RIASZTÁS

A BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM MEGSZEMÉLYESÍTŐ, KÁROS CSATOLMÁNYÚ E-MAIL KAPCSÁN

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki a Budapesti Műszaki és Gazdaságtudományi Egyetem nevében küldött, káros csatolmányt tartalmazó levéllel kapcsolatban.**

Intézetünkhöz több bejelentés is érkezett arról, hogy ismeretlen elkövetők a Budapesti Műszaki és Gazdaságtudományi Egyetem nevével és arculati elemeivel visszaélő, **káros hivatkozást tartalmazó levelet** küldenek. Az üzenetekben **árajánlatra hivatkozva** próbálják rávenni a címzetteket a csatolmány megnyitására.

A levelek feladója **hamis vagy meghamisított**, a szöveg **sürgető hangvételű**, intézményi felszólításnak álcázva igyekszik elérni, hogy a címzettek egy **ZIP formátumú csatolmányt** megnyissanak. A csatolmány **FormBook típusú infostealert tartalmaz**, amely adatlopásra, billentyűnaplózásra, clipboard-monitorozásra és további payloadok letöltésére is képes. Jellemző rá a folyamatinjektálás, a csomagolás/obfuszkáció és az anti-analysis viselkedés, ezért a detektálása sokszor viselkedésalapú jelekből a legerősebb. Kérjük, azt semmi esetre se nyissák meg!

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


Jó reggelt kívánok a Budapesti Műszaki és Gazdaságtudományi Egyetemről!

Dr. Molnár Bálint vagyok, a rektor nevében írok. Megpróbáltuk telefonon elérni a cégüket, de senki sem veszi fel a hívásaikat. Múlt héten is küldtünk Önnek egy e-mailt, de még nem kaptunk választ. Remélem, minden rendben van a cégével?

Ez egy olyan üzlet, ami rengeteg pénzt forgat meg, és körültekintően kell utánajárni.

Ha ezt az e-mail megkapja, kérjük, válaszoljon a csatolt feladatunkra (zip fájlban) 24 órán belül, különösen a 7., 8., 16., 35. és 40. számúakra, mivel az egyetemnek azonnali válaszokra van szüksége az év utolsó negyedévére vonatkozó költségvetésünknek megfelelően.

Megjegyzés: A termékek iránti sürgős igény miatt az egyetem 80%-os támogatást hajlandó nyújtani.

Várjuk mielőbbi válaszát .

Üdvözlettel.

Dr. Bálint Molnár

MŰEGYETEM 1782

BME

lookup host

1. ábra A káros csatolmányt tartalmazó levél szövegezése

Az eddig ismert indikátorok az alábbiak:

DOMAIN	IP
www[.]1xbet-yhmxpzo[.]top	38[.]182[.]168[.]212
www[.]67545319[.]xyz	38[.]182[.]168[.]222
www[.]cavonixa[.]shop	66[.]29[.]130[.]63
www[.]colorsp[.]wiki	188[.]114[.]96[.]3
www[.]dieteloise[.]com	34[.]133[.]74[.]21
www[.]faithwonderacademy[.]org	216[.]227[.]142[.]170
www[.]h8lcg[.]cc	142[.]251[.]110[.]121
www[.]mattsports[.]wine	43[.]200[.]42[.]56
www[.]nuvo77[.]work	118[.]139[.]162[.]144
www[.]popnov[.]shop	198[.]2[.]218[.]117
www[.]ralcede[.]hair	51[.]77[.]236[.]208

DOMAIN	IP
www[.]richard-win[.]com	103[.]224[.]182[.]219
www[.]silverbotanic[.]site	
www[.]siontrail[.]info	
www[.]dbzo52[.]beer	
www[.]enuri[.]com	
www[.]imamatfoundation[.]com	
www[.]ourtruegod[.]shop	
www[.]track-e9n50i[.]link	

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet ezen indikátorok védelmi eszközökön történő beállítását és a munkatársak mielőbbi tájékoztatását javasolja. Amennyiben a hivatkozott csatolmány megnyitásra került javasoljuk az érintett munkaállomás hálózatról történő leválasztását, illetve újratelepítését.

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

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