Bereits dieser Weg ist gepflastert mit Schadcode, der nur darauf lauert, vom User aufgesammelt und aktiviert zu werden. In der (trügerischen) Gewissheit mit aktueller und leistungsfähiger **Security Suite** allen Gefahren auf diesem virtuellen Minenfeld trotzen zu können, wird schon mal den Anweisungen der Crackanbieter Folge geleistet, denn man will ja schließlich auch den gewünschten **Crack** bekommen. Also mache ich das genauso und klicke mehrfach auf "OK" und manchmal auch auf "Fenster schließen", wenn mir zwischen "nackten Tatsachen" (wörtlich gemeint) und Online- Casinos das Umfeld zu "bunt" und unübersichtlich wird. Schließlich möchte man ja nur schnell den gewünschten **Crack** downloaden und wieder verschwinden. Merkwürdigerweise beschert jedes geschlossene bunte Fenster mindestens 2 neue und manche lassen sich gar nicht schließen. Auch wird man aufgefordert, Dinge zu installieren, die angeblich notwendig sind, damit man diesen **Crack** downloaden kann und darf. Was soll's, die **Security Suite** wird schon aufpassen, daß nichts ernstes passiert, also wird kurzerhand trotz Browserwarnung (übrigens wurde **Internet Explorer 7** verwendet) das **ActiveX- Control** installiert**.** Schließlich funktioniert auch der Download des ersehnten **Cracks** mit einigen Umwegen und man kann endlich den PC herunterfahren, um wieder geordnete Verhältnisse herzustellen, denn manche Fenster sind sehr hartnäckig und lassen sich einfach nicht schließen. Nach einem erfrischendem Reboot wird natürlich der **Crack** ausprobiert. Es handelt sich dabei um einen **Key- Generator**, der einen Aktivierungscode der Originalsoftware bereit stellt. Dabei läuft eine verhältnismäßig lang dauerende Prozedur ab, wobei auch kurz mal eine DOS- Box auftaucht, aber so schnell wieder verschwindet, daß man nicht erkennen konnte, was da geschehen ist. Ernüchternd ist das Ergebnis - der Key funktioniert nicht...

Die Analyse

Obwohl dieser Test und die Vorgehensweise sehr individuell war, denke ich, daß es dennoch repräsentativ sein könnte. Jetzt sind die Sicherheitstools an der Reihe, die ja während meines Onlineaufenthaltes so ausgesprochen wenig Präsenz gezeigt hatten. Die Malwaretools von AVG und Lavasoft sind sowieso nicht als Hintergrundprozess aktiv und können daher auch nichts bewirken. Sie dienen lediglich der nachträglichen Räumung des "Minenfeldes". **NIS2008** hatte sich ebenfalls sehr zurückhaltend gezeigt, ist aber angeblich ein gewünschtes Feature, damit der User nicht ständig mit unverständlichen Bestätigungs- Popups genervt werden soll. In etwa gleichzeitig startete ich alle Tools und ließ sie ihr Tagewerk vollbringen. Das sind die Ergebnisse:





Die Ergebnisse sind eher ernüchternd und gerade von **NIS2008** hätte ich mehr erwartet. Soll das nun doch nicht so schlimm gewesen sein ? Jedoch hat sich schon was getan und in der Taskbar macht dieses "Etwas" sehr unruhig auf sich aufmerksam:

Ein weises Kreuz auf rotem Grund blinkt hektisch und wartet darauf, daß der User nachsieht, was es damit auf sich hat. Jetzt bin ich doch mal gespannt, was passiert, wenn ich dort den schnellen Klickfinger ran lasse...

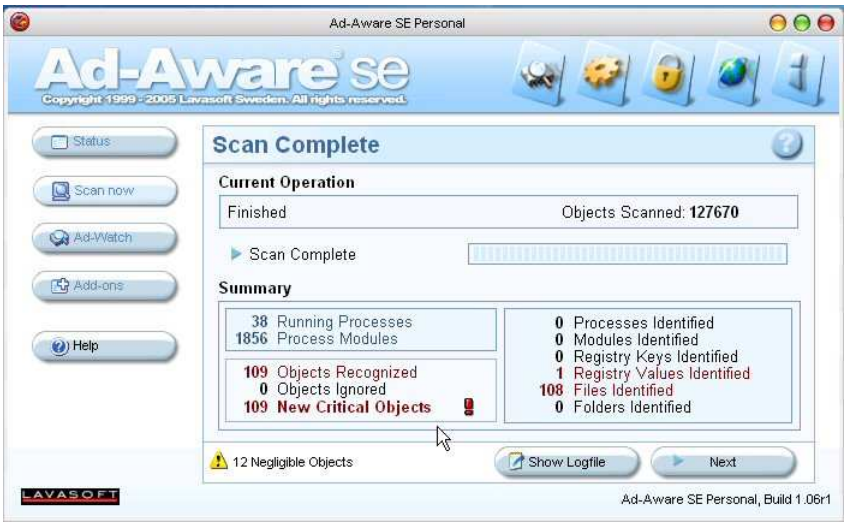
Nebenbei meldet sich nun auch noch ein besorgniserregendes Fenster:

Jetzt wird's doch noch interessant ! Eine Bestätigung über den Button "Ja" ist für einen erschrockenen User in der Regel eine Pflichtaufgabe...

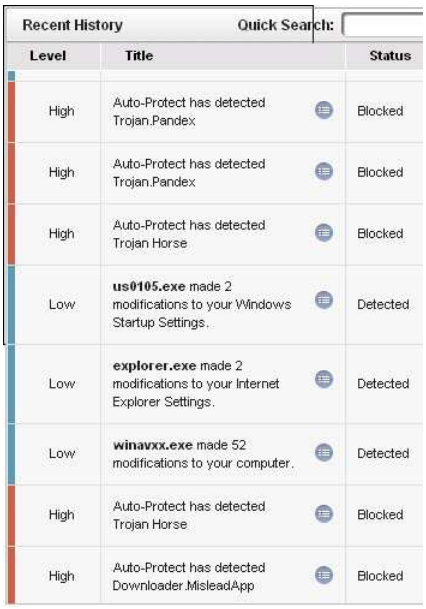
Sowas wie "Spyware Defender" hat sich installiert und bietet dem User nun seine Dienste an und ständig neue Meldungen irritieren nun die Person vor dem Bildschirm:

Wenn man schon so aufgefordert wird, um das System zu überprüfen und die anderen Tools nicht gerade überzeugen konnten, dann läßt man auch schon mal andere Tools ran. "In der Not frißt der Teufel Fliegen" - In vielen Fällen ist der User auch noch so leichtgläubig, daß er annimmt, diese Tools können doch gar nicht böse sein, weil sie ja Spyware aufspüren wollen. Das kann ein fataler Fehler sein, wie sich noch herausstellen wird...

Die Löschung der entdeckten Schädlinge durch die eingesetzten seriösen Tools war übrigens nicht sonderlich erfolgreich:



Im Gegenteil - AdAware meldet nun mehr als doppelt soviele "Objekte" und zwischen den Neustarts lag maximal eine halbe Stunde. Auch **NIS2008** wird langsam wach und meldet ständig was. Jetzt lohnt sich ein Blick in die "History":



NIS 2008 blockt nun einige üble Dinger, die versuchen, Schadcode aus dem Internet nachzuladen. Das ist jedoch keineswegs ein Grund zur Beruhigung. Erinnern wir uns etwa eine halbe Stunde zurück: da hat **NIS2008** sich nicht geregt, obwohl offensichtlich bereits das Übel seinen Gang nahm. Die Antimalwaretools von **AVG** und insbesondere **AdAware** belegen hachhaltig, daß eine Infizierung stattgefunden hat, wo **NIS2008** gerademal ein **Cookie** beanstandete. Jetzt mag es wieder so aussehen, daß ich gegen Symantec- Produkte ins Feld ziehe. Es war reiner Zufall, daß ich **NIS2008** für den Test eingesetzt hatte, weil ich die Trial- Version noch gerade auf dem USB- Stick als Installations- Setupprogramm hatte. Ich kann daher auch nicht beurteilen, wie andere Security Suiten sich in diesem Test verhalten hätten und das ist auch weniger die Intension. Dieser Test hat mir bewiesen, daß eine Malwareinfektion allein durch die Präsenz einer oder mehrerer Sicherheitssoftwares nicht verhindert werden kann. Selbst wenn nun **NIS2008** aktiv das Nachladen weiteren Schadcodes verhindert, ist es durchaus möglich, dass andere Komponenten unbehelligt die Firewall von **NIS2008** umgehen. Das ist leider nicht eindeutig nachvollziehbar gewesen, aber ganz sicher zu vermuten, da **AdAware** ja ständig neue Infektionen erkennt, obwohl jedesmal "alles" gelöscht wurde.

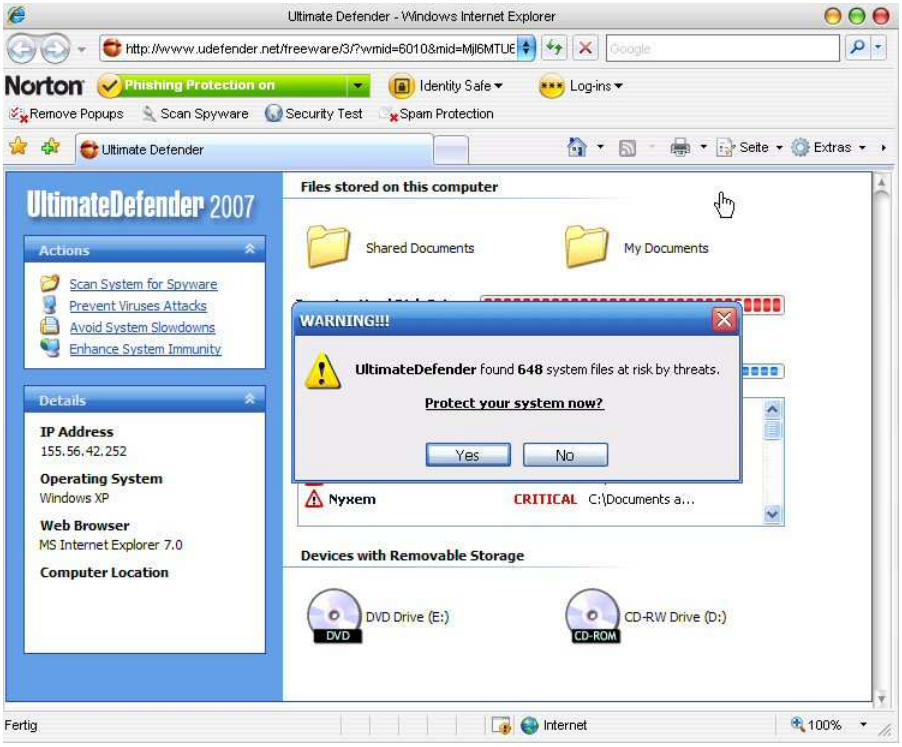
Daß die sich selbst installierte angebliche Antimalwaresoftware mit dem markanten Namen **Spyware Defender** (nicht zu Verwechseln mit seriösen Produkten von Microsoft oder anderen Herstellern) anschickt, sich selbst zu updaten und dafür die Inanspruchnahme des Users einfordert, ist lediglich eine weitere Alternative, um dadurch die eigentliche Schutzsoftware auszuhebeln. Denn der User als oberste Instanz kann ja bestimmen, was sein darf und was nicht. So ist es auch nicht verwunderlich (für einen Laien wohl eher doch), daß nun das Windowssystem ein merkwürdiges Verhalten an den Tag legt. Dabei ist die rapide gesunkene Performance noch das geringste Übel. Beim Versuch, Hilfe per Online- Virenscan (www.virustotal.com) anzufordern, wird dies einfach durch **Browser Hijacking** geblockt. Statt der angeforderten Internetpräsenz zeigt sich folgendes:

Für gänzlich unerfahrene User, die womöglich in Internetforen von hilfsbereiten Experten, den Rat erhalten haben, einen solchen Onlinescan durchzuführen, dürfte das zur absoluten Kompromittierung führen. Wer nun dieser Aufforderung Folge leistet, gerät immer tiefer in den Sumpf der Malware. Übrigens war es auch nicht mehr möglich, eine **HiJackThis**- Auswertung zu versuchen. Der Grund dafür ist eine Manipulation der **Hosts** - Datei gewesen, die jegliche Internetpräsenz von seriösen Security- Anbietern nicht mehr akzeptierte. Die **AdAware**- Auswertung zeigt es auf:

Stattdes werden andere, sehr fragwürdige Angebote offeriert:

Ganz sicher ist das alles andere als "sicher". Versuchen kann man's ja, es gibt immer wieder welche, die darauf reinfallen. Jedenfalls wurde jede Anfrage auf Seiten von Herstellern von Sicherheitssoftware u.ä. in etwa so quittiert:

Wenn ich nun schon mein Testsystem bis zum Anschlag verseucht habe, dann möchte ich jetzt auch noch sehen, was dieser Download zu bieten hat:



Mit falschen Vorgaben von Inhalten der angeblich eigenen Systemumgebung wird der User aufgefordert: **Protect your system now !** Was bitte gibt es denn jetzt noch zu schützen ?

Solche Dinge laufen nun ständig automatisch ab. Die Buttons "Weiter >" und "Abbrechen" sind völlig überflüssig, weil das gesamte Fenster einen riesigen Button darstellt. Das ist also wiederum nur eine Falle...

Solche Meldungen sind spätestens seit der letzten Stunde fest ins Regelwerk eingebunden. Nicht einmal 2 Stunden hat es insgesamt gedauert, um das Windows- System fast völlig zum Erliegen zu bringen. Sogar die **Systemsteuerung** von Windows wurde aus der Programmauswahl entfernt und der Taskmanager wurde deaktiviert. Das System ist in fremder Hand und nicht mehr kontrollierbar. Sehr eindrucksvoll konnte mir anhand dieses Tests bestätigt werden, daß eine Verseuchung eines Systems trotz moderner Security Software problemlos möglich ist. Im parallel bestehenden Forum zu diesem Thema darf man gerne die eigenen Erfahrungen mitteilen oder Fragen dazu stellen. Vielleicht hat auch jemand ähnliche Screenshots zur Analyse gemacht: **www.ayin.at/firewall**

Weiterführende Erklärungen zu Malware: Wikipedia

Anmerkung: Es ist nicht ratsam, besonders für Laien, diesen oder ähnliche Tests nachzuvollziehen oder die hier sichtbaren Internetpräsenzen mit einem Produktivsystem ergründen zu wollen. Für Schäden, die daraus entstehen, ist jeder selbst verantwortlich!


OBERTHAL-ONLINE