Iknedēļas ziņas
Sagatavotas 03.03.2017.
Numurs 2017/6

Uzbrūk ar atjauninājumu palīdzību

Latvijā parādījušās vairākas inficētas mājas lapas, kas apmeklētājiem piedāvā viltus Adobe Flash atjauninājumus. Ja lietotājs instalē piedāvāto atjauninājumu, tas tiek inficēts ar banku vīrusu Qadars.

CERT.LV apzināja visas kompromitētās lapas un lūdza nekavējoties izņemt kaitniecisko skriptu no lapas, lai neapdraudētu lietotājus, atgādinot, ka, lai nepieļautu atkārtotu kaitīga satura izvietošanu, nepieciešams atjaunināt CMS Joomla, un pārbaudīt lapas drošību.

Vīrusa instalācijas ekrānšāviņš:

Vairāk par Quadars banku vīrusu:

https://malwarebreakdown.com/2017/02/12/thousands-of-compromised-websites-leading-to-fake-flash-player-update-sites-payload-is-qadars-banking-trojan/

Tāpat nesen kļuva zināms par līdzīgu veidu, kā inficēt lietotāju datorus, piedāvājot uzinstalēt "Chrome's language pack" lai it kā novērstu radušos problēmu ar fontiem.
Vairāk: https://neosmart.net/blog/2017/beware-of-this-new-chrome-font-wasnt-found-hack/

Ieraksta video zvanu un izspiež naudu

Kāds vīrietis CERT.LV ziņoja par krāpniekiem, kas veic šantāžu un naudas izspiešanu. Krāpnieciskā shēma ir tāda, ka sociālajos tīklos vai iepazīšanās aplikācijā tiek piedāvāts iepazīties, tad krāpnieki aicina sarunu turpināt Skype platformā, kur lietotājs tiek mudināts veikt dažādas intīmas darbības. Visu notiekošo video zvanu Skype krāpnieki nofilmē.
Konkrētajā gadījumā krāpniece esot bijusi no Lielbritānijas un pieprasīja 500 mārciņas, pretējā gadījumā video tiks izplatīts youtube un tiks nosūtīts visiem vīrieša kontaktiem Facebook.

CERT.LV ir zināmi vairāki līdzīgi gadījumi, kad sociālo tīklu lietotāji cietuši no šādas krāpniecības, kuras rezultātā nofilmētas un publiski izplatītas viņu pašu darbības. CERT.LV atgādina, ka sociālie tīkli ir publiska vide, un jebkura it kā privāta sarakste vai privāti video zvani ir viegli ierakstāmi un publicējami tīmeklī.

Iesakām nekādā gadījumā nemaksāt izspiedējiem, jo izspiedēji var draudēt atkārtoti, un pieprasīt lielāku summu.
Ja šāds incidents ir noticis, iesakām pārliecinieties, ka sociālo tīklu un e-pasta paroles ir drošībā, nepieciešamības gadījumā tās jānomaina, lai krāpniekiem nebūtu pieeja sociālo tīklu kontiem, kā arī vērsties policijā.

Tiek mainīts eParaksta radīšanai izmantotais kriptogrāfijas algoritms - aicina veikt atjauninājumus

No 01.03. ir pieejams programmatūras eParakstītājs 1.4.1. atjauninājums, kurā mainīts eParaksta radīšanai izmantotais kriptogrāfijas algoritms.

Drošības atjauninājums ieviests, ņemot vērā pagājušajā nedēļā starptautiskā tehnoloģiju uzņēmuma Google publiskoto informāciju par kriptogrāfijas algoritma SHA1 ievainojamību. Latvijā šāds kriptogrāfijas algoritms tiek izmantots virknē informācijas sistēmu un lietotņu, tostarp eParaksta radīšanai kopš tā ieviešanas 2006.gadā. Kopš Google paziņojuma par SHA1 ievainojamību š.g. 23.februārī, LVRTC speciālisti ir veikuši eParaksta un saistīto sistēmu drošības auditu un izstrādājuši programmatūras atjauninājumu, izmantojot jaunākas paaudzes kriptogrāfijas algoritmu SHA256.

Kopš 28.februāra virtuālā eParaksta lietotājiem portālā www.eparaksts.lv nav pieejama dokumentu parakstīšanas PDF formātā, jo arī portālā tiek veikta kriptogrāfijas algoritma nomaiņa.

LVRTC aicina eParaksta lietotājus un informācijas sistēmu izstrādātājus sekot līdzi informācijai un lietotņu atjauninājumiem portālā www.eparaksts.lv, jo visdrīzākajā laikā lietotājiem būs pieejams arī informācijas sistēmās izmantoto JAVA bibliotēku atjauninājums, savukārt turpmākajās dienās lietotājiem un informācijas sistēmu izstrādātājiem tiks nodrošināts vēl viens programmatūras un JAVA bibliotēku atjauninājums, kas ļaus atpazīt parakstāmos dokumentus, kurus potenciāli ietekmējusi kriptogrāfijas algoritma ievainojamība.

Lietotājiem eParakstītājs 1.4.1. versijas atjauninājums tiek piedāvāts automātiski, atverot programmatūru.

Programmatūras jaunākā versija lejupielādei pieejama portālā www.eparaksts.lv sadaļā Palīdzība->Lejupielādes->eParakstītājs 3.0 https://www.eparaksts.lv/lv/palidziba/lejupielades/eparakstitajs-3/.

Vairāk informācijas par SHA1 ievainojamību:
https://www.bleepingcomputer.com/news/security/google-announces-first-ever-sha1-collision-attack/

CloudFlare ievainojamības dēļ noplūst sensitīvi dati

Tika atklāta nopietna ievainojamība Cloudflare programmatūrā, kā rezultātā noplūda konfidenciāli mājas lapās esoši dati, piemēram, paroles, sīkdatnes un autentifikācijas rīki. Tāpat daļa nopludināto datu bija nokļuvuši meklētājprogrammu kešatmiņā, kas radīja papildu grūtības ievainojamības seku novēršanā.
Vairāk par ievainojamību: http://thehackernews.com/2017/02/cloudflare-vulnerability.html

CloudFlare maršrutē mājaslapas apmeklētāju plūsmu caur savu globālo ģeogrāfiski izkliedēto serveru tīklu un sniegtos pakalpojumus izmanto vairāk nekā 5 miljoni tīmekļa vietnes.
Nav zināms, cik daudz vietnes Latvijā izmanto Cloudflare risinājumus.

Jauns uzbrukumu vektors

Parādījies jauns uzbrukumu veids - interneta kešatmiņas pārtveršanas uzbrukums. Ar šādu uzbrukumu palīdzību iespējams pārņemt kontroli pār atsevišķu pakalpojumu sniedzēju kontiem, piemēram, PayPal.
Vairāk: http://omergil.blogspot.in/2017/02/web-cache-deception-attack.html