Nemzeti Kibervédelmi Intézet
Kormányzati Eseménykezelő Központ

Ikt. sz.: 30700-0/4871-8/2017

TLP: WHITE
Szabadon terjeszthető!

Riasztás a Petya zsarolóvírus PetrWrap variánsának kampányáról

(2017.06.27.)

Tisztelt Ügyfelünk!

A Kormányzati Eseménykezelő Központ riasztást ad ki a **PetrWrap zsarolóvírus növekvő fertőzési mutatói kapcsán.**

A kártevővel való fertőződéseket jelentettek Oroszországból, Ukrajnából, Spanyolországból, Franciaországból, az Egyesült Királyságból és Indiából is.

A PetrWrap zsarolóvírus a tavaly megjelent **Petya egyik variánsa**. A korábban észlelt WannaCry kártevőhöz hasonlóan a Windows operációs rendszerekben lévő **SMBv1 sérülékenységet (EternalBlue) használja ki** a terjedéshez, ezáltal a lokális hálózaton is képes további eszközök megfertőzésére. A sérülékenység kihasználása mellett, kéretlen levélként is terjed, amelyben **álláshirdetésre való jelentkezésnek** álcázza magát, ezzel hívja fel magára a figyelmet. A mellékletként érkező **dokumentum** tartalmaz egy parancsot, amely **letölti** a kártékony kódot.

A WannaCry zsarolóvírustól eltérően nem csak a számítógépen található **fájlokat titkosítja**, hanem felülírja és titkosítja a **Master Boot Record** (MBR) bejegyzést is. A számítógép újraindítása után nem engedi bootolni a Windows-t, helyette a saját bootloader-jét tölti be, amely megjeleníti a titkosított fájlrendszer dekódolásához szükséges instrukciókat. A titkosított fájlrendszer dekódolásáért **300 dollárnak megfelelő bitcoin** virtuális fizetőeszközt várnak a kártevő készítői.

A Kormányzati Eseménykezelő Központ a védelem első lépéseként ajánlja, hogy telepítse az EternalBlue sérülékenységre kiadott, SMB sérülékenységet foltozó javítást, amennyiben az a WannaCry fertőzés feltűnése óta még nem került telepítésre, továbbá a felhasználók legyenek

elővigyázatosak az e-mailekben csatolt dokumentumokkal szemben. Továbbá ellenőrizzék a mentőrendszerek helyes és megbízható működését, hogy fertőzés bekövetkezése esetén visszaállíthatóak legyenek a dokumentumok.

Amennyiben bekövetkezett a fertőzés, az GovCERT nem javasolja a váltságdíj megfizetését, mert nincs rá semmilyen garancia, hogy valóban feloldásra kerülnek a titkosított dokumentumok. Ilyen esetben a rendszer újratelepítése szükséges és az adatok visszaállítása a biztonsági mentésből.

Tájékoztatjuk, hogy Petya / PetrWrap zsarolóvírussal összefüggő technikai információk a GovCERT weboldalán is elérhetőek, melyeket folyamatosan aktualizálunk:

http://govcert.hu/node/381

Kormányzati Eseménykezelő Központ
GovCERT-Hungary
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@govcert.hu