Iknedēļas ziņas
Sagatavotas 21.10.2015.
Numurs 2015/11

Kontakti: prese@cert.lv
Tālrunis: 67085888

Izplata Zeus banku trojāni, lai nelegāli iegūtu naudu no lietotāju kontiem.

Novērojami uzbrukumu viļņi, kuros tiek izplatītas bēdīgi slavenā Zbot jeb Zeus banku trojāna modifikācijas.
Uzbrucēju mērķis ir pārtvert tiešsaistes maksājumu/transakciju informāciju un nelegāli iegūt naudas līdzekļus no inficēto datoru īpašnieku internetbanku kontiem. Lai arī Zbot/Zeus trojānis ir pazīstams jau kopš 2007. gada, tas ir piedzīvojis vairākas modifikācijas un papildinājumus un joprojām tiek plaši pielietots kibernoziedzībā. Diezgan plaši Latvijā tiek izplatīts arī Dyre Trojan. Kaitīgā koda piegādei uzbrucēji izmanto e-pasta sūtījumus ar pielikumiem, kur ZIP arhīvā ir izpildāmais fails .EXE vai .SCR.
E-pastu tematika parasti ir saņemts vai neapmaksāts rēķins, kurjerpasta informācija, administratīvi jautājumi. Valoda pārsvarā ir angļu, bet epizodiski tiek sagatavoti kvalitatīvi teksti arī latviešu valodā. Pastāv aizdomas, ka uzbrucēji uzrunā jauniešus, studentus, dažkārt citus kibernoziedzniekus, lai par dažiem desmitiem Eiro pārtulkotu un pielāgotu uzbrukuma tekstu.
Diemžēl uzbrucēju rīcībā ir rīki, kas spēj apiet lielāko daļu pretvīrusu risinājumu un nepieciešamības gadījumā arī izslēgt pretvīrusu programmatūru.
Līdz šim konstatētie inficētie datori ir saturējuši novecojušu programmatūru, nav ieviesta drošības politika un pretvīrusu risinājumi ir izvēlēti tādi, kas pieejami bezmaksas.
Svarīgi apzināties, ka gadījumos, lai uzbrukums izdotos, nepieciešama lietotāja "līdzdalība" - pielikuma atvēršana un kaitīgās programmas izpildīšana, tādēļ piegādātā e-pasta teksti tiek veidoti pēc iespējas saistošāki plašai sabiedrības daļai.
CERT.LV aicina interneta lietotājus iepazīties ar savas pretvīrusu programmatūras iespējām un iespējot paroles pieprasīšanu gadījumā, ja tiek veikts mēģinājums izslēgt pretvīrusu programmatūru. Tas nenodrošinās absolūtu aizsardzību, taču apgrūtinās uzbrucēja mērķu sasniegšanu.

Pikšķerēšanas uzbrukumos pielieto PDF pielikumus.

CERT.LV novērojis pikšķerēšanas mēģinājumus ar PDF dokumentu palīdzību e-pasta pielikumos. PDF dokuments satur īsu, provokatīvu informāciju un maskētu saiti uz uzbrucēja sagatavotu tīmekļa vietni, kurā savukārt notiek tālākas uzbrukuma darbības. Pats par sevi PDF dokuments nav kaitīgs un nesatur vīrusu, vai kaitīgu kodu.
Atverot PDF dokumentu, tas informē lietotāju par it kā ar paroli aizsargātu saturu, kuru var apskatīt klikšķinot uz "Click HERE to login and view file"

Ja tiek noklikšķināts uz “HERE”, lietotāja pārlūkā tiek atvērta vietne no zemāk minētajām, kaitīgām saitēm, kas paredzētas lietotāju datu izkrāpšanai dažādos tiešsaistes servisos.

hxxp://pdfviewers.atspace[.]cc/
hxxp://adobfies.site50[.]net/

Šobrīd kaitīgās saites nav pieejamas.

Kaitīgā e-pasta un PDF dokumenta piemērs (teksts un tematika var atšķirties):

From: orders@hk. hk<mailto:orders@hk .hk> [mailto:order@tu i.com]
Sent: Wednesday, October 14, 2015 4:36 PM
To: lcod
Subject: Re: Proof of Payment

Good Morning,

Today we have able to remit the total amount of US$ 47,704.97 to your account.

Details of our payments are as follows:

Total Remittance: US$ 47,704.97

Attached is the TT copy, check with your bank and let us know when you confirm Payment.

Thank you very much.

Best regards,
Sofia

This document is password protected.

Click HERE to login and view file

Aicina piedalīties mediju Kiberdrošības brokastīs.

CERT.LV aicina mediju pārstāvjus piedalīties kiberdrošības brokastīs par aktualitātēm IT drošības jomā. Pasākums notiks **27.10.2015. pl. 10.30, Eiropas Savienības mājā, Aspazijas bulvārī 28, 1. stāvā.**

Mediju pārstāvji tiks informēti par aktuālākajiem apdraudējumiem, kas skar interneta lietotājus un iespējām, kā pasargāties no jaunākajiem vīrusiem un krāpšanas shēmām interneta vidē.

Kiberdrošības brokastīs piedalīsies:
Baiba Kaškina, CERT.LV vadītāja
Varis Teivāns, CERT.LV vadītāja vietnieks
Kārlis Podiņš, CERT.LV IT drošības eksperts

Pasākums tiek organizēts Eiropas Kiberdrošības mēneša ietvaros. Kiberdrošības mēneša mērķis ir veicināt sabiedrības izpratni par kiberdrošību. Pasākumu uzsvars tiek likts uz lietotāju izglītošanu par virtuālās vides apdraudējumiem un atbildīgu attieksmi pret datu un informācijas drošību.

Pieteikšanās mediju pasākumam iespējama līdz 26.10. ieskaitot, rakstot uz prese@cert.lv, vai zvanot pa tālruni 67085851.

CERT.LV aicina uz bezmaksas datora pārbaudi pie datorologa.

Datorologs ir IT drošības speciālists, kurš var diagnosticēt un, ja iespējams, novērst e-slimības un ļaunatūras datorā un sniegt konsultācijas kā pasargāt datoru nākotnē. Visi datorologa padomi ir bez maksas.

Datorologs pieņems trešdien, 28. oktobrī no pl. 10.00 līdz 16.00, Raiņa bulvārī 29, Rīgā (netālu no Stacijas laukuma).

Datorologa pakalpojums pieejams jebkuram datorlietotājam, kurš vēlas pārliecināties, ka viņa dators nav inficēts, kā arī tiem, kas vēlas izārstēt datoru no iegūtiem datorvīrusiem. Datorologa konsultācija palīdz arī tiem, kuri nezin kā pasargāt savu datu, privātās dzīves un naudas drošību e-vidē. Datorologi pārbaudīs arī Android un Apple ierīču (planšetes, mobilie telefoni) veselību.

Šogad „Datorologa akcijā" iesaistīsies drošības eksperti no CERT.LV, kā arī eksperti no SIA Latnet Serviss un SIA Stream Networks.
SIA Latnet Serviss ir to interneta pakalpojumu sniedzēju vidū, kas īpaši rūpējas par savu klientu drošību un drošas interneta vides veidošanu, ko apliecina iegūtā kvalitātes zīme "Atbildīgs interneta pakalpojumu sniedzējs".

„Datorologa akcija" notiek Eiropas kiberdrošības mēneša ietvaros. Kiberdrošības mēnesis tiek rīkots ar mērķi veicināt sabiedrības izpratni par kiberdrošības jautājumiem.