Conturi sparte: ce să faci când ești hacked

29 martie 2024 /
online

Alex Ștefănescu
folosesc pronume feminine
alex.stefanescu@protonmail.com

Cine suntem și ce facem

- **Advocacy**
- **Educație**
- **Conștientizare**

Susține și promovează o lume digitală liberă și deschisă, prin respectarea drepturilor fundamentale ale omului.

ApTI pentru libertatea Internetului

ApTI pentru dreptul la viață privată

ApTI pentru cultură liberă

Ce se poate întâmpla?

- Conturi sunt sparte și preluate
- Informație este copiată, ștearsă sau criptată
- Dispozitive sunt infectate

…și alte variațiuni pe aceleași teme.

ApTI

Pas cu pas, o dregem și pe asta

Pasul 1: oprim dauna din a se înteți
Pasul 2: facem inventarul răului făcut
Pasul 3: care sunt cauzele plauzibile?
Pasul 4: altă dată, să nu se mai întâmple (sau cel puțin, nu *așa*)!

😳 Contul ne-a fost spart

Cum oprim dauna?

- Ne putem loga? Schimbăm parola, schimbăm (sau activăm) 2FA
- Nu ne putem loga? Urmăm instrucțiunile de recuperare ale contului.

ApTI

😳 Contul ne-a fost spart

Cum oprim dauna?

- Ne anunțăm comunitatea (informațiile postate de cont nu mai sunt sub controlul nostru).
- Securizăm celelalte conturi ale asociației (parolă schimbată, 2FA).

ApTI

😳 Contul ne-a fost spart

Inventarul răului făcut

- La ce are acces atacatorul (fișiere, alte conturi)?
- Ce acțiuni face atacatorul?
- Cum putem opri informație nouă să mai ajungă la contul compromis?

ApTI

😳 Contul ne-a fost spart

Inventarul răului făcut

- Cum era protejat contul?
- Cine avea acces la el? (sesiuni active, dispozitive asociate - inventar al tuturor persoanelor cu acces)

😳 Contul ne-a fost spart

Care sunt cauzele plauzibile?

- Dispozitiv pierdut? Sau infectat?
- Parolă spartă / ghicită, sau phishing?
- Care sunt ultimele acțiuni făcute de pe contul respectiv?
- Cine a avut acces la cont de-a lungul timpului?

😳 Contul ne-a fost spart

Altă dată să nu se mai întâmple (așa)

- Cine trebuie să aibă acces la cont? Facem protocol de revocare.
- De pe ce dispozitive lucrăm? Parolăm dispozitivele. Dacă se poate, nu de pe dispozitive folosite la comun.

ApTI

🥰 Prevenție

- Listă cu conturi de social media
  - Cine are acces? De pe ce dispozitiv?
  - Cum se distribuie parolele? Dar 2FA?
- Curățenie prin sesiunile active / dispozitivele asociate din social media.
- Ce conturi nu mai sunt folosite? Pot fi închise?

😳 Informație copiată, ștearsă sau criptată

Cum oprim dauna?

- De unde a venit informația?
  - Calculator / laptop / smartphone / tabletă
    - **Deconectăm de la Internet**
    - **Închidem complet**

ApTI

😳 Informație copiată, ștearsă sau criptată

Cum oprim dauna?

- De unde a venit informația?
  - Website / aplicație de stocare
    - Pași similari cu contul furat
    - Mutăm informația, ștergem din online

😳 Informație copiată, ștearsă sau criptată

Cum oprim dauna?

- Dacă este vorba de informație legată de beneficiari, urmăm pașii Regulamentului GDPR - anunțăm *nu mai târziu de 72 de ore de la detectare*

😳 Informație copiată, ștearsă sau criptată

Inventarul răului făcut

- Documente pe Google drive? Putem vedea istoricul editărilor.
- Documente Office / Libre Office etc.? Dacă avem acces la ele, ne uităm la metadate.

😳 Informație copiată, ștearsă sau criptată

Inventarul răului făcut

- Avem copii ale informației? Unele site-uri de găzduire fac back-up-uri, unele suite de editare de documente salvează copii și în cloud.

😳 Informație copiată, ștearsă sau criptată

Inventarul răului făcut

- Dacă e vorba de ransomware, căutăm pe Internet conținutul e-mail-ului de ransom / structura fișierelor. **E posibil să existe deja mecanism de decripatre**.

ApTI

😮‍💨 Nu recomandăm plata unei cereri se răscumpărare

Plata răspumpărării nu garantează că veți primi informația înapoi.

Nu ștergeți datele de pe dispozitiv.

Mai devreme sau mai târziu se va publica o modalitate de decriptare.

😳 Informație copiată, ștearsă sau criptată

Care sunt cauzele plauzibile?

- *Întrebări similare cu cele din cazul unui cont spart.*

😳 Informație copiată, ștearsă sau criptată

Altă dată să nu se mai întâmple (așa)

- Pași similari cu securizarea conturilor. Parole pentru toate dispozitivele. Utilizatori separați pe dispozitivele partajate. Software de control parental, dacă e cazul.

ApTI

😳 Informație copiată, ștearsă sau criptată

Altă dată să nu se mai întâmple (așa)

- Antivirus (mai ales dacă lucrați cu mult fișiere trimise de persoane necunoscute).
- Dangerzone (pentru PDF-uri)
- Nu instalăm programe crack-uite, nu deschidem fișiere necunoscute și neașteptate.

ApTI

😭 Uneori *trebuie* să deschidem fișiere necunoscute

- Urcăm în Google Drive și le vizualizăm acolo
- Folosim un laptop vechi, fără conexiune la Internet
- Tails OS (sistem de operare rulat de pe un stick USB - așa ne putem și conecta la internet).

ApTI

🥰 Prevenție

- Toate dispozitivele sunt cu sistemul de operare la zi și versiunile de aplicații, de browser, la zi.
- Back-up-uri (în cloud și / sau pe dispozitiv fizic)

🥰 Prevenție

- Antivirusul poate să ajute (și Windows Defender e gratis!) dar și mai mult ajută **precauția**.
- Dacă primim fișiere / e-mail-uri ciudate de la cineva pe care cunoaștem, putem confirma pe alt canal de comunicare.

ApTI

😳 Dispozitive sunt infectate

Cum oprim dauna?

Oprim dispozitivul, deconectăm de la Internet.

Ajută mult să verificăm dacă semnele infectării se întâmplă și când dispozitivul e deconectat.

ApTI

😳 Dispozitive sunt infectate

Inventarul răului făcut

- **MVT** (mobile verification toolkit)
  - Documentație
  - Metodologie
  - Are indicatori de **spyware** și **stalkerware**

ApTI

😳 Dispozitive sunt infectate

Inventarul răului făcut

- Dacă e vorba de un telefon mobil, putem presupune că și numărul de telefon asociat trebuie **scos din uz**.
- Numărul poate fi folosit pentru a infecta dispozitivul din nou.

ApTI

😳 Dispozitive sunt infectate

Care sunt cauzele plauzibile?

- Ce aplicații am instalat recent?
- Ce fișiere am deschis recent?
- Ce SMS-uri sau mesaje (mai ales de la persoane necunoscute - Requests - am primit recent)?

ApTI

😳 Dispozitive sunt infectate

Care sunt cauzele plauzibile?

- În cazul laptop-urilor / calculatoarelor
  - Am introdus stick-uri USB?
  - Folosim software crack-uit?
  - **Rulăm un antivirus**

ApTI

😳 Dispozitive sunt infectate

Altă dată să nu se mai întâmple (așa)

- În cazul spyware / stalkerware, pe smartphone: **ajută să dăm restart la dispozitiv o dată pe zi**
  - Totuși, asta va șterge semnele că s-a încercat infectarea dispozitivului

ApTI

😳 Dispozitive sunt infectate

🤔 De ce ajută să dăm restart la dispozitiv?

Dacă **nu le-am instalat noi** (crezând că sunt altceva) sau, dacă **nu ni le-a instalat cineva**, atunci poate că am fost ținta unei infectări. **Majoritatea infectărilor nu pot persista după un restart.**

ApTI

😳 Dispozitive sunt infectate

Altă dată să nu se mai întâmple (așa)

- De obicei, **nu există motive bune** să dăm click pe link-uri primite în SMS sau să deschidem fișiere primite fără să știm cine ni le-a trimis și de ce. Sigur, există excepții.

ApTI

🥰 Prevenție

- Toate dispozitivele sunt cu sistemul de operare la zi și versiunile de aplicații, de browser, la zi.
- **Lockdown mode activat**, pe orice dispozitiv Apple.
- **Graphene**, pentru Android (cel mai sigur sistem de operare de smartphone non-Apple)

ApTI

🥰 Prevenție

- Firewall activ pe laptop / calculator (fiecare sistem de operare are un firewall).
- Separarea dispozitivelor de muncă de cele personale.
- Separarea conturilor de stocat fișiere personale de cele de muncă.

Întrebări?

📬 alex.stefanescu@protonmail.com

👉 https://chaos.social/@catileptic

❤️ https://apti.ro/

ApTI

Mulțumim!

pentru libertatea Internetului pentru
dreptul la viață privată pentru cultură
liberă pentru libertatea Internetului
pentru cultură liberă pentru libertatea
Internetului pentru dreptul la viață
privată pentru cultură liberă pentru
libertatea Internetului pentru dreptul
la viață privată pentru cultură liberă
pentru libertatea Internetului pentru
dreptul la viață privată pentru cultură
liberă pentru libertatea Internetului
pentru dreptul la viață privată pentru
cultură liberă pentru libertatea
Internetului pentru dreptul la viață
privată pentru cultură liberă pentru
libertatea Internetului pentru dreptul
la viață privată pentru cultură liberă
pentru libertatea Internetului pentru
dreptul la viață privată pentru cultură
liberă pentru libertatea Internetului
pentru dreptul la viață privată pentr

alex.stefanescu@protonmail.com
https://chaos.social/@catileptic