Sicherheitsmeldung: Generich PUA FF detection in DARWINDUMPER.APP !

Beitrag von „Ghostbuster“ vom 5. Dezember 2016, 17:47

@Patricksworld
Das removel-Tool greift wohl unter Windows bzw. war nur Recherche hatte ich nicht geprüft. Bei mir wurde der Alarm schon im Gateway erkannt, habe ihn dann trotzdem durchgelassen um zu testen ob mein Mac das auch selbst findet. Beides wurde ja von Sophos geschützt.

Gute Frage woher ich den "DarwinDumper" damals geladen hatte... aber nachdem ja CleanMyMac den Code im letzten Update mir einbringen wollte, schätz ich mal das hier der Hersteller selbst gehackt wurde um den Mist zu verteilen. So wird das ja heute immer gemacht... Angriffe und Schadenscode wird immer von Dritten verteilt die Ansicht seriös und sicher eingeschätzt werden, sonst bekommt man ja eh keinen Zugriff. Dumm sind die schon lange nicht mehr oder noch nie gewesen.

> Zitat von lupotmac
>
> Mit Anti-Viren Programmen ists immer so ne Sache. Richtig eingesetzt können sie sinnvoll wirken, ansonsten können die Programme u.U. sogar selbst zur Gefahr werden. Ich habe mal vor einiger Zeit einen Artikel gelesen, in dem erklärt wurde, warum man auf Mac normalerweise keine Firewall benutzen sollte, weil diese selbst zum Risiko werden kann.

Mus ich hier mal bei mir aufklären. Ich habe unten ein "Sophos Security Gateway" in Betrieb, auf dem Mac die AV-Lösung von denen und zusätzlich den Kleinen-Snitch. Beruflich verwalte ich die Firewall beim LKA und bin Datenschutzbeauftragter. Also ist das ganze für mich privat wie beruflich ein Steppenpferd.

Mein Beitrag war lediglich eine Information an euch... bei mir hat das Gateway schon allarm geschlagen, dies hatte ich dann erlaubt um zu schauen wo es bei meinem Client landet da ich zu faul war das Datenpaket zu analysieren.

@Ploker

> Zitat von Plonker
>
> Habe ich das richtig verstanden: Durch einen Zugriff von Außen wurde der Inhalt einer Datei im Filesystem deines Macs verändert????
> Oder beinhaltet DarwinDumper einen Schadenscode?

Aufklärung. Die App: CleanMyMac 3, bei mir die Vollversion... hat in die Anwendung von "DarwinDumper" beim aktualisieren versucht mir den Schadenscode einzuspielen. Wie und warum der eine es im anderen Versucht hat weis ich nicht. Ich könnte jetzt mal im Security-Gateway rein schauen wo das initialisiert wurde. Meine Erfahrung sagt aber, das hier sicher CleanMyMac nicht der Urheber sondern der Wirt für diese Attacke darstellt und das ganze von DarwinDumper ausgelöst wurde.. Vermutung... daher, wer eine AV von Sophos in der aktuellen freien Variante nutzt hat kein Problem, selbst dieser verhindert dieses tuneling zuverlässig.

Ich wollte nur informieren und mal wieder aufzeigen wie auch in der Mac-Welt Angriffe im Moment erfolgen. Wir sind schon lange nicht mehr sicher, bzw. auch der Mac-Benutzer sollte sich zusätzlich schützen. Wer denkt es betrifft ihn nicht ist schon lange hinter her... entschuldigt, aber Sicherheit betrifft auch den einzelnen Computer.

Ich danke Sophos das sie uns den Schutz anbieten, das auch inzwischen für Windows kostenfrei erfolgt und die Nachteile der Datensammlung im Hintergrund erfolgt sowieso, warum dann nicht auch profitieren.

Egal... entscheidet selber... Ober nur mal Mitgeteilt!