

PRESSEMITTEILUNG

Stuxnet macht Schule: Ver mehrt LNK-Sicherheitslücken für Windows im Umlauf

Kaspersky Lab Top 20 der Schadprogramme, August 2010

Moskau/Ingolstadt, 1. September 2010 – Der Wurm Kido ist nach wie vor auf zahlreichen Anwendercomputern zu finden. Im Internet werden die Nutzer aktuell von vielen Exploits zu bereits bekannten Schwachstellen belästigt. Das zeigen die Kaspersky Lab Top 20 der Schadprogramme für August 2010. Die mit Hilfe des Kaspersky Security Network (KSN) gewonnenen Daten basieren auf Rückmeldungen der Heimanwender-Programme Kaspersky Anti-Virus und Kaspersky Internet Security. Aufgelistet werden zum einen die am weitesten verbreiteten Schad- und Werbeprogramme. Zum anderen zeigt die Aufstellung, mit welchen Schadprogrammen die Anwendercomputer am häufigsten infiziert waren.

Die erste Hitliste präsentiert die am weitesten verbreiteten Schad- und Werbeprogramme (Mal- und Adware), die die Computer der Anwender attackierten:

Position	Positionsänderung	Name
1	0	Net-Worm.Win32.Kido.ir
2	0	Virus.Win32.Sality.aa
3	0	Net-Worm.Win32.Kido.ih
4	0	Net-Worm.Win32.Kido.iq
5	+1	Trojan.JS.Agent.bhr
6	-1	Exploit.JS.Agent.bab
7	0	Worm.Win32.FlyStudio.cu
8	0	Virus.Win32.Virut.ce
9	Neu	Exploit.Win32.CVE-2010-2568.d
10	-1	Trojan-Downloader.Win32.VB.eq1
11	Neu	P2P-Worm.Win32.Palevo.arxz

12	Neu	Exploit.Win32.CVE-2010-2568.b
13	-3	Worm.Win32.Mabezat.b
14	Neu	Worm.Win32.VBNA.b
15	Neu	AdWare.WinLNK.Agent.a
16	Neu	Virus.Win32.Sality.ag
17	Neu	Trojan-Dropper.Win32.Sality.r
18	Neu	Trojan.Win32.Autoit.ci
19	-8	Trojan-Dropper.Win32.Flystud.yo
20	Neu	Packed.Win32.Krap.ao

Wie im Vormonat, bleiben die obersten Plätze der Top 20 bleiben bis auf einige Kleinigkeiten unverändert. Der Netzwurm Kido (1., 3. und 4. Platz) sowie die Viren Virut (8. Platz) und Sality (2. Platz) behaupten ihre Positionen mit Nachdruck. Dasselbe gilt für die Exploits, die die Sicherheitslücke CVE-2010-0806 ausnutzen: Trojan.JS.Agent.bhr und Exploit.JS.Agent.bab belegen die Plätze 5 und 6.

Sicherheitslücken in LNK-Dateien

Im Juli hat Kaspersky Lab bereits auf eine neue Sicherheitslücke in LNK-Dateien (Shortcuts) in Windows hingewiesen, die später die Bezeichnung CVE-2010-2568 erhielt. Wie vermutet, war diese Schwachstelle unter Cyberkriminellen sehr beliebt: Im August platzierten sich gleich drei Schädlinge im Monatsranking, die auf die eine oder andere Weise damit in Verbindung stehen. Zwei von ihnen – die Exploits Exploit.Win32.CVE-2010-2568.d (9. Platz) und Exploit.Win32.CVE-2010-2568.b (12. Platz), nutzten die Sicherheitslücke direkt aus. Der dritte Schädling, Trojan-Dropper.Win32.Sality.r (17. Platz), setzt die Schwachstelle zu seiner Verbreitung ein. Er generiert LNK-Shortcuts mit Bezeichnungen, die das Interesse des Anwenders wecken sollen, und verbreitet diese über das lokale Netz. Wenn der Anwender einen Ordner öffnet, der einen solchen Shortcut enthält, wird der Schädling gestartet. Hauptaufgabe von Trojan-Dropper.Win32.Sality.r ist die Installation der neuesten Modifikation des Schadprogramms Virus.Win32.Sality.ag (16. Platz) im System des Anwenders. Interessant ist, dass die beiden Exploits zur Schwachstelle CVE-2010-2568 am häufigsten auf Anwendercomputern in Russland, Indien und Brasilien entdeckt werden. Indien ist die Hauptverbreitungsquelle des Wurms Stuxnet (des ersten Schädlings, der

diese Sicherheitslücke ausnutzte), doch im Fall von Russland ist die Sache (noch) nicht so klar.

Die zweite Hitliste zeigt, mit welchen Schadprogrammen Anwender ihre PCs beim Surfen im Internet am häufigsten infiziert haben. Sie spiegelt also die Schädlingssituation im Internet wider:

Position	Positionsänderung	Name
1	Neu	Trojan-Downloader.Java.Agent.ft
2	-1	Exploit.JS.Agent.bab
3	+9	Exploit.HTML.CVE-2010-1885.a
4	+2	Trojan.JS.Agent.bhr
5	+4	AdWare.Win32.FunWeb.ds
6	Neu	Exploit.HTML.CVE-2010-1885.c
7	Neu	AdWare.Win32.FunWeb.di
8	-4	AdWare.Win32.FunWeb.q
9	Neu	Exploit.HTML.HCP.b
10	-6	Exploit.Java.CVE-2010-0886.a
11	-5	Trojan-Downloader.VBS.Agent.zs
12	+8	Trojan.JS.Redirector.cq
13	Neu	Trojan-Clicker.JS.Iframe.fq
14	+5	AdWare.Win32.FunWeb.ci
15	Neu	Exploit.Java.CVE-2010-0094.a
16	Neu	Exploit.JS.Pdfka.cop
17	Neu	Exploit.HTML.CVE-2010-1885.d
18	Neu	Exploit.JS.CVE-2010-0806.b
19	Neu	AdWare.Win32.FunWeb.fb
20	Neu	Exploit.HTML.CVE-2010-1885.b

Verglichen mit den vergangenen Monaten sehen wir im August viele Neueinsteiger – 10 Stück. Die meisten von ihnen sind neue Modifikationen von Exploits zu bereits

bekanntesten Schwachstellen. Insgesamt sind in den Top 20 zwölf Exploits vertreten, die zu sechs verschiedenen Sicherheitslücken gehören.

Exploits ohne Ende

Am beliebtesten unter den Cyberkriminellen war in diesem Monat die Schwachstelle CVE-2010-1885. Sie wurde von gleich fünf Exploits ausgenutzt. Zum Vergleich: In der Juli-Statistik war nur ein Exploit zu dieser Sicherheitslücke vertreten. Die Schwachstelle CVE-2010-1885 betrifft eine Unzulänglichkeit im Windows-Hilfe-Center („Windows Help and Support Center“) und ermöglicht die Ausführung von schädlichem Code auf den Systemen Windows XP und Windows 2003. Offensichtlich führte die Popularität dieser Systeme zum Anstieg der Exploits für diese Windows-Lücke.

Sehr beliebt ist auch die Sicherheitslücke CVE-2010-0806, die ihre Position vermutlich so bald nicht aufgeben wird. Sie wird von drei verschiedenen Exploits aus den Top 20 ausgenutzt, und zwar von drei Skripts, die bereits früher des Öfteren auftauchten: Exploit.JS.Agent.bab (2. Platz), Trojan.JS.Agent.bhr (4. Platz) und dem Neuzugang Exploit.JS.CVE-2010-0806.b auf Platz 18.

Drei weitere Exploits aus unseren Top-20 nutzen Sicherheitslücken in Software aus, die auf einer Java-Engine laufen. Den ersten Platz belegt im August Trojan-Downloader.Java.Agent.ft, der die recht alte Schwachstelle CVE-2009-3867 ausnutzt. Das Exploit.Java.CVE-2010-0886.a (10. Platz), das die Sicherheitslücke CVE-2010-0886 ausnutzt, war schon im Vormonat in den Top 20 vertreten. Interessant ist auch, dass im August das erste Exploit für die Sicherheitslücke CVE-2010-0094 aufgetaucht ist, die bereits im April 2010 entdeckt wurde.

Der Schädling Exploit.Java.CVE-2010-0094.a (15. Platz) führt eine Reihe von Funktionsaufrufen durch, die in der Folge zur Ausführung von schädlichem Code führen. Dieses Exploit wurde im August von Cyberkriminellen ausschließlich in Industrienationen eingesetzt – in den USA, in Deutschland und in Großbritannien. Das hängt vermutlich damit zusammen, dass in diesen Ländern Programme beliebt sind, die Java verwenden.

Kaspersky Lab ist Europas größtes Unternehmen für Antivirus-Technologie und reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Das Unternehmen gehört zu den weltweit vier erfolgreichsten Herstellern von Sicherheits-Lösungen für den Endpoint (IDC 2008). Die Produkte von Kaspersky Lab haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und kurzen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

Weitere Details zum Unternehmen sind unter www.kaspersky.de zu finden. Kurzinformationen von Kaspersky Lab erhalten Sie zudem über http://twitter.com/Kaspersky_DACH. Aktuelles zu Viren, Spyware und Spam sowie Informationen zu anderen IT-Sicherheitsproblemen und Trends sind unter www.viruslist.de abrufbar.

Redaktionskontakt:

essential media GmbH
Florian Schafroth
Florian.Schafroth@essentialmedia.de
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-843
Augustenstraße 24
80333 München

Kaspersky Labs GmbH
Christian Wirsig
christian.wirsig@kaspersky.de
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt

© 2010 Kaspersky Lab. The information contained herein is subject to change without notice. The only warranties for Kaspersky Lab products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Kaspersky Lab shall not be liable for technical or editorial errors or omissions contained herein.