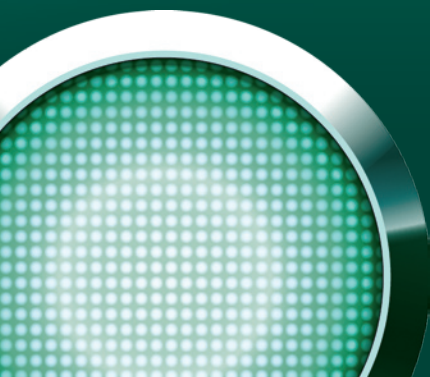




W H I T E P A P E R

**Methoden zum Schutz
vertraulicher Informationen
in aktuellen
Security-Suiten**



Die Website der US Federal Trade Commission über Identity Theft beschreibt ausführlich die verschiedenen Aspekte des Diebstahls vertraulicher Informationen (www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html). Es geht hier um eine Vielzahl traditioneller Arten des Diebstahls vertraulicher Informationen, der nicht mit Hilfe von Computern organisiert wird, unter anderem um Hand- und Brieftaschendiebstahl, um die Suche nach Papierschnipseln im Abfall, um Anrufe im Namen von Finanzorganisationen, um den Einsatz spezieller Geräte zum Lesen von Kreditkartennummern und weiteres mehr.

Neben den oben aufgezählten Methoden des Informationsdiebstahls existieren allerdings auch solche, die unter Verwendung von PCs umgesetzt werden, wobei mindestens drei verschiedene Arten zu unterscheiden sind. Im ersten Fall übermittelt der Anwender selbst den Kriminellen die Informationen, nachdem er einer gefälschten Aufforderung zur Eingabe der entsprechenden Daten gefolgt ist, welche üblicherweise als Spam per E-Mail verbreitet wird. Die Kriminellen erstellen dabei eine Website, die von der Site einer tatsächlich existierenden Bank oder einer anderen Finanzorganisation kaum zu unterscheiden ist. Diese Art von Online-Verbrechen wird *Phishing* genannt.

Die zweite Methode des Diebstahls vertraulicher Informationen basiert auf der Beobachtung der Aktivitäten des Anwenders und deren anschließender Protokollierung. Diese Art der E-Spionage wird mit Hilfe spezieller trojanischer Programme realisiert, die entsprechend der Klassifizierung von Kaspersky Lab als *Trojan-Spies* bezeichnet werden. Zu den populärsten Vertretern der Kategorie *Trojan-Spies* gehören die *Keylogger* (Tastaturspione), die in einem gesonderten Whitepaper bereits ausführlich beschrieben werden.

Eine dritte Möglichkeit, Informationen zu stehlen, besteht in der Suche nach vertraulichen Daten auf dem Computer des Anwenders und der anschließenden Weiterleitung an die Kriminellen mit Hilfe von schädlichen Programmen (in den meisten Fällen Trojanern). Bei dieser Methode können die Kriminellen ausschließlich in den Besitz solcher Daten gelangen, die der Anwender im Speicher des Computers abgelegt hat. Dieser „Nachteil“ wird allerdings durch den Umstand wieder wettgemacht, dass bei der Übermittlung der vertraulichen Informationen eine Beteiligung des Anwenders nicht notwendig ist. Entsprechend der Klassifizierung von Kaspersky Lab gehören derartige Schadprogramme zur Familie *Trojan-PSW*.

Zur Verbreitung derartiger Programme existiert eine Vielzahl von Möglichkeiten: Sie können beim Öffnen einer an eine E-Mail angehängte Datei aktiviert werden, beim Klicken auf einen Link innerhalb einer Instant Message oder beim Öffnen einer Datei aus einem Verzeichnis mit allgemeinen Zugriffsrechten innerhalb eines

Peer-to-Peer-Netzes. Auch mit Hilfe eines Scripts, das Besonderheiten von Internet-Browsern ausnutzt, die es Programmen ermöglichen, sich bei Besuch der entsprechenden Seiten automatisch selbst zu starten oder mit Hilfe von vorher installierten schädlichen Programmen, die in der Lage sind, andere Schadprogramme aufs System zu laden und dort zu installieren, verbreiten sich Trojaner.

Das eigentliche Ziel von Schadprogrammen des Typs *Trojan-PSW* besteht darin, so viele Informationen wie möglich über das System des Anwenders sowie Passwörter für verschiedene Programme und Dienste des Betriebssystems zusammenzutragen. Zu diesem Zweck durchsuchen sie sämtliche Speicherplätze nach derartigen Informationen: Den geschützten Speicher von Windows, Registry-Schlüssel und bestimmte, für die Kriminellen interessante Programmdateien (üblicherweise sind das Instant-Messenger-Clients, E-Mail-Clients und Internetbrowser).

Wurden die gewünschten Informationen an den beschriebenen Orten gefunden, werden sie von dem trojanischen Programm in der Regel verschlüsselt und in einer binären Datei von geringer Größe komprimiert. Daraufhin kann die entsprechende Datei per E-Mail versendet oder auf einem FTP-Server der Kriminellen abgelegt werden.

Die Funktionsprinzipien der oben beschriebenen Typen von Schadprogrammen werden in der Analyse „Eigentumsdiebstahl von Computernetzen“ detailliert beschrieben. Im vorliegenden Whitepaper hingegen richtet sich das Augenmerk auf zwei unterschiedliche, in aktuellen Sicherheitssystemen umgesetzte Ansätze zum Schutz vertraulicher Daten.

Aufbau der Komponente zum Schutz vertraulicher Daten in der Mehrzahl der derzeit erhältlichen Produkte

Nahezu alle aktuellen Security-Suiten enthalten eine Komponente zum Schutz vertraulicher Informationen, die üblicherweise Privacy Control genannt wird. Es sei angemerkt, dass diese Komponente in einigen Anwendungen unter einer allgemeinen Bezeichnung mit anderen Schutzkomponenten, wie etwa dem Schutz vor Phishing zusammengefasst ist. Die Hauptaufgabe dieser Komponente besteht im Schutz der vertraulichen Daten auf dem Computer des Anwenders vor unberechtigtem Zugriff und vor Weiterleitung über Datenübertragungskanaäle.

An dieser Stelle soll der Schutz vertraulicher Informationen am Beispiel der Produkte der Firma Symantec näher untersucht werden. Es wurde speziell dieses Unternehmen ausgewählt, weil es als erstes eine Komponente zum Schutz vertraulicher Informationen in seine Produkte integrierte, woraufhin die gesamte Branche begann, analoge Komponenten einzuführen.

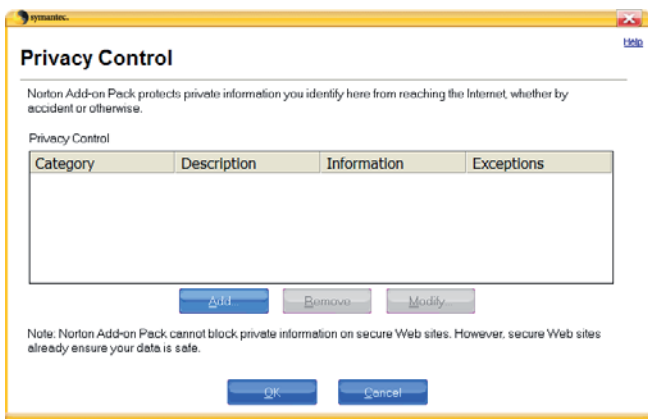
Bereits Ende 1999 veröffentlichte Symantec Informationen über das neue Produkt Norton Internet Security 2000 mit der neu integrierten Privacy-Control-Komponente. Deren Hauptbestandteil ist das Modul zum Schutz vertraulicher Informationen, das Confidential Data Blocking. Diese Komponente funktioniert nach dem folgenden Prinzip:

- ▶ Der Anwender gibt alle Informationen ein, die er für vertraulich hält.
- ▶ Das Produkt analysiert daraufhin den vom Computer des Anwenders ausgehenden Netz-Traffic und schneidet alle im Traffic enthaltenen vertraulichen Daten aus oder ersetzt diese durch bedeutungslose Zeichen, zum Beispiel Sternchen.



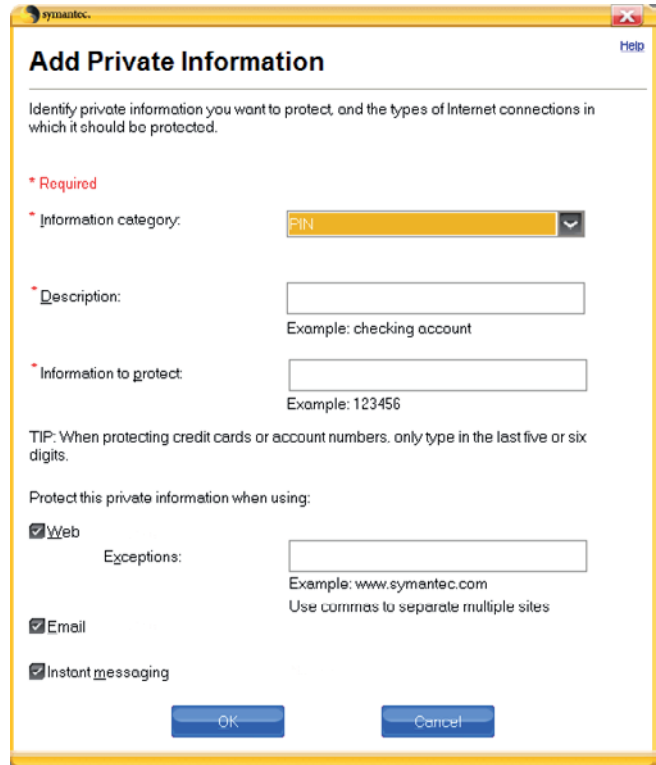
Setup der Privacy-Control-Komponente in Norton Internet Security

Norton Privacy Control wurde in alle neuen Versionen der Produkte Norton Personal Firewall und Norton Internet Security integriert. Im 2007 erschienenen Produkt Norton 360 ist die Komponente Privacy Control zwar nicht mehr in der Grundausstattung enthalten, sie kann jedoch als Add-on-Pack von der Symantec-Webseite heruntergeladen werden.



Privacy-Control-Komponente im Produkt Norton 360

Das grundlegende Funktionsprinzip der Komponente hat sich allerdings nicht geändert: Auch hier gibt es eine Tabelle, in die der Anwender seine vertraulichen Daten einträgt.



Auch in Norton 360 muss der Benutzer die zu schützenden Daten selber eintragen

Unzulänglichkeiten der traditionellen Verfahren zum Schutz vertraulicher Informationen

Was hat die Autoren des Programms dazu bewogen, die Komponente zum Schutz vertraulicher Daten aus der Grundausstattung von Norton 360 herauszunehmen? Vermutlich gibt es dafür verschiedene Gründe, einer allerdings liegt auf der Hand. Dieser Ansatz zum Schutz vertraulicher Daten ist nämlich ineffektiv, er erzeugt beim Anwender nur eine Illusion von Sicherheit!

In der Feature-Liste von Norton Internet Security 2007 fand sich weit oben der Punkt „blockiert Versuche, persönliche Daten zu stehlen“. Das allerdings entspricht nicht der Realität.

Sieht man sich das Fenster links unten einmal genauer an, so entdeckt man im unteren Teil eine Anmerkung, die in der deutschen Übersetzung etwas wie folgt lautet: „Das Norton Add-on-Pack kann keine vertraulichen Informationen auf sicheren Websites blockieren. Sichere Websites garantieren allerdings schon an sich, dass Ihre Daten geschützt sind.“ Der Grund für diese Anmerkung ist leicht verständlich, denn der Austausch mit sicheren Websites läuft über ein Protokoll, in dem alle übermittelten Daten verschlüsselt werden. Ein Dritter hat so nicht die Möglichkeit, den übertragenen Datenstrom zu analysieren – auch kein Security-Produkt.

An dieser Stelle sollte man sich noch einmal vor Augen führen, wovon die Komponente zum Schutz vertraulicher Daten eigentlich schützen soll, nämlich vor trojanischen Programmen des Typs *Trojan-PSW*. Was sollte nun diese trojanischen Programme daran hindern, ihrerseits die übermittelten Daten zu verschlüsseln? Rein gar nichts, wie man weiß, denn über 80 Prozent aller Trojaner tun genau das. Daher ist eine Komponente zum Schutz vertraulicher Informationen, deren Funktion auf der Analyse des Traffics und der Suche vorher eingegebener Anwenderdaten basiert, in den meisten Fällen nicht in der Lage, das Versenden dieser Daten zu verhindern, da sie diese im verschlüsselten, von einem trojanischen Programm übertragenen Datenstrom ganz einfach nicht findet.

In diesem Zusammenhang sei außerdem darauf hingewiesen, dass die Verwahrung sämtlicher vertraulichen Daten an einem einzigen Ort – nach deren Eingabe in einem Fenster – schon für sich gesehen das Sicherheitsniveau keineswegs erhöht. Ganz im Gegenteil, denn die Kriminellen sind nun nicht mehr gezwungen, verschiedene Orte des Dateisystems zu durchsuchen, sondern benötigen lediglich Zugriff auf die von der Schutzkomponente verwendete Datei. Zweifellos sind die Autoren dieses Schutzprogramms bemüht, die vom Anwender eingegebenen Daten bestmöglich zu schützen, eine Sicherheitsgarantie ist hier aber keinesfalls gegeben.

In der folgenden Situation ist die Komponente voll funktionstüchtig: Wird der Anwender auf einer Website zur Eingabe seiner Telefonnummer aufgefordert, fragt Norton Internet Security ihn – nachdem er die Nummer eingegeben hat –, ob er tatsächlich persönliche Daten versenden will.

Allerdings ist ein solcher Warnhinweis im wahren Leben nicht unbedingt hilfreich, denn die Entscheidung des Anwenders darüber, ob er die geforderten Daten eingibt oder nicht, ist in erster Linie davon abhängig, wie vertrauenerweckend ihm die jeweilige Website erscheint. Hält der Anwender die Website für echt, so wird ihn der Warnhinweis des Programms nicht abhalten, die entsprechenden Daten einzugeben. Hält der Anwender die Website aber für gefälscht, so wird er gar nicht erst beginnen, irgendwelche Daten einzugeben. In der letzten Zeit gibt es unglücklicherweise immer mehr von Kriminellen erstellte Websites, die kaum mehr von den Original-Sites verschiedener Finanzinstitute zu unterscheiden sind, und viele Anwender geben dort ihre vertraulichen Daten ein – ungeachtet der Warnhinweise von Schutzprogrammen.

Alternativer Ansatz zum Schutz vertraulicher Daten

Es existiert noch ein anderer Ansatz zum Schutz vertraulicher Daten, der auf der Blockierung der Aktivitäten von Schadprogrammen in einem früheren Stadium als der Übertragung von Daten über Verbindungskanäle

basiert. Denn dann lässt sich, wie oben aufgezeigt wurde, meist kaum noch etwas ausrichten.

Ein Schadprogramm muss zwei Aktionen ausführen, um in den Besitz vertraulicher Daten zu gelangen: Zunächst müssen die entsprechenden Informationen gefunden und aus dem jeweiligen Speicher gezogen werden (dabei kann es sich um eine Datei, einen Registry-Schlüssel oder einen speziellen Speicher des Betriebssystems handeln), um daraufhin an den Autor des Schadprogramms über Verbindungskanäle übermittelt zu werden. Dabei ist es dem Schadprogramm nicht möglich, die ausgewählten Daten in eigenem Namen zu übertragen, da auf vielen Computern bereits Firewalls installiert sind, die die Netzaktivität der installierten Anwendungen kontrollieren. Daher verwenden viele trojanische Programme der Klasse *Trojan-PSW* unterschiedliche Methoden zur Umgehung des Firewall-Schutzes und zur Versendung von Daten im für den Anwender verborgenen Modus.

Daher erscheint der folgende Ansatz durchaus sinnvoll: Die Schutzkomponente sollte genau die Aktivität der Anwendungen verfolgen, die auf einen möglichen Versuch, vertrauliche Informationen zu stehlen, hinweisen könnte:

- **Der Versuch, Zugriff auf die im geschützten Speicher (Protected Storage) von Windows enthaltenen persönlichen Daten und Passwörter zu erhalten.**

In diesem Speicher werden vertrauliche Informationen abgelegt, beispielsweise lokale Passwörter, E-Mail-Logins, Internet-Zugangspasswörter, Passwörter für den automatischen Zugriff auf verdeckte Bereiche von Websites, Webdaten und Passwörter für das automatisierte Ausfüllen von Webformularen und andere. Diese Daten werden in die entsprechenden Felder der E-Mail-Clients und Browser eingetragen. In der Regel hat der Anwender die Möglichkeit, die eingegebenen Daten zu speichern, wofür er aber unbedingt ein spezielles Kästchen mit einem Haken versehen muss. In diesem Fall legt Windows die eingegebenen Daten im geschützten Speicher ab.

Hierbei gilt es zu bedenken, dass selbst Anwender, die sich der Gefahr des Informationsdiebstahls bewusst sind und daher Passwörter und Daten nicht im Browser speichern, für gewöhnlich die Passwörter des E-Mail-Systems abspeichern, da es zeitlich zu aufwändig wäre, diese bei jedem einzelnen E-Mail-Versand und -Empfang erneut einzugeben. Berücksichtigt man zudem, dass bei einigen Internet-Providern die Passwörter für den Internet-Zugang und den E-Mail-Account identisch sind, wird klar, dass den Kriminellen hier die Arbeit erleichtert wird: Gelangen sie in den Besitz dieses Passwortes, ermöglicht es ihnen sowohl Zugriff auf den E-Mail-Account als auch auf die Parameter der Internetverbindung.

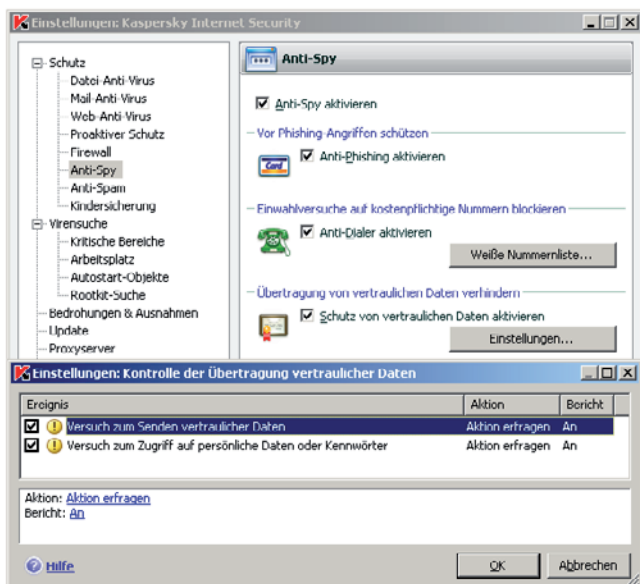
► Der Versuch, verdeckt Daten über Verbindungskanäle zu versenden.

Zur Weiterleitung der gesammelten Daten verwenden schädliche Programme verschiedene Methoden zur Umgehung der potentiell auf dem Anwender-PC installierten Firewall. So können sie etwa den Browser-Prozess im verborgenen Modus starten und diesem die Daten mit Hilfe von Programm-Schnittstellen (COM, OLE, DDE und andere) übermitteln, die in den meisten Browsern verfügbar sind. Da in der Mehrzahl der aktuellen Firewalls eine Vielzahl von Regeln vorinstalliert ist, die vertrauenswürdigen Anwendungen Netzaktivität gestattet, reagiert eine solche Firewall nicht auf die Datenübermittlung durch den Internet-Browser. Der Anwender wird dementsprechend nicht darüber informiert und kann das Abfließen der Daten nicht verhindern.

Wichtig ist auch, dass die Datenverschlüsselung durch ein Schadprogramm für diesen Schutzansatz kein Problem darstellt, da die Aktivität von Schadprogrammen bereits vor der Weiterleitung verschlüsselter Daten über Verbindungskanäle abgefangen wird. Der beschriebene Ansatz ist unter anderem im Produkt Kaspersky Internet Security von Kaspersky Lab umgesetzt.

Schutz vor Diebstahl vertraulicher Informationen mit Kaspersky Internet Security am Beispiel von Trojan-PSW.Win32.LdPinch

Das Modul zum Schutz vertraulicher Informationen ist als Subsystem der Komponente *Anti-Spion* in das Produkt Kaspersky Internet Security integriert. Es analysiert das Verhalten aller Prozesse im System des Anwenders. Beim Erkennen einer der oben beschriebenen Aktivitäten besteht die Möglichkeit, den Anwender entweder zu warnen oder die entsprechende Aktivität automatisch zu blockieren.



Konfiguration des *Anti-Spion* in Kaspersky Internet Security 7.0

Der in Kaspersky Internet Security umgesetzte Schutz vor Versuchen, vertrauliche Daten zu stehlen, wird am Beispiel des realen trojanischen Programms *Trojan-PSW.Win32.LdPinch* erläutert. Dieses stiehlt eine Menge an Daten: Informationen über die Festplatte des Computers, den Account des jeweiligen Anwenders, den Netznamen des Computers, die Betriebssystem-Version, den Prozessortyp, die Bildschirmoptionen, die auf dem Computer installierten Programme, die laufenden Prozesse und die im System enthaltenen Dialup-Verbindungen. Nicht zu vergessen das begehrteste Diebesgut, nämlich Passwörter einer Vielzahl von Programmen, einschließlich der folgenden:

- 1 **Instant Messenger:**
 - ICQ 99B-2002a
 - ICQ 2003/Lite/5/Rambler
 - Miranda IM
 - Trillian
 - &RQ, RnQ, The Rat
 - QIP
 - GAIM
 - MSN & Live Messenger
- 2 **E-Mail-Clients:**
 - The Bat!
 - Microsoft Office Outlook
 - Mail.Ru Agent
 - Becky
 - Eudora
 - Mozilla Thunderbird
 - Gmail Notifier
- 3 **Internet-Browser:**
 - Opera
 - Protected Storage (IE, Outlook Express)
 - Mozilla Browser
 - Mozilla Firefox
- 4 **Autodialer:**
 - RAS
 - E-Dialer
 - Vdialer
- 5 **Dateimanager:**
 - FAR
 - Windows/Total Comander
- 6 **FTP-Clients:**
 - CuteFTP
 - WS FTP
 - FileZilla
 - Flash FXP
 - Smart FTP
 - Coffee Cup FTP

Die gestohlenen Daten werden zur weiteren Verbreitung des Schadprogramms eingesetzt. Ist der Trojaner etwa in den Besitz eines ICQ-Passwortes gelangt, ändert er dieses auf der ICQ-Site, um daraufhin im Namen des Opfers Mitteilungen mit einem Link auf seine eigene ausführbare Datei zu versenden und so die Anzahl der infizierten Computer zu erhöhen. Alle gestohlenen Da-

ten werden in verschlüsselter Form entweder an eine E-Mail-Adresse versandt oder auf einem FTP-Server der Kriminellen abgelegt.

Ein System zum Schutz vertraulicher Informationen, das auf der Analyse des Traffics basiert (wie Norton Privacy Control), ist nicht in der Lage, den Versand verschlüsselter Daten zu verhindern, selbst wenn der Anwender alle Passwörter zu allen Programmen in die Liste der zu überprüfenden Daten eingegeben hat. Problematisch wird dies, wenn ein durch das Subsystem Privacy Control der Firma Symantec oder ein vergleichbar arbeitendes Produkt „geschützter“ Rechner von einem Trojaner angegriffen wird: Handelt es sich beispielsweise um eine neue Version des trojanischen Programms *Trojan-PSW.Win32.LdPinch*, die noch nicht in der Antiviren-Datenbanken enthalten ist und nicht von anderen Schutzkomponenten erkannt wird, so kann der Kriminelle die Mehrzahl der Passwörter stehlen und ganz nach seinem Ermessen verwenden.

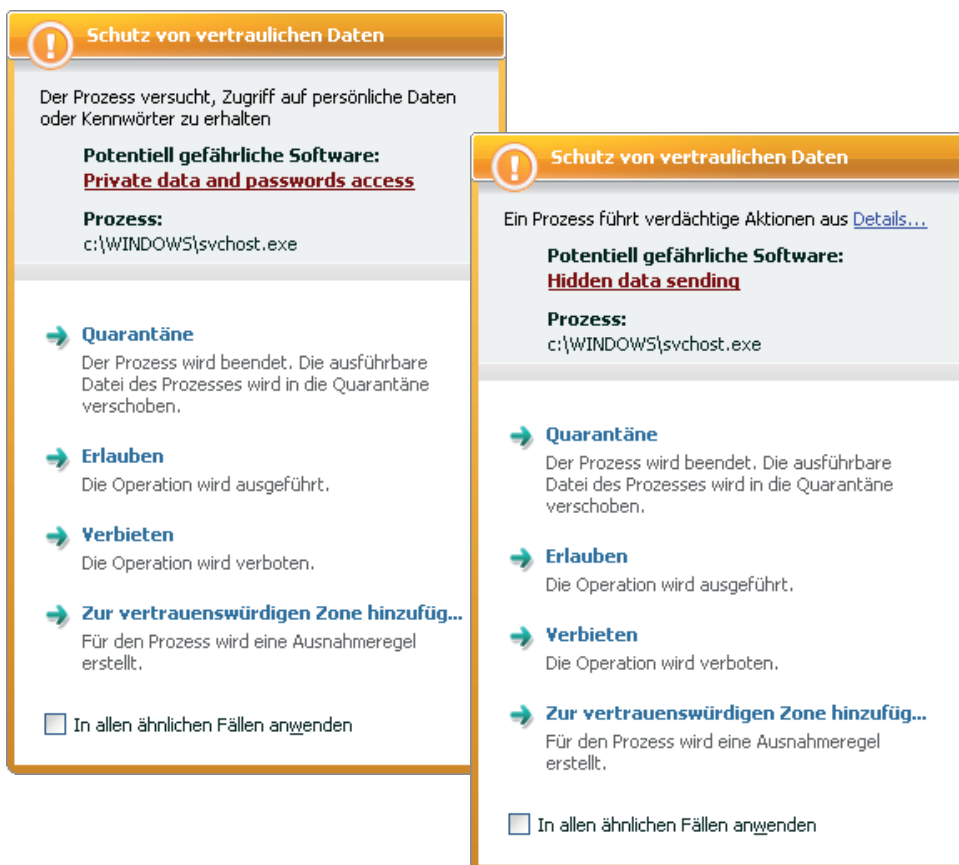
Ein Schutzsystem hingegen, das auf der Aktivitätsanalyse der geöffneten Anwendungen basiert, macht es möglich, sowohl das Versenden einer Datensammlung als auch das verborgene Versenden der von *Trojan-PSW.Win32.LdPinch* auf dem Opfercomputer zusammengetragenen vertraulichen Informationen zu blockieren.

Fazit

In der vorliegenden Analyse wurden die Methoden des Diebstahls vertraulicher Informationen mittels Computer klassifiziert und zwei prinzipiell unterschiedlich aufgebaute Komponenten zum Schutz vertraulicher Informationen, wie sie in derzeit aktuelle komplexe Sicherheitssysteme integriert sind, erläutert. Die Effektivität beider Ansätze wurde am Beispiel der Konfrontation dieser Schutzsysteme mit einem weithin bekannten trojanischen Programm analysiert.

Der Vergleich beider Ansätze zum Schutz vertraulicher Informationen zeigt deutlich die Überlegenheit desjenigen Ansatzes, der auf der Verhaltensanalyse der geöffneten Anwendungen und auf der Beobachtung der Aktivität basiert, die von einem möglichen Versuch des Diebstahls vertraulicher Daten zeugt. Als wesentlich weniger effektiv erweist sich der Ansatz, bei dem die Schutzkomponente eine vom Anwender erstellte Liste vertraulicher Informationen verwendet und zu verhindern versucht, dass ein Fragment dieser Daten in den ausgehenden Traffic gelangt.

Nikolay Grebennikov
 Stellvertretender Direktor der Abteilung für innovative Technologien, Kaspersky Lab



Kaspersky Internet Security warnt, wenn *Trojan-PSW.Win32.LdPinch* versucht, auf vertrauliche Daten zuzugreifen (links) und diese dann zu versenden (rechts)

Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Kontakt

Kaspersky Labs GmbH
Steinheilstr. 13
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0
Telefax: +49 (0)841 981 89 100

info@kaspersky.de
www.kaspersky.de