Iknedēļas ziņas
Sagatavotas 13.04.2016.
Numurs 2016/14

Kontakti: prese@cert.lv
Tālrunis: 67085888

Pikšķerēšanas saite Latvijas vietnē

Kompromitētā mājas lapā tika izvietota pikšķerēšanas saite, kas paredzēta "Tesco Bank" bankas lietotāju informācijas izkrāpšanai. Mājas lapa tikusi kompromitēta dēļ neatjauninātas Joomla satura vadības sistēmas. Nav saņemta informācija par šajā incidentā cietušiem datorlietotājiem.

Iespējams atgūt ar Petya šifrējošo vīrusu sašifrētos cietos diskus

Pagājušajā nedēļā informējām par šifrējošā datorvīrusa paveidu Petya, kas atšķirībā no citiem šifrējošajiem datorvīrusiem šifrē datora cietos diskus, tādējādi padarot datorus nelietojamus.
Datorvīrusa koda kļūdas dēļ pētniekiem ir izdevies izstrādāt rīku, ar kura palīdzību iespējams uzģenerēt vajadzīgo atslēgu, lai atšifrētu cieto disku, neko nemaksājot.
Plašāka informācija: http://www.bleepingcomputer.com/news/security/petya-ransomwares-encryption-defeated-and-password-generator-released/

Draud veikt DDoS uzbrukumus

Kāds populārs Latvijas interneta portāls saņēma draudu vēstuli, ka pret portālu tiks veikts DDoS uzbrukumu līdz 1 TB sekundē, ja netiks veikta samaksa. Uzbrukumus sola sākt piektdien, un tiklīdz uzbrukums tiks sāks, samaksa par tā apturēšanu tiks palielināta ar katru uzbrukuma dienu. Draudu vēstulē nav minēts periods, cik dienas ir plānots šis uzbrukums. Vēstuli sūta bēdīgi slavenais Armada kibernoziedznieku kolektīvs.

Sūtītās vēstules piemērs:

---------- Forwarded message ----------
From: Armada Collective <emailimportant@protonmail.com>
Date: 2016-04-10 0:48 GMT+03:00
Subject: DDOS ATTACK
To:

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://lmgtfy.com/?q=Armada+Collective

You will be DDoS-ed starting Friay (April 15) if you don't pay protection fee - 25 Bitcoins @ 1LkNZUBGhuPobxVJTWHRDCcUW9XPXUPfLM
If you don't pay by Friday, attack will start, yours service going down permanently price to stop will increase to 50 BTC and will go up 20 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - sometimes over 1 Tbps per second. And we pass CloudFlare and others remote protections!
So, no cheap protection will help.

Prevent it all with just 25 BTC @ 1LkNZUBGhuPobxVJTWHRDCcUW9XPXUPfLM

Do not reply, we will not read. Pay and we will know its you. AND YOU
WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

Valsts iestāde veiksmīgi izvairās no šifrējošā vīrusa

Kāda valsts iestāde saņēma e-pastu ar pielikumā esošu Locky šifrējošo vīrusu no it kā zināma sūtītāja citā iestādē, ar kuru bija notikusi iepriekšēja e-pasta sarakste. E-pasta saņēmējs uz aizdomu pamata pievienoto failu neatvēra, tādējādi izvairoties no datora inficēšanas ar šifrējošo datorvīrusu.
Pēc veiktās izpētes secināts, ka e-pasts sūtīts no adreses ar domēna vārdu saturn-internet.ru.

Šifrējošo vīrusu izplata arī caur ievainojamību Adobe Flash Player

Pagājušajā nedēļā tika atklāta jauna Adobe Flash Player ievainojamība, kas izmantota Neclear un Magnitude izpildes rīkos, izplatot šifrējošos datorvīrusus Locky un Cerber. Adobe ir novērsis ievainojamību un izlaidis ārkārtas atjauninājumus pagājušajā ceturtdienā.
Ievainojamība ietekmē visas Flash Player versijas uz Windows 10 un senākām versijām.

Plašāka informācija: https://threatpost.com/latest-flash-zero-day-being-used-to-push-ransomware/117248/
Atjauninājumi pieejami: https://helpx.adobe.com/security/products/flash-player/apsb16-10.html