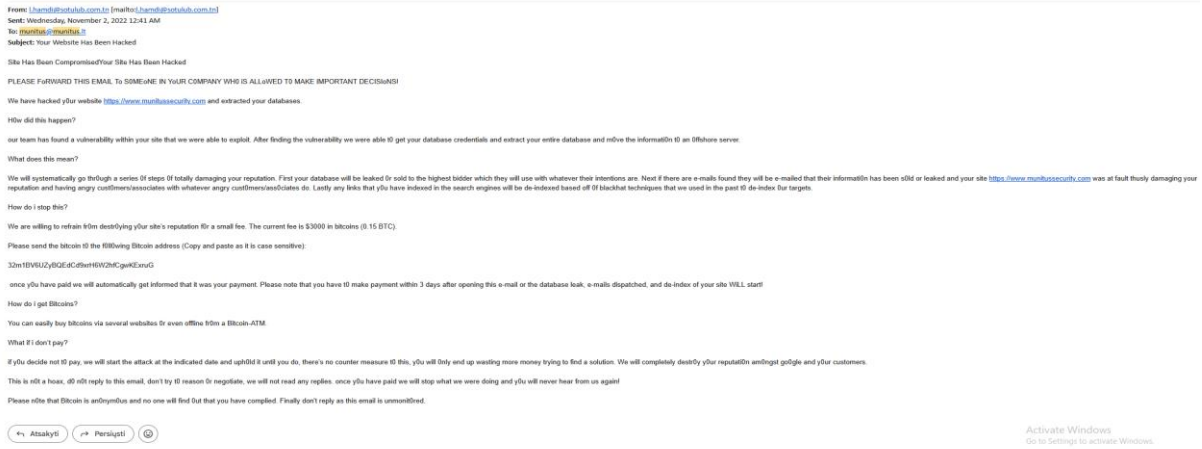
LAB 6. Socialinės inžinerijos atakos ir jų tipai

1. Kokią(-ias) socialinės inžinerijos ataką(-as) jūs patyrėte?
Atakuotojas/atakuotojų grupė vykdė masinę wordpress svetainių socialinės inžinerijos atakas ir į vieną iš jų pateko svetainė, kurią administravau.
Laiško nuotrauka:



From: l.hamdi@sotulub.com.tn [mailto:l.hamdi@sotulub.com.tn]
Sent: Wednesday, November 2, 2022 12:41 AM
To: munitus@munitus.lt
Subject: Your Website Has Been Hacked

Site Has Been CompromisedYour Site Has Been Hacked

PLEASE FoRWARD THIS EMAIL To S0MEoNE IN YoUR COMPANY WHo IS ALLoWED T0 MAKE IMPORTANT DECISIoNS!

We have hacked y0ur website https://www.munitussecurity.com and extracted your databases.

H0w did this happen?

our team has found a vulnerability within your site that we were able to exploit. After finding the vulnerability we were able t0 get your database credentials and extract your entire database and m0ve the informati0n t0 an 0ffshore server.

What does this mean?

We will systematically go thr0ugh a series 0f steps 0f totally damaging your reputation. First your database will be leaked 0r sold to the highest bidder which they will use with whatever their intentions are. Next if there are e-mails found they will be e-mailed that their informati0n has been s0ld or leaked and your site https://www.munitussecurity.com was at fault thusly damaging your reputation and having angry cust0mers/associates with whatever angry cust0mers/ass0ciates do. Lastly any links that y0u have indexed in the search engines will be de-indexed based off 0f blackhat techniques that we used in the past t0 de-index 0ur targets.

How do I stop this?

We are willing to refrain fr0m destr0ying y0ur site's reputation f0r a small fee. The current fee is $3000 in bitcoins (0.15 BTC).

Please send the bitcoin t0 the fll0lwing Bitcoin address (Copy and paste as it is case sensitive):

32m1BV6UZyBQEdCd9wrH6W2hfCgwkExruG

once y0u have paid we will automatically get informed that it was your payment. Please noto that you have t0 make payment within 3 days after opening this e-mail or the database leak, e-mails dispatched, and de-index of your site WILL start!

How do I get Bitcoins?

You can easily buy bitcoins via several websites 0r even offline fr0m a Bitcoin-ATM.

What if I don't pay?

If y0u decide not t0 pay, we will start the attack at the indicated date and uph0ld it until you do, there's no counter measure t0 this, y0u will 0nly end up wasting more money trying to find a solution. We will completely destr0y y0ur reputati0n am0ngst g0ogle and y0ur customers.

This is n0t a hoax, d0 n0t reply to this email, don't try t0 reason 0r negotiate, we will not read any replies. once y0u have paid we will stop what we were doing and y0u will never hear from us again!

Please n0te that Bitcoin is an0nym0us and no one will find 0ut that you have complied. Finally don't reply as this email is unmonit0red.

Atsakyti | Persiųsti

jei nuotrauka neryški, palieku nuordodą:
https://firebasestorage.googleapis.com/v0/b/cms-test-d56c9.appspot.com/o/munitus%20laiskas.png?alt=media&token=64f50f55-712a-43d0-8d48-8dcbf53f6587

2. Aprašyti atakos(-ų) scenarijų(-us). Kodėl jūs manote, kad tai buvo socialinės inžinerijos ataka? Identifikuoti socialinės inžinerijos atakos tipą.
Tai buvo panašiausia į phishing ataką. Atakuotojai bandė apgauti, jog nulaužė įmonės svetainę ir planuoja nutekinti duomenų bazę arba parduoti ją, jei nesumokėsime jiem už to nedarymą.
3. Ar patyrėte kokių nors nuostolių (moralinių, finansinių, psichologinių, sveikatos sutrikdymų ir pan.)?
Buvo patirti nebent minimalūs psichologiniai nuostoliai(iki kol nepatvirtinau, kad tai yra tušti grasinimai, buvo dalinai tuo patikėjusių - "išsigandusių" žmonių).
4. Kokių veiksmų ėmėtės, kad apsisaugotumėte?
Jokių(apart įskiepių atnaujinimų, kas būtų buvę padaryta ir be šios netikros atakos).