

Botnetz via Twitter: Bei Cyberkriminellen immer beliebter

Web-2.0-Dienste werden für Kriminelle zunehmend lukrativ

Moskau/Ingolstadt, 20. Mai 2010 – Kaspersky Lab warnt vor dem Hackertool „TwitterNET Builder“, mit dem Cyberkriminelle Botnetze via Twitter steuern können. Derzeit sind zwei Varianten des Programms bekannt. Die erste erlaubt schädliche Kommandos mit statischen Namen, die zweite Version – entdeckt von Kaspersky Lab – erlaubt Nutzern des Microblogging-Dienstes, die Kommando-Namen zu ändern. Die Entdeckung von Twitter-Accounts, die Botnetze kontrollieren, wird so erschwert.

„TwitterNET Builder“ ermöglicht mit nur wenigen Mausklicks die Erstellung von Schadcode, mit dem infizierte Computer zu einem Botnetz zusammengeschlossen werden können. Die Zombie-Netzwerke werden über ein bei Twitter erstelltes Konto gesteuert. Die Botnetze können von Cyberkriminellen – wie üblich – zur Verbreitung von Spam oder für die Durchführung von DDoS-Attacken missbraucht werden.

„Der entdeckte Schadcode enthält keinen eigenen Verbreitungsmechanismus. Daher muss er manuell auf dem Computer des Opfers gestartet werden. Allerdings können diese Programme ausgeführt werden, wenn sie mit einer Drive-By-Attacke oder einem Wurm, der über eine neu gefundene Schwachstelle verbreitet wird, kombiniert werden“, erklärt David Jacoby, Senior Malware Analyst bei Kaspersky Lab.

Twitter bei Cyberkriminellen immer beliebter

Nach Angaben von Kaspersky Lab steht Twitter bei Cyberkriminellen zunehmend im Blickfeld. „Der Diebstahl von Twitter-Daten und die Veröffentlichung von schädlichen Links über Twitter hat seit Mitte März stark zugenommen. Wir sehen vermehrt Modelle, die darauf abzielen, aus den gestohlenen Daten Geld zu machen“, so Costin Raiu, Director des Global Research & Analysis Teams von Kaspersky Lab.

Aktuell werden in russischen Foren verseuchte Twitter-Konten für gutes Geld gehandelt. So werden für bis zu tausend infizierte Accounts zwischen 100 und 200 US-

Dollar gezahlt. Der Preis hängt von der Anzahl der Follower des jeweiligen Kontos ab. Die Infizierung erfolgt dabei nach zwei unterschiedlichen Mustern: Entweder stehlen Trojaner die Twitter-Daten direkt oder sie werden über gefälschte Berechtigungsanfragen gehischt. Haben Cyberkriminelle Zugang zu einem Twitter-Konto, können sie diese für die Verbreitung von schädlichen Mailings missbrauchen, oder schlichtweg verkaufen.

Twitter-Anwender sollten auch offiziellen Applikationen misstrauisch gegenüber stehen. So kann die neue iPhone-Applikation „Twitter for iPhone“ Cyberkriminellen Tür und Tor öffnen, um beispielsweise über eingeschleuste Trojaner Bankdaten zu stehlen. Wie der Trojaner dabei genau vorgeht, kann in einem Kaspersky-Blog-Beitrag eingesehen werden:

http://www.securelist.com/en/blog/2166/Twitter_for_iPhone_and_unexpected_malicious_results

Ein Blogbeitrag von David Jacoby zu diesem Thema kann in englischer Sprache unter http://www.securelist.com/en/blog/2163/New_tool_allows_script_kiddies_to_build_botnets_via_Twitter abgerufen werden. Weitere News zum Thema Internetbedrohungen gibt es im Analysten-Tagebuch unter: <http://www.viruslist.com/de/weblog>

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 <http://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.