Phishing, zsarolólevél, spambot a szolgáltatók életében

Gervai Péter, Tarr Kft.

2018-11-14

Az adathalászat céljai

Valószínűleg már elhangzottak:

- A „polgári” halászat fő célja a pénzszerzés
  - Közvetlenül pénzszámláról pénz megszerzése
  - Közvetett módon értéket képviselő elektronikus elérés elvétele (például fizetett szolgáltatásokat tartalmazó játék account)
  - Közvetett módon értékesíthető adatok szerzése (zsarolás, üzleti titkot tartalmazó email, spam email account, installált spambot)
  - Spammelésen keresztüli bevétel

Az adathalászat céljai

Valószínűleg már elhangzottak:

- A „polgári” halászat másodlagos célja a károkozás
  - „Ellenfél” adataihoz hozzáférés (kölyök-bosszú)
  - Adatok megsemmisítése
  - „Defacing”: nyilvános tartalmak módosítása
- A „kormányzati” halászat fő célja a hatalomszerzés
  - Hozzáférés zárt rendszerekhez
  - Illegális (vagy ellenőrizetlen) adatszerzés
  - Az „ellenség” létfontosságú informatikai rendszerei feletti hatalom (irányítás, megzavarás, megsemmisítés), cyber-hadviselés

Это война. - 这是战争。 - This is War.

- Polgári szempontból általában a szolgáltató **ügyfelei** a célpontok
  - Nem a szolgáltató *felelőssége* az ügyfeleket megvédeni, de tudjuk, hogy a szolgáltató feladata az ügyfeleket segíteni mindenben, az elromlott porszívótól a lelkisegélyig. ☺
- Kormányzati szempontból a célpont a **szolgáltató** és annak **munkatársai**.
  - Egy cég akkor nem érdekes, ha világpolitikailag teljesen ismeretlen országban pár száz ügyfélnek szolgáltat…
  - …vagyis mi már egy háború közepén élünk.

Az adathalászat eszközei

Jelszólopás: **a cél az azonosító+jelszó megszerzése**

- Azonosítók megszerzése: legyűjtés weblapokról, lopott címlistákból, weblapos regisztrációkból
- Jelszavak az azonosítókhoz
  - *Jelszógyűjtő weblap:* olyan weblap aminek a regisztrációit üzemeltetői illegálisan felhasználják
  - *Brute force:* a gyenge jelszavak próbálgatásos felfedezése
  - *Malware (vírus, trójai, ...):* a **titkosítatlan** jelszó megszerzése a használt számítógépről
  - *Phishing (adathalászat):* a jelszó megjegyzése hamisított belépéssel (hamis weblap)

Adathalászat – az azonosító

Jelszólopás: a cél az azonosító (...) megszerzése

- Azonosítók megszerzése: legyűjtés weblapokról, lopott címlistákból, weblapos regisztrációkból
  - A szolgáltató (vagy az ügyfél) nem tud ellene védekezni, nem érdemes erőlködni.
  - „Spamtrap” címekkel a szolgáltató a **spambotok** későbbi felismerését segítheti, de ehhez speciális infrastruktúra szükséges (felismerés, védekezés)
  - Így keletkeznek a „spamlisták”

Adathalászat – a jelszó (esetleg PIN)

Jelszavak az azonosítókhoz

- *Jelszógyűjtő weblap:* olyan weblap aminek a regisztrációit üzemeltetői illegálisan felhasználják
  - Az ügyfél tud védekezni: nem használja ugyanazt a jelszót több helyen!
  - Jelszótároló alkalmazások (PasswordSafe, KeePass[2,X,...]; BitWarden, LastPass, 1password, ...)

Adathalászat – a gyenge jelszó

Jelszavak az azonosítókhoz

- *Brute force:* a gyenge jelszavak próbálgatásos felfedezése
  - Ügyfél: biztonságos jelszó (10+ karakter, nem szótári és nem ügyfélből kitalálható)
    - Szolgáltató: jó jelszó *kierőszakolása*
  - Szolgáltató: a próbálgatások lehetőségének radikális korlátozása. Rate limit, túl sok próbálkozás letiltása.
    - Probléma: az ügyfelek N+1 hibás jelszóval letiltják magukat, jó, ha van egy „ügyfélkapu”, ahol vissza tudja magát engedélyezni
    - Ismert spambot letiltás: rendszerigény

Adathalászat – jelszó „betörésből”

Jelszavak az azonosítókhoz

- *Malware (vírus, trójai, ...):* a **titkosítatlan** jelszó megszerzése a használt számítógépről
  - Az ügyfél ne installáljon *malware*-t. :-) Használjon folyamatos víruskeresőt, ne töltsön le bármit, ...
  - A szolgáltató elvileg figyelheti a *malware* jeleket a hálózatán, de mindig le lesz maradva a legújabb példányokkal, és az ügyfelek nem „hálálják meg”.
  - Az ügyfél ne tároljon **titkosítatlan** jelszavakat: ez is egy vágyálom, nincs befolyásunk a használt programok minőségére.
  - A szolgáltató nagyrészt itt is tehetetlen, oktathat...

Adathalászat – klasszikus átverés

Jelszavak az azonosítókhoz

- *Phishing (adathalászat):* a jelszó megjegyzése hamisított belépéssel (hamis weblap)
  - Social engineering – pszichológiai manipuláció
  - Adatok elkérése hamis indokokkal (pénzéhség: nyeremény; jobb élet: ingyen vízum, ...)
  - Igazinak kinéző hamis beléptető weblapok
  - Sajnos itt is az ügyfélnek kellene odafigyelnie, a szolgáltató nem sokat tud ellene tenni.
  - Céges környezetben lehet forgalmat szűrni, de ISP esetében ez nem megvalósítható.

Nincs remény? (De van.)

A szolgáltató védekezési pontjai:

- Megakadályozni, hogy a legjobban fenyegetett forma, az **e-mail bejuttassa** az adathalász fenyegetését:
  - Spam-védelem, malware védelem (open source, saját fejlesztés vagy kereskedelmi termékek; online RBL adatbázisok; publikált malware minták)
  - Saját domaines feladók védelme
- **Felismerni** az illetéktelenül megszerzett jelszavakat és az azzal próbálkozó spambotokat és zombikat.
- **Megakadályozni**, hogy a megszerzett azonosító+jelszó párost illetéktelenek használják.

Illegális jelszóhasználat - felismerés

Felismerni az illetéktelenül megszerzett jelszavakat és az azzal próbálkozó spambotokat és zombikat.

- Gyanús jelek detektálása (egy azonosító sok címről vagy extrém országokból; túl sok email egy azonosítóval; eltérő vagy hamis feladók, ...)
- SMTP authentication (hitelesítés)? Mire jó? Mire nem?
- Az udvarias spambotok szép sorban végigpróbálják a lopott jelszavakat, ezzel önkéntesen segítve a szolgáltatót abban, hogy melyik ügyfeleket kell letiltania (ha egyezik a jelszó).
- Ezzel a szolgáltató **segíti az ügyfelet** az adatlopás és a még nagyobb kár megelőzésében!

Illegális jelszóhasználat - akadályozás

Megakadályozni, hogy a megszerzett azonosító+jelszó párost illetéktelenek használják.

- Lopott jelszó letiltása.
  - Az ügyfél értesítése; a magyarázat hogy elhiggye, hogy ez a jelszó közkincs; **ÁSZF háttér szükséges** a tiltáshoz.
  - Jelszóváltás kényszerítése (biztonságosra)
  - Az ügyfél „ügyfélkapun” tudja engedélyezni, vagy a jelszóváltás automatikusan.
  - Konfliktushelyzet, ha az észlelés túl szigorú vagy téved.
  - A kétfaktoros azonosítás ISP szinten nem életszerű.

Zsarolólevelek

Nem szorosan a témához tartozik, de ez felfutó trend.

- Nem összetévesztendő a *ransomware*-rel, amikor az adatokat titkosítják-törlik-eldugják; itt csak a **fenyegetés** van jelen.
- A levél tartalmaz egy **valódi** jelszót, és egy történetet, hogy a *szuperhekker* hogy szerezte meg, és még mit, és mi lesz ha *nagyonsokpénzt* nem fizetünk.
- A történetből még a kötőszavak sem igazak.
- A jelszót az internetről lehívható betörések adataiból másolták ki. (https://haveibeenpwned.com/)
- Levelet kidobni, egyedi jelszavakat használni, a kikerült jelszót mindenütt lecserélni. (https://gringoto.page.link/zsarol)

Műszaki eszközök

A cél az adathalász e-mail (vagy Spam általában) **bejuttatásának megakadályozása** illetve az email kézbesítés (spam akadályozás) hibáinak felderítése.

- SPF: „melyik server küldhet ilyen feladót?”
- DKIM: „a levél valóban átment egy adott domain serverén, és »pár levélrészlet« garantáltan változatlan”
- DMARC ("v=DMARC1;p=quarantine;adkim=s;aspf=s;rua=mailto:rep@minta.uh;"):
  - Mit tegyen a **fogadó** a beérkező emaillel, ha az SPF vagy DKIM ellenőrzés elbukik?
  - Küldjön-e a sikertelen levelekről a **fogadó** riportokat? Mikor, mennyit, hogyan, kinek?

Műszaki eszközök

- Kézbesítési problémák felderítése könnyebb lehet DMARC-kal: a riportok jelzik, hogy milyen okból kerülnek e-mailek elutasításra vagy spam-be.
- A DMARC riport jelezheti, ha a szolgáltató domainjeivel spammelés történik.
- Nem biztos, hogy a szolgáltató ezekkel tud mit kezdeni, ha nincs automata analízis a riportokról, ami alapján konkrétan cselekedni tudna.
- Nagyobb szolg. Postmaster Tooljai hibakereséshez:
  - GooGle: https://postmaster.google.com/
  - Micro$oft: https://postmaster.live.com/snds
  - Yahoo?: https://help.yahoo.com/kb/postmaster

** Too Many Slides Error in line 17 PERFORMER HALTED

Köszönöm a figyelmet!

Gervai Péter <grin@grin.hu>

2018-11-14