## APRĪLĪ AKTUĀLI:

- Gotcha.pw dzīves mācībstunda slinkajiem
- „Drupalgeddon 2" ievainojamība
- MikroTik maršrutētāja ievainojamība
- Kiberstāsti
- CERT.LV aktivitātes
- Interesanti fakti par „Locked Shields 2018"
- Pasākumu kalendārs

Attēli: Pixbay.com

## GOTCHA.PW DZĪVES MĀCĪBSTUNDA SLINKAJIEM

Aprīļa beigās šķietami katrs otrais Latvijas interneta lietotājs ziņkārības vai satraukuma dzīts centās sevi sazīmēt gotcha.pw publiskotajā e-pastu un paroļu datubāzē. Daži varēja atvieglojumā uzelpot, savukārt citus sagaidīja nepatīkams pārsteigums.

CERT.LV vēlas nomierināt un **vēlreiz uzsvērt, ka paroles, lai arī reālas, nav konkrēto e-pastu paroles, bet gan to vietņu paroles, kurās cilvēks ir pierakstījies,** izmantojot konkrēto e-pasta adresi.

Problēma var rasties situācijā, kad lietotājs (bieži vien slinkuma iedvesmots) **izmanto vienu un to pašu paroli vairākos tīmekļa resursos - šādā gadījumā norādītā parole ļoti iespējams ir arī attiecīgā e-pasta parole,** un CERT.LV aicina nekavējoties to nomainīt, izmantojot katrai tīmekļa vietnei unikālu un drošu paroli. Vienas paroles izmantošana vairākās vietnēs ir pretrunā labajai praksei, un no šādas rīcības būtu jāizvairās.

VAIRĀK INFORMĀCIJAS:

- **Piedāvājam padomus savai aizsardzībai:** https://cert.lv/lv/2018/04/nopublicetas-paroles-atgadinajums-ieverot-labo-praksi

## KIBERLAIKAPSTĀKĻI

|  |  |  |  |  |
|---|---|---|---|---|
| **PAKALPOJUMA PIEEJAMĪBA** | **LIETU INTERNETS** | **DATU NOPLŪDE** | **ĻAUNATŪRA UN IEVAINOJAMĪBAS** | **KRĀPŠANA** |
| Būtiski incidenti netika reģistrēti | Būtiski incidenti netika reģistrēti | Gotcha.pw publicētie e-pasti un paroles | Drupalgeddon2, Mikrotik ievainojamības | Šantāža un pikšķerēšanas kampaņas Facebook |

## MAIJA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

**Biļetena tēma: "Vispārīgā datu aizsardzības regula"**

Jauno Vispārīgo datu aizsardzības regulu (GDPR) ir sagatavojusi Eiropas Savienība un tā stāsies spēkā 2018.gada 25.maijā. GDPR būs piemērojama visām organizācijām, kas apstrādā Eiropas Savienības iedzīvotāju personas datus, neatkarīgi no tā, kur atrodas pati organizācija. GDPR paredz, ka organizācijai ir jānodrošina ES iedzīvotāju personas datu privātums un drošība.

**Pilna raksta versija pieejama:** https://cert.lv/uploads/201805-OUCH-Maijs-Latvian.pdf

## „Drupalgeddon2" ievainojamība

Aprīļa TOP ievainojamības

Marta beigās Drupal izstrādātāji nāca klajā ar labojumiem kritiskai Drupal satura vadības sistēmas ievainojamībai ar identifikācijas kodu - **CVE-2018-7600** jeb plašāk popularizētai arī kā Drupalgeddon2. **Ievainojamībai pakļautas vairāk kā miljons mājaslapu** ar noklusēto vai standarta konfigurāciju, un tā **sniedz iespēju ļaundariem attālināti pārņemt kontroli pār vietnes serveri, un augšupielādēt izpildāmo kodu.** Ievainojamība ietekmē Drupal versijas 7.x un 8.x. Aprīlī konstatēti neskaitāmi gadījumi, kad *Drupalgeddon2* arī sekmīgi ticis izmantots ļaunprātīgiem nolūkiem.

Ļaundari minēto ievainojamību izmanto, lai uz neaizsargātās vietnes servera augšupielādētu ļaunatūru, kas **inficē vietnes apmeklētājus**. Kā viens no populārākajiem infekcijas mērķiem **ir izmantot apmeklētāju inficēto iekārtu jaudu, lai slepus „raktu" kriptovalūtu.** Citi nesankcionēti ievainojamības pielietojumi ir **robotu tīkla jeb *botnet* paplašināšana** piekļuves atteices uzbrukumu (DDoS) veikšanai un **šifrējošo vīrusu augšupielāde uz vietnes servera.**

CERT.LV aicina Drupal lietotājus pēc iespējas ātrāk veikt atjauninājumus, pasargājot gan savu vietni, gan tās apmeklētājus no nepatīkamiem pārsteigumiem.

**Vairāk informācijas:**

- **Hackers Exploiting Drupal Vulnerability to Inject Cryptocurrency Miners:** https://thehackernews.com/2018/04/drupal-cryptocurrency-hacking.html
- **Drupal users take cover - code – execution bug is being actively exploited:** https://arstechnica.com/information-technology/2018/04/with-drupalgeddon2-still-under-attack-drupal-fixes-a-new-critical-flaw/
- **Attēls:** www.onlinewebfonts.com/icon/288845

## MikroTik maršrutētāja ievainojamība

Aprīļa TOP ievainojamības

CERT.LV aprīlī brīdināja par jaunu, kritisku *MikroTik* maršrutētāja (*RoutersOS*) ievainojamību, kas **skar visas maršrutētāju versijas, sākot ar *v6.29*.** Uzbrukumu iespējams veikt, izmantojot *Winbox* pieslēguma portu.

**Lai novērstu apdraudējumu:**

- **jāierobežo piekļuve *Winbox* portam** no publiskā tīkla, izmantojot ugunsmūri (*Firewall*), vai iekārtas konfigurācijā "*IP -> Services*" norādot, no kurām IP adresēm atļauts pieslēgties "*Allowed From*";
- jānomaina parole;
- jāveic atjauninājumi, tiklīdz tādi ir pieejami.

**Vairāk informācijas:**

- **Par ievainojamību un atjauninājumiem:** https://forum.mikrotik.com/viewtopic.php?f=21&t=133533&p=656255#p656255

## Locked Shields 2018

CERT.LV aktivitātes

No š.g. 23. līdz 27. aprīlim notika NATO apvienotā kiberaizsardzības izcilības centra organizētās ikgadējās "Locked Shields 2018" mācības. Tās ir vērienīgākās starptautiskās kiberdrošības mācības pasaulē, un tā ir arī unikāla iespēja kiberdrošības ekspertiem intensīva stresa apstākļos trenēt iemaņas IT sistēmu un kritiskās infrastruktūras aizsardzībā.

Šogad Latvijas apvienotā komanda, kuru veidoja eksperti no CERT.LV un Kiberaizsardzības vienības, kā arī pārstāvji no Amerikas Savienoto Valstu (US EUCOM) un Kanādas bruņotajiem spēkiem, **21 komandas konkurencē ieguva 8. vietu.**

**Vairāk par „Locked Shields 2018" lasi šeit:** https://cert.lv/lv/2018/04/starptautiskas-kiberdrosibas-macibas-locked-shields-2018

## Baltic Domain Days 2018


„Par godu .LV 25 gadu jubilejai aprīlī Melngalvju Namā, Rīgā, noritēja pirmais īpaši Baltijas valstu domēnu nozarei veltītais pasākums - Baltic Domain Days. Pārstāvji no .LV, .LT , .EE, .EU, .UA, un .SE reģistriem, reģistratūrām, ICANN, LIKTA, VID, Valsts Policijas un CERT.LV dalījās pieredzē un diskutēja par domēna vārdu atslēgšanu, bloķēšanu, kibernoziegumu un intelektuālā īpašuma tiesību aktualitātēm Baltijas valstīs.

.LV reģistra uzturētājs īpaši pateicas CERT.LV vadītājai B. Kaškinai par moderēto paneļa diskusiju "Domains and cybercrime: is there a light at athe end of the tunnel?", kurā tika spriests, kā domēna vārdus padarīt uzbrucējiem nepievilcīgus un vai nākotnē tiks atrasts līdzsvars starp privātumu un drošību," komentē D.Ludviga, .LV reģistra uzturētāja mārketinga un komunikāciju vadītāja.

**Vairāk par pasākumu:** https://www.nic.lv/lv/baltic-domain-days-apkopojums

## Dalība RSA konferencē Sanfrancisko



Aprīļa pirmajā pusē CERT.LV IT drošības speciālists Kārlis Podiņš kopā ar zinātnieku *Kenneth Geers* no *Comodo Cybersecurity* uzstājās starptautiskajā kiberdrošības konferencē „RSA Conference" Sanfrancisko, kur abu prezentēto **pētījumu vēlāk citēja arī viens no vadošajiem pasaules tiešsaistes tehnoloģiju ziņu portāliem „The Register".**

Kārlis Podiņš: „Pētījums ir par izpildāmo datņu rediģēšanu/mainīšanu bez pieejas pirmkodam. Konkrēti, kā tehnoloģiski sarežģītā (APT) ļaundabīgā datnē iespējams nomainīt komandcentra (C&C) domēnu, tādējādi iegūstot kodu, ar ko veikt kiberuzbrukumu. Principā ļaundabīgā datne tiek atkal izmantota (vai nozagta). Tas ir ievērojami lētāk nekā patstāvīgi izveidot visu no nulles, kā arī tas dod iespēju ticami izlikties par oriģinālo uzbrucēju (false flag). Pētījumā praktiski demonstrēts, kā veikt šādas darbības, kā arī apskatīta izrietošā ietekme stratēģiskā līmenī."

**Portāla „The Register" raksts:** https://www.theregister.co.uk/2018/04/18/researchers_warn_of_regifted_malware/
**K. Podiņa prezentācija:** https://www.youtube.com/watch?v=HonVm8eSf2c

## Interesanti fakti par „Locked Shields 2018"

## KIBERSTĀSTI

**Aprīļa** otrajā pusē CERT.LV saņēma ziņojumu no kāda vīrieša par naudas izspiešanas mēģinājumu sociālajā tīklā *Facebook.* Vīrieti *Facebook* uzrunāja kāda nepazīstama sieviete, kas šķietami vēlējās iepazīties. Sieviete ar upuri sazinājās, izmantojot video zvanu, un tā saturu slepeni ierakstīja. Pēc tam sieviete draudējusi publicēt video ierakstu internetā, ja vīrietis nepārskaitīs noteiktu naudas summu. Incidenta izpētes laikā CERT.LV secināja, ka sievietes *Facebook* profils jau ir ticis veiksmīgi bloķēts. CERT.LV atgādina, ka šādos gadījumos efektīvākā taktika ir pārtraukt jebkādu komunikāciju ar izspiedēju, izvairoties radīt iespaidu, ka esat gatavi maksāt. Jo, ja tiek radīts iespaids, ka upuris ir gatavs maksāt, – pieprasītā summa var tikai pieaugt.

• • •

**CERT.LV** saņēma ziņojumu no kādas satrauktas mātes par šaubīgu Latvijas interneta veikalu, kas tirgo zīmola apavus par aizdomīgi zemām cenām. Sieviete atklāja, ka minētais interneta veikals sekmīgi piesaistījis jauniešu auditoriju, un arī viņas meita plānojot te pasūtīt apavus. Tādēļ sieviete lūdza CERT.LV pārbaudīt, cik uzticama ir šī vietne. Izpētes rezultātā tika secināts, ka vietne visticamāk tiešam ir krāpnieciska rakstura, par ko liecina sekojošie faktori: vietne izveidota nesen, tā izvietota bezmaksas lapu uzturēšanas vietnē WIX, kas ir populāra krāpnieku vidū, kā arī veikalam trūkst vajadzīgās kontaktinformācijas, kas paredzēta MK "Noteikumi par distances līgumiem". Attiecīgi CERT.LV ieteica sievietei šajā vietnē pirkumus neveikt, jo, pat saņemot gaidīto preci, tā var izrādīties viltojums.

• • •

**Tika** saņemts ziņojums no kāda interneta lietotāja par tipisku krāpniecisku e-pastu sliktā latviešu valodā, kas sūtīts it kā *Facebook* korporācijas biroja vārdā. E-pasts informē, ka tā saņēmējs ir izvēlēts saņemt naudas balvu 500 000 ASV dolāru apmērā. Cik noprotams no e-pasta satura, tad balvu iespējams izņemt bankomātā ar tam speciāli izsniegtu bankas karti, kuru iespējams saņemt, sūtot savus datus uz *Lloyds Bank.* E-pasta turpinājumā tiek norādīts e-pasts, caur kuru ar šo banku iespējams sazināties. Lietotājs krāpniecisko e-pastu savlaicīgi atpazina, un finansiālus zaudējumus necieta.

## TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

**29.** **MAIJS – 1. JŪNIJS -** CyCon 2018 konference, Tallina

**01.** **JŪNIJS** - Accenture Night Hack 2018

**05.-08.** **JŪNIJS** - Cyber Europe 2018 mācības

**22.** **JŪNIJS** - Referātu pieteikšanas termiņš konferencei "Kiberšahs 2018"

**ADRESE:** RAIŅA BULVĀRIS 29, RĪGA, LV-1459, LATVIJA;
**TELEFONS:** +371 67085888;
**E-PASTS:** ZIŅOT PAR INCIDENTU: CERT@CERT.LV / SABIEDRISKĀS ATTIECĪBAS: PRESE@CERT.LV
**VIETNE:** WWW.CERT.LV