NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Informacinis biuletenis „Petya“ v.2

TLP:WHITE

2017-06-28

2017-06-27 pastebėta nauja didelio masto žalingos programinės įrangos ataka „Petya“, kuri išnaudoja tuos pačius operacinės sistemos pažeidžiamumus kaip neseniai kompiuterius puolęs „WannaCry“. Pradiniai pranešimai apie viruso plitimą gauti iš Ukrainos ir Rusijos organizacijų, kurių kompiuterių tinklai tapo pirmosiomis aukomis. Tinklo kompiuteriai užkrečiami naudojantis atrastu *SMB* protokolo pažeidžiamumu *Microsoft Windows* operacinėse sistemose (šios operacinės sistemos spraga užtaisoma atnaujinimo paketu MS17-010). Naudotojų kompiuterių kietieji diskai ir prieiga prie operacinės sistemos yra užšifruojami (arba naudotojo dokumentai, jei pirmasis variantas techniškai neprieinamas), o už prieigos prie duomenų atgavimą reikalaujama išpirkos.

NKSC neturi duomenų apie paveiktas LR viešojo sektoriaus institucijas ar ypatingos svarbos informacinę infrastruktūrą.

Pažeidžiamos sistemos: visos Microsoft operacinės sistemos versijos nuo Windows XP iki Windows 10.

Kenksmingo kodo plitimui galimai yra naudojama keletas plitimo vektorių:

- Ataka per trečių šalių programinės įrangos atnaujinimo mechanizmus (pvz.: Ukrainos programinės įrangos gamintojo produktas MeDoc).
- Elektroniniai laiškai su priedais, kuriuos atidaręs naudotojas apkrečia savo sistemą.
- Nuotolinis kodo vykdymas pasinaudojant pažeidžiamomis Windows sistemomis (prievadai 445 ir 139).
- Plitimas vidiniame tinkle per užsikrėtusių naudotojų kompiuterius.

Kenksmingas kodas „Petya“, patekęs į sistemą, stengiasi paplisti tinkle prieš tai atlikęs tinklo įrenginių enumeraciją ir administratorių lygmens bendrųjų katalogų paiešką (ADMIN$). Jei naudotojas, kurio kompiuteris buvo užkrėstas, turi įrašymo teises bendrinamuose kataloguose, kenksmingas kodas perkeliamas kitiems tinklo dalyviams ir aktyvuojamas (PSEXEC pagalba).

Pažeistame kompiuteryje, papildomų įrankių pagalba (Mimikatz), gali būti perimama administratoriaus paskyros prieiga (duomenys perimami iš lsass.exe proceso), kuri vėliau panaudojama kodo platinimui tinkle. Kenksmingas kodas bando nuotoliniu būdu jungtis ir įvykdyti kodą kituose vietinio tinklo naudotojų kompiuteriuose – tam pasinaudojama Windows Management Instrumentation Command-line (WMIC) įrankiu arba jei naudotojų sistemos neturi operacinės sistemos saugumo atnaujinimo paketo (MS17-010), kenksmingas kodo platinimui pasinaudojama naujomis EternalBlue ir EternalRomance įrankių versijomis.

Jei kenksmingai programinei įrangai pavyksta gauti administratoriaus lygmens privilegijas, po priverstinio operacinės sistemos perkrovimo šifruojamas operacinės sistemos įkrovos sektorius (Master boot record - MBR) ir dokumentų išdėstymo failų sistemoje indeksas (Master file table - MFT). Po šių veiksmų naudotojui nebeįmanoma naudotis savo kompiuteriu ar jame esančiais duomenimis.

Jei kenksmingas kodas negauna privilegijų leidžiančių perrašyti MBR, be sistemos perkrovimo šifruojami naudotojo duomenys.

Rekomendacijos:

- Visiems tinkle esantiems ir ypač prie interneto prisijungusiems įrenginiams būtina ištaisyti *SMB* protokolo pažeidžiamumą (būtina įdiegiant *Microsoft* saugumo atnaujinimą MS17-010).

- Organizacijos ir įstaigos privalo turėti kritinių duomenų atsargines kopijas, kurios turėtų būti reguliariai atnaujinamos, o duomenų atstatymo mechanizmas išbandomas.
- Užkardyti prieigą prie SMB protokolo naudojamų (CIFS ir NetBios) prievadų iš išorinio pasaulio (ne vidiniame tinkle) – TCP/445, TCP/137, TCP/139, UDP/137, UDP/138 prievadų blokavimas perimetro apsaugos įrenginiuose.
- SMBv1 protokolo naudojimas gali būti uždraustas techninėmis priemonėmis, jei jis nėra naudojamas.
- Privaloma taikyti tinklo segmentaciją ir apriboti prieigą prie tinklo resursų darbuotojams pagal poreikius.
- Uždrausti WMIC įrankio naudojimą techninėmis priemonėmis.
- Atnaujinti naudojamas antivirusines programas.
- Taikyti griežtą administratoriaus privilegijų kontrolę – naudotojai, kurių tiesioginėms darbo funkcijoms atlikti administratoriaus privilegijų nereikia, negali turėti perteklinių teisių.
- Jei po kompiuterio perkrovimo pamatoma žinutė įspėjanti apie užšifravimą – nedelsiant išjungti kompiuterį rankiniu būdu, nes tarnybinių sektorių ir disko šifravimas pradedamas būtent po operacinės sistemos pakartotinio įkrovimo.

Kompromitavimo indikatoriai

Failų kontrolinės sumos (SHA256):

f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5 (signed PSEXEC.EXE)
64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1 (main 32-bit DLL)
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745 (main 32-bit DLL)
02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f (64-bit EXE)
eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998 (32-bit EXE)

Failai sistemoje:

c:\windows\dllhost.dat
c:\windows\<malware_dll> (failas be galūnės)
%TEMP%\<random name>.tmp (EXE sukuriamas failas)

Kiti indikatoriai:

PIPE: \\.\pipe\{df458642-df8b-4131-b02d-32064a2f4c19}
Automatizuoto užduočių sąrašo įrašas (Scheduled task) “shutdown -r -n”

Šaltiniai:

1. Petya Ransomware, ThaiCERT, Version 0.3 (28 June 2017)
2. https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported
3. https://securelist.com/schroedingers-petya/78870/
4. https://twitter.com/ericgeller/status/879798460421197824
5. https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759
6. https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/
7. http://misti.com/infosec-insider/news-in-a-minute/petya-ransomware-spreads-quickly-wreaks-havoc-across-the-globe

Nacionalinis kibernetinio saugumo centras
Kibernetinio saugumo ir telekomunikacijų tarnyba
prie Krašto apsaugos ministerijos
Šilo g. 5A, LT-10322 Vilnius
Tel. +370 5 210 3849, www.nksc.lt, el. p. info@nksc.lt