Ikmēneša Informācijas drošības izdevums Tev

Personalizēta krāpšana

Pārskats

Kibernoziedznieki turpina rast arvien jaunus veidus, kā cilvēkus apmuļķot. Arvien populārāks kļūst jaunais krāpšanas veids – personalizētā krāpšana. Kibernoziedznieki ievāc vai nopērk informāciju par miljoniem cilvēku, un tad izmanto šo informāciju, lai personalizētu uzbrukumus. Zemāk mēs nodemonstrēsim, kā šie uzbrukumi darbojas, izanalizējot tipisku piemēru. Jo vairāk jūs zināsiet par šādiem uzbrukumiem, jo vieglāk būs tos atpazīt un apturēt.

Kā tas strādā?

E-pasta un telefona krāpniecības nav jaunums, kibernoziedznieki ir centušies apmuļķot cilvēkus gadiem. Kā piemērus var minēt "Jūs esat vinnējuši loterijā" vai slaveno Nigērijas prinča krāpniecību. Taču šajos tradicionālajos uzbrukumos kibernoziedznieki nezina, ar ko viņiem būs darīšana. Viņi vienkārši sagatavo vispārīgu vēstuli un izsūta to miljoniem cilvēku. Tā kā šie krāpnieciskie e-pasti ir tik vispārīgi un vienādi, tos parasti ir viegli atpazīt. Personalizēta krāpniecība ir citāda, kibernoziedznieks vispirms veic izpēti, un katram upurim sagatavo tam pielāgotu vēstuli. Viņi to dara, ievācot informāciju vai nopērkot datubāzi ar cilvēku vārdiem, parolēm, telefona numuriem un citu informāciju. Šāda informācija ir viegli pieejama, pateicoties daudzajām uzlauztajām tīmekļa vietnēm. Bieži vien tā ir arī brīvi pieejama sociālo tīklu vietnēs un publiski pieejamos valsts iestāžu resursos. Pēc tam kriminālnoziedznieki uzbrūk visiem, par kuriem ir ieguvuši informāciju.

Viens no izplatītākajiem paņēmieniem, ko lieto kibernoziedznieki, ir baiļu iedvešana vai izspiešanas mēģinājumi, tā panākot, ka jūs tiem samaksājat naudu. Uzbrukums darbojas sekojoši: viņi atrod vai nopērk informāciju par cilvēku lietotājvārdiem un parolēm, kas iegūtas no uzlauztām tīmekļa vietnēm, tad atrod jūsu e-pasta adresi un ar jums saistītu informāciju šādā datubāzē un nosūta jums (kā arī visiem pārējiem, kas iekļauti šajā datubāzē) e-pastu, kurā norāda šādu tādu ar jums saistītu informāciju, ieskaitot paroli, kuru jūs izmantojāt uzlauztajā tīmekļa vietnē. Kibernoziedznieki uzdod šo paroli par "pierādījumu", ka ir uzlauzuši jūsu datoru vai iekārtu, kas, protams, nav taisnība. Kibernoziedznieki arī apgalvo, ka, uzlaužot iekārtu, pieķēruši jūs vērojam pornogrāfiska rakstura materiālus internetā. E-pastā tiek draudēts, ka, ja nesamaksāsiet izpirkuma maksu, liecības par jūsu apkaunojošajām tiešsaistes aktivitātēm tiks nosūtītas jūsu ģimenei un draugiem.

Āķis ir – šajā un gandrīz visos citos šādos gadījumos kibernoziedznieki nav uzlauzuši jūsu iekārtu. Viņi pat nezina, kas jūs esat, nedz arī kādas tīmekļa vietnes apmeklējat. Krāpnieki vienkārši cenšas izmantot dažas viņiem par jums zināmās lietas, lai jūs iebiedētu un liktu jums noticēt, ka viņi ir uzlauzuši jūsu iekārtu, un panāktu, ka jūs tiem samaksājat. Atcerieties, ka sliktie var izmantot šos pašus paņēmienus arī krāpnieciskos telefona zvanos.

Ko man darīt?

Atpazīstiet šādus e-pastus un telefona zvanus kā krāpnieciskus. Tas ir dabiski just bailes, ja kāds ir ieguvis jūsu personīgo informāciju. Taču atcerieties, sūtītājs melo! Uzbrukums ir daļa no automatizētas masveida kampaņas, nevis mēģinājums uzbrukt tieši jums. Mūsdienās kriminālnoziedzniekiem kļūst arvien vieglāk atrast vai nopirkt personīga rakstura informāciju, līdz ar ko gatavojieties lielākam personalizēto uzbrukumu apjomam nākotnē. Dažas pazīmes, pēc kurām atpazīt uzbrukumu:

⚠

- **Vienmēr esiet aizdomu pilns, kad saņemat ļoti steidzinošu e-pastu, ziņu vai telefona zvanu. Ja kāds izmanto tādas emocijas kā bailes vai steidzamību, viņš cenšas panākt, lai jūs steigā kļūdītos.**
- **Ja kāds pieprasa maksājumu BitCoin kriptovalūtā, dāvanu kartēs vai citos neizsekojamos maksājumu līdzekļos.**
- **Ja saņemat aizdomīgu e-pastu, veiciet meklēšanu Google, lai noskaidrotu, vai citi nav ziņojuši par līdzīgu uzbrukumu.**

Visbeidzot, veselais saprāts ir jūsu labākā aizsardzība. Taču mēs arī iesakam vienmēr izmantot garas, unikālas paroles katram jūsu tiešsaistes kontam. Nevarat atcerēties visas paroles? Izmantojiet paroļu pārvaldnieku. Papildus tam, izmantojiet divu pakāpju autentifikāciju, kad vien tas ir iespējams.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Viesredaktors

Lenny Zeltser *ir kiberdrošības veterāns. Viņš cīņai ar ļaunatūru veido drošības risinājumus Minerva Labs, kā arī pasniedz lekcijas SANS institūtā. Lenny ir aktīvs Twitter lietotājs -* @lennyzeltser, *un raksta arī blogu* zeltser.com *par IT drošību.*

Resursi

Sociālā inženierija:	https://www.sans.org/u/MUU
Kā atpazīt pikšķerēšanu:	https://www.sans.org/u/MUZ
Pārbaudiet informāciju par sevi tiešsaistē:	https://www.sans.org/u/MV4
Paroļu pārvaldnieki:	https://www.sans.org/u/MV9

OUCH! izdod SANS institūts programmas "Security Awareness" ietvaros un tas tiek izplatīts saskaņā ar Creative Commons BY-NC-ND 4.0 licences nosacījumiem. *Jūs varat izplatīt šo biļetenu vai izmantot to savā informācijas tehnoloģiju drošības izglītošanas programmā ar nosacījumu, ka biļetens netiek izmainīts Papildu informācijai vai jautājumiem par tulkošanu izmantojiet* www.sans.org/security-awareness/ouch-newsletter e-pasta adresi. *Redakcija: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: Edgars Tauriņš*

CERT.LV Information Technologies Security Incident Response Institution