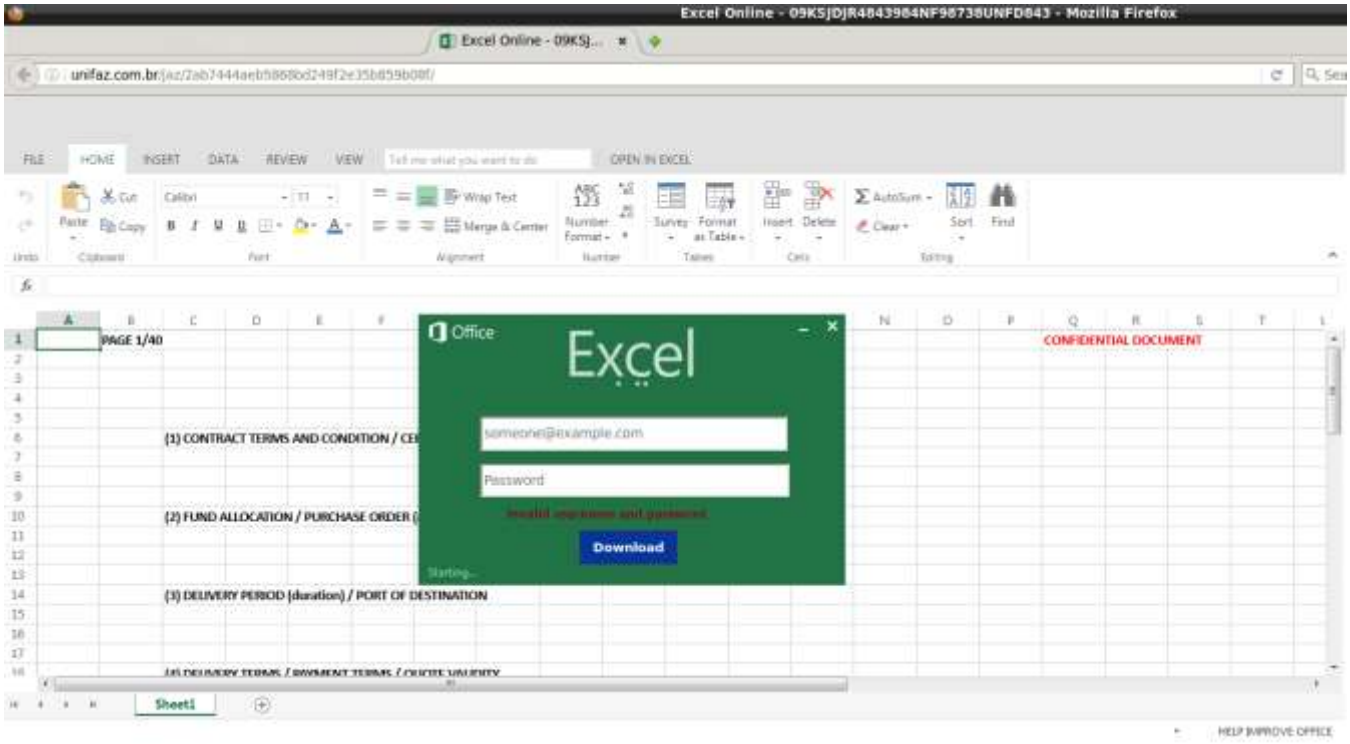
Iknedēļas ziņas
Sagatavotas 30.08.2016.
Numurs 2016/32

Turpinās mērķēti uzbrukumi finanšu sektoram

Arī šajā periodā novēroti rafinēti, mērķēti kiberuzbrukumi kādai Latvijā strādājošai bankai. Uzbrukums tika noformēts kā e-pasta vēstule, kas it kā sūtīta no bankas prezidenta e-pasta un aicina atvērt pielikumā esošu PDF dokumentu, kas lietotāju maldina, liekot domāt, ka tas ir aizsargāts dokuments. Lai to apskatītu, nepieciešams autentificēties, spiežot uz pogas PDF dokumentā.

Kad lietotājs nospiež pogu, tiek aktivizēta saite un dokumentā tiek atvērts interneta pārlūks, kurā attēlots Excel dokuments ar autentifikācijas logu.



Lietotājs tiek aicināts ievadīt sava e-pasta lietotājvārdu un paroli. Ja lietotājs izdara prasīto, tiek atvērts Excel dokuments no https://docs.google.com/, lai mazinātu lietotāja aizdomas, ka notikusi e-pasta paroļu izkrāpšana. Ņemot vērā uzbrukuma raksturu, var pieņemt, ka uzbrukumā iegūtie lietotājvārdi un paroles vēlāk tiks pielietoti

kādā no bankas sistēmām cerībā, ka bankas infrastruktūrā tiek izmantots SSO, jeb single-sign-on autentifikācijas modelis. Uzbrukuma mēģinājums nav bijis sekmīgs.
Gandrīz identiskā izpildījumā, citā uzbrukuma kampaņā lietotājus mēģināja ievilināt lejuplādēt šifrējošo izspiedējvīrusu "Locky". Arī šis uzbrukums nebija sekmīgs.

Secinājumi:
Pasta sistēmas lietotājus iespējams pasargāt no uzbrucēju noformētiem e-pastiem, kuri it kā sūtīti kolēģu vārdā. Ieteicams izmantot arī DNS protokola sniegtās iespējas (SPF, DKIM, DMARC ierakstus).
Lietotāju regulāra apmācība ir viens no svarīgākajiem IT drošības stūrakmeņiem, kas ir pierādījies arī šajā incidentā.

Izglītības iestādes tīmekļa vietne inficē apmeklētājus

Hakeri uzlauzuši kādas izglītības iestādes tīmekļa vietni un inficējuši tās apmeklētājus, izmantojot Neutrino Exploit kit rīkus. Tīmekļa vietne uzlauzta dēļ ievainojamības novecojušā WordPress satura vadības sistēmas spraudnī.
CERT.LV veic incidenta analīzi, lai noskaidrotu potenciāli ietekmēto vietnes apmeklētāju skaitu.

Robotu tīkls no interneta kamerām Latvijā

CERT.LV saņēma informāciju par ievainojamību skenēšanas uzbrukumiem, kas veikti no Latvijas IP adresēm. Veicot incidenta izmeklēšanu, tika konstatēts, ka uzbrukumos iesaistītās IP adreses tiek lietotas uz IP kamerām, kuras ir nedroši konfigurētas un tām iespējams pieslēgties ar ražotāja noklusētajiem lietotāja vārdu un paroli. Iekārtu turētāji ir informēti un CERT.LV seko incidenta novēršanai.