Iknedēļas ziņas
Sagatavotas 04.02.2016.
Numurs 2016/5

Kontakti: prese@cert.lv
Tālrunis: 67085888

Izķēmotas vairākas mājas lapas

Tika kompromitētas un izķēmotas vairākas .lv interneta vietnes. Vietņu saturs tika aizstāts ar uzrakstiem arābu un angļu valodā, kā arī dažādām bildēm. Kaitējums nodarīts dažāda satura lapām, tajā skaitā arī kādas pašvaldības vietnei**.** Citi kaitējumi bez satura izmainīšanas vietnēm nav nodarīti. Visām kompromitētajām vietnēm tika paziņots par uzlaušanas faktu un norādīts uz veicamajiem mājas lapas drošības uzlabošanas pasākumiem.

Policijas vīruss

Aktivizējusies tā sauktā "Policijas vīrusa" web versija. Apmeklējot atsevišķas mājas lapas, lietotājam parādās paziņojums par it kā bloķētu datoru, pārkāpumu uzskaitījumu un izpirkuma pieprasījumu. Šādu paziņojumu bija saņēmis kāds lietotājs, apmeklējot kādu, visdrīzāk kompromitētu, mājas lapu. Izlecošais paziņojums nenodara kaitējumu datoram, taču to ir grūti aizvērt.

Lietotājiem šādos gadījumos iesakām aizvērt interneta pārlūku - uz Windows to var izdarīt, izmantojot taustiņu kombināciju Alt+F4 vai "Uzdevumu pārvaldnieku" (Task manager). Vēl viena iespēja ir datoru pārstartēt.
Šī krāpnieciskā lapa neveic datorvīrusa instalēšanu un nekādas paliekošas sekas datoram nerada. Lai šādas nevēlamas lapas turpmāk bloķētu, iesakām izmantot labu antivīrusu programmu, kurai ir papildu tīmekļa lapu filtrs.

Uzbrukumu veikšanai izmanto Joomla ievainojamību

CERT.LV jau informēja par satura vadības sistēmas Joomla ievainojamību, kas atklāta pagājušā gada nogalē. Joprojām neatjauninātās Joomla versijās šī ievainojamība tiek izmantota, lai veiktu dažāda veida uzbrukumus. Pagājušās nedēļas sākumā ievainojamā Joomla CMS lapā tika izvietota pikšķerēšanas lapa ar mērķi iegūt e-pastu piekļuves datus. Savukārt, vēl kādas mājas lapas apmeklētāji no mobilajām ierīcēm tika pārvirzīti uz kaitīgu interneta vietni, kas mēģina veikt datorvīrusa izpildi apmeklētāju mobilajās ierīcēs. Vēl divi Joomla ievainojamas gadījumi atklāti, kad mājas lapās tika izvietots kaitīgs Javascript fails, kas satur Angler Exploit kit rīku, ar kura palīdzību apmeklētāju datoros tiek veikta datorvīrusu lejupielāde un izpilde.

Lai pasargātu Joomla vietnes no šādiem uzbrukumiem, nepieciešams atjaunināt Joomla versiju.

MS Word dokumentā iestrādā ievainojamību

Parādījies vīruss, kas izmanto RTF ievainojamību. CERT.LV saņēma paraugu ar inficētu Microsoft Word failu, ar iestrādātu RTF (Rich Text Format) failu, kas satur datorvīrusa lejupielādi, izmantojot RTF ievainojamību (Exploit.JPFD). Šī ievainojamība tiek izmantota, lai lejupielādētu un izpildītu kaitīgu saturu.

RTF ievainojamība var tikt izmantota neatjauninātās Microsoft Office versijās 2003, 2007, 2010 un 2013 ar iespēju uzbrucējam veikt attālināta koda izpildi un iegūt lietotāja tiesības.

WiFi ievainojamība Android ierīcēs

Atklāta WiFi ievainojamība, kas attiecas uz Android ierīcēm, ko uzbrucējs var izmantot esot vienā WiFi tīklā ar upuri. Šī ievainojamība var tikt pielietota, nosūtot ļaunprātīgu bezvadu kontroles ziņojuma paketi. Šādas paketes var ietekmēt kodola atmiņu un pakļaut Android ierīci attālināta koda izpildei kodola līmenī.

Vairāk par ievainojamību: https://threatpost.com/critical-wi-fi-flaw-patched-on-android/116085/

eBay apmeklējums var pakļaut pikšķerēšanas un datu zagšanas uzbrukumiem

Klajā nācis paziņojums par eBay.com ievainojamību. Ievainojamība atrodas vietnes tiešsaistes pārdošanas platformā. Izmantojot šo ievainojamību, uzbrucējs var apiet vietnes koda validāciju un izpildīt ļaunprātīgu JavaScript, izmantojot lietotāja interneta pārlūku vai mobilo lietotni.

Vairāk par ievainojamību: https://threatpost.com/ebay-vulnerability-exposes-users-to-phishing-data-theft/116113/