WWW.CERT.LV

FEBRUĀRĪ AKTUĀLI:

- Fiksēts rekordliels DDoS uzbrukums
- Facebook sāga
- WordPress spraudņu ēnas puses
- DNS RPZ jeb DNS ugunsmūris
- Kiberstāsti
- DDoS uzbrukums bilesuparadize.lv
- CERT.LV aktivitātes
- Skaitļi un fakti

Attēli: Pixabay.com

FIKSĒTS REKORDLIELS DDOS UZBRUKUMS

Marta sākumā pasaule kļuva par liecinieci jaunam rekordam - **interneta pakalpojumu sniedzējs *GitHub* piedzīvoja 1,3 Tb/s lielu piekļuves atteices jeb DDoS uzbrukumu**. Šoreiz uzbrukumam tika izmantoti *Memcached* serveri ar nedrošu noklusēto konfigurāciju, kas uzbrucējam pieejamo datu plūsmu palielināja 51 000 reizes, raidot upura iekārtu virzienā milzīgu datu plūsmu.

Tikai četras dienas vēlāk šis rekords tika pārspēts. Tīklu drošības **kompānija *Arbor Networks* fiksēja DDoS uzbrukumu kādam savam klientam, kas sasniedza 1,7 Tb/s**. Arī šajā gadījumā tas bija amplifikācijas uzbrukums, kurā izmantoti *Memcached* serveri. Uz UDP portu 11211 tika sūtīti ļaunprātīgi pieprasījumi, izmantojot viltotu (spoofed) IP adresi, kas atbilda upura IP adresei. Ļaunprātīgajā pieprasījumā tika iekļauts arī teksts ar izpirkuma maksas pieprasījumu 50 XMR (kriptovalūta Monero, apmēram 11 000 EUR) par uzbrukuma pārtraukšanu.

Memcached ir populāra atvērtā koda izkliedētās kešošanas sistēma, kas paredzēta tīmekļa lietotņu ātrdarbības uzlabošanai kā, piemēram, paātrinot datubāzei veikto pieprasījumu apstrādi. ***Memcached* izmanto tādas tīmekļa vietnes kā *Facebook, Flickr, Twitter, YouTube* un *GitHub*.**

Lai padarītu DDoS uzbrukumus globāli neiespējamus, **jāievieš BCP38 labās prakses standarts**, kas liedz izsūtīt tīkla paketes ar viltotu paketes IP adresi. Kā arī, lai nekļūtu par apdraudējumu sev un citiem, jānodrošina izmantoto *Memcached* serveru un arī citu iekārtu pietiekama aizsardzība, veicot šo iekārtu konfigurāciju atbilstoši labajai praksei un atbilstoši kontrolējot, kas un kā šīm iekārtām var piekļūt. Arī sekošana atjauninājumiem ir būtiska - *Memcached 1.5.6.* versijā tika veikta pāreja no UDP uz TCP protokolu.

VAIRĀK INFORMĀCIJAS:

- **Uzbrukumi, izmantojot Memcached:** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1
- **Uzbrukumi GitHub un Arbor Networks:** https://thehackernews.com/2018/03/ddos-attack-memcached.html
- **Memcached atjauninājumi:** https://github.com/memcached/memcached/wiki/ReleaseNotes156

KIBERLAIKAPSTĀKĻI

PAKALPOJUMA PIEEJAMĪBA	LIETU INTERNETS	DATU NOPLŪDE	ĻAUNATŪRA UN IEVAINOJAMĪBAS	KRĀPŠANA
Pasaulē lielākais DDoS un Dz.sv. biļetes	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Drupal kritiska ievainojamība	MS Outlook pikšķerēšanas kampaņas

FACEBOOK SĀGA PĀRŅEM PASAULI UN ARĪ LATVIJU

Marta nogalē Latvijas *Facebook* lietotāju sirdis un prātus satrauca datu drošības jautājumi. Plaši izskanējušās ziņas par *Cambridge Analytica* sniegto atbalstu dažādām pirmsvēlēšanu kampaņām un *Facebook* lietotāju datu neētisku izmantošanu ir kārtējais atgādinājums lietotājiem - rūpīgi sekojiet līdzi, kādās aplikācijās un vietnēs izmantojat *Facebook* autentifikācijas iespējas un kādas tiesības šai aplikācijai vai vietnei dodat savu datu izmantošanā.

Ir **vērts ik pa brīdim pārskatīt aplikāciju sarakstu**, kurām sniegtas tiesības piekļūt jūsu *Facebook* profilam, un informācijas apjomu, kuru šīs aplikācijas drīkst izgūt no jūsu profila.

Ja *Facebook* pārlūkošanai izmantojat datoru, klikšķiniet uz lejupejošās bultiņas augšējā labajā stūrī, izvēlieties *Settings*, tad *Apps*. Parādīsies saraksts ar visām aplikācijām, kurās esat autorizējušies, izmantojot *Facebook.*

Ja *Facebook* pārlūkošanai izmantojat mobilo tālruni, atveriet izvēlni (augšējā labajā stūrī Android, apakšējā labējā stūrī iOS iekārtām), izvēlieties *Settings & Privacy*, tad *Acount Settings, Apps, Logged in with Facebook.*

Jūs varat samazināt katrai konkrētai aplikācijai piešķirtās tiesības (zīmuļa ikona pie aplikācijas), kā arī atsaukt visas tiesības, izdzēšot aplikāciju.

VAIRĀK INFORMĀCIJAS:

- **Par privātumu, lietojot Facebook:** https://www.wired.com/story/facebook-privacy-apps-ads-friends-delete-account/
- **Cambridge Analytica gadījums:** https://www.theguardian.com/us-news/2018/mar/22/steve-bannon-on-cambridge-analytica-facebook-data-is-for-sale-all-over-the-world

WORDPRESS SPRAUDŅU ĒNAS PUSES

WordPress (WP) ir bezmaksas atvērtā koda satura vadības sistēma, kuras pamatā ir programmēšanas valoda – PHP un datu bāzu vadības sistēma MySQL. *WordPress* tiek plaši izmantota mājaslapu un blogu izstrādē, un tā ir pieejama ikvienam - kā iesācējiem, tā profesionāļiem. **No visām pasaules mājaslapām – 30,4% pamatā ir tieši *WordPress.***

WP piedāvāto iespēju klāsts, pateicoties spraudņu *(plugins*), tēmu *(themes)* un rīku *(widgets)* sortimentam, ir tikpat kā neierobežots. Piemēram, **šobrīd ir pieejami gandrīz 55 tūkstoši dažādu spraudņu.** Tomēr, kā liecina statistikas dati, tieši spraudņi bieži vien ir citkārt drošas mājaslapas „ahileja papēdis". Pērn, **54% no visām ievainojamībām, kas skāra *WordPress*, bija saistītas tieši ar spraudņiem.** 2017. gadā WordPress ievainojamību TOP augšgalā ierindojās – starpvietņu skriptēšana *(Cross Site Scripting)* un SQL injekcijas *(SQL Injection).*

WP spraudņus izstrādā gan *WordPress* kopienas programmētāji, gan arī privātas firmas un pašdarbnieki, un **spraudņos atklātās ievainojamības mēdz būt ne tikai nepārdomāta kļūda, bet citkārt arī - apzināta un mērķtiecīga rīcība.** Jeb salīdzinājumam no ikdienas dzīves situācijas - kāpēc gan auto pārdevējam nepaturēt tavas automašīnas atslēgas? Tomēr lielākā riska grupā ietilpst tie spraudņi, kam ir augsts izmantošanas un lejupielāžu reitings, bet ir vāja vai neeksistējoša atjauninājumu politika. **Attiecīgi mūsu mājaslapas drošība ir mūsu pašu rokās,** - ja ignorēsim atjauninājumus, spraudņus lejupielādēsim no apšaubāmiem avotiem, pieļausim neprecizitātes *WordPress* konfigurācijas procesā, tad varam arī nebrīnīties, ka kāds nelūgts ciemiņš nolems ienākt pa mūsu „vaļā atstātajām durvīm".

Ko darīt, lai sevi pasargātu? Pirmkārt, ieteikums būt modriem un **izmantot pieejamās atjauninājuma iespējas**, tiklīdz tādas parādās – gan pašam *WordPress*, gan arī spraudņiem, tēmām un rīkiem. Otrkārt, jo vairāk spraudņu mājaslapā, jo lielāka iespēja, ka kādā no tiem, ja ne šodien, tad rīt – tiks atklāta ievainojamība. Tādēļ – **visu lieko vai neizmantoto ieteikums no mājaslapas izņemt**. Treškārt, ieteikums spraudņus **lejupielādēt tikai no uzticamiem un pārbaudītiem izstrādātājiem,** un pārdomāt, vai kārdinošā bezmaksas *premium* versija no nezināma izstrādātāja patiesībā nav tikai „lāča pakalpojums" mājaslapas drošībai.

VAIRĀK INFORMĀCIJAS:

- **WordPress statistika un tirgus daļa:** https://w3techs.com/technologies/details/cm-wordpress/all/all
- **Lielākais WordPress ievainojamību avots:** https://www.wpwhitesecurity.com/wordpress-security/statistics-highlight-main-source-wordpress-vulnerabilities/

DNS RPZ JEB DNS UGUNSMŪRIS

CERT.LV sadarbībā ar NIC.LV ir uzsācis darbu pie DNS RPZ *(Domain Name Service Response Policy Zone)* jeb DNS ugunsmūra *(DNS firewall)* izveides, **kura mērķis ir aizsargāt lietotājus no ļaunprātīga satura internetā,** kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem, tādiem kā domēna vārdiem, IP adresēm, u.c. DNS RPZ ļaus DNS servera administratoram pielāgot globālo DNS informāciju un nodrošināt modificētas atbildes uz jautājumiem. Risinājums balstīts uz Šveices kolēģu veiksmīgo pieredzi.

INFORMĀCIJAI: Ikviens, kurš vēlas izmantot DNS RPZ, lūdzu, sazināties ar CERT.LV rakstot uz cert@cert.lv.

Lai nodrošinātu papildu aizsardzību, DNS ugunsmūris (RPZ) tiks uzturēts NIC.LV rekursīvajā DNS serverī cache.nic.lv. **Pakalpojums būs pieejams BEZ MAKSAS visiem**, kuri izmanto NIC kešserveri cache.nic.lv: IPv4 adress: 91.198.156.20 **VAI** IPv6 adress: 2a02:500:4400:400::4

Papildu informācija par DNS RPZ pieejama:

1. DNS Response Policy Zones: https://dnsrpz.info/
2. BIND9 - Response Policy Zone Configuration: http://www.zytrax.com/books/dns/ch7/rpz.html
3. Taking Back the DNS: http://www.circleid.com/posts/20100728_taking_back_the_dns/
4. NIC.LV ".LV Reģistratūru avīze" Nr6.: https://www.nic.lv/static/data/NIC_Newsletter_2018Nr6.pdf

SKAITĻI UN FAKTI

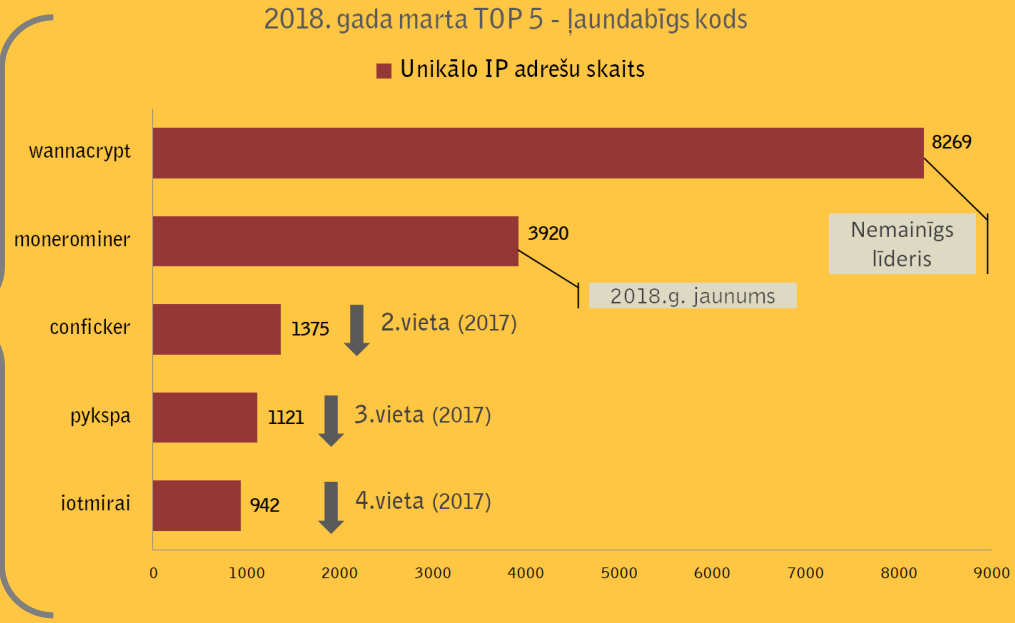
wannacrypt – Šifrējošs izspiedējvīruss. Vīruss izpilda kaitīgu kodu, kura izplatīšanā izmanto ievainojamību SMBv1 protokolā.

moneromіner – Ļaunatūra, kas tiek izmantota, lai aktīvi raktu Monero kriptovalūtu . Izmanto iekārtas CPU jaudu.

conficker – Novecojis postošs datorvīruss, kas uzbrūk Microsoft Windows operētājsistēmām.

pykspa – Datorvīruss, kas izplatās caur Skype.

iotmirai – Ļaunatūra, kas skenē nedrošas IoT ierīces un pievieno tās robotu tīklam, ko tālāk izmanto DDoS uzbrukumiem.



APRĪĻA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: "Kā atpazīt pikšķerēšanu"

E-pasta un ziņu apmaiņas pakalpojumi *(Skype, Twitter, Snapchat u.c.)* ir vieni no populārākajiem mūsdienu saziņas līdzekļiem. Mēs tos izmantojam katru dienu gan darba vajadzībām, gan arī saziņai ar draugiem un ģimeni. Ņemot vērā faktu, ka tik plaša sabiedrības daļa paļaujas uz šiem saziņas līdzekļiem, tos labprāt pikšķerēšanas uzbrukumiem izmanto arī kibernoziedznieki.

Pilna raksta versija pieejama: https://cert.lv/uploads/201804-OUCH-April-Latvian.pdf

Kiberstāsti

• • •

IT drošības speciālists Nils Putniņš sadarbībā ar biedrību *"Digital Security Alliance"* informēja CERT.LV par atklātu SQL ievainojamību kāda starptautiska uzņēmuma tīmekļa vietnē. Izmantojot ievainojamību, bija potenciāli iespējams nesankcionēti izgūt uzņēmuma klientu datus. Ievainojamības atklāšanā tika ievēroti atbildīgas ievainojamību atklāšanas (responsible disclosure) pamatprincipi un apdraudējumu izdevās operatīvi novērst.

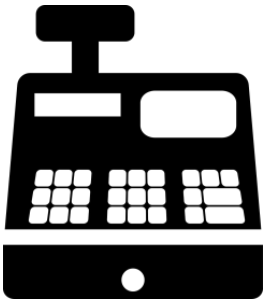
• • •

Februāra beigās un marta sākumā CERT.LV no vairākiem lietotājiem, t.sk. pašvaldību iestādēm, saņēma ziņojumus par krāpnieciskiem e-pastiem MS Outlook vārdā. E-pasti tika saņemti no kāda uzlauzta lietotāja e-pasta ar atpakaļ adresi - latviainfo@microsoft.lv. Tajos tika lūgts atjaunot e-pastu uz jaunāku MS Outlook versiju, lai saņemtu tobrīd it kā „aizturētās ziņas". Tālāk atjauninājumu iegūšanai tika piedāvāta saite uz formu, kurā lūgts ievadīt lietotāja e-pasta konta informāciju. Krāpnieciskā e-pasta mērķis bija izvilināt e-pasta lietotājvārdu un paroli. Visos gadījumos e-pasti tika atpazīti kā krāpnieciski un lietotāji zaudējumus necieta. CERT.LV sazinājās ar lapas uzturētāju, un pikšķerēšanas forma tika izņemta.

• • •

Kāda sieviete informēja CERT.LV par saņemtu krāpniecisku e-pastu Booking.com vārdā, kā rezultātā viņa cietusi zaudējumus 1200 EUR vērtībā. Sieviete, izmantojot Booking.com platformu, norezervēja kādu viesnīcu Spānijā. Pēc rezervācijas sieviete saņēma e-pastu it kā no Booking.com klientu apkalpošanas servisa, kurā tika lūgts atkārtoti veikt pārskaitījumu uz e-pastā norādītājiem rekvizītiem, jo iepriekšējā rezervācija nav bijusi veiksmīga. Tāpat arī e-pastā tika lūgts atsūtīt bankas izrakstu par veikto pārskaitījumu. Tā kā sieviete tiešām bija iepriekš veikusi rezervāciju, kā arī e-pasts izskatījās ļoti pārliecinošs un atgādināja Booking.com stilu, sieviete prasības izpildīja. E-pasts saņemts no adreses: booking@customers.services, savukārt īstā ir customer.service@booking.com. CERT.LV secināja, ka iespējams ticis uzlauzts sievietes Booking.com profils, tāpēc ieteica sievietei nomainīt konta paroli, kā arī vienu paroli neizmantot vairākās vietās.

DDoS uzbrukums bilesuparadize.lv vietnei



Š.g. 3. martā, sākoties XXVI Vispārējo latviešu Dziesmu un XVI Deju svētku biļešu tirdzniecībai, publiskajā telpā izskanēja informācija, ka sistēma iespējams piedzīvojusi pārslodzes jeb DDoS uzbrukumu. CERT.LV pēc pašu iniciatīvas sazinājās ar SIA "Biļešu paradīze" pārstāvjiem, lai gūtu skaidrojumus par publiskajā telpā izskanējušo apgalvojumu. **Uzņēmums apstiprināja, ka uzbrukums ir piedzīvots.** Lai gūtu pilnīgāku priekšstatu par uzbrukuma apstākļiem, CERT.LV lūdza uzņēmumam sniegt detalizētu tehnisko informāciju - žurnālfailus.

Tālāk **veicot uzņēmuma SIA "Biļešu paradīze" 5. martā iesniegto žurnālfailu analīzi, tika konstatēts, ka 3. martā tik tiešām ir notikusi ļaunprātīga ārēja ietekme uz sistēmas darbību, kas radīja papildu slodzi jau tā pārslogotajai sistēmai.** 3. marta notikumu hronoloģija bija sekojoša: ļaunprātīga ietekme sākās jau ap 11.00, sistēmas kopējās slodzes kulminācija bija ap 13.00, bet sistēmas lielākā atteice sākās pēc 17:00. CERT.LV arī secināja, ka pakalpojuma sniedzējs SIA "Biļešu Paradīze" nav paredzējis visas iespējamās situācijas un izdarījis visu nepieciešamo, lai pasargātu sistēmu no šāda veida uzbrukumiem.

CERT.LV AKTIVITĀTES

„ESI DROŠS" SEMINĀRS UN INFORMĀCIJA PAR IERAKSTIEM

21.03.2018 Eiropas Digitālās nedēļas ietvaros norisinājās ierastais pavasara IT drošības seminārs "Esi drošs", pulcējot teju 200 par IT drošību atbildīgos un citus nozares interesentus. Semināra tēmas: ievainojamību *Meltdown* un *Spectre* ietekme, mākoņdatošanas iespējas un riski, NIS direktīvas ieviešana Latvijā, Vispārīgā datu aizsardzības regula un drošības prasības, kā arī iepazīstināšana ar CERT.LV un NIC.LV DNS ugunsmūra projektu.

SEMINĀRA PREZENTĀCIJAS UN VIDEO TIEŠRAIDES IERAKSTI IR PIEEJAMI CERT.LV MĀJASLAPĀ:
https://cert.lv/lv/2018/02/it-drosibas-seminars-esi-dross

VALSTS POLICIJAS APLIKĀCIJA PUSAUDŽIEM - "MANA DROŠĪBA"

Valsts policija izstrādājusi preventīvu un izzinošu rīku – **"Mana drošība",** kura iedalās divās sadaļās "Drošība satiksmē" un **"Drošība internetā"**. Aplikācija radīta ar mērķi rūpēties par ikviena Latvijas iedzīvotāja drošību gan ceļu satiksmē, gan arī interneta vidē. Aplikācijas sadaļa "Drošība internetā" tapusi ar Drossinternets.lv un CERT.LV atbalstu un **veltīta drošības jautājumiem saistībā ar mūsdienu izaicinājumiem interneta vidē**. Tā ir iespēja ikvienam pārbaudīt savas zināšanas par drošības jautājumiem internetā, aizpildot interaktīvu testu un izspēlējot improvizētu "čatu".

SVARĪGI: ikvienam ir iespēja turpat lietotnē ziņot par kaitīgu un nelegālu saturu vai problēmsituāciju, nosūtot ekrānšāviņus un hipersaiti uz aizdomīgu materiālu.

- "MANA DROŠĪBA" MOBILĀ LIETOTNE LEJUPIELĀDĒJAMA BEZ MAKSAS GOOGLE PLAY UN APP STORE.
- VAIRĀK PAR APLIKĀCIJU VALSTS POLICIJAS MĀJASLAPĀ: http://www.vp.gov.lv/index.php?&relid=16242

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

11.-13. **APRĪLIS** - RIPE apmācības LIR biedriem:

11.04. NCC Basic IPv6 Training Course
12.04. RIPE NCC IPv6 Security Training
13.04. RIPE NCC Measurements and Tools Training Course

23.-27. **APRĪLIS –** Locked Shields 2018 mācības

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

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

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