Mēneša ziņu izlaidums Nr. 05/2018

WWW.CERT.LV

Maijā aktuāli:

- Krāpnieki GDPR piesegā „makšķerē" lietotāju datus
- Par „Grāmatvedi un spocīgajiem rēķiniem"
- „Zvanu troļļi" aicina ieguldīt kriptovalūtā
- Kiberstāsti
- CERT.LV eksperti atklāj 4 kritiskas ievainojamības
- Excel JavaScript jaunā funkcionalitāte
- Apdraudējums, kas ietekmē e-pastu šifrēšanu
- CERT.LV pārstāvis kļūst par NATO CCD CoE vēstnieku
- Un citi aktuāli notikumi

Attēli: Pixbay.com

Krāpnieki GDPR piesegā „makšķerē" lietotāju datus

Tā kā š.g. 25. maijā stājās spēkā Vispārīgā datu aizsardzības regula (GDPR), interneta lietotāji automātiski kļuvuši ne vien par saudzējamo „datu subjektu", bet arī par magnētu ienākošajām e-pastu vēstulēm ar aicinājumiem apstiprināt jauno pasaules kārtību un noteikumus. **Magnētisko pievilkšanās spēku savā labā steidzas ekspluatēt arī krāpnieki, kas izmanto GDPR kā piesegu, lai izkrāptu lietotāju datus.**

Krāpnieki **cenšas imitēt reālus uzņēmumus,** veidojot viltus e-pastus tā, lai tie maksimāli tuvu atgādinātu oriģinālus – ar īstā uzņēmuma logo, valodas stilu utt. E-pasta saturs gan parasti saņēmējam rada satraukuma un steidzamības sajūtu jeb „mūsu pakalpojumi nebūs pieejami, kamēr neapstiprināsiet jauno privātuma politiku". Tālāk dota norāde uz saiti, kur **lūgts atkārtoti ievadīt lietotāja datus, paroles un kredītkartes informāciju**, kas, protams, godīgam uzņēmējam GDPR ietvaros nemaz nav nepieciešama.

Tāpēc esam modri un rūpīgi izvērtējam, kam un kādu informāciju sniedzam!

Vairāk informācijas:
Phishing alert: https://www.zdnet.com/article/phishing-alert-gdpr-themed-scam-wants-you-to-hand-over-passwords-credit-card-details/

Kiberlaikapstākļi

Pakalpojuma pieejamība	Lietu internets	Datu noplūde	Ļaunatūra un ievainojamības	Krāpšana
Pārrāvums Lattelecom sniegtajos pakalpojumos	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	OpenPGP un S/MIME, kā arī enerģijas sektora protokolu un iekārtu ievainojamības	Zvanu troļļi, CEO un GDPR krāpnieciskās e-pastu kampaņas

Senais stāsts par „Grāmatvedi un spocīgajiem rēķiniem"

Maijā bija novērojams kārtējais krāpniecisko e-pastu vilnis, kam fonā piestāvētu Raimonda Paula dziesma: „Sens, tik sens ir tas stāsts..."! Jeb krāpnieki joprojām strikti pieturas pie jau labi pazīstamā scenārija - tiek **masveidā izsūtīti e-pasti iestāžu un uzņēmumu grāmatvežiem, it kā vadītāja vārdā**, aicinot veikt steidzamu maksājumu, šoreiz - uz Vāciju. CERT.LV rīcībā pagaidām nav informācijas, ka kāds kampaņas ietvaros būtu arī cietis reālus zaudējumus.

Tomēr profilakses nolūkos aicinām pievērst uzmanību *„Reply-to"* adresei un neiekrist krāpnieku izliktajos slazdos.

"ZVANU TROĻĻI" AICINA IEGULDĪT KRIPTOVALŪTĀ

CERT.LV maijā saņēma ziņojumus no vairākiem Latvijas iedzīvotājiem par **aizdomīgiem zvaniem krievu valodā it kā no kādas investīciju kompānijas**, kas piedāvā ieguldīt naudu kriptovalūtā un pasakaini labi nopelnīt.

Ar sazvanīto cilvēku procesa laikā „strādā 3 operatori", kur katrs it kā atbild par saviem jautājumiem, un saruna kādā brīdī tiek pārvirzīta uz *Skype*. Veiksmīgas sarunas gadījumā tiek panākts, ka cilvēks caur *Skype* dalās ar savas iekārtas ekrānu. Pēc tam upuris tiek aizvests uz legālu vietni – *blockchain.info*, **kur nepieciešams ievadīt kredītkartes datus. Kamēr upuris datus ievada, zvanītājs fonā visu uzmanīgi vēro un piefiksē.** Attiecīgi šīs krāpšanas shēmas viens no mērķiem varētu būt - piekļuve upuru kredītkaršu datiem.

CERT.LV aicina, saņemot šāda tipa zvanus, tos uzreiz pārtraukt un nekādā gadījumā nepildīt zvanītāja prasības.

UZMANĪBU!

PLAŠĀKA INFORMĀCIJA PAR MINĒTAJIEM ZVANIEM PIEEJAMA ŠEIT: https://cert.lv/lv/2018/05/cert-lv-aicina-uzmanities-no-viltigiem-zvanu-trolliem

CERT.LV EKSPERTI ATKLĀJ ČETRAS KRITISKAS IEVAINOJAMĪBAS ENERĢĒTIKAS SEKTORĀ IZMANTOTĀS IEKĀRTĀS

CERT.LV kolēģi Bernhards Blumbergs (CVE-2018-10603, CVE-2018-10607, un viena vēl nepublicētā CVE-2018-XXXXX) un Artūrs Daņiļēvičs (CVE-2018-10609) **atklāja četras kritiskas industriālo vadības sistēmu ICS/SCADA ievainojamības** un piecu mēnešu garumā koordinēja un sniedza atbalstu ievainojamo iekārtu izstrādātājam šo ievainojamību novēršanā.

Šo ievainojamību izmantošana varētu novest pie neautorizētu komandu izpildes industriālo procesu vadības sistēmās, pakalpojuma atteices vai koda izpildes klienta iekārtā.

Pirmā ievainojamība (CVE-2018-10603) izpaužas kā autentifikācijas trūkums kritiska procesa izpildē, kas **var novest pie neautorizētu IEC-104 komandu ievades** industriālo procesu vadības sistēmās. Otrā ievainojamība (CVE-2018-10607) izpaužas kā **nepilnīga kontrole pār resursu patēriņu** (resource exhaustion), kas var **novest pie pakalpojuma atteices (DoS) situācijas**. Trešo ievainojamību (CVE-2018-10609) rada nepietiekama ievadīto datu pārbaude, kad datu apstrādei tiek izmantots tīmekļa protokols WebSocket. **Rodas potenciāls starpvietņu skriptošanai** (XSS). Informācija par ceturto ievainojamību (CVE-2018-XXXXX) tiks izpausta, tiklīdz iekārtu ražotāji būs pilnībā novērsuši ievainojamības radīto apdraudējumu.

Atklātās ievainojamības **skar enerģētikas sektoru visā Eiropā un pasaules valstīs**, kurās tiek lietots IEC-60870-5-104 protokols. Kā arī MartemTELEM-GW6/GWM iekārtas, kas pārsvarā tiek lietotas Baltijas valstīs un Somijā.

Ievainojamībām piešķirtie CVE numuri: CVE-2018-10603, CVE-2018-10607, CVE-2018-10609, CVE-2018-XXXXX.

TEHNISKĀ INFORMĀCIJA: https://ics-cert.us-cert.gov/advisories/ICSA-18-142-01

JŪNIJA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: "Stāties pretī ļaunatūrai"

Saistībā ar kiberdrošību jūs droši vien esat dzirdējuši tādus terminus kā vīruss, trojānis un izspiedējvīruss. Tie ir apzīmējumi dažādu veidu ļaundabīgām programmatūrām, ko dēvē arī par ļaunatūru, un ko kibernoziedznieki izmanto, lai inficētu datorus un citas ierīces. Ja šāda programmatūra tiek uzstādīta, ļaundaris iegūst rīcības brīvību. Pilnajā versijā lasiet, kas īsti ir ļaunatūra, kādi ir ar to saistītie riski un kā sevi no tās pasargāt.

Pilna raksta versija pieejama: https://cert.lv/uploads/ieteikumi/201806-OUCH-June-Latvian.pdf

JAUNĀS EXCEL JAVASCRIPT FUNKCIONALITĀTES ĒNAS PUSES

Dažu dienu laikā pēc *Microsoft* paziņojuma par *JavaScript* funkcionalitātes iekļaušanu lietotnē *Excel*, drošības eksperti jau brīdināja **par iespējām šo funkcionalitāti izmantot arī ļaundabīgiem mērķiem**. Eksperti pētījuma rezultātā diezgan ātri atklāja veidu kā, izmantojot jauno funkcionalitāti, **iespējams lietotnē *Excel* augšupielādēt *CoinHive* piedāvāto kriptovālūtas „racēju".** Pagaidām gan jaunā Excel funkcionalitāte tiek nodrošināta tikai *Office Insiders* programmas lietotājiem, un plašākai publikai vēl nav pieejama.

Šobrīd atliek tikai gaidīt, kāds būs *Microsoft* piedāvātais risinājums šai problēmai, bet tikmēr **drošības nolūkos aicinām atspējot *JavaScript* funkcionalitāti *MS Office* lietotnēm**, tiklīdz tāda būs pieejama arī plašākai publikai.

VAIRĀK INFORMĀCIJAS:

- **PoC Developed for CoinHive Mining In Excel Using Custom JavaScript Functions:** https://www.bleepingcomputer.com/news/security/poc-developed-for-coinhive-mining-in-excel-using-custom-javascript-functions/
- **Microsoft Adds Support for JavaScript Functions in Excel**: https://www.bleepingcomputer.com/news/microsoft/microsoft-adds-support-for-javascript-functions-in-excel/

APDRAUDĒJUMS, KAS IETEKMĒ E-PASTU ŠIFRĒŠANU

14. maijā, vācu pētnieks *Sebastian Schinzel*, pēc nesekmīga embargo mēģinājuma, publiskoja pētījumu, kurā norāda uz divām ievainojamībām, kas skar *OpenPGP* un *S/MIME* šifrēšanas izmantošanu e-pasta lietotnēs.

Lai izmantotu ievainojamību, **uzbrucējam ir jāspēj pārtvert vai piekļūt šifrētam e-pastam un to modificēt,** pievienojot tam klāt jaunas daļas, kas satur specifisku HTML kodu. Daudzas e-pasta lasīšanas lietotnes pēc e-pasta atšifrēšanas arī automātiski ielādēs un izpildīs šo uzbrucēja pievienoto HTML kodu, **kā rezultātā uzbrucējam var tikt nosūtīts atšifrēta e-pasta saturs.**

PLAŠĀKA INFORMĀCIJA PAR IEVAINOJAMĪBĀM PIEEJAMA ŠEIT: https://cert.lv/lv/2018/05/par-ievainojamibu-kas-skar-openpgp-un-securemime-izmantosanu-e-pasta-lietotnes

CERT.LV PĀRSTĀVIS KĻŪST PAR NATO CCDCOE VĒSTNIEKU

CERT.LV ekspertam Bernhardam Blumbergam NATO apvienotais kiberaizsardzības izcilības centrs (NATO CCD CoE) par augstiem sasniegumiem, būtisku ieguldījumu centra un alianses kiberdrošības stiprināšanā un prestiža celšanā maijā piešķīra centra vēstnieka titulu - *NATO CCD CoE Ambassador*. Šāds statuss tiek piešķirts uz diviem gadiem, un vēstnieku skaits ir ļoti ierobežots, - tas nepārsniedz septiņus vēstniekus. Plašāk par iegūto statusu stāsta B. Blumbergs:

1. KO NOZĪMĒ KĻŪT PAR NATO CCDCOE VĒSTNIEKU?

Tas nozīmē augstāko atzinību par paveikto, kas tiek novērtēts kā būtisks ieguldījums ne tikai NATO CCD CoE, bet arī visā aliansē. Vēstnieka titula piešķiršana nozīmē to, ka NATO CCD CoE vēlas turpināt sadarbību arī pēc tam, kad eksperta darbības laiks centrā ir beidzies, lai turpinātu iesaistīt šo ekspertu un izmantot viņa kompetences būtiskās centra aktivitātēs un mācību sagatavošanā, ceļot centra prestižu. Tā ir arī iespēja turpināt mācīties un augt kopā ar centru.

2. PAR KO PIEŠĶIR ŠĀDU TITULU?

Vēstnieka titulu piešķir bijušajiem centra darbiniekiem, kuri ir kļuvuši par starptautiski atzītiem ekspertiem kiberdrošībā un savas darbības laikā centrā ir aktīvi sevi pierādījuši, iesaistoties centra aktivitātēs, veicot pētījumus, gatavojot materiālus, pilnveidojot un attīstot centra organizētās mācības, kas stiprina centra dalībvalstu un visas alianses kiberdrošību, kā arī ceļ centra kompetenci un prestižu kā vadošajam kiberdrošības centram ne tikai aliansē, bet arī ārpus tās.

CERT.LV saņem atzinību no Aizsardzības ministrijas

10.maijā CERT.LV vadītāja Baiba Kaškina un vadītājas vietnieks Varis Teivāns svinīgā ceremonijā Aizsardzības ministrijā saņēma pateicības rakstus no aizsardzības ministra Raimonda Bergmaņa par veiksmīgu sadarbību, atbalstu un ieguldījumu kiberdrošības stiprināšanā.

CERT.LV kolēģi patiesi lepojas un pievienojas apsveikumiem!

„Pasaule, kur lietas pieņem lēmumus!"

Cik daudz no savām ikdienas rūpēm mēs esam gatavi deleģēt "gudrajām lietām" (IoT), kādus jaunus izaicinājumus tas var radīt? Kur sākas un beidzas mūsu izvēles brīvība, un kāda varētu būt mūsu atbildība, lietojot šīs ierīces? Šos filozofiski nopietnos jautājumus savā prezentācijā 25. maijā apskatīja **CERT.LV attīstības projektu vadītājs Egils Stūrmanis, piedaloties datu drošības forumā "Digitālā Ēra: Datu regula un datu drošība".**

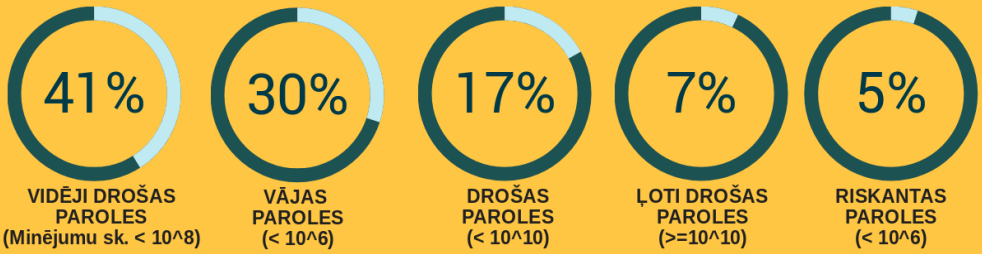
Ar prezentāciju varat iepazīties šeit: https://prezi.com/wbn_r6naytp6/pasaule-kur-lietas-pienem-lemumus/
Tiešraides video ieraksts (2:40:00 min): https://www.youtube.com/watch?v=k2awNih2KOo&t=5147s

Statistika: pētījums par gotcha.pw publiskotajām parolēm

visme

TOP10 populārākās paroles Latvijā*

#1	123456	#6	12345
#2	123456789	#7	1234567
#3	qwerty	#8	1234567890
#4	parole	#9	samsung
#5	12345678	#10	graf12345



*Aprīļa ziņu izlaidumā rakstījām par vietnē *gotcha.pw* publiskotajām parolēm un e-pasta adresēm, kur aptuveni 600 000 nāk arī no Latvijas. RTU Informācijas tehnoloģijas institūts asoc. prof. Jāņa Kampara vadībā veicis publicētās datubāzes analīzi un apkopojis Latvijā biežāk izmantotās paroles dažādiem interneta resursiem, kā arī pētījis paroļu drošības līmeni.

Piesaki prezentāciju konferencei "Kiberšahs 2018"

2018. gada 9. oktobrī CERT.LV un ISACA Latvijas nodaļa rīko ikgadējo kiberdrošības konferenci „Kiberšahs", kura ik gadu pulcē vairāk nekā 500 IT nozares ekspertus. Konferences mērķis ir aktualizēt būtiskākos apdraudējumus, veicināt pieredzes apmaiņu, raisīt diskusijas un rosināt pārdomas par Latvijas un globālās kibertelpas drošību un tās uzlabošanas iespējām.

Aicinām pieteikt prezentācijas par praktisko pieredzi, jauniem izaicinājumiem, inovatīviem risinājumiem, labo praksi un pētījumu rezultātiem kiberdrošības sfērā. Pieteikuma un tēmas kopsavilkuma iesūtīšanas termiņš - 22. jūnijs.

Plašāka informācija par pieteikšanos un tēmām: https://cert.lv/lv/2018/05/piesaki-prezentaciju-kiberdrosibas-konferencei-kibersahs-2018

Kiberstāsti

• • •

Maija sākumā CERT.LV no kādas privātpersonas saņēma ziņojumu par šķietami aizdomīgu e-pastu portāla *inbox.lv* vārdā. E-pasta noslēgumā lietotājam norādīta saite, kur iespējams iepazīties un apstiprināt jauno *inbox.lv* privātuma politiku, sakarā ar Vispārīgās datu aizsardzības regulas (GDPR) stāšanos spēkā 25. maijā. CERT.LV veica e-pasta pārbaudi un apstiprināja lietotājam, ka e-pasts ir leģitīms un tā nav krāpniecība. Kā arī piedāvāja lietotājam interneta resursus, kuros pieejama plašāka informācija par GDPR. CERT.LV arī turpmāk aicina visiem rūpīgi izvērtēt ziņojumus, ko saņemat elektroniskajā vidē, jo ārvalstīs jau ir fiksēti gadījumi, kad krāpnieki izmantojuši GDPR kā pamatu, lai nosūtītu ļaunatūru saturošus ziņojumus.

• • •

Maijā CERT.LV saskārās ar vērienīgu e-pasta paroļu izkrāpšanas kampaņu, kas bija vērsta pret vairākām valsts un pašvaldības iestādēm. Šo iestāžu darbinieki saņēma personificētus e-pastus ar aicinājumu atjaunot un uzlabot sava e-pasta drošību un norādi uz saiti, kur to iespējams paveikt. Attiecīgi nospiežot uz saites, tālāk parādās primitīva forma, kur atkārtoti tiek lūgts ievadīt e-pasta paroli. Pēc paroles ievadīšanas, tā automātiski nonāk krāpnieku rokās. CERT.LV brīdināja kaitīgās lapas uzturētājus un panāca tās slēgšanu. Krāpniecība savlaicīgi tika atpazīta, un neviens no darbiniekiem paroles krāpniekiem neatdeva.

• • •

Kāds Latvijā bāzēts uzņēmums maija beigās kļuva par kriptovīrusa upuri, kā rezultātā nopietni tika traucēti uzņēmuma darbības procesi. Tika nošifrēts gan uzņēmuma serveris, gan vairāki datori un diemžēl uzbrukumā cieta arī failu rezerves kopijas. Ļaundari par failu atgriešanu pieprasījuši uzņēmumam aptuveni 4000 ASV dolāru. Uzņēmums, nonācis bezizejā, nolēma izpildīt prasības, taču par minēto summu atguva tikai daļu no failiem, un tiek prognozēts, ka par pārējo failu atgūšanu būs jāmaksā papildus. Vīruss tika palaists, piemeklējot lokālā administratora konta RDP paroli. CERT.LV neiesaka RDP servisu atvērt internetā bez papildus aizsardzības (VPN, *Smart card* utt.).

Tuvāko plānoto pasākumu kalendārs

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