Pressemitteilungen-online.de

Pressemeldungen kostenlos veröffentlichen

Mai
12

Perfekte Tarnung - Raffinierter Rootkit-Wurm öffnet Backdoor mittels Skype

Abgelegt unter: Computer & Hardware

Holzwickede, 12. Mai 2010 - Nach dem kürzlichen Angriff durch Palevo sorgt nun ein weiterer Instant Messenger(IM)-Wurm für Aufsehen.

Wie Sicherheitsexperte BitDefender herausfand, trifft es dieses Mal die Nutzer des VoIP-/IM-Dienstes Skype. Diese erhalten während eines laufenden Chats plötzlich eine Nachricht mit einem Link, der angeblich zu einem Foto des Users persönlich führt. Hinter dem Link versteckt sich jedoch der Wurm Backdoor.Tofsee, der mit mehreren raffinierten Methoden versucht, Cyberkriminellen die Hintertür zu fremden PCs zu öffnen. Dazu deaktiviert er unter anderem Antivirusprogramme und Removal-Tools.

Angriffe durch IM-Würmer sind nichts Neues. User des Yahoo Messenger oder des MSN Messenger sind des Öfteren davon betroffen. Skype-Anwender jedoch blieben bislang weitestgehend verschont. Im Gegensatz zu durchschnittlichen IM-Würmern nutzt Backdoor.Tofsee eine ganze Reihe von Tricks, um seine Erkennung und Entfernung zu verhindern.

Backdoor.Tofsee spricht Sprache der User
Der Wurm setzt auf klassisches Social Engineering, um den Benutzer dazu zu bringen, dem Link zu folgen, und ihn so in die Falle zu locken. So erkennt er die lokalen Systemeinstellungen (Land, Sprache, Aufenthaltsort) und spricht den User via Instant Message in der entsprechenden Landessprache an. Der Wurm „spricht“ neben Deutsch und Englisch auch Spanisch, Italienisch, Niederländisch und Französisch. Die einzelnen Nachrichten unterscheiden sich dabei stets von den vorherigen, da sie ständig via Fernzugriff durch den Cyberkriminellen geändert werden.

Mehrere Täuschungsversuche in einem
Hinzu kommt, dass die Nachrichten ausschließlich während laufenden Konversationen des Anwenders mit einem seiner Skype-Kontakte versendet werden. Das soll die Glaubwürdigkeit der Messages erhöhen. Folgt der Nutzer dem infizierten Link, gelangt er auf eine gefälschte Rapidshare-Website. Fährt er mit dem Downloadprozess fort, erhält der User eine Datei mit der Bezeichnung „NewPhoto024.JPG.zip“. Extrahiert das Opfer diese Datei, wird eine .exe-Datei angezeigt mit dem trügerischen Namen: „NewPhoto024.JPG_www.tinyfilehost.com“; eine Täuschung, denn die Endung „com“ deutet zwar auf eine Website hin, verbirgt jedoch eine DOS-Anwendung, durch die sich der Wurm im System einnistet.

Rootkit-Treiber zur perfekten Tarnung
Um sich auf dem Betriebssystem zu verstecken, installiert der Wurm zusätzlich einen Rootkit-Treiber. Dieser versteckt alle Dateien, die auf eine Infektion von Backdoor.Tofsee schließen lassen. Zusätzlich überwacht er die Internetaktivitäten des PC-Nutzers und verhindert den Zugriff auf Websites von Sicherheitssoftware-Anbietern, Online-Scannern, Support-Foren und Windows Update-Seiten. Nicht zuletzt verhindert der Schädling auch den Zugriff auf populäre Download-Portale, die Removal-Tools anbieten.

Nachdem Backdoor.Tofsee auf diese Weise erfolgreich das System kompromittiert hat, fügt er einen eigenen Autostart-Eintrag in der Windows Registry hinzu. Dies ermöglicht ihm, Kopien von sich selbst auf Wechseldatenträgern, wie z.B. USB-Sticks, zu erstellen. Zudem deaktiviert er die Windows-Firewall und befähigt es so einen Remote-Angreifer, sich mit der Backdoor-Komponente des Wurms zu verbinden. Um die Katastrophe für das Opfer perfekt zu machen, verhindert die Rootkit-Komponente die Installation von sämtlichen Antiviruslösungen.

- Weitere Informationen unter: www.bitdefender.de

Über BitDefender®
BitDefender ist Softwareentwickler einer der branchenweit schnellsten und effizientesten Produktlinien international zertifizierter Sicherheitssoftware. Seit der Gründung des Unternehmens im Jahr 2001 hat BitDefender permanent neue

Standards im Bereich des proaktiven Schutzes vor Gefahren aus dem Internet gesetzt. Tagtäglich beschützt BitDefender viele Millionen Privat- und Geschäftskunden rund um den Globus und gibt ihnen das gute Gefühl, dass ihr digitales Leben sicher ist. BitDefender vertreibt seine Sicherheitslösungen in mehr als 100 Ländern über ein globales VAD- und Reseller-Netzwerk. Ausführlichere Informationen über BitDefender und BitDefender-Produkte sind online im Pressecenter verfügbar. Zusätzlich bietet BitDefender in englischer Sprache unter www.malwarecity.com Hintergrundinformationen und aktuelle Neuigkeiten im täglichen Kampf gegen Bedrohungen aus dem Internet.

Pressekontakt:
BitDefender GmbH
Robert-Bosch-Str. 2
D-59439 Holzwickede

Ansprechpartner:
Hans-Peter Lange
PR-Manager
Tel.: +49 (0)2301 - 9184-330
Fax: +49 (0)2301 - 9184-499
E-Mail: presse@bitdefender.de

Andere Artikel

- Microsoft Schwachstelle - Gefälschter Windows-Patch hat Spam-Bot und Trojaner im Gepäck
- PC-Infektionen - Die Top 10 der gefährlichsten E-Threats seit 2008
- Malware Angriffe auf Apple-Systeme - Sicherheitssoftware für Mac-Betriebssysteme
- Malware Ranking - Würmer auf Vormarsch, Trojaner aus Top 10 verschwunden
- Infizierte PCs - DE-Cleaner Rettungssystem spürt Botnetze auf dem Computer auf
- PC Echtzeitschutz vor digitalen Bedrohungen der neuen Generation
- Botnetz Attacke über Twitter - Toolkit generiert automatisch Trojaner
- Computer Schädling ” Palevo ” ist zurück - Wurm verbreitet sich über Instant Messenger
- Kostenfreie Sprach- und Videotelefonie - Skype Risiken für Unternehmen sind überschaubar
- Malware Spam E-Mails mit gefälschtem Absender von Facebook und MySpace
- Sechs neue Schädlinge verseuchen den PC mit Malware
- Online-Banking Betrugsfälle steigen - Nur 45 Prozent nutzen Firewall

Zum Thema: Betriebssystem, BitDefender, Firewall, Infektion, Messenger, PC, Sicherheitssoftware, Skype, Virus

Kein Kommentar

RSS
Trackback

Kommentar hinterlassen

Kommentieren

Name (benötigt)

Mail (wird nicht veröffentlicht) (benötigt)

Website

3 + 4 (required)

Kommentieren

XHTML: Du kannst die folgenden Tags nutzen: <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

"And strange it is / That nature must compel us to lament / Our most persisted deeds."
by William Shakespeare, *Antony and Cleopatra*

Pressemeldungen

PR-Artikel schreiben und veröffentlichen.
- **Registrieren**

Kategorien

- Auto & Verkehr
- Bauen & Wohnen
- Bücher & Medien
- Bildung & Berufe
- Computer & Hardware
- Diverse Meldungen
- Energie & Umwelt
- Essen & Trinken
- Film & Fernsehen

- Finanzen & Versicherungen
- Freizeit & Events
- Gesundheit & Medizin
- Handy & Kommunikation
- Kunst & Kultur
- Kurzmeldungen
- Mode & Lifestyle
- Musik
- Politik
- Recht & Gesetz
- Software
- Sport
- Stars & Sternchen
- Touristik & Reisen
- Werbung & Marketing
- Wirtschaft & Verbände
- Wissenschaft & Forschung
- X Englisch

Archiv durchsuchen

September 2010

M	D	M	D	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

« Aug

Letzter Leser suchte

- neue zuzahlung medikamente
- s-Broker über iPhone
- update outlook 2010 für studenten
- zumutbare eigenbelastung
- ie 9 hardwarebeschleunigung
- affäre männer
- android ar gps bilderkennung
- ads test online
- ads test online
- wer kocht beim deutschen Fernsehpreis

Letzte Meldungen

- Kundendienst - Neben Fachkompetenz ist die menschliche Ebene wichtig
- SMA Solar erhöht Jahresprognose - Deutschland bleibt wichtigster Markt
- Siemens mit mangelnder Zahlungsmoral - Rechnungen erst nach 180 Tagen beglichen
- Studie über Werbewirkung und Nutzerakzeptanz im Internet
- Gebührenstrukturen belasteten oftmals Rendite bei Kapitallebensversicherungen
- Dell stellt Hybrid aus Netbook und Tablet mit neuem Klappmechanismus vor
- Mobiles Breitbandinternet - Jeder dritte Kunde will Mobilfunkanbieter wechseln
- Renault Latitude - Neues Oberklassen Flaggschiff
- Staatliche Banken - Auf Reformen der Finanzmarktregulierung kommt es an
- Wertvolles Arzneimittel - Lizensierung von Cannabis gefordert

Beliebte Wörter

Unternehmen Urteile Umfrage Studie Forschung Banken Gesundheit Börse Internet Auto Medizin Tips Wirtschaft Kinder Geld Deutschland Finanzkrise Statistik Trend Technologie TV Test Urlaub Entwicklung Sicherheit Fussball Fahrzeuge Handy Erkrankung Computer Gesetz Risiko USA Vergleich Frauen Zukunft Beruf Behandlung Wissen Arzt Ernährung Autohersteller PC Bevölkerung Aktien Ratgeber Essen Arbeitsmarkt Konjunktur Preise Versicherung Wirtschaftslage Motor Reisen Studium Patienten Promis Nachrichten Anbieter Analyse Sparen Wettbewerb Umsatz Google Rheinische Post Steuer Krankenkasse Energie Prognose Tiere Europa Untersuchung Medikamente Arbeitnehmer Hersteller PKW Kaufen Modelle Schule Ausbildung