OUCH! 2023 - 04

SANS SECURITY AWARENESS

OUCH!

Ikmēneša informācijas drošības izdevums tev

Iebiedēšanas programmatūra (Scareware): Stāsts

Brīdinājums! Jūsu dators ir inficēts ar izspiedējvīrusu Black Basta. Zvaniet uz šo tālruņa numuru, lai nekavējoties atrisinātu problēmu! – *Ja jūsu datorā parādītos šis brīdinājuma logs, vai jūs zvanītu uz norādīto tālruņa numuru?*

Uzbrukums

Pēc trīsdesmit gadus ilga darba Debora bija uzkrājusi pietiekami daudz naudas, lai kopā ar vīru varētu doties pensijā. Vēloties pārskatīt savus pensiju kontus, viņa pārlūkprogrammā ievadīja savas bankas nosaukumu. Viņa nepamanīja, ka bija kļūdījusies bankas nosaukuma rakstībā, un tā nonāca citā tīmekļa vietnē, kurā uzreiz parādījās biedējošs brīdinājuma paziņojums, kas apgalvoja, ka viņas dators ir inficēts, un lika nekavējoties zvanīt tehniskajam atbalstam. Iznirstošais brīdinājums bija noformēts ļoti profesionāli. Tajā bija norādīts, ar kādu ļaunprātīgu programmatūru ir inficēts viņas dators, bija attēlots oficiāls uzņēmuma logotips un norādīts tehniskā atbalsta numurs, uz kuru zvanīt.

Debora nekavējoties piezvanīja uz numuru, uz kuru atbildēja šķietami profesionāls atbalsta dienesta darbinieks. Viņš paskaidroja, ka Deboras dators patiešām ir inficēts un ka viņa komandai ir nepieciešama piekļuve viņas datoram, lai problēmu atrisinātu. Deborai bija jāapmeklē konkrēta vietne, jālejupielādē drošības programmatūra un pēc tam tā jāinstalē. Viņa izpildīja lūgumu, un atbalsta dienesta darbinieks viņu informēja, ka ir gūta piekļuve, pēc kā viņi sāka pārmeklēt viņas datoru.

Drīz vien tika apstiprinātas viņas ļaunākās bažas — ne tikai viņas dators ir inficēts, bet izrādījās, ka uzlauzts arī viņas bankas konts. Par laimi, tehniskā atbalsta uzņēmumam bija tiešs kontakts ar viņas banku, un uzņēmums ātri nosūtīja viņu pie aģenta, kas strādā ar krāpšanām. Aģents apstiprināja, ka viņas konts patiešām ir apdraudēts un tiek izmantots krāpnieciski iegūtu līdzekļu pārskaitīšanai. Darbinieks lika viņai nekavējoties pārskaitīt visu savu naudu uz citu bankas kontu, lai to pasargātu. Debora rīkojās saskaņā ar norādījumiem. Pēc tam Deborai paziņoja, ka arī viņas pensijas konts ir apdraudēts. Par laimi, uzņēmums sadarbojās arī ar valsts nodokļu aģentūru. Nu viņa tika savienota ar valdības aģentu, kurš paskaidroja, ka, lai pasargātu viņas pensijas kontu, viņai ir jāizņem no konta savi mūža uzkrājumi un jāpārliek uz citu kontu, pirms noziedznieki piekļūst viņas līdzekļiem. Viņa izdarīja visu prasīto. Tas bija garš un ļoti emocionāls vakars, taču Debora bija priecīga, ka ne tikai atrisinājusi problēmu ar datoru, bet arī pasargājusi savu naudu, pārskaitot to uz jauniem, drošiem kontiem. Nogurusi viņa devās pie miera.

Nākamajā rītā viņa pierakstījās jaunajā bankas kontā, lai piekļūtu saviem nesen pārvietotajiem uzkrājumu un pensiju kontiem, taču naudas tur vairs nebija. Panikas pārņemta, viņa piezvanīja uz tehniskā atbalsta numuru, uz kuru bija zvanījusi vakar. Atbildes nebija. Drīz vien viņa saprata, ka visi viņas dzīves uzkrājumi ir zuduši. Viņa pati tos vēl vakar bija atdevusi. Labprātīgi.

Kā izvairīties no šādas situācijas

Kibernoziedznieki ir sapratuši, ka visvieglākais veids, kā inficēt jūsu datoru vai nozagt jums naudu, ir vienkārši lūdzot jūs sadarboties. Bieži izplatīts veids, kā viņi to panāk, ir iebiedēšanas programmatūras izmantošana, liekot jums domāt, ka jūsu dators ir inficēts, lai gan patiesībā tā nav. Pēc tam viņi mudina jūs veikt pārsteidzīgas darbības, lai varētu jūs izmantot savā labā. Šis stāsts ir balstīts uz patiesiem notikumiem, ko cilvēki ir piedzīvojuši. Deboras dators nebija inficēts, taču viņa nejauši apmeklēja nepareizo vietni. Tehniskā atbalsta uzņēmums nebija īsts, bet gan kibernoziedznieku komandas izgudrojums otrā pasaules galā. Pat banku krāpniecības darbinieki un valdības aģenti bija tikai vienas kibernoziedznieku komandas dažādi locekļi. Tiklīdz kibernoziedznieki jūs uzrunās pa tālruni, viņi mēģinās darīt visu iespējamo, lai nopelnītu naudu. Kā jūs varat sevi pasargāt?

- Vislabākā aizsardzība ir saglabāt aizdomīgumu. Jebkurā situācijā, kad kāds cenšas jūs pierunāt ātrāk veikt kādu darbību, mērķis var būt uzbrukums. Jo lielāka steidzamības izjūta un jo lielāks spiediens uz jums tiek izdarīts, jo lielāka iespēja, ka tiek mēģināts īstenot krāpšanu.
- Neviens likumīgs uzņēmums nekad nelūgs jums dalīties ar savu paroli. Neviena banka jums nelūgs pārvietot naudu uz citu kontu.
- Nekad neizmantojiet brīdinājumā vai uznirstošajā logā sniegto kontaktinformāciju. Ja vēlaties pārbaudīt brīdinājuma likumību, vienmēr izmantojiet jau zināmas saziņas metodes, piemēram, tālruņa numurus bankas vai kredītkartes izrakstos vai izmantojiet pārlūkprogrammā saglabātās saites.

Ja uzskatāt, ka jūs vai kāds jūsu tuvinieks ir kļuvis par finanšu krāpnieka upuri, nekavējoties ziņojiet par to tiesībaizsardzības iestādēm un savai bankai. Jo ātrāk ziņosiet par uzbrukumu, jo lielāka ir iespēja atgūt naudu.

Resursi

Sociālā inženierija: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Pārlūkprogrammas: https://www.sans.org/newsletters/ouch/browsers/
Emocionālie ierosinātāji jeb trigeri: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Pikšķerēšanas uzbrukumi kļūst piņķerīgāki: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Tulkojums: CERT.LV