Erledigt Erpesser Trojaner jetzt auch für OS & X

Beitrag von „Fab“ vom 7. März 2016, 00:13

So leute her gehöhrt under gelesen!
Kurz vorweg, an diejenigen die den Sicherheitsmechanismus von Apple Deaktiviert haben und gerne mal etwas Downloaden sollten damit ersteinmal warten und den Sicherheitsmechanismus einschalten!
Auch wenn es erstmals nur unter dem BitTorrent-Client Transmission auftaucht.
Hier der Artikel: http://www.maclife.de/news/vor...-eure-daten-10075730.html

Ich hoffe mal das es euch weniger erwischt....

Hier noch ein Auszug von der MacLife wo Ihr es Findet:

> Zitat
>
> MacLife;
>
> Wer Sorge hat, dass die Malware auf dem eigenen System aktiv ist, sollte in der Aktivitätsanzeige nach einem Prozess namens "kernel_service" Ausschau halten. Außerdem soll sich im Verzeichnis "/Applications/Transmission.app/Contents/Resources" die Datei "General.rtf" befinden. Wenn diese Datei vorhanden ist, soll der Rechner nach Angaben von Palo Alto Networks infiziert sein. Zudem sollen sich die Dateien ".kernel_pid", ".kernel_time" und ".kernel_complete" oder "kernel_service" im Library-Verzeichnis befinden.

Gruß der Fab =)

Beitrag von „Nightflyer“ vom 7. März 2016, 00:37

hier drücke ich mal nicht "Gefällt mir"
Trotzdem.....

Danke für die schlechten News 

Beitrag von „RalphD“ vom 7. März 2016, 00:50

Hab's auch gerade gelesen und wollte es hier posten. Seit bloß vorsichtig. Ich kenne Leute die es erwischt hat (Windows). Das ist kein Spaß!!!

Beitrag von „Dr.Stein“ vom 7. März 2016, 01:12

Da schaue ich morgen mal direkt nach.
Bin jetzt zu müde dafür. Dachte für den doch sehr wichtigen Hinweis.
Zu dem habe ich den Post einmal angepinnt.

Beitrag von „Raoul Duke“ vom 7. März 2016, 01:13

Ein Backup nimmt solchen Sachen ihren Schrecken. Das Perfide an dem Ding ist wohl das ALLE Laufwerke im Netzwerk verschlüsselt werden. Ich habe zur Sicherheit eins offline und außer Haus bei meinen Eltern gelagert, auch für den Fall das es brennt, Einbruch, Wasserschaden oder was sonst noch alles passieren kann.

Gruß Raoul Duke

Beitrag von „RalphD“ vom 7. März 2016, 01:38

Backup unter Umständen nur bedingt. Wenn die Backupplatte immer dran hängt wird die dann auch gleich mit verschlüsselt. Voraussetzung der Trojaner ist schon aktiv. Aber prinzipiell ist Das Backup immer gut und wichtig.

hier mal noch eine Link zu Giga wie das Ding unter Windows funktioniert:

http://www.giga.de/downloads/o...-ist-die-hoelle-los/?fo=1

Beitrag von „netzmammut“ vom 7. März 2016, 01:40

Übelst... Fehlt nur noch Linux :-/

Raoul Duke

...da hilft wohl nur noch die Radikalmethode:
nur dann mit Schreibrechten mounten resp. verbinden, wenn es unbedingt nötig ist; ansonsten alles auf RO...

@all
Nennt mich paranoid, aber ich hab meinen NAS so eingerichtet, das ich mit dem "Normalen Client-User" (Win/Mac) nur lesend auf die Shares zugreifen kann; wenn ich was auf den NAS kopieren will, muss ich mich beim NAS mit einem speziellen (neuen, nur auf dem NAS existierenden) User verbinden, der Schreibrechte auf den Shares hat... Nebst den Backups gibt das ein kleines bisschen mehr Rückversicherung... (je mehr Hürden überwunden werden müssen, desto unwahrscheinlicher der Totalverlust der Daten)

(für Nachahmer - Win-Backup läuft über nen eignen "Batch"; erst wird das Datengrab-Share mit dem Schreibrecht-Nutzer verbunden, dann rattert das Backup-Programm durch, und die Schreib-Share wird getrennt. Das Read-Only bleibt die ganze Zeit verbunden...)
(immer nach dem Motto "warum einfach wenn's auch kompliziert geht" 

...
Immerhin, EINES muss man diesen Ransomeware-Angriffen wirklich lassen:
sie zeigen auf, wie schmerzlich die IT-Sicherheit vernachlässigt wurde, und wie viele Einfallstore für Malware es gibt...

Beitrag von „Raoul Duke“ vom 7. März 2016, 01:51

Ich habe drei Backups. Eins Zuhause, eins im Atelier und eins bei meinen Eltern, das letzte ist wohl das sicherste (sollte meine Eltern öfters besuchen :/)

Gruß Raoul Duke

Beitrag von „YogiBear“ vom 7. März 2016, 02:10

Als Sofortmaßnahme ohne aufwändige BackUpStrategie sollte es ausreichen, wenn die Clover-User unter den RT-Variablen "CsrActiveConfig=0x03" setzen bzw. die Ozmosis-Anhänger mittels Boot in die Recovery/den Installer und Besuch des Terminal die SIP per

Code

1. csrutil enable --without kext

wieder anschalten - jeweils wird das LAden von Drittanbieterkexten erlaubt, weitere Systemänderungen jedoch ausgeschlossen.

Beitrag von „derHackfan“ vom 7. März 2016, 07:54

Das sind ja erschreckende Nachrichten am Morgen ...

Danke an @YogiBear für den Hinweis mit dem Clover Eintrag, das werde ich unbedingt schnellstens nachholen.

Beitrag von „biggasnake“ vom 7. März 2016, 13:50

> Zitat von YogiBear
>
> ...Clover-User unter den RT-Variablen "CsrActiveConfig=0x03" setzen...

Hab ich auch sofort erledigt! Danke!

Beitrag von „kuckkuck“ vom 7. März 2016, 14:36

Yogibear was müsste es dann in der defaults.plist sein? ZwAAAA ist derzeit die komplette Deaktivierung... Bzw in Bytes 67000000

Beitrag von „sn0wleo“ vom 7. März 2016, 16:57

Apple hat das schon gefixt

Beitrag von „Fab“ vom 7. März 2016, 22:17

Dafür mag ich Apple 

Beitrag von „sn0wleo“ vom 7. März 2016, 22:18

Jap und Microsoft bekommt Locky nicht in den Griff

Gesendet von iPhone mit Tapatalk

Beitrag von „Dr.Stein“ vom 8. März 2016, 00:48

Meiner ist sauber! 

Beitrag von „RalphD“ vom 8. März 2016, 03:10

@'SnowLeo
wie meinst du das "Apple hat das schon gefixt"? es gab doch noch kein Update.

Beitrag von „sn0wleo“ vom 8. März 2016, 06:21

Apple hat das Zertifikat was verwendet wurde ungültig gemacht sprich er kann nicht mehr ausgeführt werden

Gesendet von iPhone mit Tapatalk

Beitrag von „netzmammut“ vom 8. März 2016, 11:40

@sn0wleo

Was jetzt Vorteil ist, ist sonst meist ein Nachteil: das geschlossene System von Apple...

In Windows ist der "Infektionsverlauf" ja folgendermassen:
1. Spoofing-Mail mit "Ihre Rechnung" etc als .doc-File.
2. User öffnet jenes File
a) weil MS Office in der Standardeinstellung alle Makros blockiert (= keine Chance für Locky), meckert es so ziemlich bei jedem Start von Office (ob Word, Excel - schnurz). Also stellen viele Admins die Blockier-Einstellung runter...
b) wurde die "blockiere unsichere/nichtvertrauenswürdige/nichtsignierte/nicht von diesem System stammende" Makros NICHT deaktiviert, ists jetzt schon vorbei, leeres Word-Doc, wird geschlossen, feddich.
3. wurde "entblockt", wird nun der eigentliche Locky als .exe gedownloaded (über Makro) und ausgeführt

...währenddem Apple noch die Signatur ungültig machen kann, und somit Ausführung/Installation vom eigentlichen Schädling geblockt wird, müsste man unter Windows mal primär die Anwendung "brain.exe" in den Autostart legen...

Seitens Microsoft: mit Altlasten aufräumen, endlich sauberen Code schreiben, Makros grundsätzlich nichts downloaden und (ohne Aufforderung!) ausführen lassen... ABER dazu muss MS sowohl Windows als auch Office grundlegend überarbeiten. Und DAS ist sehr unwahrscheinlich... (wobei - heute wurde MS SQL für Linux angekündigt, ev. wird dieses Monstrum an Sicherheitslücken (Windows) eingestampft - sobald MS Office für Linux ausgibt, hat sich Windows als OS erledigt)

Beitrag von „Sascha_77“ vom 8. März 2016, 11:48

Mit PlayOnLinux (GUI für wine) kann man sich MS Office unter Linux installieren. Inwiefern allerdings VBA damit läuft .... keine Ahnung. Ich hatte mal Office 2003 damit probiert. Das reguläre Arbeiten damit hat geklappt.

Beitrag von „Ghostbuster“ vom 8. März 2016, 12:02

Bei Befall gibt es keine Lösung die Daten wieder herzustellen!

Doch der Trojaner legt von allem was er verschlüsselt davor eine Kopie auf dem Datenträger an und dann beginnt er mit seiner Arbeit, danach werden diese Kopien und das Original gelöscht. Hier besteht nachträglich eine große Chance über den Weg der Datenrettung die Dateifragmente wieder her zu stellen. Das ist allerdings ein mühsamer und langer Weg.

Unter OS X schützt Sophos-AntiVirus schon aktuell vor der Bedrohung und dieser greift ja auch auf den E-Mail Client zu, denn über diesen Weg wird er meist verbreitet. Daher sag ich mal entspannen, aber Anhänge sollte man immer mit Bedacht öffnen denn nicht nur in "exe" Dateien (Windows) sondern jetzt gerade in Office-Dokumenten liegt der Auslösende Trojaner bei.

Zudem sollte jede gute Firewall im Vorfeld den Trojaner auch schon erkennen, nur diese hat ja nicht jeder am laufen.
Sehr schade ist das die Unternehmen/Provider es überhaupt zulassen das nach der Erkennung und Bekanntgabe trotzdem noch Nachrichten mit dem Infector verteilt werden, denn die haben ja normal die Mittel das zu unterbinden, wir zahlen selbstverständlich auch für solch einen Service, nur halt nicht wirklich;)

Beitrag von „Sascha_77“ vom 8. März 2016, 12:16

Auch eine Datenwiederherstellung würde nicht viel bringen. Er schreibt ja immer und immer wieder auf die Platte indem er Kopien anlegt. Und diese überschreiben dann auch sehr wahrscheinlich die Bereiche der Platte die durch eine Löschung von davor freigeworden sind.

Da gibts nix mehr zu retten.

Ich hoffe nicht, dass man nun zukünftig auch unter OS X ein Antiviren-Programm benötigt. Das wäre eine "traurige" Premiere in meinem OS X Leben.

Beitrag von „netzmammut“ vom 8. März 2016, 12:34

@Sascha_77

Naja ich meinte eine offizielle MS-Version; über Wine ist das ein alter Hut

Wegen der Datenrettung:
ich hatte mal ein kleines Abenteuer mit Ubuntu, das ein altes Raid-Set erkannte und versuchte wiederherzustellen (obwohl der Raid unlängst gelöscht war)...

Obwohl ich die Platten damals zum x.ten neu partitioniert hatte, fand mir TestDisc Daten von fast allen Partitionen (und die Partitionen damals waren voll und ziemlich oft mit neuen Daten gefüllt)

...bringt natürlich nur bedingt was, der Aufwand für die Forensik ist immens (vor allem: der zeitliche Aufwand). Im unternehmerischen Umfeld ist das Rückspielen des letzten infektionsfreien Backups und Aufarbeiten des Hängengebliebenen/Verlohrenen meist schon schneller...

Beitrag von „Ghostbuster“ vom 8. März 2016, 12:38

Ich habe vor einiger Zeit schon eine Festplatte wieder hergestellt, das ist also möglich.
Allerdings wie gesagt, das ist ein langer und mühsamer Weg!

Alleine die Analyse und dann die Wiederherstellung dauert Stunden bis zu ein paar Tagen.
Danach liegt alles nur in einzelnen Dateien ohne Name und Datum vor und muss einzeln durchgesehen,
beschriftet und archiviert werden, Spaß ist was anderes.

Wollte damit auch nur sagen... sollte man betroffen sein ist eine Wiederherstellung über den "Erpresser" auf keinen Fall zu empfehlen, eine Meldung und Anzeige gegen Unbekannt stellen und sich an einen IT-Spezialisten wenden der einem behilflich ist wenigstens die Daten welche existenziell wichtig sind zu versuchen wieder her zu stellen. Sollte es keine Weg zum Backup geben was sehr oft der Fall ist. Bei mir selbst bewegen sich oft Daten schnell hin-und-her, ein Full-Backup mache ich selten, keine Lust und Muße.

PS: Daher habe ich meine Daten in einer aktiven Synchronisation eingebunden und diese lasse ich dann automatisch täglich archivieren. Doch es besteht immer eine Möglichkeit des Verlustes und meist dann wenn man es überhaupt nicht erwartet und gebrauchen kann.

Beitrag von „jboeren“ vom 8. März 2016, 17:14

"csrutil enable --without kext" gibt ne merkwürdige meldung!?

Bei mir steht:

- *System Integrity Protection status: enabled (Custom Configuration).*

- Configuration:
- Apple Internal: disabled
- Kext Signing: disabled
- Filesystem Protections: enabled
- Debugging Restrictions: enabled
- DTrace Restrictions: enabled
- NVRAM Protections: enabled

- This is an unsupported configuration, likely to break in the future and leave your machine in an unknown state.

Stimmt das so?

Beitrag von „kuckkuck“ vom 8. März 2016, 17:52

Alles korrekt, diese Konfiguration benutzen echte Apple Computer natürlich nicht weshalb sie auch "unknown" ist, der Rest sagt dir nur das die SIP jetzt bezüglich Apple Internal und Kext Signing deaktiviert ist --> du kannst immer noch kexte installieren

---

Beitrag von „user-michi“ vom 8. März 2016, 18:14

> Zitat von YogiBear
>
> Als Sofortmaßnahme ohne aufwändige BackUpStrategie sollte es ausreichen, wenn die Clover-User unter den RT-Variablen "CsrActiveConfig=0x03" setzen bzw. die Ozmosis-Anhänger mittels Boot in die Recovery/den Installer und Besuch des Terminal die SIP per
>
> Code

> 1. csrutil enable --without kext
>
> wieder anschalten - jeweils wird das LAden von Drittanbieterkexten erlaubt, weitere Systemänderungen jedoch ausgeschlossen.

Kann man die Einstellung "CsrActiveConfig=0x03" stehen lassen oder gibt es dadurch einen Nachteil?

Beitrag von „YogiBear“ vom 8. März 2016, 18:29

Du kannst mit 0x03 keine weiteren Änderungen am NVRAM vornehmen.

Beitrag von „jboeren“ vom 8. März 2016, 18:38

"Du kannst mit 0x03 keine weiteren Änderungen am NVRAM vornehmen."

Wenn der Hacki fertig is soll das aber kein problem sein?

Beitrag von „user-michi“ vom 8. März 2016, 18:39

> Zitat von jboeren
>
> "Du kannst mit 0x03 keine weiteren Änderungen am NVRAM vornehmen."
>
> Wenn der Hacki fertig is soll das aber kein problem sein?

Frag ich mich auch gerade. Muss ja eigentlich nichts mehr in das NVRAM oder?

Beitrag von „kuckkuck“ vom 8. März 2016, 18:41

Yogibear in wie fern sollte denn die teilweise Reaktivierung der SIP den Hacky vor DIESER Bedrohung schützen? Echte Macs können ja auch damit befallen werden

---

Beitrag von „sn0wleo“ vom 8. März 2016, 18:42

da es ein signiertes Zertifikat benutzt hat ging es trotzdem aber es ist ja gefixt von apple

Gesendet von iPhone mit Tapatalk

Beitrag von „moscaSam“ vom 24. Dezember 2016, 12:32

Danke für den Artikel und für die Warnung! für mich ist es wichtig