Riasztás

Semmelweis Egyetem nevében küldött, káros csatolmányt tartalmazó levelekkel kapcsolatban

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **riasztást ad ki a Semmelweis Egyetem nevében küldött, káros csatolmányt tartalmazó e-mail** üzenetekkel kapcsolatban.

Intézetünkhöz több bejelentés érkezett arról, hogy ismeretlen elkövetők **a Semmelweis Egyetem nevével és arculati elemeivel visszaélő** e-maileket küldenek, amelyek célja a **címzettek munkaállomásainak kompromittálása és hitelesítési adatok megszerzése**. A levelek közös jellemzője, hogy egy megrendelésre hivatkozva próbálják rávenni a címzetteket a csatolmányok megnyitására.

Az üzenetek tárgya minden esetben: „Megrendelésszám: 4110588461”.

A kártékony e-mailek feltételezhetően kompromittált magyar e-mail fiókokból kerülnek kiküldésre, a **levelek NEM a Semmelweis Egyetem informatikai infrastruktúrájából érkeznek**.

Az üzenetek két csatolmányt tartalmaznak. Egy PDF formátumú, beszkenneltnek tűnő Semmelweis-megrendelés, amely fedődokumentumként szolgál, és egy „beszerzesi-megrendeles-szama-4110588461.img” vagy „beszerzesi-megrendeles-szama-4110588461(1).iso” nevű **lemezképfájlt**.

A fertőzés a lemezképfájl megnyitásakor, illetve futtatásakor következik be; **a PDF csatolmány a megtévesztést szolgálja**. A káros csatolmány Windows 64 bites rendszereket céloz. A lemezképfájl futtatását követően **a kártevő több mappába és a Windows Registry-be települ, felhasználói jóváhagyás nélkül perzisztenciát alakít ki.**

A kártevő az alábbi tevékenységeket végzi:

NEMZETI KIBERBIZTONSÁGI INTÉZET
+36-1-336-4833 csirt@nki.gov.hu

- rögzíti a billentyűleütéseket (keylogger), és a rögzített adatokat távoli szerverre továbbítja;
- begyűjti a rendszeren tárolt hitelesítési adatokat (jelszavakat, tokeneket, mentett bejelentkezéseket), majd azokat kiszivárogtatja;
- kapcsolatot létesít egy távoli vezérlőszerverrel (C2), ahonnan további kártékony komponenseket tölthet le (akár zsarolóvírust is),
- a fertőzött munkaállomást botnet hálózatba kapcsolhatja.

A megszerzett tokenek és hitelesítési adatok révén a támadók észrevétlenül jelentkezhetnek be a fertőzött rendszerekre, a keylogger miatt pedig **a jelszóváltoztatást követően is hozzáférést szerezhetnek** a fiókokhoz.

Tárgy: Megrendelésszám: 4110588461
Dátum: 2026-07-31 02:07
Feladó: Élettani Intézet - Gazdasági Iroda <oregzsolo@hockey.hu> lookup email lookup "hockey.hu"
Címzett:
Másolat: <elettan.gazdasagi@semmelweis.hu> lookup email lookup "semmelweis.hu",
<ludman.eszter@semmelweis.hu> lookup email lookup "semmelweis.hu"

Tisztelt Ügyintéző!

Mellékelten küldöm az Élettani Intézet megrendelését.

Szállítási cím:
1094 Budapest, Tűzoltó utca 37-47. A fésű, 3. emelet 3.428 Geiszt
labor
Kapcsolattartó: Ludmán Eszter, Telefon: +36-1/459-1500/60417

Számlázási cím:
Semmelweis Egyetem
1085 Budapest, Üllői út 26.
2025. január1.-től érvényes csoportazonosító és adószám:

19308674-4-44
17784234-5-44

Kérjük a megrendelés visszaigazolását erre az e-mail címre
legyenek szívesek eljuttatni!

Az elektronikusan kiállított számlákat kérjük, az
eszamla@semmelweis.hu lookup email lookup "semmelweis.hu" email címre szíveskedjen küldeni.

Segítségét előre is köszönöm.
Üdvözlettel:

VARGÁNÉ V. NIKOLETTA
GAZDASÁGI REFERENS

SEMMELWEIS EGYETEM
ÖSSZEVONT ELMÉLETI TÖMBIGAZGATÓSÁG
ÉLETTANI INTÉZET
1094 Budapest,Tűzoltó u. 37-47.
+36 20 825 9761
+36 1 459 1500/60405
vargane.nikoletta@semmelweis.hu lookup email lookup "semmelweis.hu"

1. ábra Minta a káros csatolmányt tartalmazó levélből.

Javasolt intézkedések:

- A gyanús levelek csatolmányait semmiképpen ne nyissák meg, az üzeneteket jelöljék kéretlen (SPAM) üzenetként, majd töröljék.
- Vezessenek be, illetve erősítsék meg a csatolmány- és tartalomszűrést, különösen az ISO/IMG kiterjesztésű csatolmányok blokkolását.
- Alkalmazzanak naprakész végpontvédelmi megoldásokat (antivírus, EDR/XDR), viselkedéselemzésre képes detekciós képességekkel.
- A kritikus rendszerekhez, e-mail fiókokhoz, VPN- és adminisztrátori hozzáférésekhez kötelezően vezessenek be többtényezős hitelesítést (MFA).
- Vizsgálják át a bejelentkezési naplókat szokatlan, ismeretlen helyről vagy időpontban történt hozzáférések után.
- Mielőbb tájékoztassák a felhasználókat a hasonló e-mailek kockázatairól, valamint alkalmazzák következetesen a „gondolkodj, mielőtt kattintasz” elvet.

Amennyiben felmerül a gyanú, hogy a káros csatolmány megnyitásra került, az NBSZ NKI az alábbi lépések megtételét javasolja:

- az érintett munkaállomás azonnali leválasztása a hálózatról;
- az érintett rendszer teljes újratelepítése, megbízható forrásból származó telepítőkészlet használatával;
- valamennyi kapcsolódó hitelesítési adat (jelszavak, tokenek, alkalmazás- és böngészőmentett bejelentkezések) azonnali cseréje;
- az érintett e-mail fiókok, hozzáférések és kapcsolódó rendszerek célzott biztonsági auditja;

+36-1-336-4833 csirt@nki.gov.hu

Az eddig ismert indikátorok az alábbiak:

Indikátor típusa	Érték
E-mail tárgya	Megrendelésszám: 4110588461
Csatolmány név	beszerzesi-megrendeles-szama-4110588461.img beszerzesi-megrendeles-szama-4110588461(1).iso
Feladó	Élettani Intézet – Gazdasági Iroda
Reply-To	elettan.gazdasagi@semmelweis.hu vargane.nikoletta@semmelweis.hu ludman.eszter@semmelweis.hu
Beszerzesi-Megrendeles-szama-4110588461.img	MD5: DE586BEE3537097AC09DD6E181C7A04E SHA1: 21DA154DEF2A1CC2B18B10291DBF729F86C7EA4E SHA256: 76C104CCA240AE8BBF27941EBEBCA4296E9B22988E8D7481C50FB0F1A74953CB
1-Beszerzesi-Megrendeles-szama-4110588461.pdf.exe	MD5: 457142F0E24C04AC21FC367182C9E5A4 SHA1: 9ADC26789C178C72F66309324F0A70060A5B1AFE SHA256: DB1ABDB2326EB2FD6153BA84F27B20D3EE1CA53A64DF1776B3C820AEF340DE61
Beszerzesi-Megrendeles-szama-4110588461(1).iso	MD5: 3C81BF4E72ED4D04C9EBCD99D77BD1CF SHA1: D43466A5E0AD5D44B7E95638516405EFAA73BBE0 SHA256: FC257F9C1C4C0EC53446C966A924C9085801B0DD0F9C98EFB8343155D336169E
Beszerzesi-Megrendeles-szama-4110588461[.]txt[.]exe	MD5: 889B3959F7EB9966EF24AD629F030964 SHA1: 90C5FBD0A77BF7773D338F8C68E4E6FC1530FCB6

Indikátor típusa	Érték
	SHA256: 10F80E5E2CBDB23C8DFCBCFB618229B16483417ECEA4E3C800F786194FF0B5AD

Az NBSZ NKI javasolja ezen indikátorok védelmi eszközökön (levélszűrők, tűzfalak, végpontvédelmi rendszerek) történő beállítását, valamint az érintett munkatársak mielőbbi tájékoztatását.

A legfrissebb információkért kérjük ügyfeleinket, hogy folyamatosan kövessék a Nemzeti Kiberbiztonsági Intézet weboldalát.

+36-1-336-4833 csirt@nki.gov.hu