Variációk „phishingre”…

Avagy mindig van plusz információ….

Benyó Pál
Szenior információbiztonsági szakértő
Erste Bank Hungary Zrt.

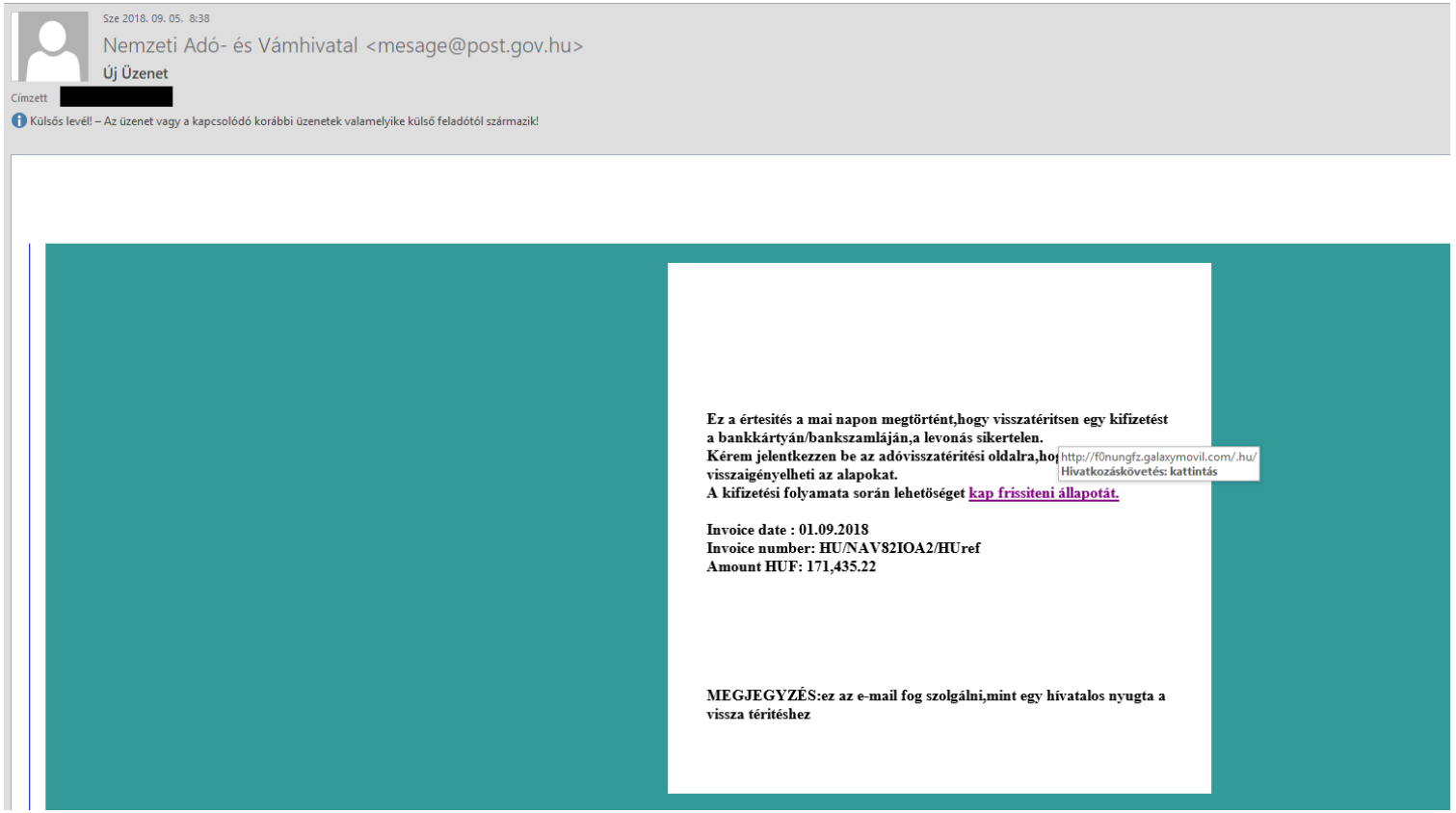
Adathalászat / phishing

- „password” + „fishing” = phishing, jelszavakat halászni
- Mindig valamilyen adatot akarnak megszerezni (bankkártya adat, vagy más hozzáférés)
- Hamisított email-ek-en keresztül
- Egy weboldalra mutató link, ami mögött az oldal akár a megtévesztésig hasonlíthat az eredeti oldalra

Adathalászat / phishing

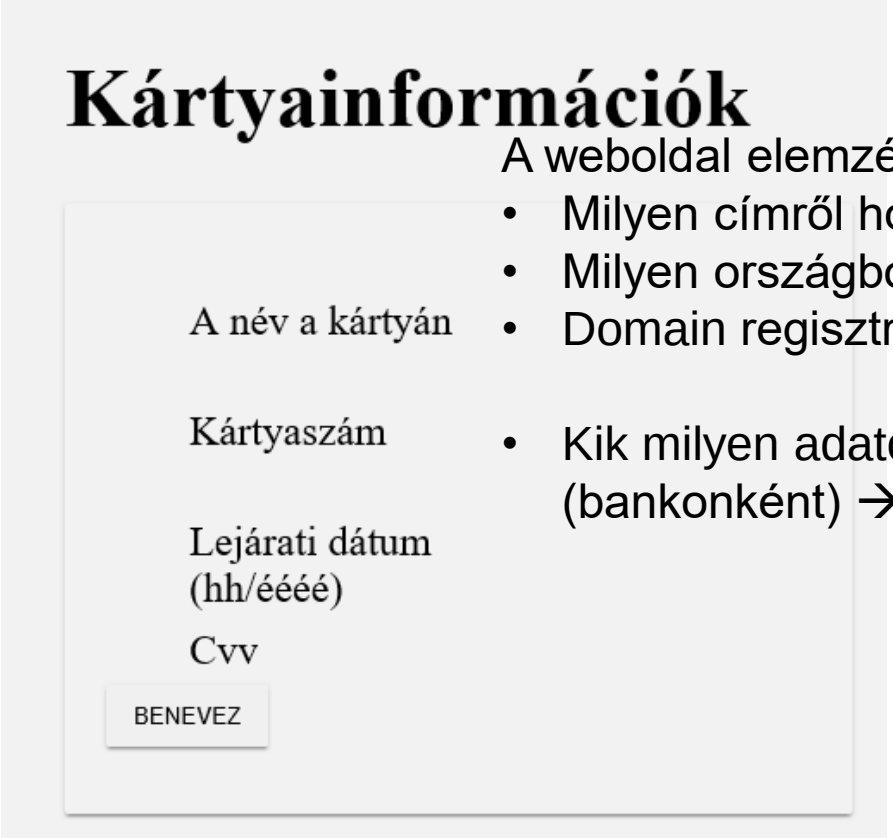
- Adathalászatra utaló jelek lehetnek:
- Nyelvtanilag helytelen mondatok, helyesírási hibák, ragozási problémák
- A weboldal megnyitásakor a címsor árulkodó
- Olyan adatokat kell megadni, amit egyébként sosem szoktak elkérni

NAV-os adathalászat



NAV-os adathalászat

NAV-os adathalászat



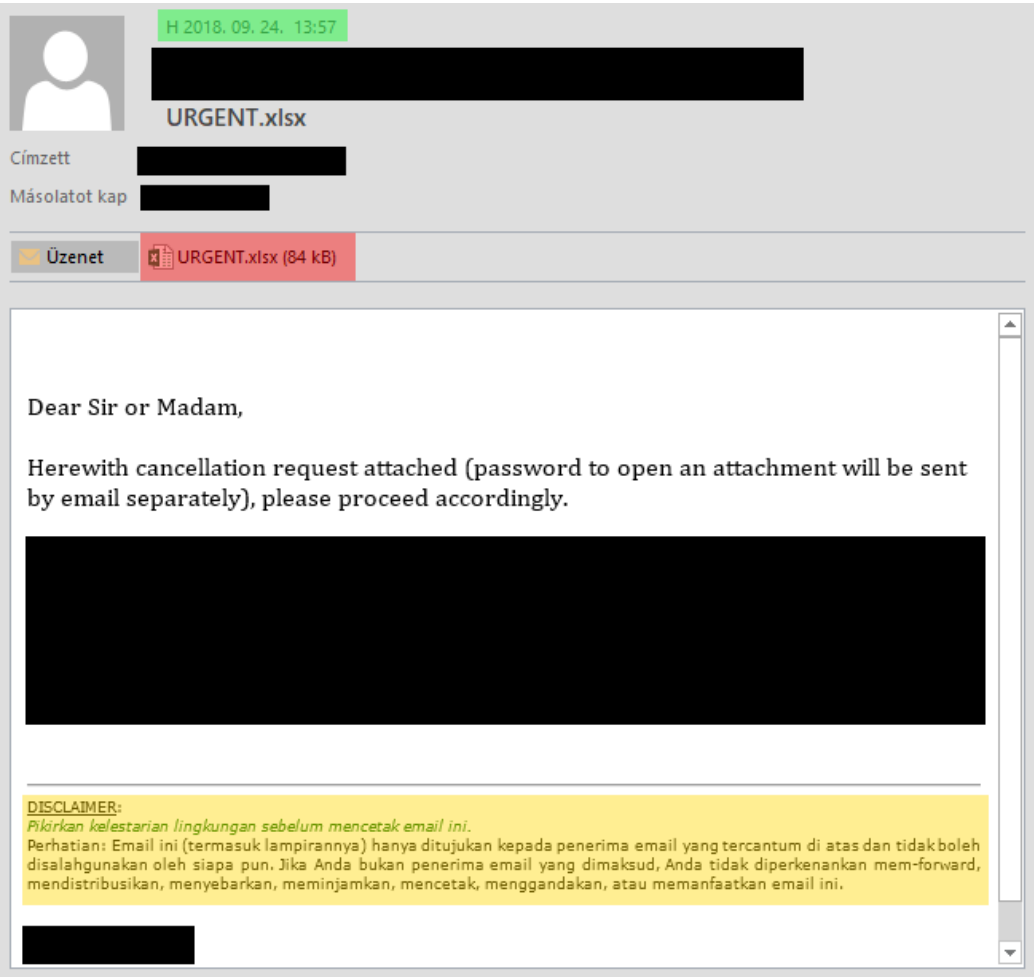
A weboldal elemzése során kiderült:

- Milyen címről hosztolták az oldalt
- Milyen országból (USA)
- Domain regisztrátor (Bahama)

- Kik milyen adatokat adtak meg (bankonként) → result.txt


[redacted] - Jegyzettömb
Fájl Szerkesztés Formátum Nézet Súgó
----------1 Card-Results----------
NAMEONCARD : AAAA BBB
CARDNO : 1234123412341234
EXPDATE : [redacted]
CVV : [redacted]
----------created by medpage----------
IP : [redacted]
BROWSER : Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
----------ReSulT----------
----------1 Card-Results----------
NAMEONCARD : [redacted]
CARDNO : [redacted]
EXPDATE : [redacted]
CVV : (02
----------created by medpage----------
IP : [redacted]
BROWSER : Mozilla/5.0 (Windows NT 6.1; rv:61.0) Gecko/20100101 Firefox/61.0
----------ReSulT----------
----------1 Card-Results----------
NAMEONCARD : kapd b[redacted]
CARDNO : jó sok
EXPDATE : 2516 14
CVV : fa[redacted]
----------created by medpage----------
IP : [redacted]
BROWSER : Mozilla/5.0 (Linux; Android 5.1.1; SAMSUNG SM-T280 Build/LMY47V) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/3.5 Chrome/38.0.2125.102 S
----------ReSulT----------
----------1 Card-Results----------
NAMEONCARD : tenéz [redacted]
CARDNO : 44342223422342
EXPDATE : 22/22
CVV : 123
----------created by medpage----------
IP : [redacted]
BROWSER : Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/65.0.3325.183 Safari/537.36 Vivaldi/1.96.1147.64
----------ReSulT----------
----------1 Card-Results----------

SPAM?



H 2018. 09. 24. 13:57

[redacted]

URGENT.xlsx

Címzett [redacted]

Másolatot kap [redacted]

Üzenet | URGENT.xlsx (84 kB)

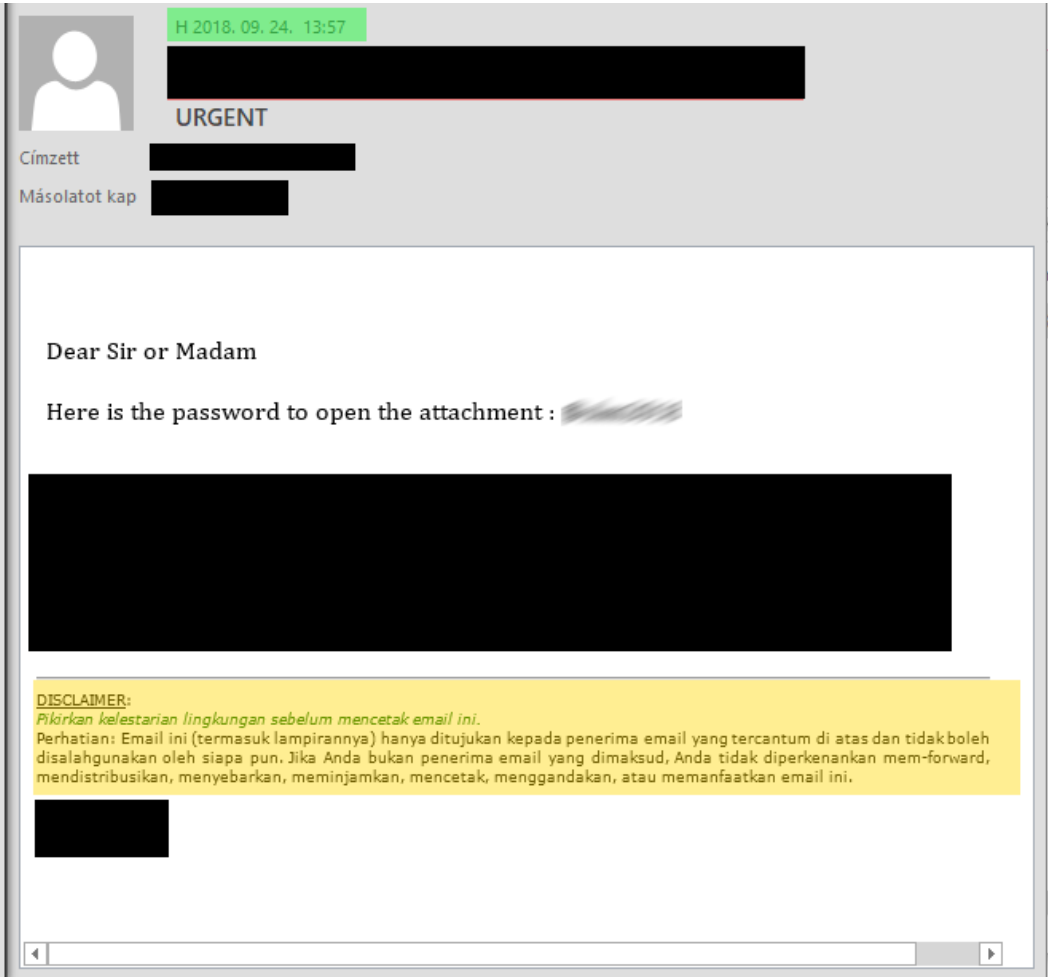
Dear Sir or Madam,

Herewith cancellation request attached (password to open an attachment will be sent by email separately), please proceed accordingly.

[redacted]

DISCLAIMER:
Pikirkan kelestarian lingkungan sebelum mencetak email ini.
Perhatian: Email ini (termasuk lampirannya) hanya ditujukan kepada penerima email yang tercantum di atas dan tidak boleh disalahgunakan oleh siapa pun. Jika Anda bukan penerima email yang dimaksud, Anda tidak diperkenankan mem-forward, mendistribusikan, menyebarkan, meminjamkan, mencetak, menggandakan, atau memanfaatkan email ini.

[redacted]



H 2018. 09. 24. 13:57

[redacted]

URGENT

Címzett [redacted]

Másolatot kap [redacted]

Dear Sir or Madam

Here is the password to open the attachment : [redacted]

[redacted]

DISCLAIMER:
Pikirkan kelestarian lingkungan sebelum mencetak email ini.
Perhatian: Email ini (termasuk lampirannya) hanya ditujukan kepada penerima email yang tercantum di atas dan tidak boleh disalahgunakan oleh siapa pun. Jika Anda bukan penerima email yang dimaksud, Anda tidak diperkenankan mem-forward, mendistribusikan, menyebarkan, meminjamkan, mencetak, menggandakan, atau memanfaatkan email ini.

[redacted]

Pro / Kontra?

- URGENT.XLSX → 99% esély arra, hogy a levél SPAM vagy malware-rel fertőzött csatolmány
- Nem volt megkeresés a másik oldalról

- Nyelvtanilag jól megfogalmazott levél (disclaimer is)
- Legitimnek tűnő email cím (IP alapján is)
- Létezik ilyen cég/szervezet
- Külön levélben a jelszó és a jelszóval védett csatolmány

Elemzési eredmények

…**it may look suspicious indeed**…

we **didn't observe any malicious activities**, while checking the xlsx in a sandbox and running it manually.

We can confirm it uses *DDE* but apparently the DDE command executed when the xlsx is opened has **no effect**.

We have also tried to scan memory to get interesting strings or URLs but **nothing has caught** our attention.

We would suggest ignoring these emails

Elemzési eredmények

[redacted]

To [redacted]
BIN [redacted]
From [redacted]
BIN/ICA [redacted]
Fax : [redacted]
Phone : [redacted]
Subject : **RELEASE PRE-AUTHORIZATION CODE**

NO	CARD NUMBER	REASON	AMOUNT	APPR CODE	TRX DATE	BANK	FAX	EMAIL
1	[redacted]							
2								
3								
4								
5								

Valid kérést tartalmazott a levél