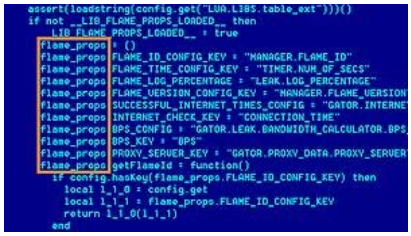
http://www.focus.de/digital/internet/tid-25952/stuxnet-nachfolger-die-fuenf-wichtigsten-fragen-zum-supervirus-flame-was-hat-der-supervirus-mit-stuxnet-zu-tun_aid_759556.html

Neuer Computerschädling

Die fünf wichtigsten Fragen zum Supervirus Flame

Dienstag, 29.05.2012, 16:01 · von FOCUS-Online-Redakteurin Claudia Frickel



Der Code des Computerschädlings Flame Kapersky

Er belauscht Computernutzer, protokolliert den Bildschirminhalt und verbreitet sich selbständig: Der Trojaner Flame ist so komplex wie kein anderes Schadprogramm bisher. Doch wen attackiert er und wer steckt dahinter?

Stuxnet, Duqu und nun Flame: Die Virenexperten von Kapersky Lab haben einen neuen Computerschädling entdeckt. Der Trojaner ist eine Art Werkzeugkasten mit zahlreichen Funktionen – und übertrifft sogar Stuxnet. Er greift Windows-Rechner an und treibt seit mindestens zwei Jahren sein Unwesen. „Flame ist extrem ungewöhnlich, in vielerlei Hinsicht“, sagt Kapersky-Experte Dimitri Bestuzhew gegenüber FOCUS Online.

Seine Firma beschreibt die Flame-Software so: „Wir können festhalten, dass Flame eine der komplexesten Gefahren ist, die je entdeckt wurde.“ FOCUS Online beantwortet auf den folgenden Seiten die wichtigsten Fragen zu Flame.

1. Was ist Flame?

dpa

Flame ist ein hochkomplexes Schadprogramm, von dem bereits mehrere Varianten existieren. Es handelt sich um einen Trojaner, der sich eigenständig duplizieren kann wie ein Computerwurm, so der Virenexperte Alex Gostev in einem Blogbeitrag von Kapersky Lab, die den Schädling entdeckt haben. Von einem befallenen Rechner aus kann sich der Trojaner in einem lokalen Netzwerk oder über Datenträger wie USB-Sticks oder CDs weiter ausbreiten.

Was genau in Flame steckt, ist nach Angaben von Kapersky sehr schwer zu analysieren. Bei dem Schadprogramm handelt es sich um ein „großes Paket von Modulen“, rund 20 Megabyte groß. Das ist ungewöhnlich für einen solchen Schädling: Normalerweise sind Trojaner eher klein, damit sie leicht übersehen werden. Doch Flame verbirgt sich zwischen großen Mengen von Programmcode. Und das Programm ist ein ganzer Werkzeugkasten: Die verschiedenen Module können die Angreifer sogar austauschen, je nachdem, für welchen Zweck sie den Schädling benutzen.

Zufällige Entdeckung

Flame wurde zufällig aufgespührt: Kaspersky Lab sollte einer UN-Organisation helfen, eine andere Schadsoftware zu identifizieren, die in mehreren Ländern im Nahen Osten Dateien löscht. Dabei stießen die Experten zufällig auf den Schädling Flame mit dem Code-Namen

„Worm.Win32.Flame“. Flame ist mindestens seit zwei Jahren aktiv, sicher seit März 2010. Entdeckt wurde es bisher nicht, weil es sehr komplex ist. Kapersky-Experte Dimitir Bestuzhew sagte gegenüber FOCUS Online: „Ein Grund für die späte Entdeckung ist auch, dass der Schädling ein Modul enthält, das sich selbst zerstören kann.“

2. Was kann der Supervirus?

dpa

Flame enthält viele verschiedene Module. Diese können je nach Verwendungszweck eingesetzt werden. Das macht Flame so gefährlich. Bisher wird er nach Analyse von Kapersky vor allem zur Überwachung benutzt.

Der Schädling greift beispielsweise auf die Mikrofone von Rechnern in einem Netzwerk zu und überträgt Gespräche. Ebenso kann er Skype- und andere Voice-over-IP-Unterhaltungen protokollieren. Die Ergebnisse überträgt Flame dann regelmäßig an die Cyber-Kriminellen. Außerdem kann Flame alles, was sich auf dem Monitor befindet, automatisch per Screenshot festhalten. Doch das Programm ist noch ausgefeilter: Nach Angaben von Kapersky macht es besonders viele Screenshots, wenn gerade bestimmte Programme verwendet werden, zum Beispiel Instant Messenger.

Zerstören statt überwachen?

Flame kann auch die Bluetooth-Schnittstelle nutzen: Ist Bluetooth aktiviert, erkennt der Schädling verbundene Geräte in der Nähe – und kann Informationen von dort auslesen. Außerdem kann er sich über USB-Sticks und im Netzwerk verbreiten.

Doch was Flame noch unberechenbarer macht ist, dass das Programm nicht nur für Spionage eingesetzt werden kann. Durch den Modulaufbau könnte der Schädling laut Experte Bestuzhev künftig auch verwendet werden, „Um nicht nur Rechner auszuspionieren, sondern auch um Dateien zu zerstören.“

3. Wer ist von Flame betroffen?

IT-Experten haben einen neuen, hochkomplexen Computervirus entdeckt

Colourbox

Nach Angaben von Kapersky sind 5000 Computer mit Flame infiziert, bisher wohl nur im Nahen Osten. Der Trojaner wurde vor allem im Iran (189 Fälle) eingesetzt, aber auch in Israel/Palästina (98 Fälle), im Sudan (32), Syrien (30), Libanon (18) und Saudi-Arabien (10). Der Schädling treibt bisher offenbar überwiegend auf Computern von Unternehmen und Bildungseinrichtungen sein Unwesen, nicht bei Privatpersonen. Das heißt aber nicht, dass ganz normale Internetuser gar nicht ins Visier des Supervirus geraten können.

Flame kann auch Internetuser treffen

Kapersky-Experte Bestuzhew sagte dazu gegenüber FOCUS Online: „Flame wurde entwickelt, um die Industrie anzugreifen. Die Macher haben kein Interesse daran, Konsumenten zu attackieren. Allerdings könnte der Trojaner sehr wohl auch gegen jeden normalen Rechner eingesetzt werden.“

Internetnutzer müssen sich nach seinen Angaben nicht besonders gegen

Flame schützen – es sei denn, sie arbeiten für eine Firma im Nahen Osten. Doch „ein Schutz gegen solche Angriffe ist unbedingt nötig“, so Bestuzhew. User sollten also immer ihre Antivirenpogramme auf dem aktuellen Stand halten.

4. Wer steckt hinter Flame?

Die Urheber von Flame sind unbekannt – genauso wie bei Stuxnet und Duqu. Allerdings hat Kapersky im Ausschlussverfahren einen Verdacht entwickelt: Es gebe grundsätzlich drei Gruppen, die Computerschädlinge entwickelten – Hacker, Cyberkriminelle und Staaten. Doch Flame werde nicht benutzt, um Bankkonten zu plündern. Der Programmiercode sei im Vergleich zu Hacker-Tools außerdem extrem komplex.

Wenn man Cyberkriminelle und Hacker ausschließe, „kommt man zu dem Schluss, dass am wahrscheinlichsten die dritte Gruppe dahintersteckt.“ Auch die angegriffenen Länder, die vorwiegend zum Nahen Osten gehören, würden dafür sprechen, dass ein Staat die Entwicklung von Flame „gesponsort“ habe. Es gebe allerdings keinerlei Hinweise im Code, die auf ein bestimmtes Land hindeuteten.

5. Ist der Supervirus mit Stuxnet verwandt?

Colourbox

Der Supervirus Flame steht nach Expertenansicht in einer Reihe mit Schädlingen wie Stuxnet und Duqu. Auch bei diesen beiden handelt es sich um gefährliche Software zur Industriespionage. Doch der Programmcode von Flame hat einen anderen Ursprung. Nach Angaben von Kapersky basieren diese beiden Trojaner auf einer Softweare namens „Tilded-Plattform“, Flame aber nicht. Er ist demnach kein „Cousin“ dieser Schädlinge.

Der Programmcode von Flame ist 20mal größer als der von Stuxnet. Außerdem ist Flame offenbar schon jetzt sehr viel weiter verbreitet als Duqu.

Ein Unterschied zwischen den Superschädlingen ist auch das System, das sie befallen: Flame attackiert Windows-Rechner, auch Windows-7-Infektionen wurden festgestellt. **Stuxnet** dagegen greift nur ein bestimmtes Siemens-System an. Der im Juni 2010 entdeckte Virus wurde wohl vorwiegend zur Sabotage der Urananreicherung in Atomanlagen im Iran benutzt. **Duqu** ist der im Herbst 2011 entdeckte Nachfolger von Stuxnet.