Erledigt Viren und Trojaner auf dem Hacki

Beitrag von „p100656“ vom 25. November 2018, 12:51

Hallo Community,

am Donnerstag habe ich mir auf einer Site eines Streaminganbieters für Live-Fernsehen auf dem Häcki 3 Trojaner eingefangen. Das meinte zumindest der Häcki unter lautem Gepiepse. Unmöglich, wie manche glauben machen möchten (und ich bis jetzt auch), ist das wohl doch nicht. Ich habe den Häcki aus einer OfflineSicherung wieder herstellen können. Die Gefahr ist also vorüber. Aber nun meine Frage: Ich habe noch eine Norton Security-Lizenz übrig. Ist dieses Produkt auch für OS X empfehlenswert?

Grüße

Holger

Beitrag von „Higgins12“ vom 25. November 2018, 12:58

Streaminganbieter ---->>>>> Joa Ich persönlich, habe weder auf meinem Hack noch auf der M$ installation seit X Jahren einen Virus/Trojaner gesehen. (3x auf Holz Klopf) bisher kam hier noch nix dergleichen durch. Wird und wurde glücklicherweise immer alles abgefangen Firewall -> SquidProxy -> PfBlocker -> ClamAV. Mein Schwager fängt sich die Dinger allerdings im Minutentakt ein. Für den sind auch Virenscanner ein völlig neuer Begriff. Da war schon alles dabei und ich muss dann immer dahin juckeln um seine Maschinen zu fixen.

Norton? Ernsthaft? Igitt Malwarebytes. Wenn Du auf Softwarelösung angewiesen bist.

Beitrag von „CMMChris“ vom 25. November 2018, 14:52

Moment, der Hacki meint von selbst unter lautem Gepiepse, dass du dir 3 Trojaner eingefangen has? Also bitte... da wirst du auf so ein typisches Scam Pop-Up reingefallen sein.

Beitrag von „p100656“ vom 25. November 2018, 16:22

Ja, so war's, Ich war auswärts und wollte auf pro7maxx das Thanksgiving Spiel in der NFL ansehen. Hab mir eine Streaming-Site gesucht die Pro7maxx angeboten hat und dann hat das Ding losgepiepst und was von 3 Trojanern gefaselt, hat sie aufgezählt und angefangen ein cleaner.dmg runterzuladen. Dann hab ich ihn fix ausgeschalten und erst nach dem Restore des Backups wieder angeknipst.

Beitrag von „Sascha_77“ vom 25. November 2018, 16:24

Ganz klar Fake. Piepen lassen (bzw. das wos piept schliessen) und weitermache. Auf KEINEN Fall so ein angebotenes dmg runterladen. Damit hast du am Ende dann echt was aufm Rechner!

Beitrag von „Higgins12“ vom 25. November 2018, 16:54

Na wenn schon was automatisch runtergelaufen wird, dann gehen doch alle Alarmlampen an  ProSiebenMaxx streamt doch direkt soweit ich weiß. Aber wer schaut denn die NFL mit den behämmerten deutschen Kommentaren, die nicht einmal während der Schiri Calls den Sabbel halten können?  ... nur so am Rande. Besser gleich NFL Gamepass. Oder das Original ...

Beitrag von „p100656“ vom 25. November 2018, 17:00

na ok, wenn Ihr meint. Aber dennoch die Frage, losgelöst von diesem Ereignis im Lichte heute

also 2018: Ist Virenüberwachung auf OS X nötig oder nicht? Ich meine, ich will jetzt auch nicht jedes Suchmaschinenergebnis erst extern untersuchen lassen. Auf Windows erledigt das halt ein Virenscanner. Was also - außer elitärem Gehabe - spricht dagegen, auch auf OS X einen Scanner einzusetzen? Gut, OS X ist UNIX-artig. Deshalb schon ist es schwierig, aber der angemeldete Account ist ja meist auch ein Admin-Account und irgendwann, man muss nur im Hintergrund lange genug zuhören, fällt einem schon das Passwort (bei sudo z.B:) in die Hände. Und dann Gute Nacht Häcki.

Beitrag von „Higgins12“ vom 25. November 2018, 17:03

Viren und Trojaner gibt es auch für OSX mit steigender Beliebtheit eines OS dann auch immer mehr. Nicht in dem Umfang wie für Windoof aber genug. Schutz ist immer gut, in welchem Umfang muss jeder selber wissen.

Beitrag von „p100656“ vom 25. November 2018, 17:03

Higgins12: Direkt streamen kann man Pro7maxx nur mit deutscher IP. Wenn man gerade im Ausland ist und keinen Proxy hat wird das nix.

Beitrag von „user232“ vom 25. November 2018, 17:09

Bitdefender kann man mit der **kostenlosen Version** aus dem Appstore ruhig mal durchlaufen lassen.

Beitrag von „al6042“ vom 25. November 2018, 17:20

Selbst wenn es weniger Viren oder Trojaner für macOS gibt, ist man als Weiter-Verarbeiter für Dateien, Mails oder Links für andere Windows-User ggf. als Viren-Schleuder aktiv und dass

empfinde ich als verantwortungslos.

Deswegen läuft auf all meinen Büchsen auch der Avast in der kostenlosen Version mit.

Beitrag von „Higgins12“ vom 25. November 2018, 17:41

Bei solchen Sachen wie automatische Downloads hilft oft auch schon ein Adblocker. AdGuard macht da einen guten Job wenn man nicht auf pihole oder ähnliches zurückgreifen kann oder will.

Beitrag von „Holz_Michel“ vom 25. November 2018, 20:11

> Zitat von p100656
>
> na ok, wenn Ihr meint. Aber dennoch die Frage, losgelöst von diesem Ereignis im Lichte heute also 2018: Ist Virenüberwachung auf OS X nötig oder nicht? Ich meine, ich will jetzt auch nicht jedes Suchmaschinenergebnis erst extern untersuchen lassen. Auf Windows erledigt das halt ein Virenscanner. Was also - außer elitärem Gehabe - spricht dagegen, auch auf OS X einen Scanner einzusetzen? Gut, OS X ist UNIX-artig. Deshalb schon ist es schwierig, aber der angemeldete Account ist ja meist auch ein Admin-Account und irgendwann, man muss nur im Hintergrund lange genug zuhören, fällt einem schon das Passwort (bei sudo z.B:) in die Hände. Und dann Gute Nacht Häcki.

Da wärst du jetzt der erste von dem ich höre, dass er auf dem Mac als Admin User unterwegs ist Normal ist der erste Schritt nach der Installation genau wie in Linux sofort einen neuen Benutzer ohne Admin Rechte zu erstellen. Never be root if you don´t need to be root.

Beitrag von „Nio82“ vom 25. November 2018, 20:40

@p100656

Das wichtigste Antivirus Tool ist & bleibt Brain.exe, unter MacOS Brain.app.

 Ist die nicht aktive, nutzt auch das beste AV Prog nichts, egal wie groß oder wie viel es kostet!

Es gibt sogar Viren/Trojaner, die AV Progs als Einfallstor/Angriffspunkt nutzen. Den diese haben ja meist hohe System Rechte & diese will die Schadsoftware ja in der Regel haben. 

Wichtig ist eine gut Hardware und/oder Software Firewall. Dann noch für den/die genutzten Browser ein guter ScriptBlocker. Früher nutzte ich NoScript, heute uMatrix. Die meiste Schadsoftware kommt nunmal über den Browser & es ist besser diese Tür von vornherein zu schließen, als erst die Polizei zu rufen, wenn der Einbrecher schon im Haus ist.

Für den gelegentlichen AV Scann reicht dann auch ein Prog wie das Windows eigene AV Prog & eine entsprechende Gegenstück unter MacOS voll aus. Da muss es nichts teuer gekauftes sein.

Beitrag von „coopter“ vom 25. November 2018, 20:53

@**al6042**

Avast !

Müßte man dann Bitdefender abmelden ?

Beitrag von „al6042“ vom 25. November 2018, 21:10

Na, ich würde den dringend deinstallieren, wenn ich mit einem anderen AV Programm arbeiten wollte... 

Beitrag von „bluebyte“ vom 25. November 2018, 21:15

Habe Malwarebytes in der Free-Version laufen. Sonst nichts.

Ansonsten Mac-Brain. Mit Abstand das beste Programm.

Nutze selbst nur Mediatheken von ARD und ZDF oder youtube

für Dokumentationen.

Das bei Dir war alles nur Fake. Die wollten Dir nur dieses

Paket aufschwatzen. Ist mir auch schon passiert.

Beitrag von „coopter“ vom 25. November 2018, 21:16

Tun.. die sich was in punkto Sicherheit Check ?

Beitrag von „revunix“ vom 25. November 2018, 21:20

Also wer auf so etwas hier reinfällt sollte das Internet ganz schnell abschalten 😆

Beitrag von „coopter“ vom 25. November 2018, 21:41

@Un!x

Ich hatte so eine Meldung schon auf einen Unserer Hackmac gesehen ! Kann ich etwas dagegen tun ?

Beitrag von „revunix“ vom 25. November 2018, 21:43

Im Grunde reicht da ein Adblocker, wobei ich einen habe und mir das auch angezeigt wurde. Aber ich schenke dem keinen glauben.

Beitrag von „Higgins12“ vom 25. November 2018, 21:47

Hab solche Meldungen noch nie gesehen auf eigenen Geräten. Bis jetzt jedenfalls.

Beitrag von „Nio82“ vom 25. November 2018, 22:04

Ein AdBlocker blockt natürlich nur Sachen die auch als Ad -> Werbung erkannt werden. Daher zusätzlich immer auch einen ScriptBlocker nutzen. Und nur die Scripte zulassen die von vertrauenswürdigen Seiten stammen oder für die Funktion der Seite unbedingt nötig sind.

Macht zu Anfang natürlich einiges an Arbeit beim Surfen, lohnt aber.

Ich mach das seit gut 12 Jahren so & nutze unter Win seit 10 Jahren die Microsoft AV Lösung. Unter MacOS z.Z. gar keins. Und hatte auch seit mindestens 10 Jahren keinen Virus mehr.

...Und das obwohl ich früher viel solche, "Alternativen Streaming Anbieter" genutzt habe.

Beitrag von „tegvlarivs“ vom 26. November 2018, 14:10

> Zitat von Un!x
>
> Im Grunde reicht da ein Adblocker, wobei ich einen habe und mir das auch angezeigt wurde. Aber ich schenke dem keinen glauben.

bin auch der meinung. der fängt mMn auch fiese seiten ab! bei mir läuft seit jahren kein virenscanner (außer der windows defender unter windows) und ich hatte noch nie einen virus. in dem zusammenhang wird ja auch gerne mal an das "common sense" als besten virenschutz verwiesen 

Beitrag von „Sascha_77“ vom 26. November 2018, 15:26

> Zitat von Holz_Michel
>
> Da wärst du jetzt der erste von dem ich höre, dass er auf dem Mac als Admin User unterwegs ist Normal ist der erste Schritt nach der Installation genau wie in Linux sofort einen neuen Benutzer ohne Admin Rechte zu erstellen. Never be root if you don´t need to be root.

Naja ich habe seit meiner Mac "Karriere", das ist seit 1999, in OSX immer einen Administrations-User benutzt. Nichts passiert bis dato. Nun ist es ja auch so, dass man selbst als Admin User für Eingriffe im System das Admin Passwort nochmal separat eingeben muss. Wenn man jetzt nicht einfach blind irgendwelche .pkg oder dergleichen installiert sehe ich den Umstand Admin-User zu sein relativ gefahrlos. Thema Brain.exe ... bzw. bei uns ja eher Brain.app.

Davon ab kann es dich als Normaluser genauso erwischen. Wenn du nämlich als Beispiel ein .pkg installierst was dich nach dem Namen und Passworts des Adminusers fragt, was Du dann unter deinem Normaluser eingibst.

Wirklich gefährlich (und somit wirklich root) wäre es, wenn Du dich schon beim Login auch als User "root" anmeldest. Das würde ich dann auch eher nicht machen. Ist aber auch niemals nötig. Dafür gibts halt den Adminuser der ein sog. sudoer ist.

Beitrag von „grt“ vom 26. November 2018, 15:31

wenn ich richtig informiert bin, heisst doch "Administrator" in osx und auch linux lediglich, dass dieser user in der sudoers-datei gelistet ist, also alle sudo .... befehle und entsprechende operationen, die zwar nicht im terminal ausgeführt werden, aber ebenfalls "sudo" im hintergrund erfordern, ausführen darf (nach passworteingabe). im "normalbetrieb" agiert der "Administrator" genauso, wie jeder normaluser auch.

Beitrag von „Sascha_77“ vom 26. November 2018, 15:34

Genau so und nicht anders ist es.

Streng genommen gibt es keinen großen signifikaten Unterschied zwischen beiden ausser die sudo-Zugehörigkeit.

Ok als Adminuser kann man ohne Passworteingabe ein Programm in Applications ablegen. Aber dieser Umstand ist ja jetzt kein potentielles Risiko.

Beitrag von „p100656“ vom 26. November 2018, 15:52

ok, um das Thema für mich jetzt mal abzuschließen: Ich schätze - wenn ich mich richtig erinnere - der Screen sah aus, wie in Post #19 gezeigt, also Trojaner-Fake-News, die mich anstiften sollte, irgendeine Software zu installieren, die wer-weiß-was tun würde. Da ich nix installiert hatte und überdies sowieso restored hatte, ist wohl nix passiert.

Gelernt habe ich, dass es sehr ambivalente Meinungen zu Thema Virenscanner gibt und es aber wohl nicht schaden kann, hin und wieder mal einen Scan zu machen, auch unter dem Aspekt, bei Datenweitergabe keine Vieren unerkannt an Dritte weiterzugeben.

Damit würde ich für mich die Sache auf sich beruhen lassen. Danke an alle Interessierten und die Infos, die sie gegeben haben.

Viele Grüße

Beitrag von „apfelnico“ vom 26. November 2018, 15:55

> Zitat von Holz_Michel
>
> Da wärst du jetzt der erste von dem ich höre, dass er auf dem Mac als Admin User unterwegs ist 😆

Ich weiß nicht, was es da zu lachen gibt. Da es die Standard-Prozedur am Mac ist, gehe ich davon aus, dass es sehr sehr viele Benutzer so handhaben. Im Übrigen …

> Zitat von Holz_Michel
>
> Never be root …

… ist ein Admin kein root. Und dieser ist standardmäßig (bis auf eine peinliche Apple-Panne) deaktiviert.

Beitrag von „Wolfe“ vom 26. November 2018, 15:59

Solche Seiten, die mit Warntönen wegen vermeintlicher Malware Alarm schlagen, hatte ich schon oft. Einfach wegklicken. Das automatisch geladene .dmg einfach löschen.

Beitrag von „user232“ vom 27. November 2018, 02:45

ich würde mir keinen Virenscanner installieren, welcher tief in das System eingreift, also quasi im Hintergrund wacht. Deshalb mein Vorschlag zu Bitdefender in der kostenlosen Version.

Das mit Brain.app find ich ,..exe was ist das?

Beitrag von „revunix“ vom 27. November 2018, 09:28

Also ich würde mir überhaupt kein AV Scanner unter macOS installieren, wozu auch... um sich da einen richtigen Virus einzufangen hat man schneller ein 6er im Lotto.

Beitrag von „Holz_Michel“ vom 27. November 2018, 16:55

> Zitat von apfelnico
>
> Ich weiß nicht, was es da zu lachen gibt. Da es die Standard-Prozedur am Mac ist, gehe ich davon aus, dass es sehr sehr viele Benutzer so handhaben. Im Übrigen ...
>
> ... ist ein Admin kein root. Und dieser ist standardmäßig (bis auf eine peinliche Apple-Panne) deaktiviert.

Nur weil es Standard ist, darf man also das Hirn ausschalten? Dass wir hier auf UNIX Grundlage arbeiten ist dir aber schon bekannt? Die normalen Mac Accounts, die das System als Admin bezeichnet, sind doch gar keine, die stehen doch nur im sudoers file. Ist bereits sinnvoll, diese accounts nur zur Verwaltung des Systems zu nutzen und für den normalen Betrieb einen eingeschränkten Nutzer zu wählen, wie von mir geschrieben. Da alle Mac Nutzer die ich bei mir im Studium kenne (Nicht IT im Übrigen!) das mit den Accounts so handhaben wie ich es auch gewohnt bin, find ich schon amüsant wenn jemand absichtlich als Sudo Nutzer unterwegs ist. Der wahre "Admin" ist und bleibt aber einfach Root. Und wer den mit Absicht aktiviert als dauerhaften Nutzer (der ist nämlich nicht standardmäßig aktiv und muss schon mit Absicht angelegt werden - zumindest bei keinem Mac den ich kenne) ist schon selber schuld.

Beitrag von „Sascha_77“ vom 27. November 2018, 17:09

Und wo ist das Sicherheits"minus" wenn ich jetzt anstatt einem Normal-User einen Admin-User benutze? In beiden Fällen muss beim Eingriff ins System das Adminpasswort erneut eingegeben werden. Einfach nur als Adminuser angemeldet zu sein reicht da nicht um im System Änderungen vornehmen zu können/dürfen.

Also ob ich jetzt das Adminpasswort auf Anfrage als Normal- oder Adminuser eingebe ... wo ist der Unterschied?

Wirklich "sicher" wäre es erst wenn Apple verbieten würde als Normaluser überhaupt irgendwie die Möglichkeit zu haben etwas im System zu installieren/ändern.

Aber wie schonmal gesagt ... wer blind einfach irgendwelche ominösen pkg under dergleichen

installiert ist selber schuld wenn er sich dann was eingefangen hat.

Beitrag von „apfelnico“ vom 27. November 2018, 17:43

> Zitat von Holz_Michel
>
> Nur weil es Standard ist, darf man also das Hirn ausschalten? Dass wir hier auf UNIX Grundlage arbeiten ist dir aber schon bekannt?

Du musst mich jetzt nicht ********, nur weil ich von Standard schreibe. Apple es hat es selbst so vorgesehen, und viele nutzen den Mac einfach so. Grundlagen von u.a. MacOS X hin zu macOS, von NeXTStep/OPENSTEP über Rhapsody hin zu Darwin als Grundlage, sowie UNIX im Allgemeinen sind mir bekannt.

> Zitat von Holz_Michel
>
> Die normalen Mac Accounts, die das System als Admin bezeichnet, sind doch gar keine, die stehen doch nur im sudoers file. Ist bereits sinnvoll, diese accounts nur zur Verwaltung des Systems zu nutzen und für den normalen Betrieb einen eingeschränkten Nutzer zu wählen, wie von mir geschrieben.

Sag das Apple. Beziehe dich darauf, dass du es hier schon im Forum geschrieben hast und biete den Kalifornier eine Schulung an, in der du nicht nur erklärst, was genau ein Admin ist, sondern auch, wie es schliesslich generell in UNIX gehandhabt wird.

> Zitat von Holz_Michel
>
> Da alle Mac Nutzer die ich bei mir im Studium kenne (Nicht IT im Übrigen!) das mit den Accounts so handhaben wie ich es auch gewohnt bin, find ich schon amüsant wenn jemand absichtlich als Sudo Nutzer unterwegs ist.

Ich lach mich auch jeden Tag schlapp, wenn ich so an meine Macs gehe. Bin aber auch ein Rebell.

> Zitat von Holz_Michel
>
> Der wahre "Admin" ist und bleibt aber einfach Root.

Wir sind hier bei macOS und ich für meinen Teil finde es gut, im Sprachgebrauch bei Apple zu bleiben. Dieser Floskel kann ich im Bezug auf macOS nichts abgewinnen. Beschwere dich bei Apple, hack nicht auf Anwender rum.

> Zitat von Holz_Michel
>
> Und wer den mit Absicht aktiviert als dauerhaften Nutzer (der ist nämlich nicht standardmäßig aktiv und muss schon mit Absicht angelegt werden - zumindest bei keinem Mac den ich kenne) ist schon selber schuld.

Da sind wir endlich einer Meinung, was den "Root" betrifft. Schrieb ich aber auch schon ...

Beitrag von „Holz_Michel“ vom 27. November 2018, 19:21

Das mit dem Hirn einschalten war nicht auf apfelnico persönlich bezogen. Was ich versuche zu sagen lässt sich vielleicht anhand von Windows 10 erklären, was haben da alle gegen die Standardeinstellungen gewettert, wie unsicher die Daten doch sind und dass der Rechner "nach Hause telefoniert" und es wurden ständig Tipps gegeben, wie man diese Standardeinstellungen umgeht. Bei Apple ist das scheinbar anders, deren Betriebssystem gilt wohl als perfekt und damit einhergehend sind auch sämtliche Standardeinstellungen einfach hinzunehmen ohne über deren Berechtigung nachzudenken, verstehe ich euch da richtig?

Der "echte" Root Nutzer - zumindest auf meinem Testsystem - erfordert für keine Installation irgendwelcher Pakete weitere Passworteingaben, dies scheint aber eine Eigenheit von MacOS zu sein, kenne ich von Linux her definitiv auch anders. (EDIT: Abgesehen davon man bootet ohne weitere Pakete direkt in die Shell). Klärt mich bitte auf, falls es auch dort noch weitere Varianten in der Benutzer-Art gibt.

PS: apfelnico solche Kommentare wie den bezüglich der Sicherheits-Schulungen in Kalifornien bin ich eigentlich aus diesem Forum nicht gewohnt, meine Absicht war es definitiv nicht, jemanden hier bloßzustellen!

Beitrag von „griven“ vom 2. Dezember 2018, 00:44

Also alle Linux Varianten untern denen ich bisher als Root unterwegs war lassen für den Root User alles zu sofern er sich denn als Root User identifiziert hat und das trifft auf alles zu was im Terminal gemacht wird nicht jedoch unbedingt im Kontext des WindowServers denn dessen Prozess läuft unabhängig vom angemeldeten User eben nicht als Root und das ist auch gut so. Vergleichbar handhabt es das Userland von macOS auch hier läuft der WindowServer nicht mit den Berechtigungen des am Server angemeldeten Users sondern eben mit seinen eigen (typischerweise mit System:Wheel) was der angemeldete User dann im System darf oder eben auch nicht hängt letztlich aber nicht am WindowServer sondern an dessen Berechtigungen und von der Warte aus wäre es fahrlässig einen Root zu verwenden...

Die Admins in der macOS Nomenklatur halte ich aber für unkritisch denn unter macOS muss, sofern nicht daran geschraubt wurde, jeder SUDO User sein Kennwort für jede systemrelevante Aktion eingeben und das sollte jedem eine Alarmglocke sein um genau hinzusehen was da eigentlich erweiterte Rechte haben will. Hier bin ich bei apfelnico die macOS Nutzer sind von der Wiege an darauf konditioniert diese Dinge genau zu betrachten und sich zu überlegen ob man erlaubt oder nicht.

Was die Eingangsfrage angeht würde ich persönlich unbedingt dazu raten auch unter macOS einen Scanner zu verwenden jedoch nicht in erster Linie weil das eigene System gefährdet sein könnte (Viren und Trojaner sind unter macOS relativ wenig verbreitet einfach weil macOS keine nennenswerte Plattform im Sinne der Progger dieser Produkte darstellt) sondern weil ein mac natürlich auch mit Windows Systemen kommuniziert und hier macht es Sinn auch Plattformfremde Viren zu erkennen und zu eliminieren bevor man sie versehentlich per Mail an Freunde und Bekannte verbreitet. In der Server Landschaft tut man das ja auch sprich Linux basierte Server Scannen unter optimalen Bedingungen eingehende Mails ja auch schon vor der Zustellung auf lokale Mailboxen auf Viren und filtern solche mails ggf. aus...

Beitrag von „user232“ vom 15. Dezember 2019, 11:11

> Zitat von user232
>
> ich würde mir keinen Virenscanner installieren, welcher tief in das System eingreift,

> also quasi im Hintergrund wacht. ~~Deshalb mein Vorschlag zu Bitdefender in der kostenlosen Version.~~

Bitdefender,... ab in die Tonne, was sucht das Programm in meinen Kontakten? 

Beitrag von „bluebyte“ vom 15. Dezember 2019, 11:52

@ ... benutze unter MacOS "Malwarebytes". Unter Windows den "Defender" und "Malwarebytes Free". Ansonsten scanne ich ab und zu die kompletten Platten im Offline-Modus mit "desinfect" von der Computerzeitschrift ct', was auch wesentlich sinnvoller ist. Wirklich gut programmierte Schadsoftware hat das System längst kompromittiert, noch bevor überhaupt ein Schutzprogramm seinen Dienst antritt.

Deshalb sind für mich die Antivirenprogramme, die im Online-Modus laufen letztendlich nur Augenwischerei.

Beitrag von „user232“ vom 15. Dezember 2019, 12:05

Ich bin grad am aufräumen. EtreCheck aus dem Appstore ist da ua ganz hilfreich. Ansonsten nutz ich am Mac jetzt auch nur noch die alte Malwarebytes Free Version, aber denk die werd ich demnächst auch entsorgen. XProtect soll ja anscheinend genügen.

Beitrag von „ozw00d“ vom 15. Dezember 2019, 12:15

Vielleicht für den einen oder anderen von interresse:

ich hab mir clamav (cli) auf dem hacki und mac installiert, dieser prüft in regelmäßigen abständen ob es irgendeine verseuchung gibt.

Gesteuert wird das ganze via plist und launchctl in /Library/LaunchAgents und entsprechendem

eintrag in cron.

Eine gute Anleitung, wenn auch nicht state of the art, da einige Pfade und co angepasst werden müssen gibt es hier und fürs system hardening zusätzlich hier einige tips .

Beitrag von „bluebyte“ vom 15. Dezember 2019, 12:18

ozw00d clamav kenne ich noch von Linux. War vor ein paar Jahren die einzige Option für den Privatanwender.

Beitrag von „mhaeuser“ vom 15. Dezember 2019, 12:33

> Zitat von bluebyte
>
> Ansonsten scanne ich ab und zu die kompletten Platten im Offline-Modus mit "desinfect" von der Computerzeitschrift ct', was auch wesentlich sinnvoller ist. Wirklich gut programmierte Schadsoftware hat das System längst kompromittiert, noch bevor überhaupt ein Schutzprogramm seinen Dienst antritt.

Leider komplett irreführend, es ist eher das Gegenteil der Fall. Die meisten (oder alle?) Offline-Lösungen haben keine Onlineanbinding (im Internet-Sinn) und somit alte Definitionen... die ganzen konventionellen Schädlinge erkennt auch ein Online-AV ohne Probleme. Zum einen muss eine Schadsoftware sich auch erst Mal einnisten, was idR in einer sehr späten Phase passiert (meistens bei eingeloggtem Nutzerkonto), zum anderen ist es Malware ohne tiefgreifende Änderungen (Kernelcode etc) nicht möglich, so früh zu starten, wie du hier suggerierst, zumindest unter Windows, Stichwort ELAM.

EDIT: OK, das von dir genannte Tool unterstützt die Signaturaktualisierung von bekannten Quellen... naja, für's Gewissen ist's in Ordnung

---

Beitrag von „Wolfe“ vom 15. Dezember 2019, 12:51

Gibt es Gründe gegen Antivir?

Beitrag von „Romsky“ vom 15. Dezember 2019, 12:53

Unter macOS nutze ich nichts (einfach nur aufpassen wenn etwas Rechte benötigt) und unter Windows den Microsoft defender. Absolut ausreichend!

Beitrag von „user232“ vom 15. Dezember 2019, 12:54

In meiner gesamten 5 jährigen macOS Zeit hat mir Bitdefender 2x einen "Virus" angezeigt. Was aber wie sich herausstellte keine waren (KextUpdater und DPCIManager). Malwarbytes hatte noch nie eine Meldung ausgegeben. Das genügt mir, sich von unnötigen Ballast zu trennen, also Malwarebytes ist nun auch weg. SIP auf Hex00 und OpenCore als Bootloader, denke mehr Sicherheit benötigt das System nicht

> Zitat von Wolfe
>
> Gibt es Gründe gegen Antivir?

eigentlich gegen jeden Virenscanner, welcher sich tief in das System einnistet und somit root-Rechte besitzt.

Beitrag von „CMMChris“ vom 15. Dezember 2019, 13:02

Ich nutze Bitdefender weil er sich nicht tief einnistet und auch nicht permanent läuft. Einmal im Monat nen tiefen Scan machen und gut ist. Unter Windows nutze ich nur den Defender. Eingefangen habe ich mir bisher weder unter macOS noch unter Windows etwas.

Beitrag von „mhaeuser“ vom 15. Dezember 2019, 13:04

Naja, in dem Fall hat bluebyte dann absolut Recht - von einem Onlinescanner *will* man, dass er sich einnistet, als Early-Launch-Treiber, damit wirklich alle nicht-Systemkomponenten ohne die Möglichkeit der zuvorigen Systemmanipulation überprüft werden. Oder verstehe ich "einnisten" falsch?

Beitrag von „user232“ vom 15. Dezember 2019, 13:14

@CMMChris Der Meinung war ich auch, aber als ich vor kurzem Bitdefender laufen lies und dieser auf meine Kontakte zuzugreifen wollte (die Meldung hatte ich leider nicht gesichert) hab ich mich von dem vermeintlichen Sicherheitsprogramm verabschiedet. Eigenlich war ich noch nie ein Freund von Virenscanner. Bei Windows den Defender ist ok und macOS das XProtect und Linux? benötigt sowieso keinen. Ich bin der Meinung ein externer Virenscanner kann mehr Schaden als Nutzen anrichten. Als Firma am besten Windows mit Kaspersky einsetzen, dann weiß der Ami und Russe auch Bescheid 

Beitrag von „bumbuy“ vom 15. Dezember 2019, 13:17

Ich nutze DetectX Swift. Einfach in der Bedienung, kostet nicht viel im priv. Einsatz.

Beitrag von „bluebyte“ vom 15. Dezember 2019, 13:39

mhaeuser ... desinfect hat Internetanbindung und aktualisiert die Datenbanken vor dem Scannen.

In Desinfect sind vier Viren-Scanner von namhaften Herstellern integriert. Mit Offline meine ich das Scannen

ohne das Laden des Betriebssystems das geprüft werden soll. Online/Offline hat in diesem Fall nichts damit zu tun, ob man eine Internetverbindung hat oder nicht. Die Lizenz gilt für ein Jahr. Die CD/DVD erscheint jährlich mit der Zeitschrift ct' vom Heise-Verlag.

https://www.heise.de/ct/artikel/Desinfec-t-2019-4427661.html

Beitrag von „svenatkins“ vom 15. Dezember 2019, 13:41

Ich habe unter Windows und macOS Sophos Home laufen.
unter macOS schlägt der auch immer wieder an, sind dann aber immer nur emails die meist im Spam Ordner gelandet sind.

Beitrag von „bluebyte“ vom 15. Dezember 2019, 13:55

Solange noch nichts passiert ist, ist gegen die Schutzprogramme nichts einzuwenden. Haben Schadprogramme erst einmal zugeschlagen, z.B. Software die sich beim Starten des Betriebssystems tarnt, nutzt die beste Schutzsoftware nichts. Dann geht das nur noch mühselig bis gar nicht. Und da kommen die Offline-Scanner zum Einsatz.

Beitrag von „CMMChris“ vom 15. Dezember 2019, 14:15

user232 Ich habe bisher keine Zugriffsanforderung von Bitdefender für Kontakte erhalten.

Beitrag von „mhaeuser“ vom 15. Dezember 2019, 14:28

> Zitat von bluebyte
>
> Haben Schadprogramme erst einmal zugeschlagen, z.B. Software die sich beim Starten des Betriebssystems tarnt, nutzt die beste Schutzsoftware nichts.

Eben doch, siehe ELAM... dafür müsste die Schadsoftware erst Mal den Kernel patchen oder dergleichen. Die Sachen aus dem anderen Post waren alle klar (dass diese CT-DVD die Signaturen aktualisiert musste ich leider per EDIT nachschieben), es geht darum, dass fast alle Offline-Lösungen eben "dumme" AVs mit Uraltdefinitionen sind, einfach, weil es für sowas kaum ein Markt gibt... deswegen wird die CD auch als Ramsch zu Zeitschriften beigelegt und nicht hauptsächlich (ja, ich weiß, dass man sie auch für 10 € separat kaufen kann) "ordentlich" vertrieben. Vier AVs auf eine Linux-CD geklatscht, wenn's dem Gewissen hilft...

Beitrag von „user232“ vom 15. Dezember 2019, 14:40

@CMMChris vlt war dieser Befehl der "Auslöser", bin mir nicht mehr sicher

```
tccutil reset AppleEvents
```

Mit Bitdefender danach nur "kritische Bereiche" gescannt und dann erschien die Zugriffswarnung auf Kontakte.

Beitrag von „Harper Lewis“ vom 15. Dezember 2019, 14:45

Bitdefener aus dem App Store nutze ich ebenfalls auf diversen Systemen, auf die Kontakte wollte die App bisher noch nicht zugreifen.

Beitrag von „bluebyte“ vom 15. Dezember 2019, 16:25

mhaeuser ... selbst schon getestet? Die Definitionen werden bei jedem Start aktualisiert. Warum sollten die Signaturen dann uralt sein? Dazu musst Du natürlich auf den USB-Stick installieren damit die Signaturen gespeichert werden können. Nur als Live-Version von DVD geht das ja schlecht. Wenn Du ESET, Sophos und Kaspersky als Ramsch betrachtest, dann ist Dir nicht mehr zu helfen. Ich weiß ja nicht was für Spezialsoftware Du nutzt. Und wenn Du immer noch nicht schnallst, was Online- bzw. Offline-Virenscanner sind, dann musst Du mal mehr lesen, als nur Computer-Bild oder PC Welt.

Daher das zu Deinem Kommentar 

Beitrag von „mhaeuser“ vom 15. Dezember 2019, 16:27

Bevor du persönlich wirst, solltest du dir Mal Lesekompetenz aneigenen, zum Beispiel die Beudetung von "fast alle", oder das Konzept eines Vetriebsweges verstehen. Liest du meine Posts als Lückentext, bei dem nur jedes vierte Wort nicht rausgestrichen ist?

Beitrag von „al6042“ vom 15. Dezember 2019, 16:41

Und bevor es hier wirklich unnötig unschön wird, möchte ich Euch beide dringend ersuchen diesen offenen Schlagabtausch einzustellen!

Danke...

Beitrag von „user232“ vom 1. Januar 2020, 08:27

> Zitat von Harper Lewis
>
> Bitdefener aus dem App Store nutze ich ebenfalls auf diversen Systemen, auf die Kontakte wollte die App bisher noch nicht zugreifen.

Heute frisch aus dem Appstore nochmals die kostenlose "Bitdefender Virus Scanner" runtergeladen, scan durchgeführt und es wurden Meldungen auf Zugriff von Kontakte, Kalender und Fotos angezeigt.

Beitrag von „CMMChris“ vom 1. Januar 2020, 10:09

Eigenartiges Verhalten bei dir. Ich nutze auch die Version aus dem App Store und habe noch nie eine Meldung diesbezüglich erhalten. Die einzigen Rechte die der Bit Defender erfragt ist Vollzugriff auf die Festplatte und auch nur hier taucht er in der Liste in den Sicherheitseinstellungen auf. Gerade noch komplett deinstalliert mittels App Cleaner und nochmal neu installiert - keine Anfrage für Zugriff auf Kontakte etc. erhalten. Wie kann denn sowas sein?!

Beitrag von „user232“ vom 1. Januar 2020, 10:14

könnte mit der Option "Vollzugriff" zusammenhängen, diese ist bei mir für Bitdefender deaktiviert.

Beitrag von „CMMChris“ vom 1. Januar 2020, 10:16

Möglich, aber Vollzugriff braucht das Ding halt um seine Arbeit zu verrichten. Wenn du den deaktiviert hast kannst du dir die App auch gleich sparen.

Beitrag von „user232“ vom 1. Januar 2020, 10:18

mein reden, muss jeder selbst entscheiden wer wem etwas anvertraut. Habe den Bitdefender nur nochmal installiert um der Sache auf den Grund zu gehen.

Beitrag von „sv0911“ vom 1. Januar 2020, 15:15

Bezüglich Sicherheits-Apps etc., benutze ich gerne Apps von folgender Seite:

Objective-See

Vieleicht für den ein oder anderen Anwender hier interessant.

Freundliche Grüße und ein frohes neues Jahr

sv

Beitrag von „Wolfe“ vom 1. Januar 2020, 15:45

sv0911 Ich bin sehr vorsichtig geworden, seit meine Installation von Catalina zerschossen worden ist. Die zeitliche Nähe des updates von Lulu auf 1.2.2 mag eine Koinzidenz sein, klar. Jedenfalls hatte ich unmittelbar darauf für zwei Wochen keinen zuverlässigen Rechner mehr, sondern massenhaft Abstürze.

Das ging so weit, dass ich zentrale Hardware ersetzt und macOS neu installiert habe und seither Ruhe ist. An eine neue Installation von Lulu auf meiner Test-SSD wage ich mich erst, wenn alles sauber läuft.

Beitrag von „user232“ vom 1. Januar 2020, 16:34

...weniger ist mehr, auch keine Software-Firewall. Ich nutz nur noch das, was das OS-System hergibt. Genauso gehört meiner Meinung auch kein Chrome oder MS-Software auf nen "Mac".

Beitrag von „user232“ vom 28. Januar 2020, 13:45

Bezahlen tut man häufig und wenn es „nur“ Daten sind, siehe Meldung Avast

---

Beitrag von „al6042“ vom 28. Januar 2020, 17:45

Habe einen ähnlichen Beitrag vorhin auch gesehen...

Die Welt ist böse, hinterhältig und gemein...

Beitrag von „user232“ vom 28. Januar 2020, 18:17

ja alle böse , ich bin regelrecht ein Gegener von Virenscanner. Ich geb doch einem fremden Programm keinen Vollzugriff auf mein System und meinen Daten. Und wenn ein App, in dem Fall Bitdefender, bei meinen Kontakte nach Viren sucht, dann ist da was faul. Ich glaube so weit sind wir noch nicht, dass ein Programm erkennt wer in Kontaktlisten die Seuche hat.

Ich habe, auch wenns wahrscheinlich nicht richtig ist, so ein Urvertrauen zu Apple, hält jetzt schon Jahre an

Wenn Firefox auch als Datenkrake mal in Verruf kommen sollte geb ichs auf ...

Beitrag von „bluebyte“ vom 29. Januar 2020, 23:43

user232 schon jahelanges Urvertrauen in Apple? Wie ist deine Meinung zu PRISM?

Beitrag von „revunix“ vom 30. Januar 2020, 00:33

> Zitat von CMMChris
>
> Eigenartiges Verhalten bei dir. Ich nutze auch die Version aus dem App Store und habe noch nie eine Meldung diesbezüglich erhalten

SIP deaktiviert? Dann bekommt man diese Meldungen z.B nicht.

> Zitat von user232
>
> Bezahlen tut man häufig und wenn es „nur“ Daten sind, siehe Meldung Avast

Als wäre das jetzt auch was neues... jeder nutz Google, da fragt sich niemand... Thema wird künstlich hochgebauscht.

Beitrag von „user232“ vom 30. Januar 2020, 07:57

bluebyte

PRISM kannte ich noch nicht, werde mir da mal bei Gelegenheit anschauen

revunix

künstlich hoch gebauscht schon, aber trotzdem sollte es erwähnt werden. Browserdaten sind mit das geringste was mich stören würde, aber wenn ein Programm in Kontakten, Bildern etc herumfummelt, dann sehr wohl.

Beitrag von „user232“ vom 9. März 2022, 18:41

heise zum Thema Kaspersky