Iknedēļas ziņas
Sagatavotas 14.10.2015.
Numurs 2015/10

Kontakti: prese@cert.lv
Tālrunis: 67085888

Agresīvi izspiedēji uzdarbojas interneta vidē.

Būtiski pieaudzis tādu gadījumu skaits, kad uzbrucēji izmanto gan datorvīrusu tehnoloģijas, gan servisa atteices uzbrukumus (DDoS), lai izspiestu naudu no mājas lietotājiem, uzņēmējiem, finanšu institūcijām un valsts iestādēm.

CERT.LV vēlas pievērst uzmanību izspiešanas paņēmieniem, un ieteikt iespējamos risinājumus:
Izspiedējvīrusi, policijas vīrusi, šifrēšanas vīrusi jeb "*ransomware*" - ir speciāli uzbrukuma mērķiem radīta programmatūra, kas pārsvarā tiek mērķēta uz MS Windows operētājsistēmu lietotājiem un pēdējā laikā arī Android ierīcēm. Šobrīd izplatības ziņā "policijas" vīrusus ir nomainījuši šifrēšanas vīrusi.
"Policijas" vīrusu gadījumā galvenā izspiešanas taktika bija lietotāja darba apgrūtināšana, bloķējot pieeju darba videi, vai gluži vienkārša apmuļķošana, "uzkarinot" jeb iesaldējot interneta pārlūku un pieprasot samaksu Paysafe vai Bitcoin veidā. Ar šiem gadījumiem varēja tikt galā salīdzinoši vienkārši, pārlūka "uzkarināšanas" gadījumā pat pārstartējot datoru.

Šifrēšanas vīrusu ietekme ir daudz nopietnāka un inficēta datora šifrētu datu atjaunošana lielā daļā gadījumu nebija iespējama, jo, uzbrucēji izmantoja spēcīgu kriptogrāfiju, lai sašifrētu lietotāja failus. Par failu atgūšanu tika prasīta samaksa. Atradās upuri, kas maksāja uzbrucējiem, lai atgūtu savu informāciju.

Kā sevi pasargāt?
1) Nevērt vaļā e-pasta pielikumus no nepārbaudītiem avotiem un vienmēr pievērst uzmanību failu paplašinājumiem. Vīrusi pārsvarā tiek izsūtīti .zip arhīvos, kuros iekšā ir .exe vai .scr izpildāmais fails. Ļoti maza ir varbūtība, ka šādus failus Jums kāds sūtīs darba vajadzībām.
2) Savlaicīgi rūpēties par rezerves kopiju izveidi. Noskaidrot, vai operētājsistēmā jau ir integrēta rezerves kopiju izveide un vai tā ir iespējota.

Servisa atteices (DDoS) uzbrukumi, kas seko draudiem un izspiešanai – šādi gadījumi ir novēroti jau agrāk, taču pēdējā gada laikā to skaits ir būtiski audzis un uzbrukumi ir daudz organizētāki un apjomīgāki. Izspiešanas DDoS uzbrukumu kampaņas DDoS4BC (DDoS for bitcoin) un Armada ir skārušas arī Latviju un izspiedēju pieprasītās summas par uzbrukuma neveikšanu vai pārtraukšanu variē no dažiem desmitiem bitcoin līdz vairākiem simtiem.
Uzbrukumus nereti organizē indivīdi vai grupējumi, kas nemaz nav IT eksperti, bet gan nopērk uzbrukuma rīkus un nepieciešamās jaudas kā interneta pakalpojumus.. Šādi pakalpojumi ir salīdzinoši pieejami.

Kā pasargāties no izspiedējiem?
1) Neiesaistīties komunikācijā ar izspiedējiem, pat ja demonstrācijas uzbrukums ir noticis un ir bijis efektīvs.
2) Ja tas nav izdarīts savlaicīgi, tad pēc pirmajiem draudiem nepieciešams apzināt kritisko servisu sarakstu un izstrādāt pakalpojuma nepārtrauktības un aizsardzības plānu. Datu kanāla pārslodzes uzbrukumiem var meklēt aizsardzību pie atbilstoši sagatavotiem pakalpojumu sniedzējiem Latvijā, vai pie starptautiskiem

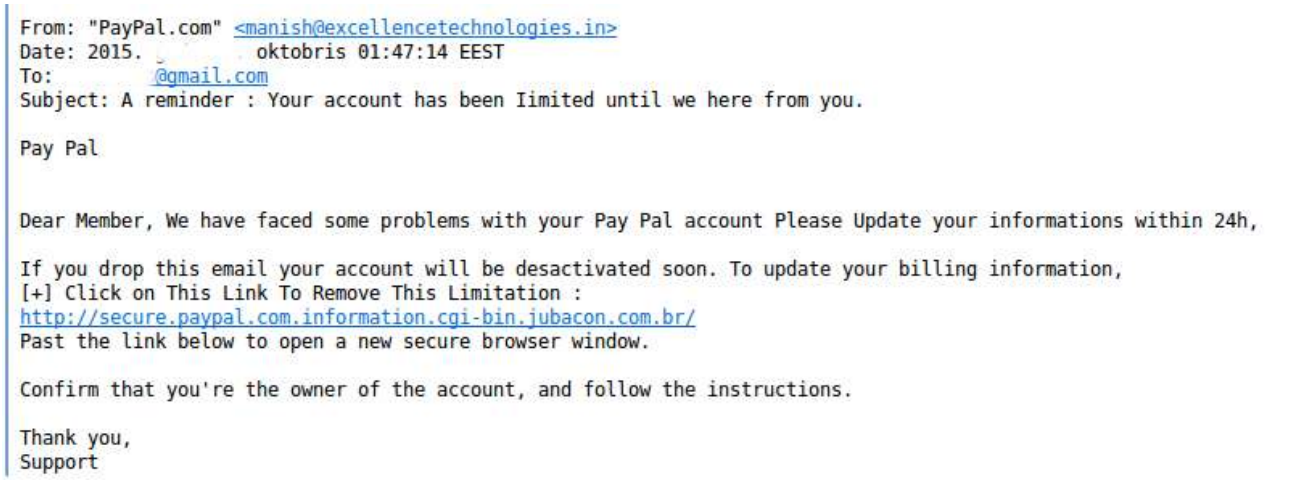
mākoņpakalpojumu servisa sniedzējiem. Protams, svarīgi, lai dārgi risinājumi nesargā cauru un nedrošu servisu, tādēļ svarīgi novērst zināmās ievainojamības un optimizēt veiktspēju pirms pārnešanas aizsargātā vidē.

3) Vienoties ar savu interneta pakalpojumu sniedzēju par iespējamo rīcību uzbrukuma gadījumā un izvērtēt, vai pakalpojuma nepieejamība no ārzemēm ir pieņemams risks, jo tieši globālā interneta atslēgšana cietušajam resursam uz laiku ir tas, ko darīs interneta pakalpojumu sniedzējs, lai pasargātu savu un klienta infrastruktūru bezizejas gadījumā.

Turpinās pikšķerēšanas uzbrukumi Paypal lietotājiem.

Aktīvas pikšķerēšanas uzbrukumu kampaņas maksājumu sistēmu Paypal lietotājiem turpinās jau vairāk kā mēnesi. Arī ļaunatūras izplatītāji ir izvēlējušies par mērķi šo maksājumu sistēmas lietotājus. Tādā veidā uzbrukumu metodes ir vairākas un kaitīgā satura piegāde lielākajā daļā gadījumu ir e-pasts ar saiti uz pikšķerēšanas vietni vai pielikumu, kurā ir ZIP arhīvs ar izpildāmo .exe vai .scr failu, kas ir vīruss.

Zemāk redzams, ka uzbrucējs mēģina maldināt saņēmēju, izveidojot domēna vārdu, kura sākums ir kā leģitīms Paypal domēna nosaukums, taču, pievēršot uzmanību pilnam domēna vārdam, ir skaidri redzams, ka tam nav nekāda sakara ar Paypal.



From: "PayPal.com" <manish@excellencetechnologies.in>
Date: 2015. . oktobris 01:47:14 EEST
To: @gmail.com
Subject: A reminder : Your account has been Iimited until we here from you.

Pay Pal

Dear Member, We have faced some problems with your Pay Pal account Please Update your informations within 24h,

If you drop this email your account will be desactivated soon. To update your billing information,
[+] Click on This Link To Remove This Limitation :
http://secure.paypal.com.information.cgi-bin.jubacon.com.br/
Past the link below to open a new secure browser window.

Confirm that you're the owner of the account, and follow the instructions.

Thank you,
Support

From PayPal <service@paypal.com>
Subject **Your PayPal Invoice is Ready**
To

Dear PayPal Customer,

Please open the attached file to view invoice.

Your monthly account statement is available anytime; just log in to your account. To correct any errors, please contact us through our Help Centre.

Please note: the attached file is in PDF format. If you are unable to open the attached file, please download the free Adobe Acrobat Reader by entering the following address in your web browser:
http://www.adobe.com/products/acrobat/readstep.html

This email was sent by an automated system, so if you reply, nobody will see it. To get in touch with us, log in to your account and click "Contact Us" at the bottom of any page.

1 attachment: paypal_851827665152821_131015.zip 20,4 KB Save

Šeit redzams, ka uzbrucējs mēģina ievilināt saņēmēju atvērt pielikumu, kas ir .zip arhīvs ar izpildāmo .exe failu tajā. Atverot kaitīgo .exe, failu dators tiek inficēts un, ja upuris lieto Paypal servisus, tad uzbrucējs nesankcionēti pārskaita līdzekļus no Paypal konta.

IKT drošības entuziasti informē CERT.LV par atklātiem trūkumiem un apdraudējumiem Latvijas interneta vidē.

Neatkarīgs pētnieks informēja CERT.LV par vairākiem desmitiem ievainojamu tīmekļa vietņu .lv domēnu zonā. Identificētie resursi satur SQL injekcijas ievainojamības, kuras uzbrucēji var izmantot nesankcionētai informācijas izgūšanai no datu bāzēm un pat pilnīgai serveru kompromitēšanai. Šāda labdabīga pētnieku aktivitāte ir ļoti apsveicama un rāda pozitīvu tendenci.
CERT.LV ir informējis visus ievainojamo resursu turētājus un seko līdzi trūkumu novēršanai.