Update zwecklos

"AtomBombing" bedroht alle Windows-Versionen

28.10.2016, 15:54 Uhr | yba, t-online.de

Sicherheitsforscher warnen vor einer massiven Schwachstelle in allen Windows-Versionen. Laut dem Bericht können weder Antiviren-Programme noch Windows-Updates vor der Attacke schützen. Denn es handele sich um keine Sicherheitslücke, sondern um eine Windows-eigene Funktion.

"It's not a bug, it's a feature", witzeln Technik-affine Menschen gerne, wenn sich ein vermeintlicher Programmfehler als integrale Funktion herausstellt. Sollten die Sicherheitsforscher des Unternehmens Ensilo recht haben, ist der auf den Namen "AtomBombing" getaufte Hackerangriff aber alles andere als witzig.

Demnach können Angreifer die Windows-Funktion Atom Tables ausnutzen, um beliebigen Schadcode auf fremde Rechner zu schmuggeln. Über die Funktion können Anwendungen wie zum Beispiel Browser und Media Player Daten untereinander austauschen. Die Atom Tables dienen sozusagen als Datenhafen für Programme.

AtomBombing beim Online-Banking

Hacker könnten den Datenfluss eines legitimen Programms aber kapern und mit Schadcode ergänzen, erklärt der Ensilo-Mitarbeiter Tal Liberman auf dem Blog "Breakingmalware". Sei der Angriff erfolgreich, können die Hacker Passwörter abgreifen, den Bildschirm

abfotografieren oder Daten während des Online-Bankings manipulieren. Für das Opfer sehe alles ganz normal aus, tatsächlich lande die Überweisung aber auf dem Konto eines Dritten, warnt Ensilo.

Je nach laufender Anwendung und Schadcode sind weitere Angriffsszenarien denkbar. Virenwächter schlagen laut dem Unternehmen – zumindest derzeit – nicht an, da es sich um legitime Windows-Prozesse handelt. Auch heuristische Scanner, die auch ohne Virensignaturen Auffälligkeiten anhand ihrer Struktur erkennen können, laufen folglich ins Leere. Liberman testete AtomBombing nach eigenen Angaben erfolgreich mit dem Google-Browser Chrome und dem Mediaplayer VLC. Zu Testzwecken ließ er die beiden Programme den Windows-Taschenrechner starten.

Wie kann man sich schützen?

Wenn Virenwächter und Sicherheitsupdates nicht mehr helfen, bleibt nur noch der gesunden Menschenverstand. AtomBombing funktioniert anscheinend nur, wenn der Nutzer zuvor schädliche Dateien geöffnet oder Browser-Plug-ins installiert hat. Ensilo drückt sich diesbezüglich leider nicht genau aus.

Auf Anfrage von t-online.de wurde AtomBombing von Microsoft weder bestätigt noch dementiert. Der Konzern rät lediglich zu allgemeinen Schutzmaßnahmen, die Nutzer ergreifen sollten:

"Um sich bestmöglich vor Schadsoftware zu schützen, bedarf es neben modernster Technik auch der Aufmerksamkeit des Nutzers: Anwendern sollte klar sein, dass ein Großteil der Angriffe via Social Engineering erfolgt. Aus diesem Grund empfiehlt Microsoft seinen Kunden, nicht nur das Betriebssystem und Anwendungen auf dem neuesten Stand zu halten, sondern sich auch bezüglich potentieller Gefahren bei der Computernutzung zu sensibilisieren und eigene Aktionen stets zu hinterfragen – ob beim Klicken auf Links, beim Öffnen unbekannter Dateien oder auch bei der Datenübertragung. Microsoft bietet Kunden umfassende Informationen zum Schutz vor Malware im Malware Protection Center sowie unter microsoft.com/protect/pc."