Erledigt Erpesser Trojaner jetzt auch für OS & X

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)