Riasztás állománynevekhez és hash-értékekhez kapcsolódó indikátorokról

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki több, elsősorban Windows-környezetre utaló állománynévhez és hash-értékhez kapcsolódó indikátorról.

Az eddig ismert indikátorok az alábbiak:

NAME	MD5	SHA1
MicrosoftEdgeUpdateCore	a2bf5196f4652069b323f7f2ba501740	3012d19c51c24c5220363b7d321ccd4e1077fff3
NVIDIA.exe	e1746ab5f1c34eeaf3535237224665e1	2eac2ffda9de70e3a8b3f9b5b509b526ed572358
RustVentTank.dll	8bab1a4feebc5d284d0da7aa53ebebc5	c43644750c5765eb3951469b970db03121291170
SafeVineTankPArk.tmp	6f44ebc4d52789609b8c7dd6c3ba493a	e73cf8dad1344047eea4cadf106cdffe544b7b69
setupact.ca	ee8616e2801f71b127a01056690a8f74	689b78f6a10cd5b3e0be506290d12ad8fc121778
SqlMetal.exe	f36632a8c3a0ec9499ba6e858b2e32d6	a5a23870b548648a02254565f6784723c688e9a4
SqlMetal.exe .config	5c041df6caea8ffc21a421d6e7a50d28	d78052867b8e432fdbc986c0fd78cda6e6c33083
1.bat	a14f6dfcf63739ce44f2a4d2842b7d94	3dcc55dd6331e25a7cdb7fdd786d932f4e80a59f
ad.exe	a9e390237a96e0c6655b1a06f8d72c6f	6b242ad80260f3cb3e67a1d2a1ee164de465c76e
result1.dat	8367b0ea8ed8f12bd1596259365895cc	480779968608214d197a0cf5f8f97e8f98ba4213

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

NAME	MD5	SHA1
dgtrayicon.exe	077abaf4c236a0e39b682df5d59d76d4	d39367abaa2952628a1d4f7b2409c9b24c51ce6c
MicrosoftEdgeUpdateCore	014b6cce5b33928cdc6d68d86a305b4a	38e94ec91fcfa1d8b7bfdfec0af44ca99edaf7c2
Microsoft.Uev.SyncController.exe	b9d4c0ea77e598b45015e36624d8fbe4	fb69e81b5d252152630d3f1b6426fef4de3fc2ee
Microsoft.Uev.SyncController.exe .config	5c041df6caea8ffc21a421d6e7a50d28	d78052867b8e432fdbc986c0fd78cda6e6c33083
RustVentTank.dll	8bab1a4feebc5d284d0da7aa53ebebc5	c43644750c5765eb3951469b970db03121291170
SafeVineTankPark.tmp	ca575a6a8a09fb336e3a5bc1c231f874	bbbef5cbb2d7168b0441558efe56061911ff7097
setupact.ca	ee8616e2801f71b127a01056690a8f74	689b78f6a10cd5b3e0be506290d12ad8fc121778
MicrosoftEdgeUpdateCore	a6fdf4707b7d97d49c8c927871b3b23e	598038dc0deb478c6f74194901230f9e1ccef20a
SqlMetal.exe	f36632a8c3a0ec9499ba6e858b2e32d6	a5a23870b548648a02254565f6784723c688e9a4
SqlMetal.exe .config	5c041df6caea8ffc21a421d6e7a50d28	d78052867b8e432fdbc986c0fd78cda6e6c33083
RustVentTank.dll	8bab1a4feebc5d284d0da7aa53ebebc5	c43644750c5765eb3951469b970db03121291170
SafeVineTankPark.tmp	6f44ebc4d52789609b8c7dd6c3ba493a	e73cf8dad1344047eea4cadf106cdffe544b7b69
setupact.ca	ee8616e2801f71b127a01056690a8f74	689b78f6a10cd5b3e0be506290d12ad8fc121778

További, hash-érték nélkül ismert fájlnevek:

- **11.txt**
- **r.txt**
- **Certificate.cer.exe**
- **NV.EXE**
- **BRIDGE.EXE**

A gép fertőzöttnek tekinthető, amennyiben az alábbi táblázat második oszlopában szereplő fájlok egyidejűleg megtalálhatók ugyanabban a könyvtárban:

C:\Windows\System32\Tasks	MicrosoftEdgeUpdateCore
C:\ProgramData\HP	Microsoft.Uev.SyncController.exe
C:\ProgramData\HP	Microsoft.Uev.SyncController.exe.config
C:\ProgramData\HP	RustVentTatk.dll
C:\ProgramData\HP	SafeVineTankPark.tmp
C:\ProgramData\HP	setupact.ca

Az érintettség vizsgálata érdekében javasolt a megadott indikátorok ellenőrzése a saját rendszerekben, elsődlegesen a hash-értékek alapján. A kizárólag fájlnév alapján történő egyezések önmagukban nem tekinthetők megerősített találatnak.

Hashérték-egyezés esetén javasolt az érintett rendszer további vizsgálata, valamint az incidenskezelési eljárásrend szerinti intézkedések megtétele.

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

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