Írta: Szabó Áron
2014. december 23. kedd, 12:09 - Módosítás: 2014. december 23. kedd, 12:22

A Sony-ra rájár a rúd... Pár évvel ezelőtt a pingvines felhasználók nyertek csatát és ezáltal lehetőséget arra, hogy bármit tudjanak futtatni a Sony PlayStation 3 konzolokon. A 27. Chaos Communication Conference (27C3) rendezvényen (2010. december 29-én) a fail0verflow tagjai által tartott előadás megmutatta, hogy nemcsak jó kriptográfiai algoritmusok kellenek, hanem jól is kell tudni őket alkalmazni (és pl. nem illik a random értéket beégetni az ECDSA aláírások titkos paramétereinél, ahogy azt a Sony fejlesztői tették).

Azóta eltelt négy év és ismét céltáblává vált a vállalat, igaz, ezúttal a filmekért felelős Sony Pictures Entertainment részleg (amely többek közt a Columbia Pictures, TriStar Pictures és a Metro-Goldwyn-Mayer cégeket is magába olvasztotta korábban). Az észak-koreai diktátorról szóló film - The Interview - bemutatása (tervezett dátum: 2014. december 11.) elleni tiltakozásul 2014. november 24-e előtt valamikor, valakik betörtek a rendszerbe, és - mint utólag láttuk - gyakorlatilag minden mozdítható adatot letöltöttek. Ezekről sokfelé sokfélét lehetett már olvasni, a jelen cikk a Kaspersky Lab blogján megjelent érdekességet járja röviden körül.

A Kaspersky Lab egy olyan malware mintát kapott 2014. december 4-én, amely a Sony nevére kiállított, DigiCert CA (pl. a Windows operációs rendszerek által megbízható CA) alá tartozó code signer tanúsítvánnyal került aláírásra. Bár, állítólag a konkrét, elfogott minta csak egy kísérletező mérnök proof-of-concept terméke, a tény attól még tény: legalább egy code signer titkos kulcs kiszivárgott a támadás során, amelyet egészen a 2014. december 7-i visszavonásig mindenféle futtatható állomány, library aláírására akár illetéktelenek is tudtak használni. (Megjegyzés: Bár, a CSOnline cikke 2014. december 7-i dátumot tartalmazó CRL-ről rakott fel egy képet, a mai napon – 2014. december 21. – azt lehet látni, hogy mind a CRL-ben, mind az OCSP válaszban 2014. november 1-jét jelölik meg a visszavonás dátumaként. Mintha utólag bütyköltek volna a CA rendszeróráján...)

A kérdés az, hogy vajon tényleg felhasználták-e ezt a kulcsot a támadók? A Flame kapcsán 2012. június 4-én már láthattuk, hogy mire képes egy megbízható root CA alá tartozó code signer tanúsítvány: a célzott támadás során malware-ek kerültek fel Windows update formájában különböző gépekre, amelyek a kritikus infrastruktúra részét képezték. A Sony esetében nem annyira a Windows lehet érdekes, hanem a hatalmas mennyiségű erőforrással rendelkező konzolgépek: a Sony PlayStation 4. A sok GPU mag csábító lehet, amikor lenyomatok alapján jelszavakat kell törni, de ugyanígy hasznos lehet néhány Bitcoin legyártásánál is. A konzolokról még nem érkezett hír, de a PlayStation Network környékén már jelentkeztek problémák a CNET szerint...

Hogy mire derül még fény a kiszivárgott adatok révén a Sony vagy más magánéletéből, azt nem tudom, de az okot adó film a (kiber)terrorizmus elleni küzdelem és a véleménynyilvánítási szabadság jelképévé válhat. A Sony bástyája megrogyott ugyan, de helyét rengeteg újabb bástya veheti át ebben a küzdelemben, ha a BitTorrent hálózatra felkerül minden. Ezzel adva példát a gondolatnak: „Nem mondhatom el senkinek, Elmondom hát mindenkinek” /Karinthy Frigyes/

A teljes cikk letölthető innen : http://melasz.hu/lang-hu/remository?func=startdown&id=179