Cyberkriminelle kommen durch die Hintertür

Facebook, USB-Sticks und Drive-by-Downloads: Virenautoren suchen ständig nach neuen Verbreitungswegen für ihre Schädlinge Malware-Wellen mit großer Medienaufmerksamkeit sind heute passé. Viren kommen lieber heimlich durch die Hintertür - mit dankbarer Hilfe der nichts ahnenden Anwender. Thomas Uhlemann zeigt die aktuellen Gefahrentrends auf und gibt Tipps, wie man sich schützen kann.

Drive-by-Downloads: Die Internetseite als Virenschleuder

Sicherheitsbewusste Anwender vermeiden Internetseiten, die auch nur im Entferntesten gefährlich sein könnten. Doch auch das Ansurfen eines vermeintlich sicheren Webauftritts kann im Malware-Fiasko enden. Immer mehr Websites werden ohne Wissen des Betreibers von Hackern gezielt manipuliert und mit Malware bestückt. Der alleinige Besuch einer solchen Webseite reicht schon aus, um den eigenen PC zu infizieren. Dafür ist nicht einmal eine Benutzeraktion notwendig, wie beispielsweise das Starten eines Downloads. Diese sogenannten „Drive-by-Downloads" haben die E-Mail als häufigsten Verbreitungsweg von Malware inzwischen abgelöst.

Uhlemann empfiehlt:

1. Nutzen Sie immer die aktuelle Browser-Version!
2. Aktualisieren Sie alle Plug-ins wie beispielsweise den Flash Player oder den Adobe Reader. Zusätzliche Sicherheit bieten Browser-Erweiterungen, die (gefährliche) Skripte erst nach Freigabe durch den Anwender zulassen (NoScript für Firefox).
3. Selbstverständlich sollte Ihre Antivirensoftware (wie ESET) Web-Traffic und Web-Downloads überprüfen und Schädlinge sicher herausfiltern können.

USB-Sticks: Schnell mal einen Computer infizieren

Smartphones, Apple-Notebooks, Netbooks mit Linux und USB-Sticks: Viele Anwender setzen ihr privates Equipment auch gerne mal am Arbeitsplatz ein. Das Vorführen der aktuellen Urlaubsbilder vom USB-Stick oder das Synchronisieren von Outlook-Daten mit dem Handy führen jedoch schnell zum Virenbefall. Denn oftmals ist auf den mobilen Geräten keine Sicherheitssoftware installiert. Cyberkriminelle wissen das und missbrauchen mobile und/oder nicht Windows basierte Betriebssysteme als Überträger ihrer Malware. Die Schädlinge verbergen dabei die Anwesenheit vor ihrem „Wirt", der von ihrer Existenz nichts ahnt. Denn Apple oder Linux gilt gemeinhin als immun vor Viren. Dieser Irrglaube wird bestraft, wenn der Kontakt zum Windows-Netzwerk hergestellt ist und die eingeschleuste Malware ihre kriminellen Machenschaften startet.

Uhlemann empfiehlt:

1. Nutzen Sie Antivirensoftware auf allen Ihren Geräten. Vertrauen Sie nicht den Mythen, dass Mac-Rechner und Smartphones nicht gefährdet sind. Dies ist schlichtweg falsch.
2. Deaktivieren Sie die Auto-Run-Funktion in Windows, die angeschlossene Wechseldatenspeicher sofort öffnet und Malware in die Karten spielt.
3. Scannen Sie Ihren USB-Stick oder Speicherkarten regelmäßig auf Viren.

Facebook & Co.: Vertrauliche Informationen auf dem Präsentierteller

Soziale Netzwerke wie Facebook oder Xing erfreuen sich bei Anwendern weltweit immer größerer Beliebtheit. Dies gilt auch für Cyberkriminelle, die einen neuen „Vertriebskanal" für ihre Malware systematisch erschließen. Die Nutzer machen es ihnen dabei recht einfach. Sie veröffentlichen in Sozialen Netzwerken private oder unternehmensinterne Daten, die für jeden ohne Einschränkung lesbar sind. Erst kürzlich ist eine Datenbank mit persönlichen Daten von 100 Millionen Facebook-Nutzern aufgetaucht. Es ist nur eine Frage der Zeit, wann Kriminelle daraus Profit schlagen werden.

Uhlemann empfiehlt:

1. Bearbeiten Sie die Sicherheitseinstellungen von Facebook manuell und schränken Sie die öffentliche Lesbarkeit Ihrer Daten ein.
2. Geben Sie lieber eine Information weniger preis als zu viel.
3. Weitere Tipps für ein sicheres Facebook finden Sie hier.

< Zurück Weiter >

Aktuelles als Feed erhalten

Aktuelle Signaturdatenbank

Update 5387 (20100823)

CeBIT Studio

Testsieger sind nicht unbedingt die besten Produkte. Erfahren Sie mehr über die wahren Hintergründe von Vergleichstests und wie man deren Ergebnisse richtig deutet.

Videovortrag auf der CeBIT 2010

ESET Viren Top 10: Gefährliches Webseiten-Script bedroht deutsche Rechner

Die Virenexperten von ESET haben im Juni 2010 eine Reihe neuer und gefährlicher Malware aufgespürt. Eine der aktuellen Top-Bedrohungen in Europa ist **JS/TrojanDownloader.Pegel.BR**. Dieser Trojaner infiziert Webseiten und befällt anschließend deren Besucher.

Streng genommen handelt es sich dabei um ein Script, das sich in Internetseiten einnistet, die iFrames einsetzen. Sobald es aktiv ist, werden alle Besucher automatisch zu einer verseuchten Malware-Seite umgeleitet. Von dort bezieht das Script weiteren Schadcode und installiert diesen auf unzureichend geschützte Rechner.

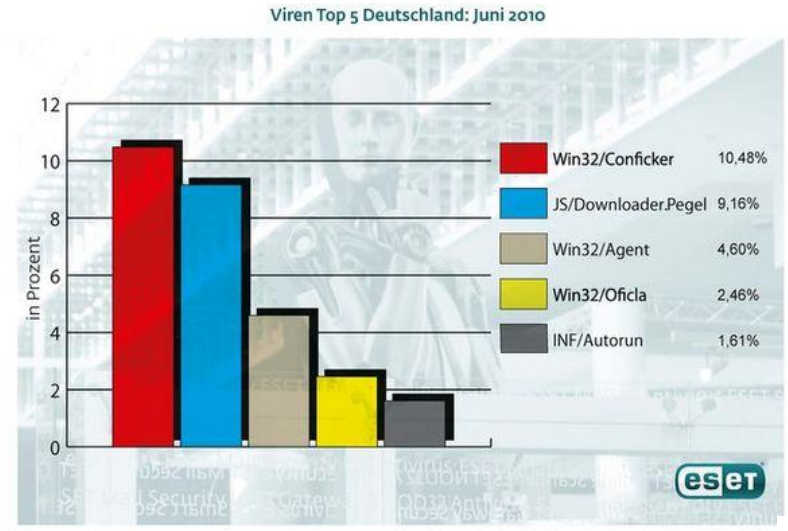
In Deutschland sprang **JS/TrojanDownloader.Pegel.BR** innerhalb von vier Wochen von „null" auf Platz zwei in der Viren Top 5. In Österreich (14,55%) und Großbritannien (12,34%) ist der Trojaner bereits Spitzenreiter und löste dort Win32/Conficker ab. Auch weltweit geht der Vormarsch weiter: Auf 2,29% aller infizierten Rechner wurde **JS/TrojanDownloader.Pegel.BR** bereits entdeckt.

Sicherheitsanalytiker Jan Vrabec rät daher allen Anwendern, die Scripting-Funktion von eingesetzten Browsern und auch PDF-Readern standardmäßig zu deaktivieren – sofern das im täglichen Betrieb keine schwerwiegende Beeinträchtigung darstellt. Für den Firefox-Browser bietet sich alternativ das kostenlose Add-In „NoScript" an. Damit kann der Anwender selektiv entscheiden, ob Javascript auf angesurften Seiten erlaubt werden soll oder auch nicht.

Vrabec weist zudem auf den minimalen Basisschutz hin, den PC-Nutzer unbedingt beherzigen sollten: aktuelle Antivirensoftware einsetzen, Betriebssystem und Programme auf dem aktuellen Stand halten und nicht mit Administratorenrechten surfen.

Mit Argusaugen beobachten die ESET-Virenjäger auch den Trojaner **Win32/Oficla**, der sich im Juni 2010 auf Platz 4 der deutschen Viren Top 5 vorarbeiten konnte. Sobald der Schädling einen Rechner infiziert hat, lädt er weitere Malware herunter und installiert sie.

Viren Top 5 Deutschland: Juni 2010



Viren Top 10 Weltweit: Juni 2010

Nach wie vor behaupten die Varianten von **Win32/Conficker** (9,79%) weltweit ihre Spitzenposition. Am stärksten sind sie in Irland (28,30%) und Slowenien (29,17%) verbreitet. In Deutschland sind 10.48% aller infizierten PCs auf Win32/Conficker zurückzuführen. Noch vor wenigen Monaten waren vor allem osteuropäische Länder wie Russland und die Ukraine von Win32/Conficker betroffen.

Mit **INF/Autorun** (6,57%), **Win32/PSW.OnLineGames** (4,26%) und Win32/Agent (3,25%) folgen weitere Schädlinge, die sich seit langer Zeit in den Top 10 befinden.

Aktuelles als Feed erhalten

RSS 2.0 ATOM 1.0
RSS 1.0 ATOM 0.3

Aktuelle Signaturdatenbank

Update 5388 (20100823)

CeBIT Studio

Testsieger sind nicht unbedingt die besten Produkte. Erfahren Sie mehr über die wahren Hintergründe von Vergleichstests und wie man deren Ergebnisse richtig deutet.

Videovortrag auf der CeBIT 2010