

vor einem Jahr

in Internet und Wirtschaft

Webbasierte Angriffe weiter auf dem Vormarsch

Onlinekriminelle setzen verstärkt auf Drive-by-Infektionen, PDF-Schwachstellen und Tauschbörsen

(ddp direct) Das G Data Schadcode-Barometer zeigte auch im vergangenen Monat nach oben. Onlinekriminelle setzen nach Analysen der G Data SecurityLabs verstärkt auf webbasierte Angriffe, wie Drive-by-Infektionen oder verseuchte Multimedia-Dateien in P2P-Tauschbörsen. Seit sechs Monaten unangefochten auf Platz eins der Schadcode Top Ten: „JS:PdfkaOE [Exp]“. Dieser Schädling setzt auf nicht geschlossene Sicherheitslücken in PDF-Programmen und versucht aus Schwachstellen in JavaScript Engines von PDF Programmen Kapital zu schlagen. Der höchste Neueinsteiger des Monats, HTML:IFrame-U [Trj], lauert auf Internetseiten und versucht Sicherheitslücken im Browser und Plug-Ins auszunutzen, um so den Rechner mit Schadcode zu infizieren.

Onlinekriminelle setzen seit längerem zur Verbreitung von Schadcode auf webbasierte Angriffe. Der Besuch einer manipulierten Internetseite mit einem ungeschützten Rechner reicht dabei bereits aus, um diesen umgehend mit Schadcode zu infizieren. Seit längerem beobachtet G Data diesen Trend und empfiehlt Anwendern neben der Installation einer leistungsstarken Internet-Sicherheitslösung, das Betriebssystem, den eingesetzten Browser und seine Komponenten immer auf dem aktuellsten Stand zu halten und alle Updates und Sicherheits-Patches umgehend zu installieren.

Rang...Name....Prozent...Trend*

- 1. JS:Pdfka-OE [Exp]: 3,9 % [Trend gleichbleibend]
- 2. HTML:Iframe-inf: 3,6 % [Trend geht nach oben]
- 3. WMA:Wimad [Drp]: 2,1 % [Trend geht nach unten]
- 4. HTML:IFrame-U [Trj]: 1,9 % [neu]
- 5. Worm.Autorun.VHG: 1,4 % [Trend geht nach unten]
- 6. HTML:Script-inf: 1,4 % [Trend geht nach unten]
- 7. HTML:RedirME-inf [Trj]: 0,7 % [neu]
- 8. Saturday 14th-669: 0,7 % [Trend geht nach unten]
- 9. Trojan.Autorun.EU: 0,6 % [neu]
- 10. Trojan.FakeAV.KZQ: 0,4 % [neu]

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

++ 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 an die G Data SecurityLabs übermittelt. Die Informationen über die Schädlinge werden in den G Data SecurityLabs gesammelt und statistisch ausgewertet. Schädlinge-Informationen

JS:Pdfka-OE [Exp]

Ist ein Exploit, der versucht, aus Schwachstellen in JavaScript Engines von PDF Programmen Kapital zu schlagen. Der Benutzer muss ein PDF öffnen, um den Exploit zu starten. Ist die Attacke auf den Rechner des Opfers erfolgreich, wird weiterer Schadcode auf den PC nachgeladen.

HTML:Iframe-inf

HTML-Iframe-inf kennzeichnet schädliche Iframes in einer Webseite. Ein <iframe> ist ein HTML Element das externe Web-Inhalte in die eigentlich besuchte Webseite integriert. Welche schädlichen Inhalte genau integriert werden, liegt in der Hand der Angreifer. Sie können auf den von ihnen kon-trollierten Webservern beliebigen Schadcode hinterlegen.

WMA:Wimad [Drp]

Dieser Trojaner gibt vor, eine normale .wma Audiodatei zu sein, welche aber nur nach Installation eines speziellen Codecs/Decoders auf Windows-Systemen abgespielt werden kann. Wird die Datei vom Anwender ausge-führt, kann der Angreifer jeglichen Schadcode auf dem System installieren. Die infizierten Audiodateien verbreiten sich hauptsächlich über P2P Netz-werke.

Computerschädlinge im Juli 2010

	Name	Anteil	Trend*
1	JS:Pdfka-OE [Exp]	3,9 %	↔
2	HTML:Iframe-inf	3,6 %	↗
3	WMA:Wimad [Drp]	2,1 %	↘
4	HTML:IFrame-U [Trj]	1,9 %	neu
5	Worm.Autorun.VHG	1,4 %	↘
6	HTML:Script-inf	1,4 %	↘
7	HTML:RedirME-inf [Trj]	0,7 %	neu
8	Saturday 14th-669	0,7 %	↓
9	Trojan.Autorun.EU	0,6 %	neu
10	Trojan.FakeAV.KZQ	0,4 %	neu

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

↑ > 2 ↗ + 1 or 2 ↔ ± 0 ↘ 1 or 2 ↓ > 2

Top 10: Computerschädlinge im Juli 2010
Detailsansicht

vor einem Jahr

Webbasierte Angriffe weiter auf dem Vormarsch



Das G Data Schadcode-Barometer zeigte auch im vergangenen Monat nach oben. Onlinekriminelle setzen ...

Pressekontakt

Herr Thorsten Urbanski
Public Relations Manager

G Data Software AG
Königsallee 178b
44799 Bochum
Deutschland

Email: [Kontakt aufnehmen](#)
Website: www.gdata.de
Telefon: +49(0).234.9762.239

Schlagworte

- gdata
- schadcode
- aktuelle
- bedrohung
- viren
- computerviren
- computer

Permanenterlink

<http://www.themenportal.de/internet/webbas-angriffe-weiter-auf-dem-vormarsch-45612>

HTML:IFrame-U [Trj]

Ein schädliches JavaScript, das einen unsichtbaren iframe in eine Webseite integriert. Der schädliche Skriptcode zielt darauf ab, den Rechner des Seitenbesuchers zu infizieren.

Worm.Autorun.VHG

Bei diesem Schädling handelt es sich um einen Wurm, der sich mit Hilfe der autorun.inf Funktion auf Windows Betriebssystemen verbreitet. Er benutzt Wechseldatenträger, wie z.B. USB-Sticks oder mobile Festplatten. Er ist ein Internet- und Netzwerkurm und nutzt die Windows Schwachstelle CVE-2008-4250 aus.

HTML:Script-inf

Befindet sich auf einer Webseite ein schädliches Skript, so wird es als HTML:Script-inf erkannt und gemeldet. Eine Infektion kann das Resultat eines gehackten Servers sein. Verschlüsselter Code in einer Webseite kann diese Detektion ebenfalls auslösen, da die Verschlüsselung als verdächtig eingestuft wird.

HTML:RedirME-inf [Trj]

Webseiten, die einen Besucher unbemerkt zu möglicherweise unerwünschten und schädlichen Webseiten weiter leiten, lösen den Alarm RedirME-inf aus. Durch die Weiterleitung ist es unter anderem möglich, Klicks zu generieren, Werbung anzuzeigen oder Drive-by-Downloads durchzuführen.

Saturday 14th-669

Bei diesem Schädling handelt es sich um einen speicherresidenten Virus. Saturday 14th-669 schreibt sich selbst ans Ende von .exe und .com Dateien. Der Virus löscht Dateien von der Festplatte C:, am 14. eines jeden Monats.

Trojan.Autorun.EU

Dieser Schädling tritt in Zusammenhang mit Würmern auf, die auf die Autorun-Funktionen von Laufwerken zurückgreifen. Dazu wird eine Datei namens autorun.inf erzeugt, die einen Verweis auf das Schadprogramm enthält. Bei aktivierter Autorun-Funktion in Windows wird die Datei beim Öffnen des Laufwerks automatisch aktiv. Trojan.Autorun.EU wird so einerseits als Ersatz für einen Autostart-Eintrag in der Registry verwendet und sorgt dafür, dass der dazugehörige Wurm ausgeführt wird. Einige Exemplare kopieren sich auf Wechseldatenträger und verbreiten sich so.

Trojan.FakeAV.KZQ

Dieses Trojanische Pferd gibt sich als Anti-Virus Programm oder als ein anderes sicherheitsrelevantes Programm aus. Es simuliert die Entdeckung von mehreren Sicherheitsrisiken oder schädlichen Infektionen auf dem System des Benutzers. Dadurch soll der Nutzer ausgetrickst werden und für die Entfernung der gefälschten Alarme Geld bezahlen.

G Data Software AG

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. G Data ist damit eines der ältesten Securitysoftware-Unternehmen der Welt.

Das Produktportfolio umfasst Sicherheitslösungen für Endkunden, den Mittelstand und für Großunternehmen. G Data Security-Lösungen sind in weltweit mehr als 90 Ländern erhältlich.

Weitere Informationen zum Unternehmen und zu G Data Security-Lösungen finden Sie unter www.gdata.de

Herr Thorsten Urbanski

G Data Software AG
Königsallee 178b
44799 Bochum
Deutschland

E-Mail: [Kontakt aufnehmen](#)
Website: www.gdata.de



