NKI-CSIRT Outlook Add-in fejlesztői útmutató

Outlook Add-in: GCNotify

A GCNotify egy olyan Outlook kiegészítő, amely megkönnyíti a gyanús e-mailek továbbítását a Nemzeti Kibervédelmi Intézet - CSIRT számára.

A kiegészítő lehetővé teszi, hogy a felhasználó a kiválasztott, vagy megnyitott e-mailt kiegészítő információkkal (pl. SMTP fejlécelemek) együtt tovább küldje elemzésre az NKI részére.

A Kiegészítő megkönnyíti a felhasználók és elemzők munkáját:

Felhasználók esetén

- nem szükséges külön foglalkozni a levelek továbbításával (egy lépésben könnyen továbbítható az e-mail)
- a megfelelő szervezet részére kerül továbbításra a levél

Elemzők esetén

- nem szükséges az eredeti e-mail továbbításának kérése
- az e-mail kiegészítő információkat tartalmaz

Funkcionalitás

A felhasználónak ki kell választania egy vagy több e-mailt a beérkező levelek közül. A Kiegészítő elindításával létrejön egy új e-mail, amely csatolmányként tartalmazza a kiválasztott e-mail-(eke)t, kiegészítő információkat és egy előre definiált sablon szöveget. Az új e-mail címzettje és tárgya is előzetesen kitöltésre kerül, a Kiegészítő beállításainak megfelelően. A felhasználónak csak a "Küldés" gombra kell kattintania.

Az e-mail csak a felhasználó hozzájárulásával kerül kiküldésre, így a felhasználónak lehetősége nyílik arra, hogy átnézze a kiküldendő levél tartalmát, esetleg további megjegyzéseket fűzzön ahhoz.

A Kiegészítő az Outlook 2013, 2016 és 2019 programokkal működik.

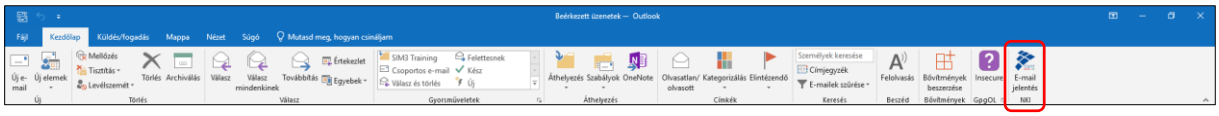
Jellemzők

- Könnyen kezelhető
- Egy vagy több e-mail küldése mellékletként
- Testre szabható

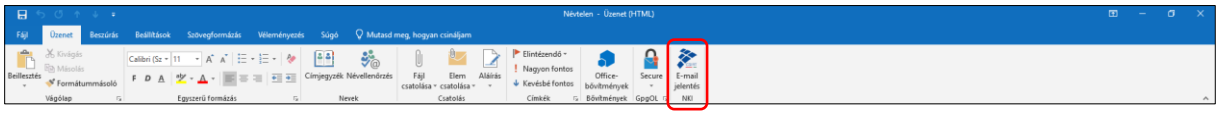
Add-in gomb helye az Outlook programban

A Kiegészítő az alábbi menüszalagokon érhető el

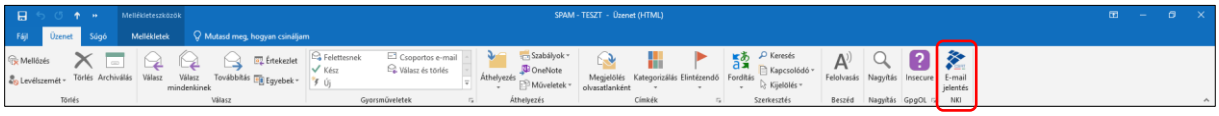
Kezdőlap (Home)



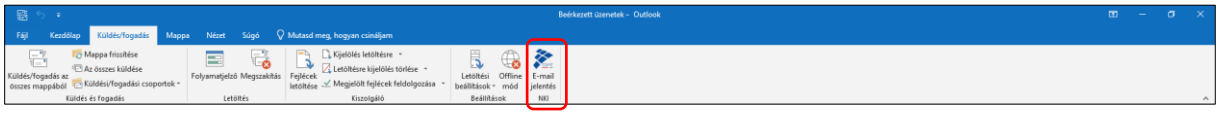
Új e-mail (New Mail)



Üzenet (Read Mail)



Küldés/fogadás (Send/Receive)



Fejlesztés

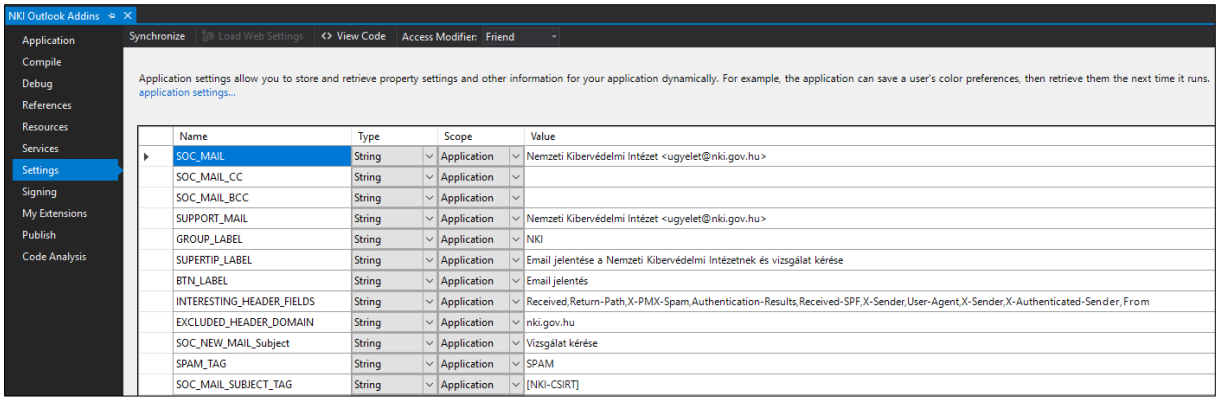
A kód Visual Basic nyelven íródott. A fejlesztéshez Visual Studio 2019 vállalati vagy közösségi kiadás szükséges.

A kiegészítő testreszabása

A kiegészítő a forráskód megváltoztatása nélkül az alábbiak szerint alakítható.

Beállítások

A Visual Studio „beállítások” menüpontjában lehetőség van a Kiegészítő alábbi adatainak módosítására. A kötelező adatok megadása szükséges a kiegészítő működéséhez.



Név	**Alapértelmezett érték**	**Leírás**	**Kötelező / nem kötelező**
SOC_MAIL	csirt@nki.gov.hu	Az NKI e-mail címe. A létrehozott e-mail-ben ez lesz a „**Címzett**” mező.	Kötelező
SOC_MAIL_CC		E-mail cím, amelyre másolatban elküldésre kerül az e-mail. Ha üres, akkor figyelmen kívül marad. A létrehozott e-mail-ben ez lesz a „**Másolatot kap**” mező.	Választható
SOC_MAIL_BCC		E-mail cím, amelyre titkos másolatban elküldésre kerül az e-mail. Ha üres, akkor figyelmen kívül marad. A létrehozott e-mail-ben ez lesz a „**Titkos másolat**” mező.	Választható
SUPPORT_MAIL	csirt@nki.gov.hu	Az az e-mail cím, amelyre hiba esetén a hiba elküldésre kerül.	Kötelező
GROUP_LABEL	NKI	A szalagcsoport címkéje.	Kötelező
BTN_SUPPERTIP_LABEL	E-mail jelentése a Nemzeti Kibervédelmi Intézetnek és vizsgálat kérése	A címke, amikor az egérmutató a gomb felett van.	Kötelező
BTN_LABEL	E-mail jelentés	A gomb címkéje.	Kötelező
INTERESTING_HEADER_FIELDS	Received,Return-Path,X-PMX-Spam,Authentication-Results,Received-SPF,X-Sender,User-Agent,X-Sender,X-Authenticated-Sender,From	Az e-mail fejléc mezői, amelyeknek meg kell jelennie az e-mailben. MEGJEGYZÉS: Az értékek vesszővel vannak elválasztva.	Kötelező
SOC_MAIL_SUBJECT_TAG	[NKI-CSIRT]	A létrehozott e-mail tárgyában használt címke.	Kötelező
SOC_NEW_MAIL_Subject	Vizsgálat kérése	Üres e-mail alapértelmezett tárgya.	Kötelező
SPAM_TAG	SPAM	Az e-mail rendszer által használt címke, arra az esetre, ha a levél SPAM-ként észlelésre került.	Kötelező

Alternatív megoldásként az értékek az „**app.config**” fájlban megváltoztathatók. Ez egy XML fájl, ahol a beállítások a következőképpen néznek ki:

```
<setting name ="SPAM_TAG" serializeAs ="String">
    <value>SPAM</value>
</setting>
```

Sablonok / Ikon

A sablonok megtalálhatók a projekt „Resources” részében vagy a „Resources” mappában.

Fájl név	Leírás	Behelyettesítő mező
EmailDetails.txt	A továbbított e-mailek kiegészítő információit tartalmazza.	{{EmailCounter}} - A továbbított e-mailek indexe {{From}} – A továbbított e-mail küldője {{HeaderDetails}} - A kibontott fejléc adatai (függ az INTERESTING_HEADER_FIELDS-től) {{Subject}} – A továbbított e-mail tárgya {{AttachmentCount}} - A csatolmányként továbbított e-mail-ek száma
ErrorMail.txt	E-mail törzssablon hiba esetén	{{Version}} - A GCNotify verziója {{Message}} – Hiba üzenet {{Stacktrace}} - alkalmazás hibás állapotának a lenyomata
NewMailBody.txt	E-mail törzssablon új, üres e-mailhez	{{HostDetails}} - A gazdagép részletes adatai {{NetworkDetails}} - A gazdagép hálózati adatai
NewResendError.txt		
NoSelectionError.txt	Üzenet, ami akkor jelenik meg, ha a felhasználó nem választott ki továbbítandó levelet a kiegészítő elindítása előtt.	
OverWriteConfirm.txt	Üzenet, ami akkor jelenik meg, ha a felhasználó új e-mail ablakot nyitott meg, kitöltött bizonyos tartalmat, majd megnyomta a „Küldés” gombot. Annak érdekében, hogy ne íródjon felül a felhasználó által már megadott információ, megkérdezik a felhasználót, hogy ezek az információk felülírhatók-e vagy sem.	

ResendError.txt	Üzenet, amely abban az esetben jelenik meg, ha a felhasználó megnyomja a GCNotify gombot a jelentési e-mail írási ablakában.	
SPAMDialogText.txt	Üzenet, ami akkor jelenik meg, ha spamként megjelölt e-mail van a továbbítandó e-mailek kiválasztásán belül.	{{Email}} - A feladó e-mail-je {{Subject}} - Az e-mail tárgya
SuspectBody.txt	E-mail törzssablonja a jelentés e-mail-hez	{{attachments}} - Az a hely, ahova az e-mail adatait el kell helyezni a testben (lásd EmailDetails.txt) {{HostDetails}} - A gazdagép adatai {{NetworkDetails}} - A gazdagép hálózati adatai

Megjegyzés: Az Add-In ikonja hasonló módon szintén megváltoztatható.

Licensz

Eredeti kiegészítő

https://github.com/GOVCERT-LU/GCNotify