MĒNEŠA ZIŅU IZLAIDUMS NR. 06/2018

WWW.CERT.LV

JŪNIJĀ AKTUĀLI:

- VPNFilter ļaunatūra;
- Praktiski rīki bērnu un jauniešu digitālajai drošībai;
- Office 365 e-pastu pikšķerēšanas kampaņa;
- Jaunais Wi-Fi šifrēšanas protokols – WPA3;
- Krāpnieki, kas izliekas par tehniskā atbalsta dienesta speciālistiem no Microsoft;
- Kiberdrošības mācības - CYBER EUROPE 2018;
- Kiberstāsti;
- Un citi aktuāli notikumi.

Attēli: Pixbay.com

VPNFILTER ĻAUNATŪRA – PŪĶIS AR VAIRĀKĀM GALVĀM

Maija beigās un jūnija sākumā globālo kibertelpu „sacēla kājās" jauna un īpaši bīstama ļaunatūra, kas pazīstama kā *VPNFilter,* un kas ir inficējusi vairāk kā 500 000 iekārtu 54 dažādās valstīs. *VPNFilter* mērķis ir vienkārši maršrutētāji, kas plaši izplatīti mazos birojos un privātā lietošanā. Uzbrucēji minētās iekārtas **inficē, izmantojot jau zināmas ievainojamības vai arī neaizsargātu vadības interfeisu** (*management interfaces).* Ļaunatūra var pārtvert un manipulēt ar datu plūsmu, kas tiek pārraidīta caur inficēto iekārtu. Viens no *VPNFilter* uzdevumiem ir datu plūsmā pārtvert lietotājvārdus un paroles. **Tāpat ļaunatūra var ne tikai pārtvert, bet arī „injicēt" pašā datu plūsmā ļaundabīgu saturu.**

Arī iekārtas pārstartēšana, kā sākotnēji tika uzskatīts, nepalīdz no ļaunatūras atbrīvoties pilnībā. Viena no bīstamākajām „pūķa galvām" ir *VPNFilter* koda daļa, kas aktivizēta, dod iespēju uzbrucējam ne tikai izdzēst *VPNFilter* atstātās pēdas ierīcē, bet arī sabojāt pašu ierīci. **Tas nozīmē, ka ar vienu komandu uzbrucējs var atslēgt no tīkla tūkstošiem iekārtu.** Tāpat *VPNFilter* satur funkcionalitāti, kas mēģina atslēgt šifrēšanu *http* savienojumos.

Risinājums ir iekārtas rūpnīcas datu atiestatīšana un jaunāko iekārtas atjauninājumu instalācija, kas ļauj pilnībā atbrīvoties no ļaunatūras. Tāpat, veicot atiestatīšanu, obligāti jānomaina arī rūpnīcas paroles, kas iekārtai ir jau „pēc noklusējuma".

Skartas tādu ražotāju iekārtas kā ASUS, D-Link, Huawei, Ubiquiti, UPVEL, ZTE, Linksys, MikroTik, Netgear, TP-Link u.c. Ar pilno sarakstu un modeļiem iespējams iepazīties organizācijas Symantec vietnē.

VAIRĀK INFORMĀCIJAS:

VPNFilter Update - VPNFilter exploits endpoints, targets new devices:
https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

VPNFilter malware now targeting Asus, D-Link, Huawei, ZTE devices:
https://www.zdnet.com/article/vpnfilter-malware-now-targeting-asus-d-link-huawei-zte/

KIBERLAIKAPSTĀKĻI

				
PAKALPOJUMA PIEEJAMĪBA	**LIETU INTERNETS**	**DATU NOPLŪDE**	**ĻAUNATŪRA UN IEVAINOJAMĪBAS**	**KRĀPŠANA**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	VPNFilter ļaunatūra	*Office 356* pikšķerēšanas kampaņa, *Microsoft Support* krāpšanas shēma

Praktiski rīki bērnu un jauniešu digitālajai drošībai

Latvijas Drošāka interneta centrs ir sagatavojis noderīgus, praktiskus materiālus drošākam darbam tīmeklī:

- **Padomi drošai dažādu sociālo tīklu lietošanai** "Galvenie riski, lietojot sociālos tīklus"
- **Praktisks gids (ar saitēm) sociālo tīklu privātuma iestatījumos** "Sociālo tīklu drošības ceļvedis"
- **Atgādinošs pārskats par drošas interneta lietošanas pamatprincipiem** "10 padomi tavai drošībai internetā"

Drošāka interneta centrs izglīto un informē sabiedrību par bērnu drošību internetā, kā arī nodrošina iespēju gan **ziņot** par atklātajiem pārkāpumiem, gan lūgt palīdzību, izmantojot uzticības tālruni 116111.

Vairāk informācijas: https://drossinternets.lv/

Office 365 e-pastu pikšķerēšanas kampaņa

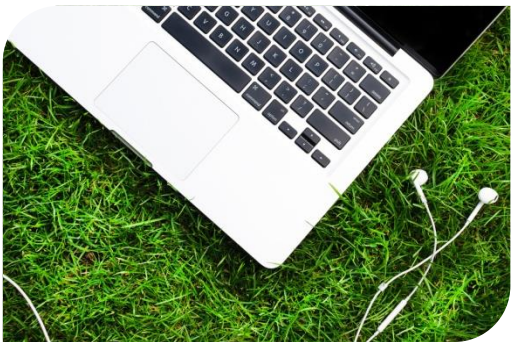
Somijas Nacionālais kiberdrošības centrs jūnija sākumā **izplatīja sarkano brīdinājumu saistībā ar straujo *Office 365* e-pastu pikšķerēšanas kampaņas izplatību** un pārkāpumiem, kas saistīti ar personas datiem. CERT.LV prognozē, ka, iespējams, **drīzumā arī Latviju un citas Baltijas valstis varētu sasniegt minētā krāpšanas kampaņa**.

Šī gada pavasarī vairāku Somijas uzņēmumu darbinieku un vadītāju e-pastu piekļuves dati tika nozagti un tālāk izmantoti vairākos krāpšanas gadījumos un tās mēģinājumos. Somijas Nacionālā kiberdrošības centra rīcībā esošā informācija liecina, ka vairāki uzņēmumi incidenta rezultātā cietuši arī būtiskus zaudējumus. Tādēļ **uzņēmumi Somijā un citur tiek aicināti atvēlēt papildu resursus tam, lai tehniski novērstu un laicīgi atklātu krāpšanas mēģinājumus**, kā arī, lai informētu darbiniekus par pastāvošajiem draudiem.

Krāpnieki par saviem **upuriem izvēlas darbiniekus, kas ikdienā izmanto *Office 365* e-pasta pakalpojumus**. Ļaundaru mērķis ir caur krāpnieciskiem e-pastiem un mājaslapām, kas, piemēram, atgādina *Office 365* ielogošanās formu, savā īpašumā iegūt upura *Office 365* e-pasta piekļuves datus. Pēc to izgūšanas ļaundari ielogojas upura e-pastā un veic izmaiņas iestatījumos, tādā veidā panākot, ka uzņēmuma vadības vai par finansēm atbildīgo darbinieku e-pastu kopijas tiek pārsūtītas ļaundariem.

Sīkāka informācija par krāpšanu un risinājumiem pieejama šeit: https://cert.lv/lv/2018/06/pastav-risks-ka-ari-latviju-varetu-skart-office-365-e-pastu-pikskeresanas-kampana

Pabeigts darbs pie jaunā Wi-Fi šifrēšanas protokola - WPA3



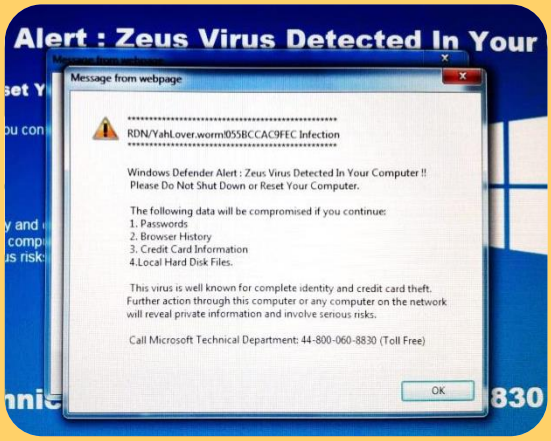
Jūnija beigās Wi-Fi ierīču ražotāju apvienība "Wi-Fi Alliance" nāca klajā ar pozitīvām un ilgi gaidītām ziņām – tā beidzot **pabeigusi darbu pie jaunā Wi-Fi šifrēšanas protokola WPA3 prasībām.** Pēdējos gandrīz 15 gadus Wi-Fi darbībai izmantots WPA2 šifrēšanas protokols. 2017. gada nogalē šis protokols tika „uzlauzts", kas attiecīgi miljardiem ierīču vēl šodien pakļauj KRACK uzbrukuma riskam. Uzbrukuma rezultātā ļaundari var pārtvert Wi-Fi savienojumu un veikt ļaundabīgas koda injekcijas.

WPA3 ir nākamās paaudzes Wi-Fi drošības standarts, kas būvēts uz jau esošā WPA2 bāzes, un kam veikti ievērojami uzlabojumi un papildinājumi ar mērķi vienkāršot Wi-Fi drošību, panākt stingrāku autentifikāciju, nodrošināt spēcīgāku kriptogrāfiju sensitīvo datu nozarei un saglabāt kritisko tīklu pretestību.

Plānots, ka pāreja no WPA2 uz WPA3 noritēs pakāpeniski, līdz jaunais standarts būs obligāta prasība, lai izietu iekārtas Wi-Fi sertifikāciju. Prognozēts, ka pirmās iekārtas ar WPA3 parādīsies jau nākamā gada laikā. **Iekārtas, kas atbalstīs jauno šifrēšanas protokolu, joprojām būs savienojamas ar vecākām iekārtām, kas savai darbībai izmanto WPA2 protokolu.**

Vairāk informācijas:
Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

Krāpnieki, kas izliekas par tehniskā atbalsta dienesta speciālistiem no Microsoft



Krāpniecības shēma, kur ļaundari izliekas par *Microsoft* tehniskā atbalsta dienesta speciālistiem, ar mērķi, protams, izkrāpt naudu, ir aktuāla arī šodien un arī Latvijā. Kā liecina *Microsoft* oficiālā statistika, tad 2017. gadā *Microsoft* **klientu atbalsta serviss saņēma 153 000 ziņojumus no klientiem, kas cietuši vai saskārušies ar minēto krāpšanas shēmu**. Satraucoši, ka tas ir par 23% vairāk nekā iepriekšējā gadā. Statistika arī liecina, ka 1**5% no ziņotājiem ir krituši par upuri krāpniekiem un cietuši finansiālus zaudējumus**, kas mērāmi robežās vidēji no 200 – 400 ASV dolāriem. **Kopējā izkrāptā summa ir lēšama vairākos miljonos dolāru**, kas ir pietiekami, lai krāpnieki uzcītīgi turpinātu iesākto. Ziņojumi saņemti no 183 valstīm, kas liecina par globālu problēmu. **Arī CERT.LV periodiski saņem ziņojumus šajā jautājumā no iedzīvotājiem Latvijā.**

Krāpnieki izmanto iebiedēšanas taktiku, lai panāktu, ka upuris samaksā par nevajadzīgiem tehniskā atbalsta dienesta pakalpojumiem, kas it kā nepieciešami, lai salabotu izdomātas programmatūras vai iekārtas problēmas.

Eksistē vairākas pieejas un metodes, ko ļaundari izmanto. Piemēram, **viņi paši piezvana upurim, un stādās priekšā kā *Microsoft* vai kādas citas kompānijas pārstāvji.** Zvana saņēmējiem nav ieteicams paļauties tikai uz telefona numura noteicēju, jo arī to ļaundariem ir iespējams viltot, piemēram, tā, lai izskatītos, ka numurs nāk no tās pašas valsts vai reģiona. Tālāk ļaundari parasti mēģina pierunāt upuri instalēt programmu, kas dod viņiem iespēju attālināti pieslēgties upura iekārtai. Izmantojot doto pieeju, **krāpnieki viltīgi cenšas normālas sistēmas darbības pazīmes stādīt priekšā kā apliecinājumu kāda vīrusa klātesamībai utt.** Katrs šāds ienākošs zvans ar lielu varbūtību ir krāpšanas mēģinājums.

Cita populāra pieeja **ir panākt, ka upuris pats piezvana krāpniekiem**. Upurim, apmeklējot kādu mājas lapu, parādās krāpnieku veidots brīdinājuma paziņojums, kas informē par nopietnām iekārtas vai programmatūras problēmām. Paziņojumā norādīts arī atbalsta telefons, uz kuru upurim jāzvana, lai savu iekārtu savestu kārtībā. **CERT.LV atgādina, ka realitātē *Microsoft* kļūdu un brīdinājuma paziņojumi nesatur nekādus telefona numurus.** Ja upuris pats piezvana, tālāk turpinās scenārijs ar attālināto pieslēgšanos un noslēdzas ar krāpnieku pieprasījumu maksāt viņiem vienreizēju abonementa maksu par piedāvāto servisu.

CERT.LV aicina, saņemot šādus zvanus, tos uzreiz pārtraukt un nekādā gadījumā nedot zvanītājam pieeju savai iekārtai un privātajai informācijai. Šaubu gadījumā zvaniet uz ražotāja mājaslapā norādīto tehniskā atbalsta telefona numuru, nevis krāpnieciskajos e-pastos vai krāpnieciskajā mājaslapā norādīto telefona numuru.

Vairāk informācijas:
Tech support scams: https://www.microsoft.com/en-us/wdsi/threats/support-scams

Teaming up in the war on tech support scams: https://cloudblogs.microsoft.com/microsoftsecure/2018/04/20/teaming-up-in-the-war-on-tech-support-scams/

Eiropas kiberdrošības eksperti gatavojas krīzes apstākļiem mācībās "Cyber Europe 2018"

Vairāk nekā 900 kiberdrošības speciālistu no 30 valstīm piedalījās virtuālas krīzes situācijas risināšanā, lai pilnveidotu sadarbību gan institūciju, gan valstu līmenī. Mācības koordinēja Eiropas Savienības Tīklu un informācijas drošības aģentūra (ENISA), bet mācību dalībnieki piedalījās mācībās, atrodoties savās ierastajās darbavietās vai speciāli organizētos krīzes centros.

Intensīvā divu dienu mācību scenārijā, kas veidoja līdz šim visaptverošākās Eiropas Savienības kiberdrošības mācības "Cyber Europe 2018" (CE2018), **mācību notikumi norisinājās simulētā mācību vidē, kurā mācību dalībniekiem nācās spēt identificēt un novērst liela mēroga apdraudējumus, kas šoreiz skāra aviācijas sektoru**, reaģēt uz tiem, kā arī labāk izprast incidentu pārrobežu ietekmi. Kopējais simulēto incidentu skaits sasniedza 23 222 incidentus.

Plašāka informācija pieejama šeit: https://cert.lv/lv/2018/06/starptautiskas-kibermacibas-cyber-europe-2018-gatavosanas-iespejamai-kiberkrizei

Kiberstāsti

• • •

Jūnija sākumā CERT.LV saņēma ziņojumu no kādas valsts institūcijas par atklātām koda modifikācijām tās mājas lapā un tur ievietotu aizdomīgu saiti. Pēc veiktās izpētes CERT.LV secināja, ka pie vainas visticamāk ir novecojusi mājaslapas satura vadības sistēma. CERT.LV informēja institūciju, ka DRUPAL satura vadības sistēmai nesen atklātas kritiskas ievainojamības, kas tiek aktīvi izmantotas, lai ievainojamās vietnēs ievietotu kaitīgus .js failus. To mērķis ir veikt virtuālo valūtu ieguvi apmeklētāju datoros. Attiecīgi tieši šāds skripts ievietots minētajā mājas lapā. Ļaundabīgais kods no vietnes tika izņemts, un pēc tam veikta arī sistēmas atjaunošana.

• • •

Kamēr jūnijā Jāņa bērni tradicionāli daudzina papardes ziedu, tikmēr citi otrpus ekrānam atrod veidus kā uz tā rēķina nopelnīt. Jūnijā vairākas privātpersonas ziņoja CERT.LV par saņemtām šantāžas vēstulēm angļu valodā. Šādi ziņojumi periodiski saņemti arī iepriekš, taču jūnijā bija jūtams ziņotāju skaita pieaugums. Ļaundari e-pastā apgalvo, ka savā īpašumā ieguvuši kompromitējošus video materiālus par lietotāju, kā arī lietotāja draugu un paziņu e-pastus un kontaktus sociālajos tīklos. Ļaundaris e-pastā pārliecinoši izklāsta kā ieguvis video materiālu – ievietojot ļaundabīgu kodu it kā lietotāja apmeklētā „18+" vietnē, kuras apmeklējums ticis, lietotājam nezinot, caur videokameru ierakstīts. Tālāk tiek pieprasīta maksa *bitkoinos* par to, lai šis materiāls netiktu izplatīts lietotāja kontaktiem. Pieprasītās summas atšķiras un tās variē no 300 – 700 ASV dolāriem. Ļaundari kā savu atrašanās vietu (protams, tikai izdomājums) norādījuši Baltkrieviju, Indiju, Ķīnu, Igauniju utt. CERT.LV informēja lietotājus, ka tā ir tikai parasta krāpšana bez reālas ielaušanās datorā. Tāpat tika dotas norādes nekomunicēt ar izspiedēju, un drošības nolūkos veikt pilnu datora pārbaudi ar atjauninātu antivīrusa programmu. Neviens no ziņotājiem necieta finansiālus zaudējumus.

• • •

Arī jūnijā CERT.LV turpināja saņemt ziņojumus no Latvijas uzņēmumiem par kompromitētām biznesa e-pasta sarakstēm. Scenārijs visos gadījumos ir līdzīgs: ļaundari dažādos veidos (datorvīruss, pikšķerēšanas e-pasti un mājas lapas) iegūst savā īpašumā uzņēmuma e-pasta lietotāja piekļuves datus, ielogojas e-pastā un veic izmaiņas uzstādījumos tā, lai turpmāk saņemtu izsūtīto e-pastu kopijas. Tālāk tiek izveidota līdzīga e-pasta adrese uzņēmuma oficiālajai ar tikko pamanāmām izmaiņām domēna paplašinājumā. Piemēram, „.lv" vai „.com" vietā parādās „.ml", „.cf" u.c. Kad tas ir paveikts, ļaundaris uzņēmuma vārdā turpina saraksti ar sadarbības partneriem vai klientiem, informējot, ka uzņēmuma rekvizīti ir mainīti, un tiek norādīts jaunais bankas konts, uz kuru jāveic apmaksa. Tādēļ CERT.LV aicina pēc šādu aizdomīgu izmaiņu veikšanas vienmēr sazināties ar sadarbības partneri vai klientu pa citiem oficiāliem kanāliem, un pārliecināties par informācijas patiesumu. Šajos konkrētajos gadījumos CERT.LV ieteica pārbaudīt datorus, kā arī informēt darījuma parterus par notikušo un lūgt arī viņiem veikt pārbaudes. Pēc datora pārbaudes tika ieteikts nomainīt arī e-pasta paroles. Saņemtie krāpnieciskie bankas konti tika tālāk nodoti Valsts policijai.

Statistika: biežāk izmantotie interneta resursi *

16,0%
ZIŅU PORTĀLI

15,1%
SOCIĀLIE TĪKLI

15,0%
PRIVĀTAIS E-PASTS

Internetbanka **11,8%**

Darba e-pasti **11,1%**

Iepirkšanās portāli **11,8%**

Spēles **9,2%**

*CERT.LV rīkotās aptaujas rezultāti valsts un pašvaldības iestādēs (2017). Aptaujā piedalījās 664 respondenti.

JŪLIJA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: "Uzmanību – zvana krāpnieks!"

Domājot par kibernoziedzniekiem, parasti iztēlojamies ļaundarus, kas ar datora starpniecību veic izsmalcinātus uzbrukumus internetā. Kamēr daudzi mūsdienu ļaundari tiešām izmanto e-pastu vai ziņojumu apmaiņu, citi ir atraduši radošus veidus kā pielietot arī telefonu potenciālo upuru apmānīšanai. Telefona izmantošanai ir divi ievērojami labumi. Pirmkārt, eksistē daudz mazāk drošības tehnoloģiju, kas uzrauga telefona zvanus, nekā salīdzinoši tas ir, piemēram, e-pastiem. Otrkārt, izmantojot telefonu, ļaundaris daudz labāk var „pārraidīt" savas emocijas, kas attiecīgi padara krāpniecību daudz efektīvāku.

Pilna raksta versija pieejama: https://cert.lv/uploads/ieteikumi/201807-OUCH-July-Latvian.pdf

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

09. **OKTOBRIS** - Kiberdrošības konference "Kiberšahs 2018"