Malware Nodersok befällt Tausende PCs

01.10.2019, 17:32 Uhr

Derzeit treibt eine neue Schadsoftware ihr Unwesen, die sich für Sicherheitsprogramme unsichtbar im Arbeitsspeicher einnistet. Welches Ziel die Angreifer mit Nodersok (Microsoft) beziehungsweise Divergent (Cisco) verfolgen, scheint aktuell unklar.

Über verseuchte Werbeanzeigen verteilen Angreifer unbemerkt Schadcode in den Arbeitsspeicher Tausender PCs. Doch die Experten von Microsoft und Cisco sind den Gaunern auf der Spur.

Mit Sicherheitsteams von Microsoft und Cisco sind gleich zwei Tech-Konzerne auf ein und dieselbe Malware aufmerksam geworden. Der Schädling hat in den vergangenen Wochen Tausende Rechner vorwiegend in den USA und Europa befallen und soll bereits seit Juli 2019 aktiv sein. Dass die Malware so lange unbemerkt blieb, erklären die Sicherheitsexperten damit, dass die Schadsoftware lediglich im Arbeitsspeicher agiert und ohne ausführbare Dateien auskommt – ein bislang blinder Fleck für die einschlägigen Sicherheitsprogramme. Die von Microsoft auf Nodersok und von Cisco auf Divergent getaufte Malware verbreitet sich über manipulierte Werbeanzeigen (Malvertising) auf regulären Webseiten.

Schadsoftware im Arbeitsspeicher

Über die Anzeigen gelangt ganz unbemerkt ein verschlüsseltes Skript in den Arbeitsspeicher. Laut der Analyse von Microsoft deaktiviert das Skript mithilfe der Kommandzeile (Powershell) den Windows Defender und lädt anschließend Node.js-Framework, also eine Art eigene Programmumgebung, die JavaScript-Befehle ausführen kann, in den Speicher. Auf

dieser Basis lädt der Schädling einige OpenSource-Tools nach und mutiert so zum vollwertigen Proxy-Server, der anschließend für verschiedenste Schandtaten bereitsteht.

Klickbetrug und Botnet: Angriff aus dem Hinterhalt

Aber welche Ziele verfolgen die Angreifer? Dazu haben Microsoft und Cisco unterschiedliche Antworten. So nehmen die Sicherheitsexperten von Cisco an, die Angreifer nutzten den virtuellen Proxy-Server, um darüber automatisierte Klicks auf Werbeanzeigen zu generieren und so Werbevergütungen im großen Stil abzugreifen. Möglicherweise steckt aber auch mehr dahinter. So fanden die Experten auch Hinweise auf die Integration weiterer Tools wie etwa Fernsteuerungssoftware. Die Microsoft-Experten hingegen sind der Überzeugung, dass über den Proxy-Server weitere Schadsoftware verteilt wird oder dieser als Teil eines größeren Botnetzes dienen soll.

Die größten Bedrohungen für Ihre Sicherheit

16 Gefahren

Zur Bildergalerie

Rechner aus, Malware gelöscht

Eine weitere Besonderheit von Nodersok beziehungsweise Divergent: Wird der Computer ausgeschaltet, verschwindet der Schadcode. Da sich die Malware lediglich im nicht persistenten Arbeitsspeicher rumtreibt, hat sie keine Möglichkeit, sich dauerhaft auf dem PC einzunisten. Das muss aber kein Nachteil für die Angreifer sein, dann so hinterlassen sie weniger Spuren und stellen sicher, dass stets nur aktuelle Varianten ihres Schadcodes im Einsatz sind. Nach den Enthüllungen von Microsoft und Cisco dürften es die Angreifer aber demnächst schwerer haben. Denn beide Hersteller kündigten an, ihre Sicherheitsprogramme entsprechend anzupassen, um den Schädling sofort zu erkennen. Auch weitere Anbieter dürften mit entsprechenden Updates ihrer Antiviren-Datenbanken folgen.