Fireball: Tracking-Netzwerk könnte zum Malware-Alptraum werden

Sicherheitsforscher von Check Point haben eine von China ausgehende Operation gründlich untersucht, der sie enormes Gefahrenpotenzial bescheinigen. Bereits jetzt seien weltweit 250 Millionen Computer mit der darüber verbreiteten, Fireball genannten, Software infiziert. Die hat zwei Funktionen: Zum einen kann sie den Web-Traffic des Nutzers kapern und manipulieren, um so auf betrügerische Art und Weise Anzeigenumsätze zu generieren. Wesentlich schlimmer ist aber, dass sie zudem genutzt werden kann, um auf dem Rechner des Opfers jedweden Code auszuführen sowie jede von den Hintermännern gewünschte Datei oder Malware herunterladen kann.

Für die Operation macht Check Point die Firma Rafotech verantwortlich, eine Digitalmarketingagentur aus Peking. Rafotech nutze Fireball, um die Browser seiner Opfer zu manipulieren, so dass diese Fake-Suchmaschinen und Startseiten aufrufen. Die leiten Anfragen direkt zu yahoo.com oder google.com weiter. Zweck der Fake-Suchmaschinen ist es lediglich, Tracking-Pixel zu verbreiten, mit dem dann die unfreiwilligen Nutzer verfolgt werden können.

Bis dahin ist das Vorgehen zwar etwas unfeiner als bei bekannten europäischen Digitalmarketingagenturen, im Ergebnis aber nicht wesentlich anders. Richtig bedenklich wird es allerdings dadurch, dass Fireball Opfer nicht nur ausspionieren, sondern auch Malware auf deren Rechnern platzieren kann und es der Software möglich ist, jedweden bösartigen Code auf infizierte Maschinen zu schleusen: So entsteht laut Check Point eine erhebliche Gefahr für betroffene Rechner und die Netzwerke, in denen sie sich befinden.

Den Untersuchungsergebnissen von Check Point zufolge sind die 250 Millionen mit Fireball infizierten Computer nahezu überall auf der Welt verteilt, wo es etwas zu holen gibt: Auffällige Ausnahmen sind lediglich die Länder der Sahelzone sowie der Iran und fast alle seine Nachbarländer. Am stärksten betroffen seien Indien und Brasilien, aber auch in europäischen Ländern scheint Fireball weit verbreitet zu sein. In Deutschland beispielsweise sei in 9,75 Prozent der Unternehmensnetzwerke mindestens ein PC mit der Malware gefunden worden.

Verbreitet wird Fireball den Sicherheitsforschern zufolge überwiegend als zusätzlicher Download zu einer anderen Software. Auch da überschreiten die Hintermänner lediglich eine Grenze, an die sich

auch große und etablierte Firmen nahe heranwagen, wenn sie zusammen mit Updates für ihre Software mittels standardmäßig gesetztem Häkchen im Download-Dialog Programme von Drittanbietern verteilen.

Besondere Gefahr in Bezug auf Fireball besteht bei dem ebenfalls von Rafotech angebotenen Browser Mustang, der als besonders schnell beworben wird, sowie dem schon länger als Adware bekanntem Programm Deal WiFi, das kostenloses WLAN überall verspricht.

Ebenso wie andere Adware-Verbreiter agiert Rafotech nicht wirklich im Untergrund: Auf seiner Website wirbt das Unternehmen offensiv damit, dass es weltweit 300 Millionen User erreicht und dafür auch Server in Deutschland, Italien, Spanien und Polen betreibt. Außerdem hat Rafotech zumindest vier SPiele entwickelt, die es offenbar mit einigem Erfolg über Google Play und in Apples App Store anbietet: Piggy Boom, Casual Warrior, Cutie Riot und Cutie Clash. Möglicherweise dienen die aber auch in erster Linie dazu, Nutzerinformationen einzusammeln.

Check Point sieht Fireball und ähnliche Browser-Hijacker als eine Art Hybrid-Schöpfungen: Einerseits bewegen sie sich ganz knapp an der Grenze des Erlaubten, andererseits sind sie schon Malware. Auf jeden Fall seien sie eine enorme Gefahr. Denn obwohl keine Anzeichen vorliegen, dass Rafotech das Potenzial für kriminelle Aktivitäten bereits ausnutzt, sei es doch gegeben und könnte jederzeit aktiviert werden.

Im Vergleich zu anderen Browser-Hijackern sei Fireball zudem sehr ausgereift und verwende ausgefeilte Techniken, um eine Entdeckung zu verhindern. Diesbezüglich sei es einer typischen Malware durchaus ebenbürtig und biete eine als kritisch einzustufende Hintertür auf das System, die nach Belieben ausgenutzt werden könne.

“Rafotech hat die Macht, eine weltweite Katastrophe auszulösen, ist aber nicht alleine damit. Bei unseren Forschungen haben wir andere Browser-Hijacker gefunden, die unserem Verständnis nach von anderen Urhebern entwickelt wurden. Eine davon ist ELEX Technology, ein Internet Service Anbieter, der ebenfalls in Peking ansässig ist und vergleichbare Produkte wie Rafotech entwickelt. Es gibt Hinweise darauf, dass beiden Firmen Verbindungen zueinander haben”, so Check Point.

Tipp: Wie gut kennen Sie die Geschichte der Computer-Viren? Überprüfen Sie Ihr Wissen – mit 15 Fragen auf silicon.de.