Iknedēļas ziņas
No 07.09. līdz 13.09.2015.
Numurs 2015/07

Kontakti: prese@cert.lv
Tālrunis: 67085888

Uzbrucēji izmanto rīku arsenālu, lai izplatītu banku datu zagšanas trojāni Dyre Troyan

Pagājušajā nedēļā masveidā tika izplatīti e-pasta paziņojumi ar it kā datoru drošības sistēmas paziņojumiem, kas lietotāju aicina atvērt pielikumu. Infekcija tika izplatīta e-pasta pielikumos, izliekoties par drošības sistēmas e-pasta paziņojumiem un bankas pārstāvjiem.
Pielikumā ir .ZIP arhīvs, kas satur .EXE izpildāmo failu. Ja e-pasta saņēmējs atver pielikumu, tad ar Upatre Trojan starpniecību tiek veikts mēģinājums inficēt datoru, lejuplādējot citus kaitīgus failus no IP adresēm Čehijā, ASV un Nigērijā. Šiem soļiem izpildoties, dators tiek inficēts ar Dyre Trojan, kas ir Zeus saimei līdzīgs banku datu zagšanas trojāns.
Incidenta analīzes brīdī kaitīgos failus spēja atpazīt mazāk kā 10 no 56 populārākajām antivīrusu programmām, uzbrucēji tos maskē kā šifrētus attēlu failus ar paplašinājumiem .PNG un .JPG.
Ir zināms, ka šīs kampaņas ietvaros atsevišķas Latvijā strādājošas bankas ir uzbrucēju interešu sarakstā.

Administratori var mēģināt identificēt sekmīgus inficēšanās gadījumus, meklējot komunikāciju ar kaitīgiem resursiem:
Protokoli: HTTP/HTTPS
IP adreses:Ports: 85.135.104.170:443, 197.149.90.166:12102, 172.73.21.168:4443, 93.185.4.90:4443
fblend22.png: sha256:dd102d94b749607fd9842a28d9c66ac191244d1ec1828737512b7ceda1f5c537
fuparfog.exe: sha256:d931a4346202421ce593e95207193007c99ea62752ebabef6dc026f92697d229

Piebilde: visos gadījumos kaitīgā programmatūra saziņu uzsāk ar hXXp://myip.dnsomatic.com/, kas ir nekaitīgs resurss apmeklētāja IP adreses noskaidrošanai. Parastam lietotājam šāda resursa apmeklēšana ir maz ticama, tādēļ var uzskatīt par aizdomīgu arī šo komunikāciju.

CERT.LV panāk Android ierīcēm paredzēta Trojāna kontrolcentra darbības pārtraukšanu Latvijā

Sadarbībā ar Spānijas sakaru operatora CERT kolēģiem ir veikta Android/Trojan.Spy.Smsthief kampaņas izmeklēšana, kuras ietvaros ir panākta Latvijā uzturēta kontrolcentra darbības pārtraukšana. Latvijā uzturētais uzbrucēju serveris tika pielietots Android mobilo ierīču uzbrukumiem pret Spānijas mobilo internetbanku lietotājiem. Incidenta tehniskās informācijas analīze turpinās.

Pikšķerēšanas uzbrukumi pret banku lietotājiem kļūst arvien mazāk izplatīti. Uzbrucēji dod priekšroku mēģinājumiem inficēt gala lietotāja datorus un mobilās ierīces

Lai arī pikšķerēšanas uzbrukumi ar mērķi iegūt e-pasta, sociālo tīklu un tiešsaistes maksājumu sistēmu kontu datus joprojām ir ļoti izplatīti, šāda veida uzbrukumi internetbanku lietotājiem kļūst arvien retāki. Tas tādēļ, ka uzbrucēji pielāgojas internetbanku drošības uzlabojumiem un arī lietotāju labākai spējai atpazīt pikšķerēšanu (phishing). Ja uzbrucēju mērķis ir internetbanku konti, tad priekšroka tiek dota mēģinājumiem inficēt lietotāja datoru – pārsvarā atsūtot e-pastu, kas vilina apmeklēt speciāli sagatavotu tīmekļa vietni, vai pielikumu, kā rezultātā dators tiek inficēts. Arī

mobilās ierīces ir augstā vērtē kibernoziedznieku vidū. Nu jau diezgan droši var teikt, ka ir daļa lietotāju, kuriem privātās informācijas vairāk ir mobilajā telefonā, nekā uz datora. Tajā skaitā arī finanšu darījumi tiek veikti no mobilajām ierīcēm. Kārtējais atgādinājums par to, ka mobilo ierīču drošība un pārdomāta lietošana ir tik pat svarīga, kā darbā ar datoru, ir šajā ziņu izlaidumā minētā Android/Trojan.Spy.Smsthief uzbrukumu kampaņa. Informācija, kā pasargāt savas iekārtas, pieejama CERT.LV uzturētajā portālā https://www.esidross.lv