AKTUELLE GEFAHREN: Tipps für mehr Sicherheit

Skype-Alarm

Mit dem Erfolg von Skype kommen nun auch die Gefahren: ein bisher noch ungefährlicher Wurm versucht per Erotik-Bild Skype-Nutzer zu überlisten und sich so zu verbreiten.

Verführerischer Virus

Wurm attackiert Skype

Skype-Nutzer, bei denen sich ein Chat-Fenster mit dem Mini-Bild einer leicht bekleideten Dame öffnet, sollten vorsichtig sein: Wer den Link dazu anklickt, sieht das Reizwäsche-Model zwar gross, fängt sich aber zugleich den Windows-Wurm Pykse ein. Der schaltet den Skype-Client in den "Do not disturb"-Modus, so dass keine neuen Anrufe mehr eingehen, und verschickt verseuchte Nachrichten an alle Kontakte, die gerade online sind. Schaden verursacht der Wurm sonst offenbar keinen, er versucht aber die Klickraten auf einigen Websites und damit die Werbeeinnahmen dort zu erhöhen.
www.sophos.com/pressoffice/news/articles/2007/04/pykse.html

Gefahr für Skype: Hinter dem Bild von "Sandra" ist ein Virus versteckt.

Trügerische Sicherheit

Lücken in virtuellen PCs

Virtuelle PCs werden gern empfohlen um echte PCs gegen Angriffe abzuschotten. Auf der Sicherheitskonferenz "Can Sec West" demonstrierte Google-Mitarbeiter Travis Ormandy, dass virtuelle Maschinen auch Lücken aufweisen können. Er fand heraus, dass hervorgerufene Pufferüberläufe ausgenutzt werden können. Bei Vmware entdeckte Ormandy einen Fehler im Power-Management, über den sich Code ins Host-System einschleusen lassen soll.
http://taviso.decsystem.org/virtsec.pdf

Tool gegen Vista-DRM

Malware in Vista

Der Programmierer Alex Ionescu will ein Tool entwickelt haben, mit dem sich DRM-Prozesse in Vista ein- und ausschalten lassen. Auf diese Weise soll es auch möglich sein, Malware im DRM-System von Vista zu verstecken. Deshalb bietet Ionescu sein Tool D-Pin Purr v.1.0 nur als Binärdatei und nicht im Quellcode zum Download an.
www.alex-ionescu.com

Rekord-Spam

Wurm warnt vor Wurm

Eine neue Welle des Sturm-Wurms aus der "Nuwar/Zhelatin"-Virusfamilie hat der Sicherheitsfirma Postini zufolge das grösste Spam-Volumen der vergangenen zwölf Monate verursacht. Allein in den ersten 24 Stunden der Attacke seien 55 Millionen bösartiger Mails beobachtet worden – das 50- bis 60fache des Üblichen. Betreff-Zeilen wie "Worm Detected" sollen die Nutzer dazu bringen, einen angeblichen Patch gegen eine Wurm-Attacke zu installieren. Die passwortgeschützte ZIP-Datei enthält eine Variante des Sturm-Trojaners.
www.postini.com/stats

Forum infiltriert

Trojaner via Teamspeak

Angreifer haben in der Software des Teamspeak-Forums Goteamspeak .com die infizierte Datei *patch.exe* hinterlegt und alle Nutzer per E-Mail aufgefordert, sie zu installieren. Teamspeak ist eine populäre Sprachkonferenzlösung für Online-Spiele.
http://forum.goteamspeak.com/showthread.php?t=37007

Lücke in ActiveX-Control

Angriffsziel Office

Die Zahl der Attacken, die Sicherheitslücken in Microsoft Office ausnutzen wollen, um vor allem in Wirtschaftsunternehmen Daten zu stehlen, hat im März 2007 weiter zugenommen. Der Messagelabs-Bericht *Targeted Attacks March 2007* verzeichnet 716 E-Mails mit infiziertem Anhang. Dabei waren erstmals mehr Powerpoint- als Word-Anhänge von Viren verseucht.
www.messagelabs.com

Trittbrettfahrer

Amoklauf-Mails

Das Informationsbedürfnis der Internetnutzer nach Tragödien nutzen Trojaner-Programmierer aus. So kursieren seit dem Amoklauf von Blacksburg Mails, die Exklusivbilder versprechen. Unter der Bezeichnung "Terror_EM_VIRGINIA.scr" offerieren sie einen Screensaver, der einen Trojaner installiert. Eine andere Mail lockt mit dem Bericht über ein angebliches Massaker durch einen Asiaten in München.
www.sophos.com/pressoffice/news/articles/ 2007/04/virginia.html

Java als Einfallstor

Hochkritische Lücke in Apples Quicktime

Die Sicherheitsfirma Secunia warnt vor einer höchst kritischen Schwachstelle im Multimedia-Player Quicktime von Apple. Sobald ein Anwender mit einem Java-fähigen Browser wie Firefox oder Safari auf eine korrumpierte Website surft, ist es dem Angreifer möglich, das System des Nutzers zu kontrollieren. Betroffen sind die Quicktime-Versionen 3.x bis 7. Als Abhilfe empfiehlt Secunia, das Update auf die Quicktime-Version 7.1.6 zu installieren.
http://secunia.com

Update angeraten

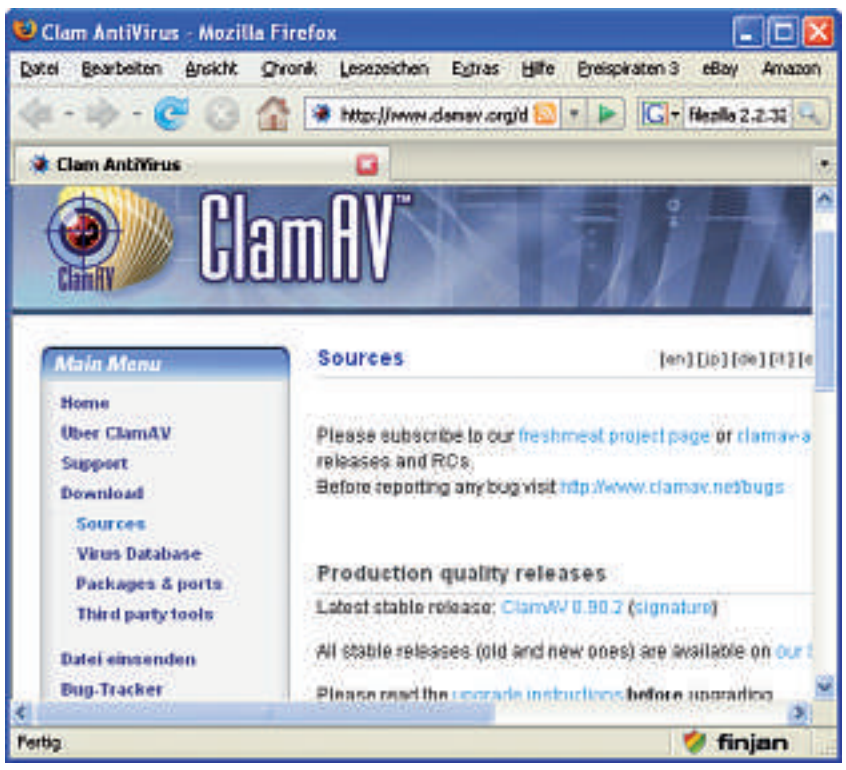
Lücken in Filezilla

Secunia hat eine Sicherheitslücke im Download-Manager Filezilla entdeckt, die sich unter Umständen dazu ausnutzen lässt, fremden Code auf dem Rechner des Anwenders auszuführen. Betroffen von der als mittelkritisch eingestuften Format-String-Schwachstelle sind alle Versionen vor Version 2.2.32
http://sourceforge.net/projects/filezilla, http://secunia.com/advisories/24894

Gefährliche CLP-Dateien

Exploit für Paintshop Pro

Das Projekt Bürger-Cert des BSI warnt vor einer als mittelschwer eingestuften Lücke in Corel Paintshop Pro Photo. Präparierte CLP-Dateien sollen es Angreifern ermöglichen, ungehindert Schadcode auf dem Rechner des Anwenders auszuführen. Solange es kein Update gibt, sollten nur CLP-Dateien aus vertrauenswürdigen Quellen geöffnet werden.
www.buerger-cert.de



Clam-AV: die kostenlose Antiviren-Software kann ohne Update von Viren und Würmern zum Absturz gebracht werden und ist somit überlistet.

Vorsicht bei Bitmap-Dateien

BMP-Befall in Photoshop

Das Bildbearbeitungsprogramm Adobe Photoshop ermöglicht es manipulierten Bitmap-Dateien, einen Pufferüberlauf herbeizuführen und Code einzuschleusen. Betroffen sind Photoshop CS2 und CS3. Ein Patch steht noch aus.
www.milw0rm.com

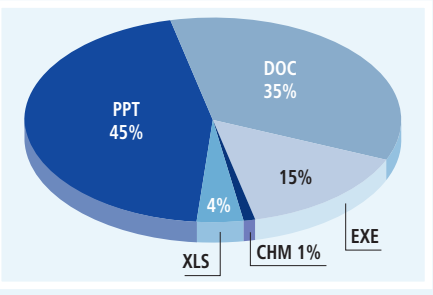
Gefährdeter Virenscanner

Schwachstellen in Clam-AV

Version 0.90.2 des freien Antiviren-Programms Clam-AV beseitigt kleinere Bugs und schliesst zwei Sicherheitslücken, mit denen sich der Scanner zum Absturz bringen und eventuell Code einschleusen lässt. Die erste Lücke kann mit Hilfe präparierter CHM-Hilfe-Dateien ausgenutzt werden, die zweite Lücke führt durch manipulierte CAB-Dateien zu einem Buffer-Overflow. Anwender sollten die neue Version so schnell wie möglich installieren.
www.clamav.org/download/sources

POWERPOINT IM VISIER

Angriffe nach Dateityp im März 2007



Verseuchte Office-Dateien: Im März gab es zum ersten Mal mehr Angriffe auf Powerpoint- als auf Word-Nutzer.