



G Data-Presseinformation 2010

## PDF-Attacken gehören zu den größten Gefahren

Der höchste Neueinsteiger sieht es auf private Mailkonten ab



**Bochum (Deutschland), 07. Mai 2010 –Die Verbreitung von Schadcode hat auch im vergangenen Monat weiter zugenommen. Die Täter setzen bei ihren Attacken dabei zunehmend auf nicht geschlossene Sicherheitslücken in PDF-Programmen. Zu diesem Schluss kommen die Experten der G Data SecurityLabs nach Auswertung der am häufigsten detektierten Angriffe im April 2010. So führt „JS:Pdfka-OE“ die Malware Top 10 unangefochten an. Der höchste**

**Neueinsteiger des Monats, Win32:Rodecap [Trj] hat es besonders auf freie E-Mail Services abgesehen, wie etwa Yahoo, Hotmail oder Google Mail.**



„Sicherheitslücken in Computerprogrammen werden seit längerem ausgenutzt, um Rechner mit Malware zu infizieren. Je größer die Verbreitung einer Anwendung, umso interessanter ist es, entsprechende Schwachstellen auszunutzen“, erläutert Ralf Benz Müller. „Eine weitere Gefahrenquelle, die ebenfalls unterschätzt wird, ist die Autorun Funktion. Unter anderem macht sich Worm.Autorun.VHG diese Methode zu nutzen, um sich zum Beispiel per USB-Stick oder mobiler Festplatte zu verbreiten. Wer die Autorun-Funktion nicht dringend benötigt, sollte sie im Windows Betriebssystem sicherheitshalber

abschalten.“

Computerschädlinge im April 2010			
	Name	Prozent	Trend*
1	JS:Pdfka-OE [Exp]	11,4 %	↔
2	Win32:Rodecap [Trj]	1,7 %	neu
3	Worm.Autorun.VHG	1,7 %	↘
4	WMA:Wimad [Drp]	1,3 %	↘
5	Saturday 14th-669	1,2 %	↘
6	HTML:Iframe-inf	1,0 %	↘
7	Trojan.PWS.Kates.Z	1,0 %	neu
8	Trojan.Boaxxe.X	0,8 %	neu
9	Win32:Sality.OG	0,6 %	↑
10	Win32:Crypt-GBX [Trj]	0,6 %	neu

\* Der Trend zeigt die Veränderung des Rangs im Vergleich zum Vormonat

↑ > 2   ↗ + 1 oder 2   ↔ ± 0   ↘ - 1 oder 2   ↓ > 2

PDF-Dokumente gelten allgemein als ungefährliche Dateien und die entsprechenden Reader sind auf den meisten Rechnern vorhanden. Insbesondere die JavaScript Funktionen machen PDFs jedoch zu einem potentiell gefährlichen Format: In PDF eingebettetes Acrobat JavaScript wird benutzt, um Angriffe vorzubereiten oder enthält selbst Schwachstellen, die es einem Angreifer ermöglichen eigenen Programmcode einzuschleusen. PDFs sollten stärker als potentiell gefährliche Dateien in das Bewusstsein rücken.



Wo es angemessen und möglich ist, sollte die JavaScript-Unterstützung in den Readern ausgeschaltet werden und der Reader sollte auf dem aktuellsten Stand gehalten werden, um vor bereits bekannten Angriffen sicher zu sein.

### **Methodik**

Die Malware Information Initiative (MII) setzt auf die Kraft der Online-Community und jeder Kunde von G Data Sicherheitslösungen kann daran teilnehmen. Voraussetzung hierfür: Er muss diese Funktion in seinem G Data Programm aktiviert haben. Wird ein Angriff eines Computerschädlings abgewehrt, so wird dieser Vorfall vollkommen anonym und an die G Data SecurityLabs übermittelt. Die Informationen über die Schädlinge werden in den G Data SecurityLabs gesammelt und statistisch ausgewertet.

---

### **25 Jahre G Data**

Die G Data Software AG, mit Unternehmenssitz in Bochum, ist ein innovatives und schnell expandierendes Softwarehaus mit Schwerpunkt auf IT-Sicherheitslösungen. Als Spezialist für Internetsicherheit und Pionier im Bereich Virenschutz entwickelte das 1985 in Bochum gegründete Unternehmen bereits vor mehr als 20 Jahren das erste Antiviren-Programm und feiert 2010 seinen 25. Geburtstag.

G Data ist damit eines der ältesten Security-Software-Unternehmen der Welt. Seit mehr als fünf Jahren hat zudem kein anderer europäischer Hersteller von Security-Software häufiger nationale und internationale Testsiege und Auszeichnungen errungen als G Data.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 60 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter [www.gdata.de](http://www.gdata.de).

### **Ihr Redaktionskontakt**

Presseservice G Data Software AG  
Thorsten Urbanski  
Königsallee 178 b  
44799 Bochum

Tel. +49 (0) 234 / 9762-239  
Fax +49 (0) 234 / 9762-299  
[thorsten.urbanski@gdata.de](mailto:thorsten.urbanski@gdata.de)  
[www.gdata.de](http://www.gdata.de)