Iknedēļas ziņas
Sagatavotas 05.04.2017.
Numurs 2017/8

Kopēta valsts iestādes mājas lapa

Martā ar CERT.LV sazinājās kāda valsts iestāde un informēja, ka parādījusies mājas lapa ar līdzīgu domēna vārdu, kurā nokopēta informācija no oriģinālās iestādes lapas.
CERT.LV ieteica vērsties policijā un ziņot par autortiesību pārkāpumu, jo sākotnēji bija pārkopēta daļa iestādes mājas lapas satura. Tomēr marta beigās tika saņemtas ziņas par nelegālu pakalpojumu sniegšanu viltotajā lapā Latvijas Republikas vārdā, tajā skaitā par datu ievades formām, kas klasificējas kā pikšķerēšanas incidents.
CERT.LV sazinājās ar .lv domēna vārdu reģistru NIC.lv ar lūgumu atslēgt domēna vārdu, taču NIC nebija tiesiska pamata atcelt domēna vārda reģistrāciju vai atslēgt domēna vārdu.
CERT.LV noskaidroja, ka viltotā mājas lapa tiek mitināta ASV. Pirms vairāk kā nedēļas CERT.LV vērsās pie US-CERT ar lūgumu palīdzēt aizvērt šo lapu, pagaidām bez rezultātiem.

Ja CERT.LV būtu likumiskas tiesības pieprasīt aizvērt .lv domēna vārdu, kādas tagad tiek iestrādātas IT drošības likumā, tad šis incidents būtu atrisināts, tikko tiktu konstatētas pikšķerēšanas pazīmes. Šobrīd iestādei ir iespēja vērsties tiesā, tādējādi panākot domēna bloķēšanu.

Kompromitēti vairāk kā 700 maršrutētāji

CERT.LV februāra beigās saņēma informāciju par vairāk kā 700 kompromitētiem maršrutētājiem, kas sūtīja lietotāju datus uz komandu un kontroles serveri. Minētās iekārtas izmantoja novecojušas DD-WRT programmatūras versijas, kas satur kritisku ievainojamību. Rezultātā uzbrucējs uz kompromitētajām iekārtām uzstādīja skriptu, lai ievāktu pa nešifrētajiem kanāliem pārsūtītu datus, ftp, http, pop u.c. paroles.
CERT.LV uzsāka iekārtu turētāju apziņošanu un ieteica, kā atbrīvoties no ļaunatūras.
Lietotājiem jāatjauno noklusētie iestādījumi maršrutizētājā, jāatjauno DD-WRT programmatūru no http://www.dd-wrt.com/site/index un jānomaina visas paroles resursiem, kuri tika apmeklēti caur inficēto iekārtu.
Latvijā tika apzinātas piecas šādas iekārtas, pārējās iekārtas atradās citās pasaules valstīs.

Kompromitētas vairāku iestāžu mājas lapas

Pagājušajā nedēļā tika saņemtas ziņas par vairākām kompromitētām iestāžu lapām. Kādas iestādes lapā tika izmantots failu menedžeris, kas bez autorizācijas atļāva augšupielādēt izpildāmus failus un kuru uzbrucējs ir izmantojis, lai augšupielādētu failu, kas nodrošina piekļuvi lapai. Lapa tika arī izķēmota.
Tāpat 28.03. tika kompromitēta www.lielvarde.lv mājas lapa, kur no meklētāja "Google" lietotāji tika novirzīti uz vietni, kura piedāvāja iegādāties viagru. Lapa tika kompromitēta dēļ ievainojamas satura vadības sistēmas "Joomla".
Līdzīgi tika kompromitētas vēl vairākas mājas lapas, kurās ievainojamību novēršana turpinās.

Kā pārņemt kontroli pār antivīrusu?

Cybellum pētnieki atklāja jaunu Zero-Day uzbrukumu, kas spēj pārņemt kontroli pār zināmajiem ražotāju antivīrusiem. Šis uzbrukuma veids ir nosaukts par DoubleAgent, jo paralēli veiktajām kaitnieciskajām aktivitātēm tas spēj uzrādīt, ka antivīruss turpina rūpēties par datoru.
DoubleAgent izmanto 15 gadus vecu ievainojamību, kas darbojas visās Microsoft Windows versijās no Windows XP līdz Windows 10.
Antivīrusa ražotāji ir novērsuši šo ievainojamību. Šāda ievainojamība ir īpaši bīstama uzņēmējiem, jo tikko uzbrucējs ir pārņēmis kontroli pār antivīrusu, tas spēj izpildīt kaitnieciskas operācijas, kuras var tikt uztvertas kā leģitīmas darbības, dodot uzbrucējam iespēju pārvarēt drošības risinājumus organizācijā.
DoubleAgent izmanto Windows rīku, kas saucas "Microsoft Application Verifier", kas tiek izmantots kā izpildlaika (runtime) verifikācijas rīks, lai atklātu un novērstu defektus aplikācijās.
Plašāka informācija: https://cybellum.com/doubleagent-taking-full-control-antivirus/