A legjobb 4 ajánlás Linuxos gépen a biztonságos böngészéshez

Írta: Konstantin Ryabitsev – Linux.com, May 9, 2017

A cikkben a szerző felhívja a figyelmet arra, hogy a Linux munkaállomások legsebezhetőbb pontja az internetes böngésző, ami eleve arra hivatott, hogy letöltsön és végrehajtson megbízhatatlan forrásból származó, gyakran ellenséges kódokat.

Számos eljárás van arra, hogyan előzzük meg a nem kívánt hatásokat, de többségük valamilyen módon már bebizonyította sebezhetőségét. Véleménye szerint a legfontosabb, hogy a munkaállomás használója az eddigi gyakorlatát gyökeresen átalakítsa, és ehhez ad tanácsokat.

1. A grafikus környezet

Az X protokollt a személyi számítógéphasználat egy egészen más környezetében találták ki és híján van a hálózati működésben alapvetőnek tekinthető biztonsági tulajdonságoknak. Például bármilyen X–alkalmazás hozzáfér a teljes képernyőtartalomhoz, beregisztrálhat az összes billentyűleütés fogadására, függetlenül attól, melyik ablakban gépelték be.

Egy megfelelő böngésző-sérülékenység lehetővé teheti billentyűfigyelő és képernyőfelvevő program beépítését és a (root) terminálon folyó összes művelet így rögzíthető.

Erősen javallt a Wayland-hoz hasonló modernebb platformra váltani, még ha emiatt számos alkalmazást X11 protokoll wrapper-ben (csomagoló, burkoló) kell futtatni.

2. Két eltérő böngésző használata

A legkönnyebben megvalósítható, de csak minimális biztonsági előnyt hoz magával. Nem minden böngészőhiba ad a támadónak teljes hozzáférést. Ha két böngészőt használunk, egyet munkára, egyet pedig minden másra, elkerülhetővé teszi, hogy kisebb böngészőhibát kihasználva a támadó hozzáférjen a teljes süti-tartalomhoz. Hátránya, hogy a két böngészőfolyamat több memóriát használ fel.

A The Linux Foundation sysadmin team javaslata:

Használj Firefox-ot a munkára és a nagy biztonságú oldalakhoz

A Firefoxot a munkával kapcsolatos oldalak elérésére használd, olyan esetekben, amikor biztosítani kell, hogy a sütik, megnyitott lapok, bejelentkezési információk, billentyűleütések stb. nem kerülhessenek támadó kezébe. NE HASZNÁLD ezt a böngészőt más oldalak megnyitására, néhány kiválasztott kivételével. Ugyanakkor telepíteni kell a következő, alapvető kiegészítőket:

NoScript

• NoScript nem engedi a felhasználó által whitelist-nek (engedélyezettek listája) jelölt oldalak kivételével máshonnan aktív tartalmak letöltését. Az alapböngészővel használni nem javasolt, működését akadályozza (miközben valóban jelentős biztonsági előnyökkel jár), ezért csak a munkával kapcsolatos oldalak elérésére javasolt böngészőben legyen bekapcsolva.

Privacy Badger

• EFF (Electronic Frontier Foundation) Privacy Badger-e megakadályozza külső nyomkövetők (tracker) és hirdetési platformok letöltését. A tracker-ek és hirdetési oldalak gyakran célpontjai a támadóknak, mivel gyorsan, világszerte meg lehet fertőzni velük rendszereket.

HTTPS Everywhere

• Ez a szintén EFF-fejlesztette kiegészítő biztosítja, hogy a hivatkozás http:// formájától függetlenül biztonságos kapcsolaton keresztül érd el a weboldalakat. (Számos támadás, pl. SSL-strip elkerülhető ez által.)

A **Certificate Patrol** is kiváló kiegészítő, mivel riaszt, ha az elérni kívánt oldal megváltoztatta TSL bizonyítványát, különösen, ha az nem volt lejárófélben. Hasznos különösen man-in-the-middle próbálkozások esetén – ekkor a kapcsolat közé ékelődően hamis pozitív visszajelzéseket ad valaki.

Hivatkozások megnyitására alapnak a Firefox legyen beállítva, így elkerülhető aktív tartalmak letöltése, vagy végrehajtása.

Használj Chrome/Chromium-ot minden más esetben

A Chromium fejlesztői a Firefox előtt járnak biztonsági kiterjesztések készítésében (legalábbis Linuxon) – sandbox, kernel user namespaces stb., amik plusz réteget adnak a meglátogatott oldal és a rendszer közé, elszigetelve egymástól azokat.

A Chromium a Google nyílt forráskódú projektje, a Chrome pedig a zárt forráskódú. Olyan oldalak felkeresése esetén, amikről nem akarod, hogy a Google tudjon, jobb kerülni használatukat.

A Privacy Badger és HTTPS Everywhere kiterjesztések telepítése Chrome esetén is javasolt. A Firefox-tól megkülönböztetéshez használj eltérő témát, hogy lásd, ez a „nem megbízható” böngésződ.

3. Használj Firejail-t

A Firejail Linux namespaces-t és seccomp-bpf-t használ, hogy sandbox-ot építsen a Linux-alkalmazások köré. További védelmet telepít a böngésző és a rendszer többi része közé. A Firejail-lel egymástól elszigetelt, eltérő célú Firefox-példányok futtathatók – egy munkára, egy más megbízható oldalhoz (pl. bank) és egy sokkal alkalmibb célokra (szociális média stb.).

A Firejail leginkább Wayland esetén hatékony, X11 esetén használj ahhoz való izolációs eszközt (--x11 jelzőt). A Firefox melletti használathoz tanulmányozd a projekt által készített dokumentációt:

• Firefox Sandboxing Guide

4. Virtualizációval teljesen válaszd szét a munka- és a játékkörnyezetet

Ez a lépés egy kicsit paranoiás, de miként az író állítása szerint szokta mondani, a biztonság hasonlít autópályán közlekedéshez – mindenki, aki vezet nálad, az hülye, aki pedig gyorsabban, az őrült.

A teljesen izolált „virtuális gépek” tekintetében a QubesOS projekt tanulmányozását javaslom, ami „elég biztonságos” munkaállomás-környezetet biztosít. A SubgraphOS-t is érdemes megnézni, ami hasonló célt valósít meg konténer–technológia alkalmazásával (jelenleg Alfa-állapotú).

Az író ígérete szerint a sorozat pár héten keresztül folyatódik. A következő alkalommal a hitelesítő adatok ellopását célzó FidoU2F elleni küzdelem módja és ajánlások jelszókezelő használatára biztonságos jelszó generálása céljából lesznek napirenden.