Phishing a scam

Richard Gerboc, Tomáš Žalobín
Gymnázium Poštová 9, Košice

Projekt pod záštitou CSIRT UPJŠ

Phishing

„pokus o podvodné získanie citlivých informácií, ako sú heslá a podrobnosti o kreditných kartách, maskovaním sa za dôveryhodnú osobu alebo obchod pri elektronickej komunikácii“

zdroj: sk.wikipedia.org/wiki/Phishing

Dobry den vazeni klienti!

Leto roku 2006 bylo pro Banku nejzavaznejsim z hlediska poctu nelegalnich operaci. Cim dal vice maji podvodnici zajem o duvernou informaci nasich zakazniku. Velke mnozstvi lidi se na nas obraci s zadosti zamezit vzniku nebezpeci ztraty peneznich prostredku z uctu. S ohledem na soucasny stav vyhlasuje Banka nasledujici mesic za mesic boje s frodem. Do 1. listopadu musi vsechny nasi klienti aktivovat novy system bezpecnosti vlastnich uctu. Provedli jsme velkou praci pro zlepseni bezpecnosti. System byl zkontrolovan uznavanymi odborniky v oboru elektronickych plateb, a vsechny nezavisli experti potvrdili ucinnost systemu proti frodu. Z duvodu nebezpeci mozneho zneuziti techto udaju podvodniky nejsou tyto data zverejnena v otevrenych zdrojich.

Vy jste byl(a) zvolen(a) jako jeden z ucastniku finalniho stadia testovani systemu. V soucasne dobe Vam navrhujeme vyuzit odkaz a standardnim zpusobem prihlaseni do Internet bankingu aktivovat novy bezpecnostni system. V aktualnim stadiu provozu jsou mozne nektere nesrovnalosti. Pripoustime jejich existenci, a proto prosim nezasilejte dodatecne popisy vznikajicich potizi, prace na jejich odstraneni jiz probihaji. Musime Vas informovat o bezpodminecnem pouziti noveho systemu od listopadu, v opacnem pripade budou Vase ucty zablokovany do okamziku uplne identifikace Vasi osoby. proto doporucujeme v nejkratsi mozne dobe prejit na novy bezpecnostni standard.

S pozdravem, Oddeleni Banky pro ochranu pred frodem.

Falošná správa 1 - url adresa otvorí elektronické bankovníctvo ak ste klientom tejto banky a snaží sa previesť z vášho účtu 1,34€

Od: Tatra banka <a @ japanlokad.com>
Predmet: Nova funkcia
Dátum: Sob, 5.Jan 2019 04:38:10

Vážený pán / pani,

Radi by sme Vás informovali, že sme pridali novú funkciu na ochranu vášho účtu pred podvodným pokusom a neoprávneným používaním vašej bankovej karty.
Táto prísada je veľmi dôležitá pre vašu ochranu a pohodlie našich zákazníkov.
Aktivujte ho na svojej banke a odpočítajte veľmi jednoduchú sumu:
1,34 EUR
Ak chcete svoju kreditnú kartu overiť a aktivovať ju vo svojom účte.
Na platbu a aktiváciu :
https: / / moja.tatrabanka.sk/cgi-bin/blablablablablablablablab
Funkcia sa po zaplatení automaticky aktivuje.
Zuzana Povodová

Falošná správa 2 - url adresa otvára nib.vub.sk, ktorý je presmerovaný na ib.vub.sk

Od: VUB Banka <test @ wizgreeting.company>
Predmet: oznámenia
Dátum: Sob, 29.Dec 2018 11:09:47
Komu: <monika.perez @ gmail.com>

Vážený zákazník,

Teraz sme aktualizovali naše ďalšie bezpečnostné prvky v bezpečné a bezpečné zabezpečenie online bankovníctva. Ostatní, ktorí čakajú na aktualizáciu, by mali posilniť autentifikáciu prostredníctvom on-line bankovníctva. Ak chcete potvrdiť svoju totožnosť a zabrániť blokovaniu účtu, navštívte stránku:

https: // nib.vub.sk/portal/blablablb

Toto sú pokyny zaslané všetkým klientom VUB a musia byť dodržané.

Vďaka,
VÚB Banka

Falošná správa 3 - Slovenska Sporitelna - zrušený prevod

Od: SLSP <slsp1@cluster007.hosting.ovh.net>

Predmet: Slovenska Sporitelna

Dátum: Ned, 22.Mar 2020 08:01:22

Vazeny klient,

Vas posledny bankovy prevod bol zruseny z bezpecnostnych dovodov. Kliknite sem a postupujte podla pokynov na okamzite vratenie vasich penazí.

Dolezite: Ak nebudete postupova podla pokynov do 24 hodín, vase peniaze v nas zostanu v bezpecí, kym nevykonate potrebne kroky.

S pozdravom.

Falošná správa 4 - OTP BANKA - DÔLEŽITÉ SPRÁVY

Od: OTP BANKA SK <blblbla@servis369.com>

Predmet: DÔLEŽITÉ SPRÁVY

Dátum: Pia, 20.Sep 2019 13:37:23

Vážený zákazník, Z dôvodu našej nedávnej bezpečnostnej kontroly vašich služieb OTP BANKA požadujeme, aby ste si overili údaje o vašom účte zaregistrované u nás, aby ste sa uistili, že váš účet nebol porušený. Jednoducho kliknite na náš odkaz na zabezpečený server a prihláste sa a overte svoje údaje. ZOBRAZIŤ NA BEZPEČNÝ SERVER:https: //otpdirekt.otpbanka.sk/login /login_main_jelszoalapu.jsp Zabezpečenie účtu je jednou z našich najvyšších priorít. Ak neoveríte svoj účet do 48 hodín, povedie to k pozastaveniu prístupu k vášmu online účtu. Ospravedlňujeme sa za nepríjemnosti. S pozdravom, OTP BANK SK

Falošný oznam 7 - Váš balík čaká na potvrdenie platby[32]

Subject: Predmet: Váš balík čaká na potvrdenie platby
Sender: Slovenská pošta <support@blaorlandowelcomecenterbla.com> Dátum: Uto, 6.Okt 2020 05:31:06

Vážený zákazník,

Vaše balenie čaká na doručenie

Prepravný kód: 293845678

Posledná aktualizácia: prijaté na pošte (08:15AM | 06-10-2020).

Stav zásielky: čaká na platbu.

Platbu 4,99 EUR potvrďte nasledujúcim odkazom:

https://www.posta. blablabla **adresa na ktorú odkaz skutočne smeruje (bit.ly/3lcabzn) je prekrytá adresou akože textu na stránke pošty https://www.posta.sk/Track=2938456778**

Poznámka: Do odoslania vám neúčtujeme žiadne poplatky.

©Slovenská pošta

Najčastejšie druhy emailov

1. Emaily od štátnych inštitúcií
2. Pomoc!
3. Updatni/aktualizuj svoj účet
4. Stali ste sa víťazom!
5. Vydieranie
6. Bol s vami zdieľaný súbor
7. Pošta
8. Pozri na to!

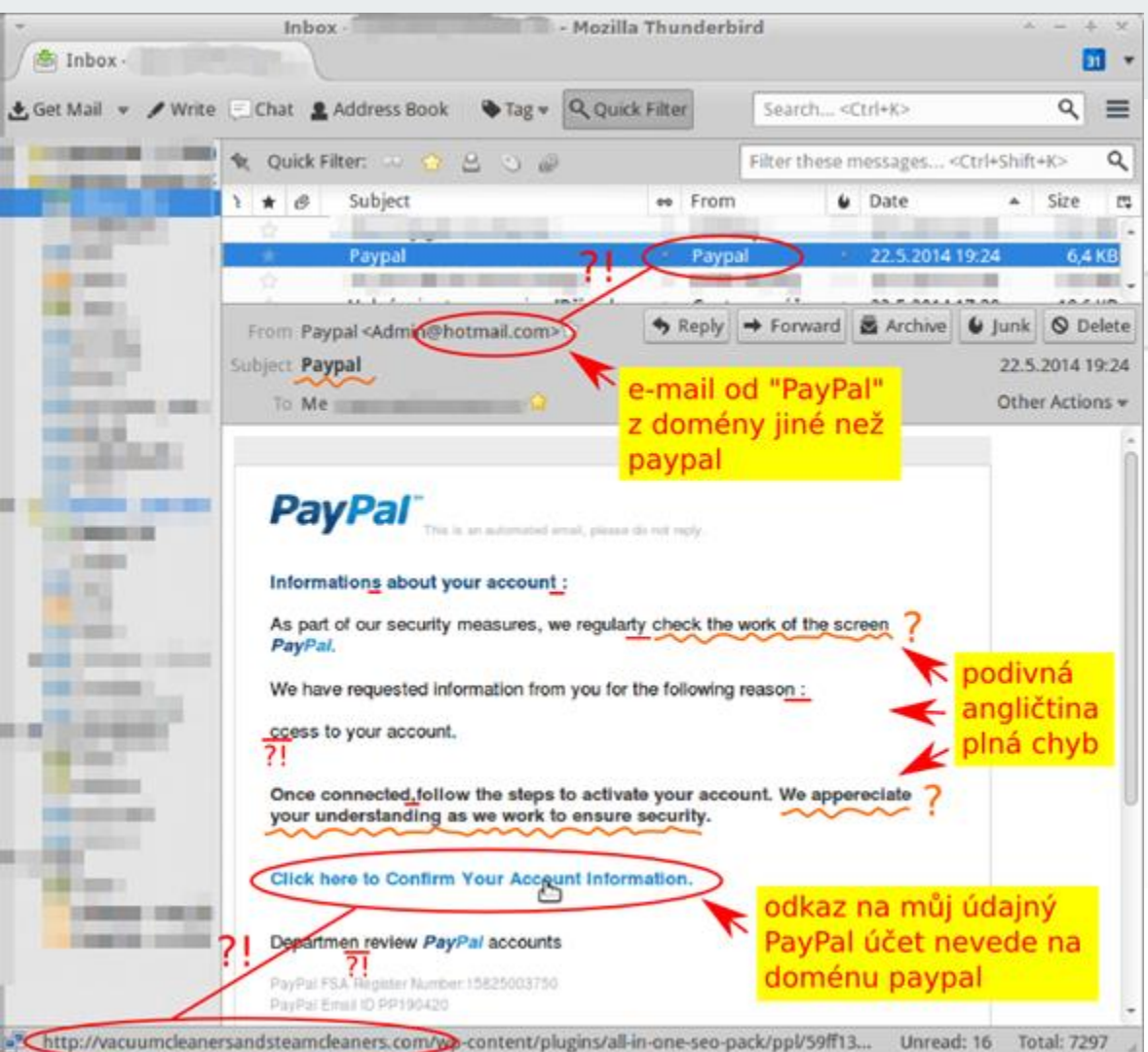
Zdroj: https://www.broadbandsearch.net/blog/popular-email-phishing-scams

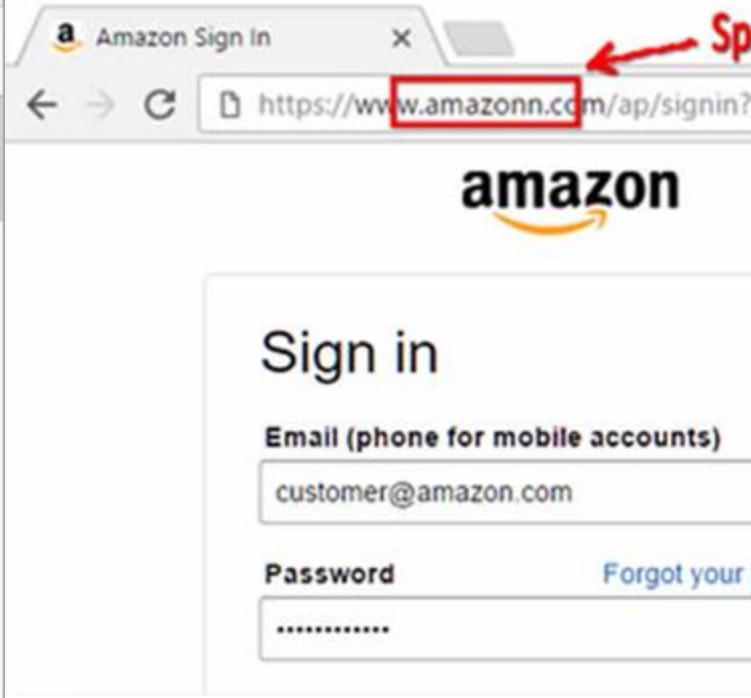
Techniky phishingu

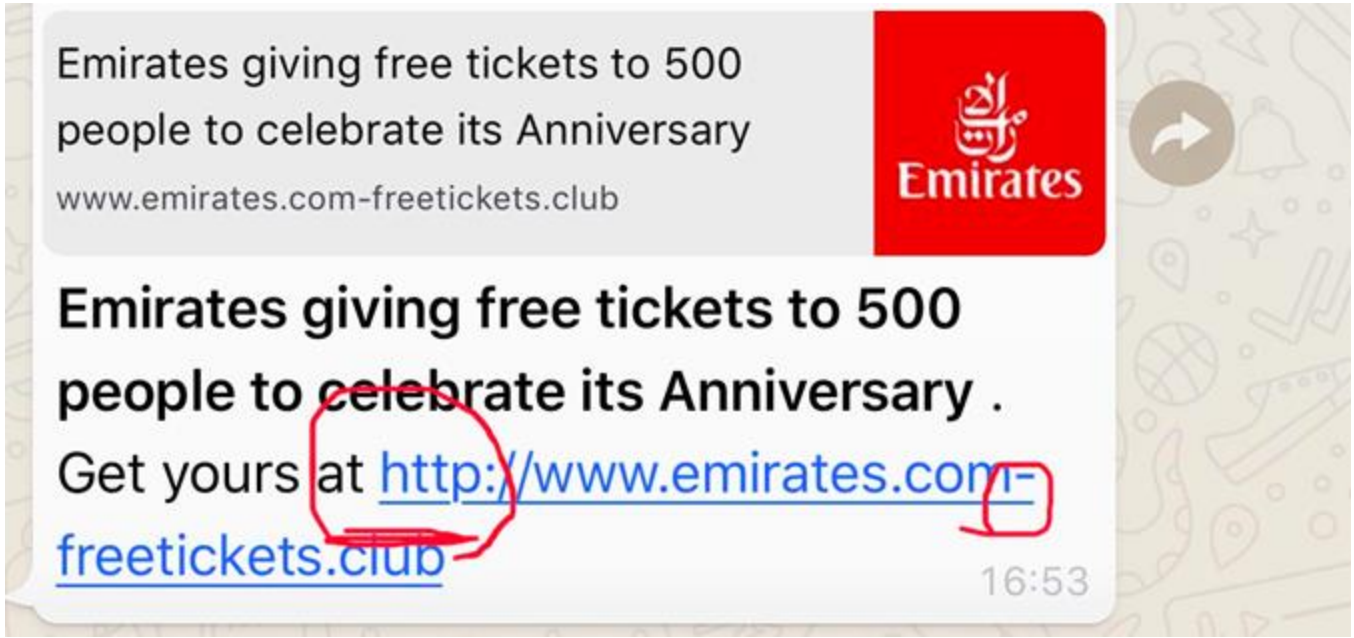
1. Hacking zdieľaného serveru
2. Využitie poddomén

   http://www.konkretnibanka.novasluzba.cz/

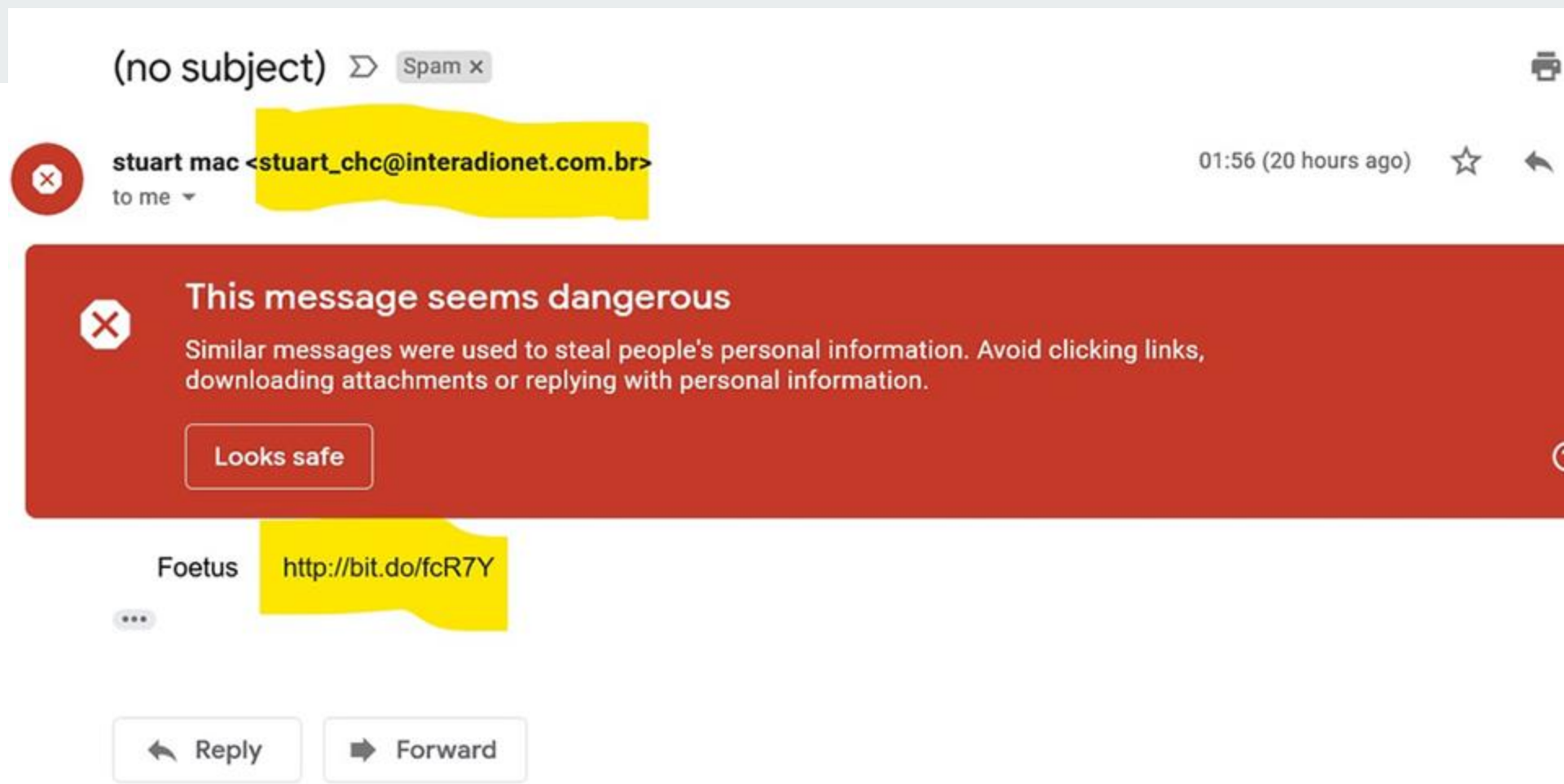
3. Preklepy a skreslenie odkazov
4. Skracovanie adries


Inbox - Mozilla Thunderbird
Get Mail
Write
Chat
Address Book
Tag
Quick Filter
Search... <Ctrl+K>
Filter these messages... <Ctrl+Shift+K>
Subject
From
Date
Size
Paypal
Paypal
22.5.2014 19:24
6,4 KB
From Paypal <Admin@hotmail.com>
Reply
Forward
Archive
Junk
Delete
Subject Paypal
22.5.2014 19:24
To Me
Other Actions
e-mail od "PayPal" z domény jiné než paypal
PayPal
Informations about your account :
As part of our security measures, we regularty check the work of the screen
PayPal.
We have requested information from you for the following reason :
ccess to your account.
Once connected,follow the steps to activate your account. We appereciate your understanding as we work to ensure security.
podivná angličtina plná chyb
Click here to Confirm Your Account Information.
odkaz na můj údajný PayPal účet nevede na doménu paypal
Departmen review PayPal accounts
http://vacuumcleanersandsteamcleaners.com/wp-content/plugins/all-in-one-seo-pack/ppl/59ff13...
Unread: 16
Total: 7297


Amazon Sign In
https://www.amazonn.com/ap/signin?
amazon
Sign in
Email (phone for mobile accounts)
customer@amazon.com
Password
Forgot your



https://smex.org/a-few-tips-to-detect-phishing-links/



https://mackytechnologies.com/phishing-scam-through-shortened-urls/

Techniky phishingu

5. Používanie obrázkov namiesto textu
6. Telefonický phishing
7. Vyskakovacie okná

when Indian tech support calls:

Red flags

- Všeobecné oslovenie
- Pochybná emailová adresa odosielateľa
- Urgentnosť
- Zmenené URL adresy
- Príloha
- Zlá gramatika
- Too good to be true

Ako sa chrániť

- Kontrolujte linky
- Pozrite si, či email spĺňa štandardy danej spoločnosti
- Kontrolujte https a certifikáty
- Ak si nie ste istí, napíšte na podporu
- Používajte dobré zabezpečenie
- Pripájajte sa na bezpečné siete
- Skontrolujte stránku (hlavne e-shopy)

Scam a ďalšie hrozby

- Sociálne inžinierstvo
- Malware
- Hacking

NOVINKY

Pozor! Falošná podpora spoločnosti Microsoft opäť úraduje

Známy malvér pre Android je ešte nebezpečnejší. Po útoku vymaže celý telefón

Sociálne inžinierstvo

“Hackovanie ľudí”

a) Podvodná komunikácia
b) Fyzické prelomenie
c) Podvodné telefonáty

Autor: pch.vector

Post.sk
From: Post.sk <support@dsasp.sohag-univ.edu.eg>
To: <kermit@gmail.com>
Date: Fri 8/13/2021 3:56 AM

Slovenská POŠTA

Zásielka čaká na doručenie

Slovenská pošta vyvinula iniciatívu a poslala vám tento e-mail s cieľom informovať vás, že vaša zásielka stále čaká na vaše pokyny.

Ref. Č.: SK66902371WS

Prepravné náklady: 02,80 €

Potvrďte platbu nákladov na doručenie kliknutím na nasledujúci odkaz:

Potvrďte tu

Malware

Malware = škodlivý kód

Ransomware, Trojský kôň, Spyware…

Čo môže spôsobiť:

- ťaženie kryptomien
- získať prístup k účtom
- zasielanie údajov
- stiahne ďalší škodlivý kód
- šifrovanie a následné žiadanie výkupného…

Hacking

Hackers leak full EA data after failed extortion attempt

- Hackers leak 751GB of compressed EA data containing FIFA 21 source code.
- Data dump comes from a hack that took place in June 2021.
- EA says no player data was included in the stolen data, confirmed by the data leaked this week.

Gaming service Valve falls victim to massive data breach

A gaming company recently experienced a massive data breach, as hackers infiltrated its community forums and a database containing customer credit card information.

Gaming service Valve falls victim to massive data breach

Použité články

Hackers leak full EA data after failed extortion attempt - The Record by Recorded Future

Gaming service Valve falls victim to massive data breach (secure128.com)

https://zive.aktuality.sk/clanok/16rgfs6/znamy-malver-pre-android-je-este-nebezpecnejsi-po-utoku-vymaze-cely-telefon/

https://www.mojandroid.sk/pozor-falosna-podpora-spolocnosti-microsoft-vas-moze-pripravit-o-peniaze/

Ďakujeme Vám za pozornosť!