Az adathalászat trendjei

Mi változott, mi változik és mi fog változni…

Szekeres Balázs

ERSTE Bank

Phishing azaz adathalászat

Phishing is a **cybercrime** in which a target or targets are **contacted by email, telephone or text message** by someone **posing as a legitimate institution** to **lure individuals** into **providing sensitive data** such as **personally identifiable information**, **banking and credit card details**, and **passwords**. (phishing.org)

Azaz egy olyan „social engineering” támadás, amely során érzékeny adatok megszerzése a célja a támadónak.

15 Top Cyber Threats (ENISA)

	2014	2015	2016	2017
1	Malware	Malware	Malware	Malware
2	Web based attacks	Web based attacks	Web based attacks	Web based attacks
3	Web application attacks	Web application attacks	Web application attacks	Web application attacks
4	Botnets	Botnets	Denial of Service	Phishing
5	Denial of Service	Denial of Service	Botnets	Spam
6	Spam	Phisical manipulation/damage/theft/loss	Phishing	Denial of Service
7	Phishing	Insider threat	Spam	Ransomware
8	Exploit kits	Phishing	Ransomware	Botnets
9	Data breaches	Spam	Insider threat	Insider threat
10	Phisical manipulation/damage/theft/loss	Exploit kits	Phisical manipulation/damage/theft/loss	Phisical manipulation/damage/theft/loss
11	Insider threat	Data breaches	Exploit kits	Data breaches
12	Information leakage	Identity theft	Data breaches	Identity theft
13	Identity theft	Information leakage	Identity theft	Information leakage
14	Cyber espionage	Ransomware	Information leakage	Exploit kits
15	Ransomware	Cyber espionage	Cyber espionage	Cyber espionage

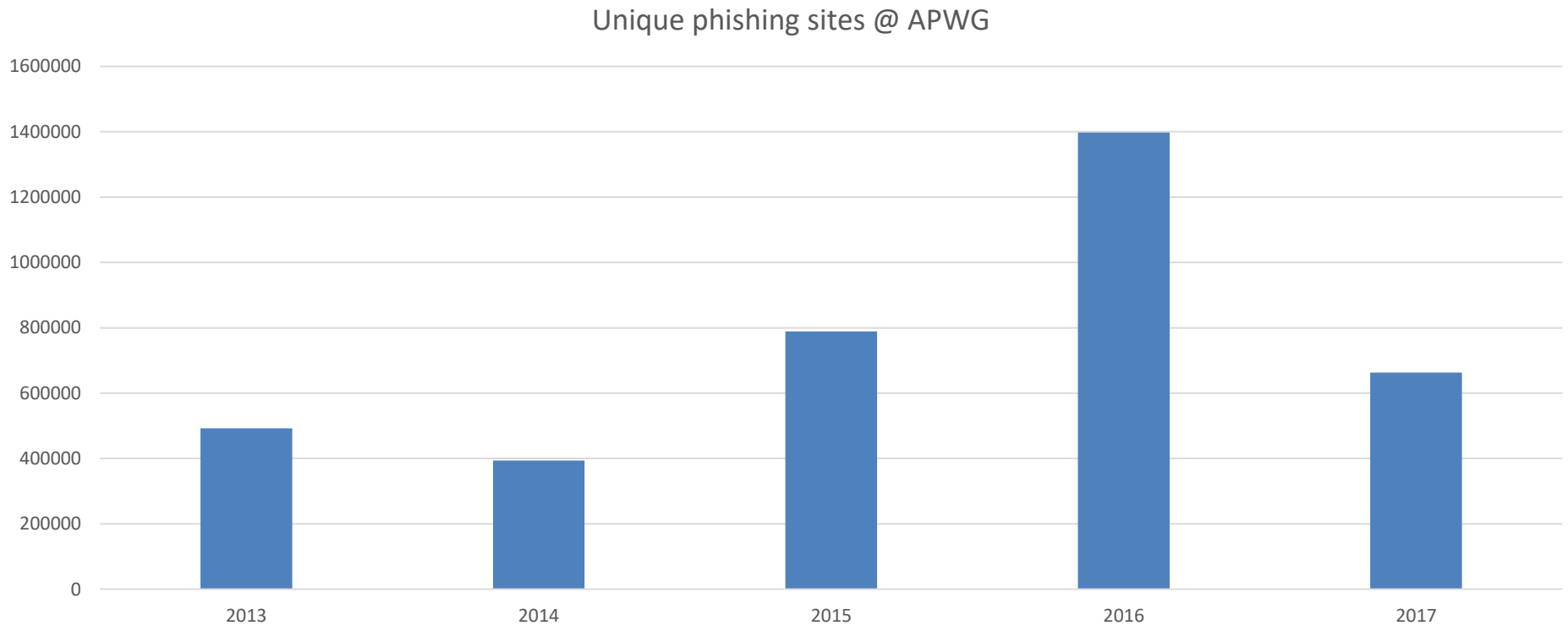
15 Top Cyber Threats (ENISA)

	2014	2015	2016	2017
1	**Malware**	**Malware**	**Malware**	**Malware**
2	**Web based attacks**	**Web based attacks**	**Web based attacks**	**Web based attacks**
3	**Web application attacks**	**Web application attacks**	**Web application attacks**	**Web application attacks**
4	**Botnets**	**Botnets**	Denial of Service	Phishing
5	Denial of Service	Denial of Service	**Botnets**	Spam
6	Spam	Phisical manipulation/damage/theft/loss	Phishing	Denial of Service
7	Phishing	Insider threat	Spam	**Ransomware**
8	**Exploit kits**	Phishing	**Ransomware**	**Botnets**
9	Data breaches	Spam	Insider threat	Insider threat
10	Phisical manipulation/damage/theft/loss	**Exploit kits**	Phisical manipulation/damage/theft/loss	Phisical manipulation/damage/theft/loss
11	Insider threat	Data breaches	**Exploit kits**	Data breaches
12	Information leakage	Identity theft	Data breaches	Identity theft
13	Identity theft	Information leakage	Identity theft	Information leakage
14	Cyber espionage	**Ransomware**	Information leakage	**Exploit kits**
15	**Ransomware**	Cyber espionage	Cyber espionage	Cyber espionage

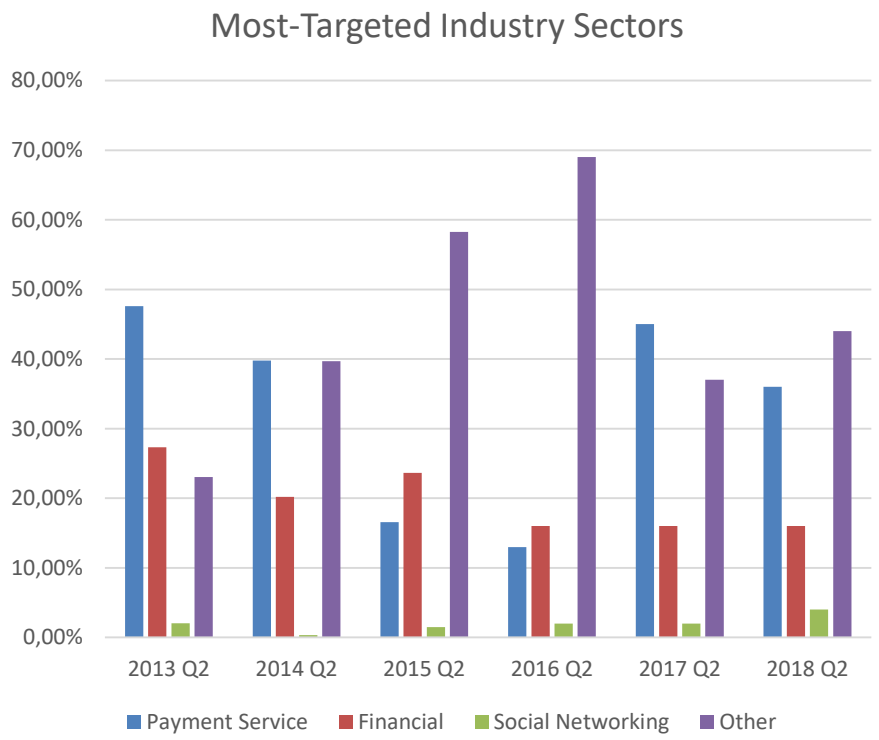
15 Top Cyber Threats (ENISA)

	2014	2015	2016	2017
1	Malware	Malware	Malware	Malware
2	Web based attacks	Web based attacks	Web based attacks	Web based attacks
3	Web application attacks	Web application attacks	Web application attacks	Web application attacks
4	Botnets	Botnets	Denial of Service	**Phishing**
5	Denial of Service	Denial of Service	Botnets	Spam
6	Spam	Phisical manipulation/damage/theft/loss	**Phishing**	Denial of Service
7	**Phishing**	Insider threat	Spam	Ransomware
8	Exploit kits	**Phishing**	Ransomware	Botnets
9	Data breaches	Spam	Insider threat	Insider threat
10	Phisical manipulation/damage/theft/loss	Exploit kits	Phisical manipulation/damage/theft/loss	Phisical manipulation/damage/theft/loss
11	Insider threat	Data breaches	Exploit kits	Data breaches
12	Information leakage	**Identity theft**	Data breaches	**Identity theft**
13	**Identity theft**	Information leakage	**Identity theft**	Information leakage
14	Cyber espionage	Ransomware	Information leakage	Exploit kits
15	Ransomware	Cyber espionage	Cyber espionage	Cyber espionage

Az APWG-hez bejelentett phishing incidensek



Leginkább támadott szektorok (APWG)



Others?

2018 – Webmail és Cloud storage 30%

2017 - Webmail és Cloud storage 24%

2016 – Retail / service 43%

2015 – Retail / service, multimédia és ISP 34%

2014 – Retail / service és ISP 26%

2013 – Retail / service és ISP 16%

Adathalászat céljai

Általában

- Social engineering
- Személyes adatok
- Felhasználói szokások
- Máshol is felhasználható felhasználói azonosítók

Pénzügyi szektor

- Social engineering
- Közvetlen hozzáférés az ügyfél pénzéhez
- Mule account
- Felhasználói / pénzügyi szokások
- Máshol is felhasználható adatok

Védelem? Kockázatcsökkentés

Több faktoros azonosítás, jóváhagyás

- Pénzügyi szektorban használják, nagy szolgáltatóknál megjelent (Google, facebook) → Probléma a mobil készülékek esetén
- A felhasználói élményt rontja

Cyber fraud monitoring and handling

- Endpoint fraud monitoring → költséges, nagyon sok a fals pozitív, nem kellően stabil, mit kezdjünk a jelzésekkel (egy eszköz, több eszköz probléma, üljünk át egy másik autóba)?
- Központi fraud monitoring → költséges, szabály alapú, sok emberi erőforrást, folyamatot igényel

Incidens kezelés

- Szervezeti → a 7/24 sok erőforrást igényel, a túloldali reakció kétséges, reaktív
- Központi → vannak megfelelő szolgáltatók, költséges, reaktív, a proaktivitás kétséges
- Állami, szektorális → az információ megosztás nincs rendezve, reaktív, lassú

Mit hoz nekünk 2018-2019? PSD2 és IP!

- Ha az ügyfél jelzi a banknak, hogy a fizetést nem ő hajtotta végre, akkor a Banknak azonnal (1 napon belül) vissza kell fizetnie a pénzt
- A Banknak meg kell nyitnia a rendszerét térítés mentesen az arra jogosult Külső szolgáltatók felé (fizetési kezdeményezési és számlainformációs szolgáltatások)
- A hazai átutalásokat, fizetéseket 5 másodpercen belül teljesíteni kell
- 1 éven belül maximum 1 napot állhat a banki rendszer (tervezett és nem tervezett együtt)
- A banknak erős ügyfél azonosítást kötelező alkalmazni (SCA). Vannak kivételek (pl. közlekedés), illetve lehet adaptív azonosítást alkalmazni (Transaction Risk Analysis)
- A Screen Scraping csak tartalék megoldás lehet

Mit jelent ez biztonsági szempontból?

- Masszív fejlesztés, új rendszerek, nagyobb kapacitás
- Cyber threat, security and fraud monitoring
- 7/24 órás működés
- 3rd party security
- API security
- Együttműködések és információ megosztás
- …??? A többit majd meglátjuk!