OUCH! 2024. gada

SANS SECURITY AWARENESS

Ikmēneša informatīvais biļetens drošības izpratnes veicināšanai

Atklājot ēnu pasauli: kā kibernoziedznieki nozog jūsu paroles

Digitālais murgs: Lizas nevēlamā publiskošana

Liza, grafiskā dizainere ar talantu radoši izpausties, lielāko daļu savas dzīves pavadīja tiešsaistē. Viņa pārvaldīja savus banku pakalpojumus, iepirkšanos un sociālo mijiedarbību, izmantojot dažādas lietotnes un vietnes. Kādu dienu viņa pamanīja, ka no viņas bankas konta tiek veikti daži dīvaini maksājumi – preces, ko viņa nekad nav pirkusi veikalos, kurus nekad nav apmeklējusi. Pēc tam viņas sociālo tīklu kontos sāka publicēt surogātpasta ziņojumus, kas reklamēja dīvainus produktus un pakalpojumus, un draugi ziņoja, ka saņem no viņas neparastus e-pastus.

Lizu pārņēma panika, jo viņa saprata, ka ir zaudējusi kontroli pār savu digitālo identitāti. Tika nopludinātas viņas privātās fotogrāfijas un atklātas privātas sarunas. Klienti sāka apšaubīt viņas uzticamību, un viņas reputācija bruka. Pēc konsultācijām ar kiberdrošības ekspertiem Liza atklāja, ka viņas paroles ir uzlauztas. Kibernoziedznieki bija ieguvuši piekļuvi viņas sensitīvākajiem kontiem, pa gabaliņam izjaucot viņas digitālo pasauli. Jautājums palika neatbildēts: Kā tas notika?

Kibernoziedznieku izmanīgā taktika: piecas izplatītākās metodes

Kibernoziedznieki izmanto dažādas metodes, lai iegūtu paroles. Lūk, pieci izplatītākie veidi, kā viņi varētu iegūt jūsu paroli, tāpat kā to izdarīja Lizas gadījumā:

1. **Sociālās inženierijas uzbrukumi**

   Sociālā inženierija ir uzbrucēju maskēšanās par kādu, ko jūs pazīstat vai kam uzticaties, un viņi ar viltu piespiež jūs darīt kaut ko tādu, ko nevajadzētu. Viņi sūta e-pasta vēstules vai ziņojumus, kas izskatās patiesi, bieži radot spēcīgu steidzamības, baiļu vai ziņkārības sajūtu.

   *Kā tas notika:*Liza saņēma e-pasta vēstuli, kas izskatījās kā no viņas bankas, ar oficiāliem logotipiem un zīmoliem. E-pastā tika apgalvots, ka viņas kontā ir aizdomīgas darbības, un viņa tika aicināta noklikšķināt uz saites, lai pārbaudītu savu identitāti. Saite aizveda uz viltotu tīmekļvietni, kurā tika saglabāti viņas pieteikšanās dati, kad viņa tos ievadīja.

2. **Ļaunatūra**

   Ļaunatūra ir ļaunprātīga programmatūra, kas izstrādāta, lai inficētu datorus. Pēc inficēšanas kibernoziedznieki var darīt, ko vien vēlas. Taustiņspiedienu reģistrētāji (keyloggers) (dažkārt saukti par *informācijas zagļiem*) ir ļaunatūras veids, kas ieraksta katru ierīcē veikto taustiņa nospiedumu, tostarp jūsu lietotājvārdus, paroles un citus konfidenciālus datus.

   Kā tas notika: Liza lejupielādēja, kā viņa domāja, īstu fontu paketi savam dizaina darbam. Tajā bija paslēpts taustiņu reģistrētājs, kas instalējās viņas datorā. Laika gaitā tas ierakstīja viņas dažādu kontu pieteikšanās datus un nosūtīja tos uzbrucējam.

3. **Pilnās pārlases uzbrukumi**

   Pilnās pārlases (brute-force) uzbrukumos kibernoziedznieki izmanto automatizētus rīkus, lai izmēģinātu daudzas paroļu kombinācijas, līdz uzmin pareizo. Vājas paroles ir īpaši neaizsargātas pret šo metodi.

   Kā tas notika: Liza daudziem saviem kontiem izmantoja vienkāršas paroles, piemēram, "lisa2020". Uzbrucēji izmantoja programmatūru, kas sistemātiski izmēģināja bieži sastopamās paroles un viegli uzlauza viņas kontus.

4. **Datu noplūdes**

   Ja tiek uzlauzta tīmekļvietne vai pakalpojums, tas var ietekmēt ikviena lietotāja kontus, kas var būt saglabāti serverī. Ja kāds izmanto vienu un to pašu paroli vairākiem kontiem, tad, ja šī parole tiek uzlauzta vienam kontam, to var izmantot, lai piekļūtu arī citiem cietušā kontiem.

   *Kā tas notika:*Populārā sociālā tīklu platformā, ko izmantoja Liza, notika datu noplūde. Tā kā viņa izmantoja vienu un to pašu paroli arī citur, uzbrucēji piekļuva citiem viņas kontiem, izmantojot noplūdušos piekļuves datus.

5. **Iegūtie piekļuves dati**

   Kibernoziedznieki var vienkārši nopirkt jūsu paroles internetā, bieži vien tumšajā tīmeklī. Daži kibernoziedznieki specializējas upuru paroļu zagšanā, izmantojot jebkuru no līdz šim aplūkotajām metodēm. Pēc tam nozagtās paroles viņi uzglabā un pārdod citiem kibernoziedzniekiem.

   Kā tas notika: Kibernoziedznieks nolēma, ka nedēļas nogalē vēlas nopelnīt pēc iespējas vairāk naudas, tāpēc devās uz tumšo tīmekli un iegādājās vairāk nekā 100 000 kompromitētu kontu ar visām to parolēm. Viens no Lizas kontiem bija šajā sarakstā.

Trīs galvenie soļi, ko varat veikt

Par laimi, veicot trīs vienkāršus soļus, jūs varat ievērojami uzlabot savu kontu un tiešsaistes, digitālās dzīves aizsardzību.

1. Katram kontam izmantojiet garu, unikālu paroli. Mēs iesakām izmantot frāzveida paroles, kas ir garas paroles, kuras sastāv no vairākiem vārdiem.
2. Izmantojiet paroļu pārvaldnieku, lai droši uzglabātu un pārvaldītu visas šīs paroles.
3. Iespēju robežās iespējojiet daudzfaktoru autentifikāciju (MFA) svarīgākajiem tiešsaistes kontiem.

Viesredaktore

Lekšmi Naira (Lekshmi Nair) ir vadošā kiberdrošības speciāliste ar 22 gadu pieredzi informācijas drošības konsultāciju un kiberdrošības stratēģijas jomā. Pašlaik viņa ir vecākā lietojumprogrammu drošības konsultāciju direktore uzņēmumā BlackDuck Software. Viņa ir WiCyS India dibinātāja un prezidente.

Resursi

Iedomātās balsis: Aizsardzība pret balss klonēšanas uzbrukumiem: https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Teksta ziņojumapmaiņas uzbrukumi: Smikšķerēšanas sāga: https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/
Trīs populārākie veidi, kā kiberuzbrucēji vēršas pret jums: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Frāzveida paroļu spēks: https://www.sans.org/newsletters/ouch/power-passphrase/
Paroļu pārvaldnieku spēks: https://www.sans.org/newsletters/ouch/power-password-managers/

Tulkojums: CERT.LV