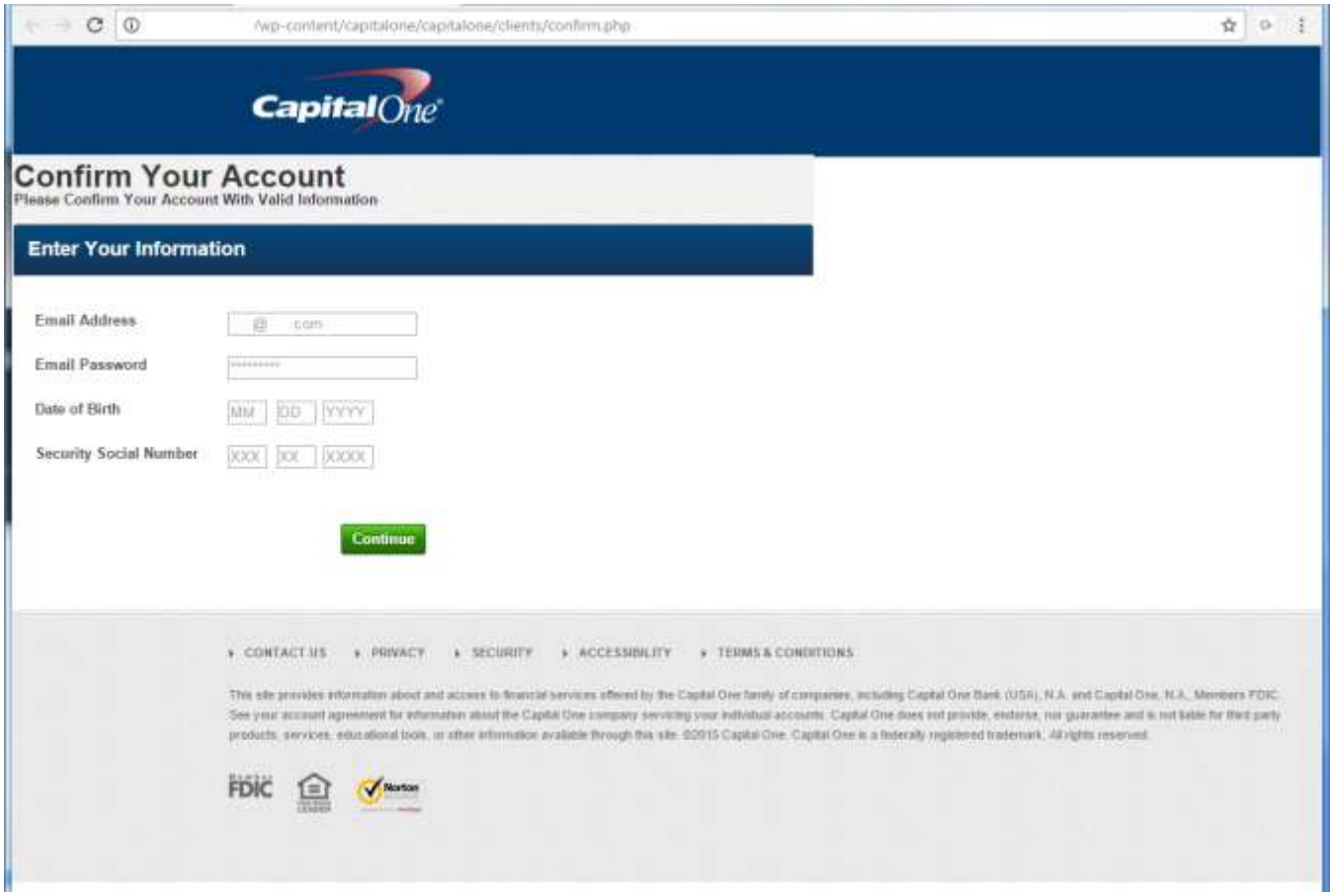
Iknedēļas ziņas
Sagatavotas 17.01.2017.
Numurs 2017/2

Pikšķerēšanas lapa izmanto Wordpress ievainojamību

Novecojušu satura vadības sistēmu izmantošana arvien ir biežākais iemesls to uzlaušanai. Kārtējā Wordpress CMS bāzēta lapa tikusi izmantota, lai izvietotu bankas karšu datu izkrāpšanas vietni.



Uzņēmuma vadības vārdā mēģina izkrāpt naudu

10.01.2017. kāda uzņēmuma grāmatvedība saņēmusi viltotu e-pastu, kur tās valdes locekļa vārdā pieprasīts veikt 15000EUR pārskaitījumu uz banku Austrijā:

UniCredit Bank Austria AG
Schottengasse 6-8 1010 Wien
Account name: Sabine Toifl
IBAN: AT041200050194075516
BIC: BKAUATWW

Grāmatvede sazinājās ar uzņēmuma vadību un noskaidrojot, ka pieprasījums nav īsts, maksājumu neveica. Šāds incidents ir uzskatāms kā "CEO Krāpšanas" gadījums.

Linux Venom Rootkit

Eiropas E-infrastruktūras drošības komanda EGI (EGI CSIRT) izanalizēja Linux sistēmlauzni (rootkit), kas nesen tika atklāts. Venom Rootkit dod iespēju uzbrucējam attālināti pārņemt kontroli pār Linux iekārtām.
Balstoties uz terminu, kas tika lietots sistēmlaužņa komunikācijas protokolā, tas tika nosaukts par Venom.
Detalizēta analīze ir pieejama: https://wiki.egi.eu/wiki/Venom_Rootkit

Padziļināti testi atklāj kritiskas ievainojamības pašvaldību lapās

CERT.LV jau ziņoja, ka tika veiktas Latvijas pašvaldību interneta vietņu drošības pārbaudes.
Pamatojoties uz pārbaužu rezultātiem, ar CERT.LV sazinājās kāda pašvaldība un lūdza veikt padziļinātus ielaušanās testus visās tās vietnēs.
Padziļinātie testi netika veikti vietnēs, kas izmanto atvērtā koda CMS, un par kuru ievainojamībām ir ziņots pašu izstrādātāju vietnēs. Taču veicot vispārējo apskati, CERT.LV konstatēja, ka tajās izmantotās CMS versijas ir novecojušas un dažas no tām satur kritiskas ievainojamības. Kritiskas ievainojamības tika identificētas četrās pašvaldības uzturētās vietnēs.

2017. gadā ļaunatūra kļūs gudrāka

Gada sākums parasti ir laiks, kad tiek apkopti pagājušā gada notikumi un izteikti minējumi par nākamā gada tendencēm.
Pēc CERT.LV novērojumiem, pagājušajā gadā izplatītākais apdraudējums bija izspiedējvīrusi. No tiem cieta gan valsts un pašvaldību iestādes, gan uzņēmēji, gan privātpersonas. Labākajā gadījumā vīruss traucēja iestādes vai personas ikdienas darbu, bet sliktākajā, tika zaudēti dati. Vīruss radīja ievērojamus materiālos zaudējumus, jo vairākiem mazajiem un vidējiem uzņēmumiem nebija citas iespējas, kā atjaunot uzņēmuma datoru darbu, kā vien samaksāt izspiedējiem. Pēc CERT.LV aplēsēm aptuveni 20% cietušo maksā izspiedējiem par datu atgūšanu.
Finansiāli apjomīgus zaudējumus uzņēmumiem radīja "CEO krāpšana" jeb biznesa e-pasta kompromitēšana, kur vienas krāpniecības radītie zaudējumi bija līdz pat vairākiem simtiem tūkstošu EUR. Par šādiem incidentiem tika ziņots visa gada garumā vairākas reizes mēnesī.

2017. gada prognoznes ir, ka pilnveidosies uzbrukumu dažādība - vairāk tiks uzbrukts IoT (Internet of Things) jeb lietu interneta ierīcēm un aplikācijām. Turpinās augt arī mobilo draudu apjoms, jo tiks pilnveidotas iespējas izkrāpt bankas datus un piekļūt naudas līdzekļiem. Kopumā uzbrukumi kļūs sarežģītāki un vairāk tiks izmantotas pieejamās tehnoloģiskās iespējas.
Lietu internets ietver sevī dažādu veidu ierīces vairākās industrijās - medicīnā, ražošanā, izglītībā, sadzīvē, mājsaimniecībā. Izplatītākie uzbrukumu veidi var būt datu zādzība, piekļuves lieguma uzbrukumi citām sistēmām, haktīvisms. Lietu interneta apgūšana arī ievērojami samazinās patērētāju privātuma iespējas, jo pārāk daudzas iekārtas novēro, klausās, ieraksta un apkopo lietotāja darbības.
Savukārt mobilo iekārtu lietotājiem galvenie apdraudējumi būs izspiedējvīrusi, banku vīrusi un kompromitētas aplikācijas.
CERT.LV par savām 2017. gada prioritātēm ir izvēlējies mobilo incidentu izpēti un lietu interneta iekārtu drošību.

2016. gadā nebijis notikums ir lietu interneta (IoT) robotu tīkla veiktais masīvais DDoS uzbrukums DNS pakalpojuma nodrošinātājam *Dyn*, kurš uz dažām stundām padarīja nepieejamas daudzas populāras globālā tīmekļa vietnes, tādas kā *Twitter*, *Reddit*, *Github*, *Soundcloud*, *Spotify* u.c. Latvijā tika identificēti vairāki simti ievainojamu iekārtu, kas varētu būt daļa no 100 000 inficēto IoT iekārtu, kas piedalījās pirmajā globālajā lietu interneta uzbrukumā.