Bevezetés a kiberbiztonságba és biztonságtudatosság
Levelezés biztonsága

Levelezés biztonsága

Szarvák Anikó

2023. Tavaszi félév

E-mail szolgáltatások

- Milyen gyakran kapunk ismeretlen feladóktól származó leveleket?
    - Mit tehetünk velük?
- Miért tekinthetők károsnak a SPAM (kéretlen) levelek?
- Mennyire tekinthetők privátnak a magánleveleink?
    - Ki és mikor olvashatja el őket?

Levelezőrendszerek - kliens

Levelező kliens (Mail User Agent, MUA)

- Elsődleges felhasználói felület
- Feladata az üzenetek megjelenítése és elkészítése
- Az RFC524 és MIME (Multipurpose Internet Mail Extensions) szabványokat használja
- Egyéb protokollok: SMTP, MAPI, IMAP, POP3

Levelező szerver

Levelező kiszolgáló (Message Transport Agent, MTA)

- Feladata az üzenetek küldése és fogadása
- Az SMTP (Simple Mail Transfer Protocol) szabványt használja

E-mail: fejléc

Fejléc mezők (kulcs- értékek)

- From (üzenet feladó)
- To (üzenet címzett)
- CC (másolat)
- Dátum (a feladó rendszerben)
- Subject (tárgy)
- A tartalom típusa és sok minden más…

Tartalom

Üzenettörzs (fő tartalom)

- Tartalom típusok
  - multipart/mixed – több rész
  - text/plain – szöveges rész
  - text/html – formázott szöveges rész
  - application/octet-stream – mellékletek
- Számos kódolási típus

SMTP protokoll alapok

Szöveg alapú ősprotokoll:

- SMTP bővítmények

Küldő oldali üzenetek:

- HELO – kezdő üzenet
- MAIL FROM – boríték feladó
- RCPT TO – boríték címzett DATA – e-mail adatok

(fejlécek és törzs)

(új sorban álló pont) – adat vége

Protokoll kiegészítések (eg. 8 bit a 7 bit helyett)

- SASL (felhasználó/jelszó)
- PKI (tanúsítványok) Titkosítás
- SSL/TLS

E-mail biztonsági lehetőségek

Üzenet hitelesítés:

- S/MIME – megbízható külső felek (CA-k)
- PGP – bizalmi háló („kulcsaláíró bulik”)
- **Nem terjedtek el – elég – széles körben**

Titkosítás:

- Üzenetek: S/MIME és PGP
- Kommunikáció: SMTPS (SSL/TLS)
- **Nem oldanak meg mindent!**

Küldő fél azonosítása:

- Sender Policy Framework (SPF)
- Domain Keys Identifed Mail (DKIM)

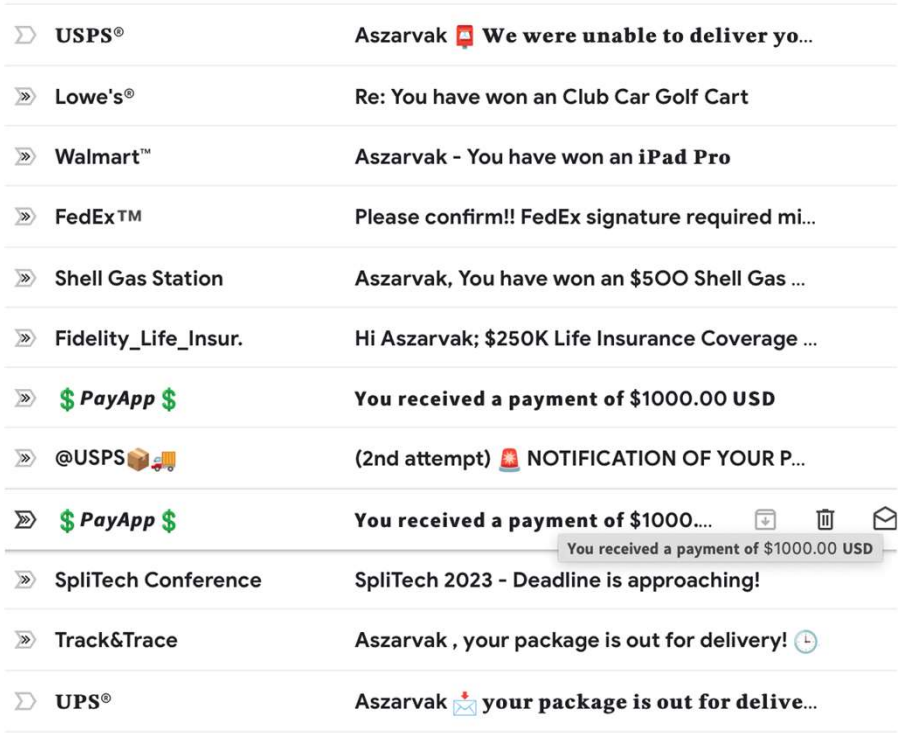
Spam, malware

Kéretlen levél (spam):

- Hirdetés
- Phishing levél
- Malware-t terjesztő levelek

Rosszindulatú kód (Malware):

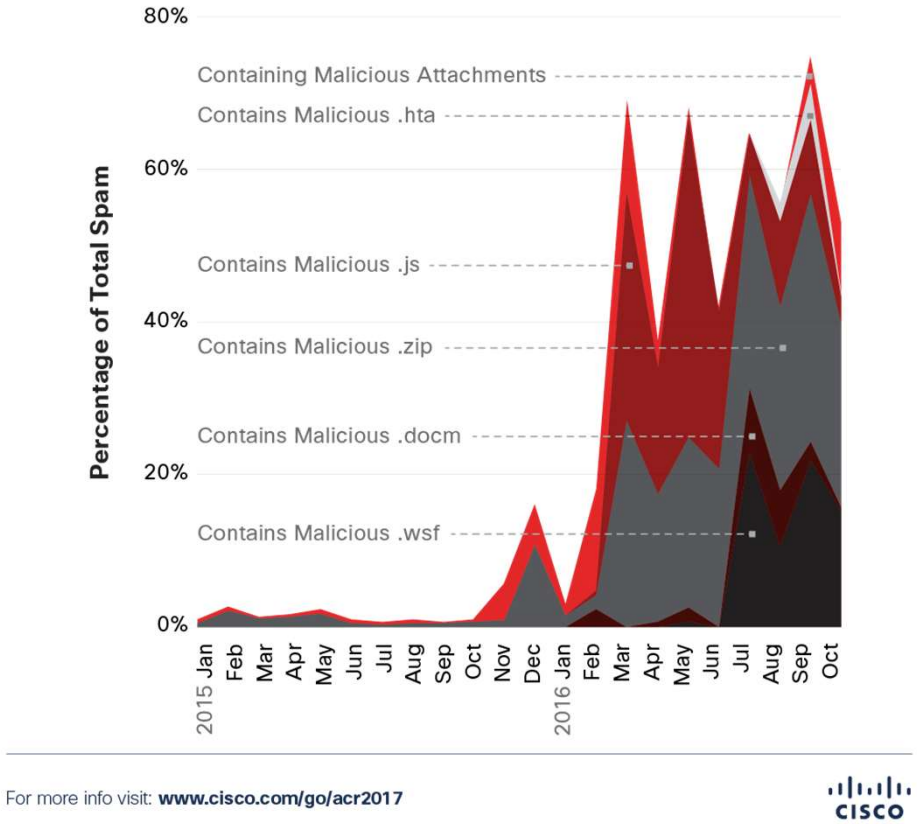
- Vírus, féreg, kémprogram
- Reklámprogram
- Zsarolóprogram



Spam + Malware

Figure 17 Percentage of Total Spam Containing Malicious Attachments

Source: Cisco Security Research



For more info visit: **www.cisco.com/go/acr2017**

cisco

Védekezés

SPAM és Malware elleni küzdelem:

- DNS alapú szűrőlisták
- Azonosítás (SPF/DKIM)

Szabályrendszer alapú szűrések

- Antivirus rendszerek (általános célú) Antispam rendszerek (specifikus)
- Adatelemzés (pl. bayes alapú szűrés, képfelismerés)
- Protokoll alapú trükkök (pl. graylisting)

További támadások

Scam-ek, csaló üzenetek (pl.: nigériai levelek)

- Kártékony szoftver terjesztés
- Phishing (“Fiókja felfüggesztésre került, kattintson ide: URL”)

Feladó hamisítás:

- üzenet küldő (RFC524 From fejléc)
- boríték küldő (SMTP MAIL FROM)

Rendszerek (MUA, MTA) elleni támadások

- Pufer túlcsordulás…

E-mail szolgáltatások – záró kérdések

- Hogy ellenőrizhetünk egy eddig ismeretlen levél feladót?
- Miért van jelentősége a külső erőforrások (pl. beágyazott képek) letöltésének a HTML e-mailek megjelenítésekor?
- Mit tegyünk egy jelszóval védett ZIP fájlt tartalmazó e-mail esetén, ha a jelszó a levél törzsében megadásra került?
    - Mi lehet egy ilyen üzenet küldésének az oka?