Sicherheitsmeldung: Generich PUA FF detection in DARWINDUMPER.APP !

Beitrag von „Ghostbuster“ vom 5. Dezember 2016, 14:13

Wie gerade bemerkt versuchte man mir den "PUA Generic" einzuschmuggeln. War aber nichts! Hier zur Info sowie ein Tool zum entfernen für Betroffene und - Nicht geht über eine AV-Schutz auch unter OSX.

https://www.sophos.com/en-us/t...ruses-and-spyware/Generic PUA FF/detailed-analysis.aspx

---

Beitrag von „Patricksworld“ vom 5. Dezember 2016, 15:52

> Zitat von Ghostbuster
>
> Nicht geht über eine AV-Schutz auch unter OSX.

Nichts geht über Scriptblocker. Aktuelle Browser, sichere/seriöse Webseiten und open source Software 😛

Das ist doch ein Hauptgrund warum man linux und OSX nutzt. Die Virenscanner bringen nur falsche Sicherheit.
Also auf meine Kiste kommt mit Sicherheit nicht so ein Quatsch wie einen Virenscanner.

Beitrag von „Ghostbuster“ vom 5. Dezember 2016, 15:57

Hey.. Dicker.. nicht gleich so unwissend losschießten, Sophos macht einen Guten Jop. Wenn dem nicht so wäre könnt ich meine Arbeit an den Nagel hängen. Aber ein guter Skript-Blocker als Plugin, oder, empfiehlt sich. Welchen hast du im Einsatz?!

PS: Das war eine OSX Angriff, erst in meiner Firewall geloggt und dann am Client eingefangen.

Beitrag von „Patricksworld“ vom 5. Dezember 2016, 16:03

Hey Dünner 

Ich selber benutze noscript. Da muss man allerdings halt immer selber entscheiden, was man denn für scripte benötigt und welche nicht. Von daher installiere ich allein Freunden und bekannten ghostery. Außerdem habe ich auch das automatische Ausführen von Plugins deaktiviert. Aber wie gesagt. Virenscanner unter OSX finde ich immernoch Quatsch.
Da kann man lieber mal alle seine Ports und co kontrollieren wenn man da so ängstlich ist.

Aber das kann ja jeder für sich entscheiden. 

War nicht böse gemeint großer 

Beitrag von „Ghostbuster“ vom 5. Dezember 2016, 16:07

Von mir auch nicht!

Super, also ich hab mit noscript noch keine Erfahrungen, werde mich hier weiter bilden und anchecken. Welche Source kann ich nutzen um nicht direkt an falscher Stelle zu laden..?

Gesendet von iPhone mit Tapatalk

Beitrag von „connectit“ vom 5. Dezember 2016, 16:19

NoScript ist aber viele Sachen mMn. zu heavy...
Macht die Bedienung nur schwieriger 

Beitrag von „lupotmac“ vom 5. Dezember 2016, 16:33

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.

Beitrag von „Patricksworld“ vom 5. Dezember 2016, 16:35

> Zitat von connectit
>
> NoScript ist aber viele Sachen mMn. zu heavy...

Deswegen habe ich ja gesagt das ich Freunden und bekannten immer nur ghostery installiere. Noscript ist schon eher was für Fortgeschrittene da es bedingslos alles blockiert und Anfänger dann wieder alles freigeben. Das würde wiederum nichts bringen.

Aber einmal noscript richtig eingerichtet, passt das dann schon.

@Ghostbuster

Ich nutze chrome (mit ghostery) und firefox (mit noscript) als browser. Da ist das im offiziellen Store bei Erweiterungen dabei. Das heißt, alle "Erwachsenen Seiten" wo ich so meine Bedenken habe nutze ich Firefox. Für die Sicheren normalen seiten halt chrome. Außerdem weiß dann wenigstens nicht google auch noch, "auf was ich so stehe" 

MFG Patrick

EDIT:

> Zitat von lupotmac
>
> warum man auf Mac normalerweise keine Firewall benutzen sollte, weil diese selbst zum Risiko werden kann

Stimme ich auch zu. Also Softwarefirewalls! Ne Hardwarefirewall sollte schon jeder im router drin haben und möglichst nur die nötigen/sinnvollen Ports geöffnet halten.

Beitrag von „Plonker“ vom 5. Dezember 2016, 16:35

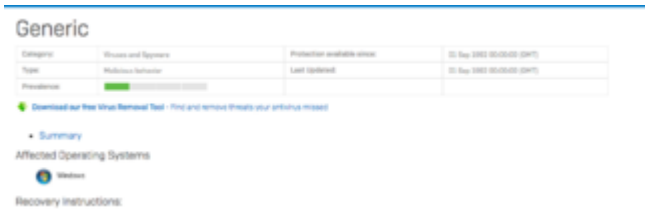
Habe ich das richtig verstanden: Durch einen Zugriff von Außen wurde der Inhalt einer Datei im Filesystem deines Macs verändert????
Oder beinhaltet DarwinDumper einen Schadenscode?

Beitrag von „Patricksworld“ vom 5. Dezember 2016, 16:42

> Zitat von Ghostbuster
>
> sophos.com/en-us/threat-center…ruses-and-spyware/Generic PUA FF/detailed-analysis.aspx

OMG. Den Link hab ich jetzt erst angeklickt.

Hast du den Selber mal Überprüft? Hier mal einen Screenshot. Finde den Fehler. Oder ist dein link der Falsche?



Denn sonst ist das wie ein Virenscanner für Linux. Die suchen schadhafte Windowsdateien um die Win PC's zu schützen. Nicht sich selbst.

MFG Patrick

EDIT: Und @Ghostbuster von welcher Seriösen Quelle hast du denn die Datei geladen?

Ich muss gestehen das es mitlerweiler ziemlich viele gute Fakes gibt. Eines der Besten ist vlc.de Die bringen den Vlc-Player mit bloatware.

vlc.org wäre die orignale seite.

Das ist wohl für Anfänger scheinbar nicht immer klar.

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!

Beitrag von „al6042“ vom 5. Dezember 2016, 21:48

Ich nutze hier "Avast Mac Security 2016" und habe den DarwinDumper im "Programme"-Ordner...

Der spricht auch darauf an... ist halt nur die Frage ob man den integrierten Kext "DirectHW" tatsächlich als Malware/Trojaner bezeichnen muss oder ob es sich hier nur um einen Sicherheitsmechanismus handelt, der bei Original-Apple-Geräten halt sinnvollerweise halt anschlagen würde, da dort so ein Programm nicht genutzt werden muss, während die Hardware/System-nahe-Abfrage für Hackis unter Umständen wichtig ist.
Ich gehe davon aus, dass dies als sogenannter "False-Positive" gewertet werden kann.

Beitrag von „Ghostbuster“ vom 6. Dezember 2016, 19:12

Das Unangenehme ist nur versucht wurde den Exploide einzuspielen.
Wäre es eine Aktualisierung der App selbst gewesen hätte ich mir das sogar gefallen lassen, aber diesen über eine Dritte zu integrieren zweigt mir das es sich hier nicht nur um eine Integration handelt.

Oft wird Code erkannt der funktional benutzt wird, das ist richtig.. aber warum nicht sauber integrieren sondern heimlich einschleusen?