JANVĀRĪ AKTUĀLI:

Attēli: Pixbay.com

E-VESELĪBA UGUNSKRISTĪBĀS

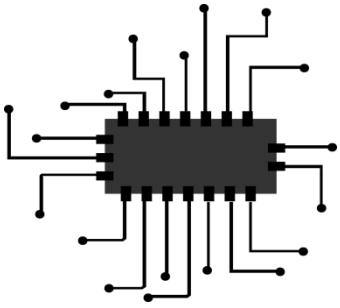
Šis gads iesākās trauksmaini, ar ziņu par uzbrukumiem veselības aprūpes kvalitātes un efektivitātes uzlabošanas programmai e-veselība. Pirmatnējā izpēte apliecināja, ka 16.janvārī e-veselības sistēma piedzīvoja pārslodzes uzbrukumu (DDoS). Šāda uzbrukuma mērķis ir padarīt sistēmu nepieejamu, **bet datu noplūde nenotiek.**

Šādam uzbrukumam var tikt pakļauta jebkura sistēma. Uzbrukuma ietekmes mazināšanai pirms sistēmas nodošanas ekspluatācijā sistēmai vēlams nodrošināt aizsardzību pret DDoS uzbrukumiem, kā arī vēlams izstrādāt rīcības plānu situācijai, kad uzbrukumu neizdotos atvairīt un tā sekas būtu jūtamas lietotājiem.

KIBERLAIKAPSTĀKĻI

PAKALPOJUMA PIEEJAMĪBA	LIETU INTERNETS	DATU NOPLŪDE	ĻAUNATŪRA UN IEVAINOJAMĪBAS	KRĀPŠANA
Uzbrukumi e-veselības sistēmai	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Meltdown un Spectre ievainojamības	Viltotu rēķinu vilnis

JAUNI RISKI, KAS BALSTĪTI IEKĀRTU PAMATFUNKCIONALITĀTĒ



2017. gada nogali un 2018. gada sākumu iezīmēja vairākas nopietnas, datoru un procesoru darbību ietekmējošas ievainojamības: **aparātprogrammatūras (firmware) līmeņa ievainojamība** IntelME (CVE-2017-5705 līdz CVE-2017-5712) un **„dzelžu" (hardware) līmeņa ievainojamības** Meltdown (CVE-2017-5754) un Spectre (CVE-2017-5753 un CVE-2017-5715), **kuru visu kopīgā raksturīgā iezīme – tās sniedz iespēju uzbrucējiem pārņemt vadību pār datorsistēmu un palikt nepamanītiem.**

Ievainojamību labojumi šādās situācijās nav vienkārši, jo nepietiek tikai ar mikroprocesora ražotāja (piem., Intel, AMD, ARM u.c.) izlaistiem atjauninājumiem, tie jāpielāgo katra iekārtu ražotāja dažādo produktu vajadzībām. Tas var izraisīt neparedzētas izmaiņas iekārtu darbībā, piemēram, neprognozējamu restartēšanos (Intel sākotnēji izlaistais Spectre ielāps) vai pat darbības pilnīgu

pārtraukšanu (AMD sākotnēji izlaistais Spectre ielāps). Rezultātā atsevišķi labojumi var radīt lielākas problēmas, nekā tie novērš, un tos nepieciešams atsaukt, kā to 30.janvārī izdarīja Microsoft.

Tomēr, lai arī atjauninājumu izstrādes process ir sarežģīts un laikietilpīgs, šobrīd tas ir vienīgais veids kā pasargāt iekārtas no ļaunprātīgiem mēģinājumiem izmantot jaunatklātās ievainojamības. Lielāko apdraudējumu šīs ievainojamības rada datu centriem un mākoņpakalpojumu sniedzējiem, kuru pamatdarbība ir balstīta uz ievainojamo funkcionalitāti, kā arī lietotājiem, kas izmanto interneta pārlūkprogrammas ar iespējotu JavaScript koda izpildi, kas pakļauj lietotājus privāto datu zādzībai, ja nejauši tiek apmeklēta inficēta tīmekļa vietne.

VAIRĀK INFORMĀCIJAS:

- **IntelME ievainojamība**: https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00086&languageid=en-fr
- **Meltdown un Spektre ievainojamības:** https://cert.lv/lv/2018/01/meltdown-un-spectre-ievainojamibas-procesoru-darbiba
- **Microsoft atsauktie atjauninājumi:** https://support.microsoft.com/en-us/help/4078130/update-to-disable-mitigation-against-spectre-variant-2

KRIPTOVALŪTA – PIEVILCĪGS „BURKĀNS" ĻAUNATŪRAS IZSTRĀDĀTĀJIEM

2017.gada nogalē, par spīti skeptiķiem, kriptovalūtas tirgus piedzīvoja lēcienu (mēneša laikā bitcoin vērtība pieauga par 144%, bet monero par 170%), izpelnoties gan sabiedrības, gan hakeru uzmanību.

Aizsākās sacensība par radošākajiem veidiem, kā, patērējot minimālu apjomu savu resursu, iegūt maksimālu labumu kriptovalūtas veidolā. Vairāku tīmekļa vietņu īpašnieki sāka izmantot Coinhive – uz Javascript bāzētu rīku, kas tiek ievietots tīmekļa vietnē un darbina kriptovalūtas ieguves procesu lietotāja datorā, kad lietotājs apmeklē noteikto tīmekļa vietni (metode nav jauna, tā tiek izmantota vismaz kopš 2011.gada). Kriptovalūtas ieguve tiek pārtraukta, kad lietotājs pamet vietni vai aizver pārlūku. Lai šo „problēmu" apietu, kriptovalūtas ieguve tika ievietota papildu logā, kas atvērās reizē ar tīmekļa vietni un tika paslēpts ekrānā zem rīkjoslas aiz pulksteņa, nodrošinot kriptovalūtas ieguves procesa turpināšanos arī pēc vietnes un šķietami arī pārlūka aizvēršanas, ja vien netiek pārtraukti visi pārlūka procesi. Kriptovalūtas ieguves process ir efektīvāks, ja tajā ir vairāk iesaistīto lietotāju, tāpēc notiek arī mēģinājumi uzlauzt populāras tīmekļa vietnes, kā piemēram www.politifact.com, lai tajās ievietotu kriptovalūtas ieguves rīkus.

Kriptovalūtas ieguves rīki tiek ievietoti arī interneta pārlūku paplašinājumos. Janvāra sākumā tika konstatēts, ka Google Chrome paplašinājums Archive Poster ar vairāk kā 100 000 lietotājiem bez lietotāju brīdināšanas veic kriptovalūtas Monero (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvi. Paplašinājuma izstrādātāji apgalvoja, ka paplašinājums ir ticis uzlauzts. Decembrī tika atklāts kriptovalūtas ieguves rīks Digmine, kas izplatījās Facebook tērzētavā (Messenger) un lejuplādēja pārlūka Google Chrome paplašinājumu kriptovalūtas ieguvei.

Kriptovalūtas ieguves process būtiski noslogo lietotāja datoru un var pat radīt tehniskas problēmas, kā arī, ne visi tīmekļa vietņu uzturētāji, kas ievieto kriptovalūtas rīku savā tīmekļa vietnē, informē par to lietotāju un iegūst tā piekrišanu. **Lai liegtu savu iekārtu bez brīdinājuma izmantot sveša kriptovalūtas maciņa pildīšanai, iesakām izmantot JavaScript funkcionalitāti ierobežojošu pārlūka paplašinājumu**, piemēram NoScript priekš Firefox, vai antivīrusu programmatūru, kas bloķē kriptovalūtas ieguves kodu, (piem., Malwarebytes).

VAIRĀK INFORMĀCIJAS:

- **Kriptovalūtas ieguve, izmantojot tīmekļa vietnes:** https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency
- **Kriptovalūtas ieguve, izmantojot pārlūku paplašinājumus:** http://fortune.com/2018/01/02/google-chrome-extension-cryptocurrency-mining-monero/
- **Kriptovalūtas ieguves ļaunatūra Facebook Messenger:** https://blog.trendmicro.com/trendlabs-security-intelligence/digmine-cryptocurrency-miner-spreading-via-facebook-messenger/

Viltotu rēķinu vilnis

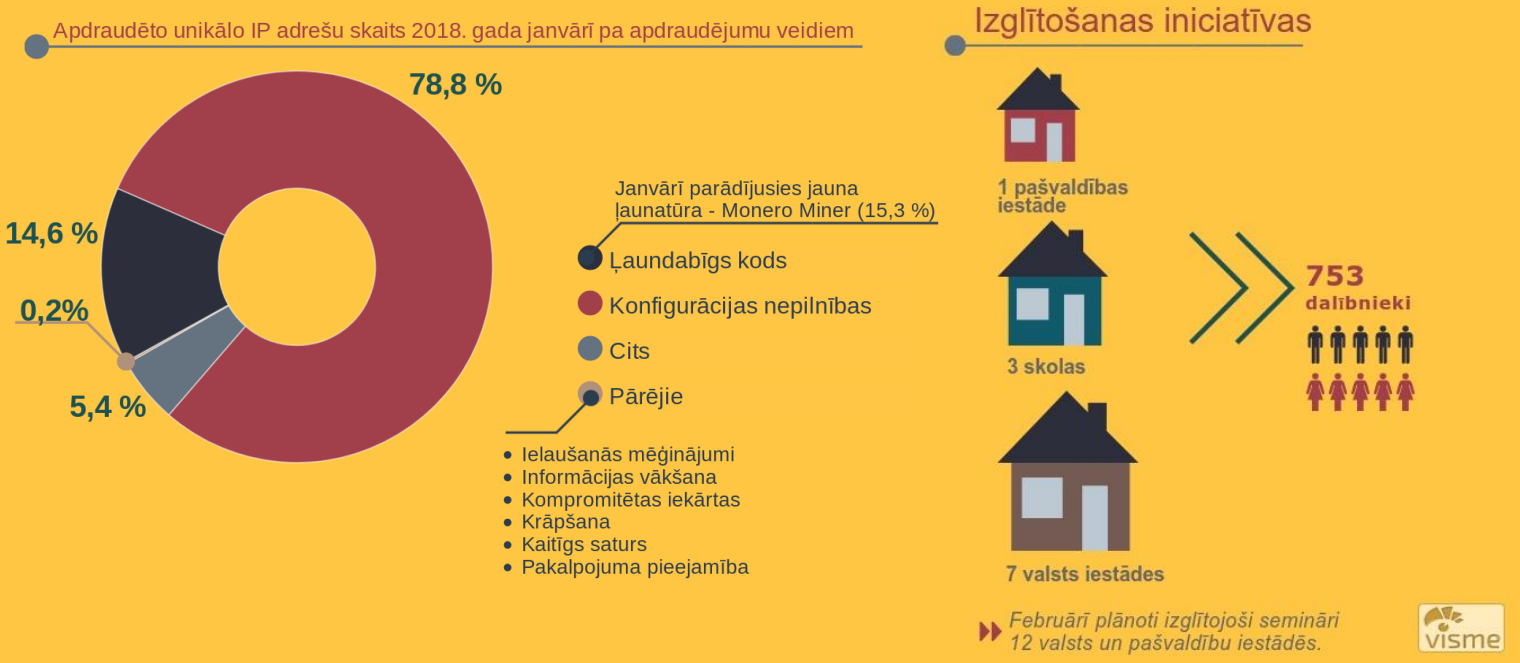
Pagājušā gada nogalē un šogad janvārī CERT.LV saņēma vairākus ziņojumus no dažādiem avotiem par viltus rēķiniem.

Decembra vidū CERT.LV tika informēta, ka kāda persona saņēmusi aizdomīga izskata paziņojumu par neapmaksātu rēķinu it kā augstākā līmeņa .lv domēna vārdu reģistra NIC.lv vārdā. E-pasts bija angļu valodā un saturēja aizdomīga izskata brīdinājuma paziņojumu par rēķina apmaksu. Savukārt, kāds ārvalstu klients janvārī informēja, ka saņēmis aicinājumu turpmāk .lv domēna vārda lietošanas tiesības apmaksāt e-pastā norādītajam sūtītājam. Tiesa, ieskatoties vērīgāk, varēja pamanīt norādi, ka sūtītajam paziņojumam ir reklamējoši informatīvs saturs. Šādi sūtījumi nav masveida, tomēr aicinām būt vērīgiem.

Padoms: Saņemot aizdomīga izskata, satura, valodas e-pastus, nekādā gadījumā nevērt vaļā tajos norādīto saiti vai pielikumu un pārliecināties par sūtītāja leģitimitāti.

Janvāra vidū CERT.LV saņēma vairākkārtējus ziņojumus par it kā tūroperatora "Travel RSP" vārdā izsūtītiem e-pastiem. Tūroperatora klienti e-pastā saņēma lūgumu steidzami apmaksāt pielikumā pievienoto, it kā neapmaksāto rēķinu. Ziņojumā tika norādīta apmaksājamā summa un korekta tūroperatora kontaktinformācija. CERT.LV noskaidroja, ka **tūroperatora "Travel RSP" e-pastu sistēma tika uzlauzta, un ziņojumiem bija krāpniecisks raksturs.** To mērķis bija saņēmējam likt lejupielādēt uz savas ierīces pielikumā esošo izpildāmo failu ar .exe paplašinājumu. Atverot kaitīgo failu, tas šķietami pazuda no ekrāna, taču neredzami fonā tika palaista programma, kas „ražoja" kriptovalūtu.

Skaitļi un fakti



Janvāra OUCH!

Ikmēneša informācijas drošības biļetens ikvienam

Biļetena tēma: "Mājas kiberdrošība: bezvadu tīkls, ierīces, paroles, rezerves kopijas"

Pirms vairākiem gadiem kiberdrošība mājās bija vienkārša: vairumā māju bija tikai bezvadu tīkls un daži datori. Šodien tehnoloģijas ir kļuvušas sarežģītākas un ir integrētas visos mūsu dzīves aspektos, no mobilajām ierīcēm un spēļu konsolēm līdz mājas termostatam un, iespējams, ledusskapim.

Pilna raksta versija pieejama: https://cert.lv/uploads/ieteikumi/OUCH-201801_lv.pdf

Kiberstāsti

• • •

Tika saņemta ziņa no kāda Latvijas uzņēmuma par nošifrētu uzņēmuma failu serveri, kurš bija pieejams caur attālās piekļuves protokolu RDP (Remote Desktop Protocol). Rezerves kopijas nebija pieejamas. Uzņēmums papildus pieaicināja arī IT drošības ekspertu, kurš apliecināja, ka faili nav atgūstami bez atšifrēšanas. Uzņēmums nolēma maksāt ļaundariem par failu atgūšanu.

• • •

CERT.LV rīcībā tika nodota informācija par veiksmīgu krāpšanas mēģinājumu, kurā izmantota sociālā inženierija (cilvēka psiholoģiska manipulēšana). Kāda sieviete internetā iepazinās ar vīrieti, kurš tajā laikā it kā strādāja uz kuģa. „Jūrnieks" sarakstes laikā atklāja, ka viņam noslēgts līgums uz 10 gadiem darbam uz kuģa. Alga esot vairāk kā apmierinoša, un izdevies iekrāt jau pietiekami daudz, lai gribētu doties atpakaļ uz Latviju. Tomēr, lai varētu atgriezties Latvijā, „Jūrniekam" bija nepieciešami 1000 EUR – jurista pakalpojumiem, - lai lauztu līgumu un saņemtu sapelnīto naudu. Sieviete „Jūrniekam" noticēja un nepieciešamos 1000 EUR pārskaitīja, izmantojot krāpniecisku vietni. Tikai pēc naudas pārveduma sieviete saprata, ka ir apkrāpta. CERT.LV ieteica ar iesniegumu vērsties policijā, kā arī sazinājās ar krāpnieciskās vietnes uzturētāju un lūdza vietni, caur kuru tika veikts naudas pārvedums, slēgt. Šobrīd vietne vairs nav pieejama.

• • •

No kāda lietotāja tika saņemta sūdzība par krāpniecisku interneta vietni - https://bilablau.com/, kas konkrētajā gadījumā gan īsti neatbilda CERT.LV kompetencei, jo skāra patērētāju tiesību jautājumus – vietnes lietošanas nosacījumus, ar kuriem lietotājs nebija rūpīgi iepazinies pirms pirkuma izdarīšanas. Lietotājs minētajā vietnē bija iegādājies kādu produktu. Līdz ar produkta iegādi, pašam nezinot, lietotājs automātiski piekrita kļūt arī par vietnes „biedru" (member), kas ir maksas pakalpojums. Rezultātā lietotājs novēloti pamanīja, ka no viņa kredītkartes 6 mēnešu garumā kopā novilkti 72,00 EUR (12,00 EUR mēnesī). Vēlāk, analizējot situāciju, lietotājs konstatēja, ka saņemtajā e-pastā par produkta iegādi – pašā apakšā, sīkā drukā ir komentārs par šo maksas pakalpojumu. Attiecīgi e-pastā minēts, ka lietotājam ir dotas 14 dienas, lai bez maksas izmēģinātu „biedru" piedāvājumu, bet pēc 14 dienām no lietotāja katru mēnesi tiks iekasēta „biedra" nauda. Lietotājs sazinājās ar Bilablau.com administrāciju, un lūdza summu atgriezt, jo minēto pakalpojumu nebija ne vēlējies, ne izmantojis, - tomēr administrācija šo lūgumu noraidīja. Tāpat lietotājs kopš produkta iegādes nebija saņēmis nevienu citu rēķinu vai e-pastu par „biedra" naudu, kas tika iekasēta katru mēnesi. Lietotājs tālāk sazinājās ar Eiropas Patērētāju informēšanas centru, kas lietu tālāk nodeva Eiropas Patērētāju centram Dānijā.

Tuvāko plānoto pasākumu kalendārs

16. **Februāris -** Idea Garage Cyber Security Riga

19.-25. **Marts -** Digitālā drošības nedēļa

20. **Marts -** Digitālās drošības diena

21. **Marts -** IT drošības seminārs "Esi drošs"

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