Iknedēļas ziņas
Sagatavotas 07.10.2015.
Numurs 2015/09

Kontakti: prese@cert.lv
Tālrunis: 67085888

Satraucas par viedierīču ietekmi uz skolas datortīklu drošību.

Viedtelefoni, planšetes, portatīvie datori un citas mobilās ierīces ir jau pašsaprotama ikdienas sastāvdaļa arī lielai daļai skolnieku. Pieaugot šo ierīču pielietojamībai skolēnu un arī mācībspēku ikdienas darba procesā, skolas uztraucas par viedierīču ietekmi uz skolas datortīklu drošību.

Pie CERT.LV pēdējo mēnešu laikā pēc padoma bezvadu tīkla drošības jautājumos ir vērsušās vairākas skolas. Strauji pieaug viedierīču pieejamība un šo ierīču skaits arī skolās. Tās ir gan skolēnu privātās ierīces, gan skolas mācību procesā izmantotās. Arvien biežāk arī saskaramies ar drošības incidentiem, kas skar tieši mobilās platformas, tādēļ jāuzteic skolu administrācija par savlaicīgu pievēršanos šo apdraudējumu apzināšanai un risināšanai. Jau iepriekš ziņots, ka mobilām ierīcēm paredzēti vīrusi un trojāni tiek izplatīti arvien biežāk arī Latvijā. Mobilo ierīču un bezvadu tīklu drošas lietošanas prakses iesakām skatīt CERT.LV uzturētā portālā esidross.lv

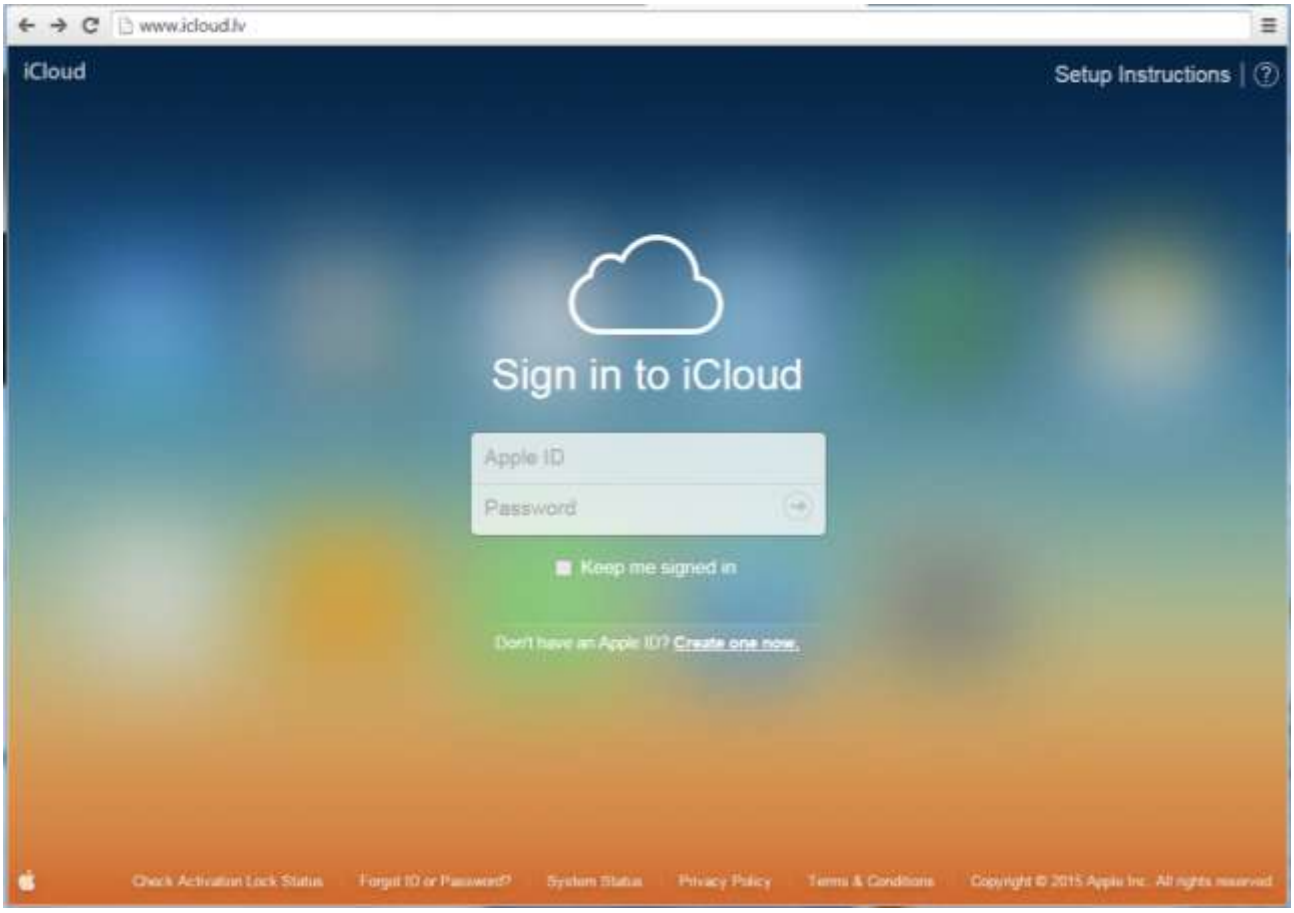
Tīmekļa vietnes Latvijā turpina izplatīt datorvīrusus ar Neutrino exploit kit starpniecību, kā arī piedalās pikšķerēšanas uzbrukumu kampaņās.

Pēdējās divās septembra nedēļās konstatētas vairākas Latvijas interneta tīmekļa vietnes, kuras izplata datorvīrusus ar Neutrino exploit kit starpniecību, kā arī piedalās pikšķerēšanas uzbrukumu kampaņās.
Visas uzbrukumos iesaistītās tīmekļa vietnes ir uzlauztas, jo tika uzturētas uz novecojušām Wordpress un Joomla satura vadības sistēmu versijām.

Uzbrucēji, neizmainot vietnes oriģinālo saturu, ievieto neredzamo instrukciju <iframe>, kura interneta pārlūku instruē apmeklēt nākamo, uzbrucēju sagatavoto resursu, kā rezultātā inficē apmeklētāja datoru ar mērķi iegūt autentifikācijas operāciju detaļas un internetbanku transakciju datus. **Latvijā aptuveni 50% no kompromitētām tīmekļa vietnēm tiek kompromitētas atkārtoti, kas norāda uz šo resursu turētāju un/vai administratoru paviršo attieksmi pret drošības ielāpu ieviešanu.**
Lielā daļā gadījumu uzlauztā lapa tiek atjaunota no rezerves kopijām ar tām pašām vecajām ievainojamībām un netiek izlabots problēmas cēlonis. Ir tikai laika jautājums (parasti dažas dienas līdz nedēļai), kad uzbrucējs atkal izmanto tos pašus "vārtus", pa kuriem ienācis iepriekš. Pikšķerēšanas kampaņas, kas uzturētas uz Latvijā esošām tīmekļa vietnēm, lielākajā daļā gadījumu ir paredzētas ārvalstu maksājumu sistēmu lietotāju datu izkrāpšanai. Divu nedēļu laikā ir aizvērtas piecas šādas vietnes.

Latvijā uztur tīmekļa vietni www.icloud.lv, lai izkrāptu Apple lietotāju datus.

Pateicoties vērīgajiem Latvijas interneta lietotājiem, CERT.LV redzeslokā nonāca krāpnieciskiem mērķiem radīta tīmekļa vietne www.icloud.lv. Tā apzināti izveidota, lai izkrāptu Apple lietotāju datus. Domēna vārda reģistrācijas detaļas nodots skaidrot Valsts policijai. Tīmekļa vietne šobrīd ir aizvērta. Vietnes ekrānšāviņš redzams zemāk.



CERT.LV publicē pētījumu par interneta troļļu aktivitātēm ar mērķi izplatīt datorvīrusus.

CERT.LV 1. oktobrī notikušajā IT drošības konferencē prezentēja pētījuma rezultātus par interneta troļļu aktivitātēm Latvijas interneta vidē. ar mērķi izplatīt "smalkus" datorsistēmu inficēšanas rīkus "Turla", kurus, iespējams, sagatavojušas ar Krievijas valdību saistītas organizācijas vai dienesti.

Šo interneta troļļu atšķirība no klasiskā gadījuma, kad galvenais mērķis ir šķobīt sabiedrības viedokli, ir papildaktivitātes Latvijas interneta ziņu resursos, kur ar komentāru starpniecību tie izplata saites uz plašu un sarežģītu uzbrukumam sagatavotu infrastruktūru, kura vērtīgos mērķus (pārsvarā valsts iestādes) atlasa pēc dažādiem nosacījumiem inficēšanās procesā. Visbiežāk parasts mājas lietotājs nemaz netiek "apkalpots". Prezentācija par pētījumu pieejama:
https://cert.lv/uploads/uploads/Teivans%20CERT_trollis_2015%20v3.1.pdf

Maldina klientus, radot aizdomas par rēķinu apmaksas krāpniecību.

IT ārpakalpojuma kļūda degvielas tirgotājam Latvijā maldina desmitiem klientu, radot aizdomas par iespējamu degvielas rēķinu apmaksas krāpniecību interneta vidē.

CERT.LV saņēma informāciju no vairākiem interneta lietotājiem par aizdomīgiem e-pasta ziņojumiem, kuros tiek pieprasīta degvielas rēķinu apmaksa. Tā kā arī datorvīrusu izplatīšanas kampaņās vairākkārt pielietota

rēķinu tematika, tad šie kļūdaini atsūtītie e-pasti saņēmējus darīja bažīgus. Noskaidrojot apstākļus, secināts, ka šis gadījums nav krāpniecība. Ļeģitīma degvielas tirgotāja e-rēķinu pārvaldība ir nodota ārpakalpojumā, kur datorsistēmas kļūdas rezultātā ir izsūtīti e-pasti nekorektiem adresātiem. Šādi gadījumi uzskatāmi demonstrē, cik daudz mūsu ikdienā ir uzticēts datorsistēmām un atgādina, ka ar naudu saistītās lietas interneta vidē ir vairākkārt jāpārbauda. **Cilvēku ziņošana par šādiem gadījumiem pozitīvi iezīmē Latvijas interneta sabiedrības attīstības tendences un spēju pievērst uzmanību detaļām, lai izvairītos no iespējamas krāpniecības.**

IKT drošības entuziasts informē CERT.LV par apjomīgu mājas/ofisa maršrutētāju kompromitēšanas kampaņu.

Pārbaudot sniegto informāciju CERT.LV secina, ka tā ir patiesa un noderīga incidenta izmeklēšanai. Uzbrukuma kampaņas tiešie mērķi pagaidām nav skaidri, bet zināms, ka tiek mainīta DNS serveru konfigurācija, lai kompromitētā maršrutētāja lietotāji DNS pieprasījumus vaicātu uzbrucēju sagatavotam serverim.