



Pressemitteilung – Freigegeben zur sofortigen Veröffentlichung

## Malware-Diskussion in der IT-Welt: Macht es wirklich Sinn, infizierte PCs zu reinigen?

**Emsi Software, Anbieter von Sicherheits-Software wie a-squared Malware 4.0, greift eine aktuelle Diskussion aus der IT-Security-Welt auf: Macht es überhaupt Sinn, einen mit Schad-Software infizierten Rechner zu reinigen? Kann der Anwender einem solchen System überhaupt noch einmal vertrauen? Um diese Frage zu klären, muss beleuchtet werden, ob eine vollständige Säuberung technisch überhaupt möglich ist.**

Bei den kleinsten Störungen am PC mutmaßen die Anwender bereits das Wirken eines Virus. Der Drucker funktioniert nicht? Sicherlich ein Virus! Die Internet-Verbindung wirkt so behäbig? Sicherlich funkt ein Spyware-Programm gerade die persönlichen Daten des Anwenders in ein Land, das auf keinem europäischen Atlas mehr zu finden ist!

Die meisten Anwender haben nur wenig Wissen darüber, wie ein Schadprogramm aufgebaut ist, wie es funktioniert und was es auf dem PC anrichten kann. Sie installieren einfach ein Schutzprogramm und delegieren alle Verantwortung an dieses Programm. Die IT-Security-Szene gibt sich mit diesem Schutz aber nicht zufrieden und fragt sich zurzeit selbst sehr provokant: Lohnt es sich überhaupt, einen infizierten Rechner zu reinigen?

Übersetzt bedeutet das nicht, dass die Schadprogramme so harmlos sind, dass der PC-Anwender sie getrost ignorieren kann. Stattdessen steht die Frage im Raum, ob es den modernen Schutzprogrammen überhaupt möglich ist, ein befallenes System restlos zu säubern oder ob es nicht besser wäre, es komplett neu aufzuspielen. Um das zu entscheiden, muss man sich ein wenig mehr mit der Materie beschäftigen.

### **Basiswissen: Wie wirken Viren, Trojaner und Spyware-Tools?**

Viren benötigen andere Wirt-Anwendungen, um funktionieren zu können. Ein Virus hängt sich an ein "gutes" Programm an, indem es den eigenen Virencode in eine bereits vorhandene, ausführbare Datei einbaut. Erst wenn das gutartige Programm geladen wird, kann das Virus aktiv werden und weitere Programme befallen.

Deutlich bedeutsamer im täglichen Malware-Ansturm auf die eigene Festplatte sind inzwischen die **Trojaner, Backdoors, Bots und Würmer**. **Trojaner und Bots** sind eigenständige Programme, die sich in den Tiefen des Systems verstecken und hier möglichst kein Aufsehen erwecken möchten. Sie sind dafür da, einem außenstehenden Hacker die Hintertür zum PC zu öffnen, sodass dieser die Kontrolle über den PC übernehmen kann - etwa für den heimlichen Massen-Versand von Spam-Mails. Trojaner und Bots sind nur dann gefährlich, wenn sie in den Arbeitsspeicher geladen wurden. Sie nutzen deswegen Autostartfunktionen, die sicherstellen, dass sie bei jedem Boot-Vorgang wieder mit aufgerufen werden.

**Spyware, Adware, falsche Sicherheits-Software:** Spyware-Programme belauschen den Anwender heimlich und zeichnen etwa die Bankverbindung und die Zugangsdaten auf, um sie dann unbemerkt an die Online-Mafia zu übermitteln. Diese Spionage-Programme werden immer raffinierter programmiert. So starten sie manchmal mehrere aktive Prozesse, die sich gegenseitig überwachen. Wird einer der Prozesse beendet, so kann er über einen anderen Prozess gleich wieder neu gestartet werden. Falsche



Pressemitteilung – Freigegeben zur sofortigen Veröffentlichung

Sicherheitsprogramme geben vor, Jagd auf Schadroutinen zu machen - dabei gehören sie selbst in diese Kategorie. Einige von ihnen injizieren sich in essentielle Systemprozesse wie z.B. in die winlogon.exe. Beim Versuch, die Schadprogramme zu entfernen, kommt es dann zum Systemabsturz.

Die **Rootkits** sind am gefährlichsten. Diese Schadprogramme manipulieren das Betriebssystem so sehr, dass sie für das System selbst unsichtbar werden - sie werden einfach nicht mehr im Datei- oder Prozessmanager angezeigt. Somit können auch die Antiviren-Programme diese Rootkits nicht mehr aufspüren. Sie schaffen es sogar, Registry-Einträge, offene Ports und aktive Prozesse unsichtbar zu machen.

### **Desinfektion: Reinigung manchmal mit Problemen behaftet**

Sind die Schadprogramme erst einmal auf den eigenen Rechner gelangt und hier aktiviert worden, so steht die Frage im Raum, ob sie sich auch wieder entfernen lassen - und zwar restlos und ohne unerwünschte Rückstände.

Wunderbar: Bei einfach gestrickter Malware ist es mit relativ hoher Sicherheit möglich, die Schad-Software restlos vom System zu entfernen. Bei Viren ist es am einfachsten, die befallenen Dateien zu löschen. Dabei kann es sein, dass die infizierten Programme anschließend nicht mehr funktionieren. Kein Problem: Die lassen sich ja leicht neu aufspielen. Bei Trojanern reicht es aus, die aktiven Prozesse zu schließen, die Autostart-Einträge zu beseitigen und die ausführbaren Trojaner-Dateien zu löschen. Klassische Spyware-Programme können ganz einfach deinstalliert werden. So gesehen ist es auch bei ihnen möglich, das System nach einem Fund schnell wieder in den Ursprungszustand zurückzusetzen.

Anders sieht das bei moderneren Spyware-Programmen oder bei falschen Antiviren-Programmen aus. Diese graben sich so tief in das System ein, dass Spezialwerkzeuge nötig werden, die diese Dateien noch vor dem eigentlichen Boot-Vorgang löschen. Diesen Infektionen ist nur sehr schwierig auf endgültige Weise beizukommen. Das gilt auch für die Rootkits, die nahezu perfekte Tarn Eigenschaften besitzen. Abgesehen davon, dass kein Anwender genau sagen kann, ob er auch wirklich alle Rootkits auf seinem PC aufspüren kann: Kann er denn auch sicher sein, dass ein Rootkit vollständig entfernt wurde? Die Hacker finden immer neue Wege, um ihre Schad-Software zu verstecken.

Oft genug ist es auch so, dass eine Malware zwar entfernt wird, durch sie verursachte Änderungen am System aber bestehen bleiben. So kann es sein, dass Ports geöffnet wurden, die einem Hacker dann trotzdem den Angriff von außen auf das System erlauben.

### **Ist der PC erst einmal infiziert: System neu aufsetzen!**

Emsi Software aus Österreich bietet Schutz-Software für den Windows-PC an. Geschäftsführer Christian Mairoll: "Aus unserer Erfahrung heraus lassen sich gerade Rootkits und die falschen Antiviren-Programme nicht mit letzter Sicherheit von den infizierten Rechnern entfernen. Wir raten unseren Kunden deswegen, nach der Erstinstallation des Rechners mit allen wichtigen Programmen ein Backup-Image der ganzen Partition anzulegen. Das kann dann im Schadensfall auf eine frisch formatierte Festplatte zurückgespielt werden."



Pressemitteilung – Freigegeben zur sofortigen Veröffentlichung

Wichtig ist natürlich, dass trotz aller Bedenken ein Schutzprogramm auf dem Rechner vorliegt, das Malware sofort anzeigen kann, sobald sie auf den eigenen PC gelangt. Das Emsi-Software-Programm **Mamutu 1.7** achtet auf verhaltensauffällige Aktionen auf dem eigenen PC und kann so Schad-Software selbst dann enttarnen, wenn sie noch gar nicht in der Szene bekannt ist.

Für Privatanwender kostenfrei ist **a-aquared Free 4.0** (zurzeit in der Beta-Phase). Dieses Programm scannt den ganzen Rechner und spürt bereits vorhandene Infektionen auf, um diese dann sogleich zu beseitigen.

Zur Königsklasse gehört das Programm **a-squared Malware 4.0**. Es nutzt gleich zwei ständig im Hintergrund aktive Scanner, um Malware aller Art aufzuspüren, bevor sie sich überhaupt im System einnisten kann. Ein doppelter Echtzeitschutz besteht durch einen Signaturescan und eine zusätzlich vorhandene Verhaltensanalyse (Malware-IDS). Mehrere Updates am Tag stellen sicher, dass diese Waffe immer scharf bleibt. Ein Jahresabo der Software kostet 29,95 Euro.

Homepage: <http://www.emsisoft.de/>

Downloads: <http://www.emsisoft.de/de/software/download/>

**Über den Sinn und Unsinn von Malware -Säuberung (Wissensdatenbank-Artikel):**

<http://www.emsisoft.de/de/kb/articles/tec081111/>

## ÜBER EMSI SOFTWARE

Emsi Software ist ein privat geführtes Unternehmen mit Sitz in Österreich. Das schnell wachsende Unternehmen bilanziert seit der Gründung im Jahr 2003 positiv und ohne Fremdkapital. Ziel von Emsi Software ist es, ein führender europäischer Anbieter für Verhaltensanalyse-Technologie zum Analysieren von Software, insbesondere Malware, zu werden.

Gegründet wurde das Unternehmen 2003 von Christian Mairoll, der damit seine Vision einer virtuellen Firma umsetzt: Die 15 Mitarbeiter der Firma sind auf der ganzen Welt verteilt, arbeiten aber über das Internet so zusammen, als würden sie nebeneinander im echten Büro sitzen. Um die technischen Visionen kümmert sich Georg Wicherski, der als Mitbegründer des "Nepenthes" HoneyPot Projekts sowie der mwcollect Alliance (Zusammenschluss von HoneyPot Netzen zum automatisierten Einfangen von Schadsoftware aus dem Internet) ein großes Ansehen in der Sicherheitsbranche genießt. Zur Produktpalette von Emsi Software gehören die Sicherheitsprogramme a-squared Anti-Malware, a-squared Free, a-squared HiJackFree, a-squared Anti-Dialer und seit Ende 2007 Mamutu.

## PRESSEKONTAKT

Thomas Günther

PR-Manager

Mail: [tg@emsisoft.com](mailto:tg@emsisoft.com)

Fon: +43 664 344 60 68

Fax: +43 6235 200 53