NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Biuletenis

TLP:WHITE

2017-05-12

Pastarąsias kelias savaites yra stebima itin didelio masto tikslinės auditorijos užkrėstų laiškų kampanija. Ši žalingos programinės įrangos ataka vadinama *WannaCry*. Nuo gegužės 12 dienos buvo pastebėta, kad kampanijos mechanizmas yra patobulintas – užkrečiami kiti kompiuteriai lokaliame tinkle naudojantis neseniai atrastu *SMB* pažeidžiamumu *Microsoft Windows* operacinėse sistemose (pažeidžiamumo kodai: CVE-2017-0143 iki CVE-2017-0148).

Tikslesnė informacija administratoriams:

Kadangi yra tik labai ribotos informacijos apie atakos vektorių, pirmas indikatorius yra tikslinės auditorijos elektroniniai laiškai (angl. *spear-phishing*), kuriuose yra prisegamas *MS Office* dokumentas su žalingos programinės įrangos makro komandomis, paremtomis *JavaScript* ar *PowerShell*. Tikslinės auditorijos žalingos programinės įrangos elektroniniai laiškai yra ganėtinai dažni ir paplitę, tačiau suveikimo tikimybė padidėjo kai buvo pasitelktas *SMB* protokolo pažeidžiamumas *Microsoft Windows* operacinėse sistemose.

Jei nors vienas kompiuteris yra pažeidžiamas lokaliame tinkle, žalinga programinė įranga automatiškai išplis pasinaudodama *SMB* protokolu, prievadais 137 ir 138 UDP, ir 139 ir 445 TCP. Itin svarbu paminėti, kad **neatnaujinti** kompiuteriai ir tinklai su *SMB* protokolu (ir anksčiau minėti prievadai) internete gali būti tiesiogiai užkrėsti be jokio pristatymo mechanizmo. Užtenka tik to, kad kompiuteriai naudojasi *SMB* protokolo sujungimais.

Naudojama žalinga programinė įranga užšifruoja bylas ir taip pat įrašo iššifravimo programinę įrangą. Tuomet yra prašoma apytiksliai 300 $ Bitcoin valiutos, kad gauti iššifravimo raktą, kuriam sukuriama grafinė sąsaja, palaikanti daugybę kalbų. Žalinga programinė įranga pasinaudoja kontroleriu ir paleidžia *Tor* vykdomąjį servisą, kad prieiti prie *Tor* tinklo.

Bylų galūnės, formatai, kuriais naudojasi žalinga programinė įranga:

- MS Office galūnės: .ppt , .doc , .docx , .xlsx , .sxi
- Mažiau populiarūs ir šalims specifiniai MS Office formatai: .sxw , .odt , .hwp
- Archyvai, medijos failai: .zip , .rar , .tar , .bz2 , .mp4 , .mkv
- El. paštai ir el. paštų duomenų bazės: .eml , .msg , .ost , .pst , .edb
- Duomenų bazių failai: .sql , .accdb , .mdb , .dbf , .odb , .myd
- Programuotojų ir projektų failai: php , .java , .cpp , .pas , .asm
- Šifravimo raktai ir sertifikatai: .key , .pfx , .pem , .p12 , .csr , .gpg , .aes
- Grafikos dizainerių, menininkų ir fotografų failai: .vsd , .odg , .raw , .nef , .svg , .psd
- Virtualių mašinų failai: .vmx , .vmdk , .vdi

Grėsmių indikatoriai (angl. *IOC*):

24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2

5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9

76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf

be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844

f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494

fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a

09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa

aee20f9188a5c3954623583c6b0e6623ec90d5cd3fdec4e1001646e27664002c

c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25

Vykdomojo failo pavadinimas:

@WanaDecryptor@.exe

Kontrolerio serveriai (*Tor* tinkle):

57g7spgrzlojinas.onion

76jdd2ir2embyv47.onion

cwwnhwhlz52ma.onion

gx7ekbenv2riucmf.onion

sqjolphimrr7jqw6.onion

xxlvbrloxvriy2c5.onion

Stebimi domenai:

iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Paveikta programinė įranga:

- Microsoft Windows Vista SP2
- Microsoft Windows Server 2008 SP2 ir R2 SP1
- Microsoft Windows 7
- Microsoft Windows 8.1
- Microsoft Windows RT 8.1
- Microsoft Windows Server 2012 ir R2
- Microsoft Windows 10
- Microsoft Windows Server 2016
- Microsoft Windows Server 2003
- Microsoft Windows XP

Rekomendacijos:

Būtina ištaisyti *SMB* pažeidžiamumą, kuris yra prieinamas *Microsoft* saugumo biuletenyje **MS17-010.** Atnaujinimai turi būti įdiegti **nedelsiant**.

Papildomi veiksmai:

- Atnaujinti sistemas apie kurias pranešė gamintojas.
- Sistemoms, kurioms nėra išleista atnaujinimų rekomenduojama užkirsti priėjimą prie tinklo arba visiškai išjungti.
- Izoliuoti prievadų 137 ir 138 UDP, 139 ir 445 TCP komunikacijas organizacijos tinkluose.
- Rasti sistemas, kurios potencialiai galėjo būti atviros grėsmei, izoliuoti, atnaujinti ar/ir išjungti.

Jei užšifruojamos bylos, rekomenduojama turėti, pasidaryti atsarginę duomenų kopiją prieš išvalant kompiuterius, kadangi iššifravimo raktas gali būti prieinamas ateityje. Žinoma, tai nėra garantas. Taip pat, perspėjame, kad apmokėjimas, norint išsipirkti duomenis, neužtikrina to, kad užpuolikas atsiųs iššifravimo raktą.

Biuletenis parengtas remiantis CERT-EU saugumo biuleteniu.

Šaltiniai:

1. https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-deransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
2. https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacksall-over-the-world/
3. https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
4. https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign
5. https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/
6. https://support.kaspersky.com/shadowbrokers
7. http://www.cio.com/article/3196667/desktop-computers/microsoft-issues-first-windows-xp-patch-in-3-years-to-stymie-wannacrypt.html

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