NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Biuletenis

TLP:WHITE

2017-05-15

Pastaruoju metu buvo stebima itin didelio masto žalingos programinės įrangos ataka „WannaCry“. Tinklo kompiuteriai užkrečiami naudojantis atrastu *SMB* pažeidžiamumu *Microsoft Windows* operacinėse sistemose (pažeidžiamumo kodai: CVE-2017-0143 iki CVE-2017-0148).

Šios atakos metu buvo užkrėsta daugiau nei 200 000 kompiuterių visame pasaulyje (tarp jų daug ligoninių ir kitų svarbių valstybinių institucijų). „WannaCry“ sulaukė didelio atgarsio dėl kelių priežasčių:

1. Virusas sparčiai plito iš kompiuterio į kompiuterį pasinaudodamas Windows sistemų pažeidžiamumu.
2. Atakai buvo panaudota kenkėjiška, išpirkos reikalaujanti programinė įranga (angl. Ransomware), kuri pasireiškia visų kompiuteryje esančių naudotojo duomenų užšifravimu ir prieigos prie šių bylų panaikinimu. Už prieigos grąžinimą ir duomenų iššifravimą buvo prašoma 300 JAV dolerių išpirkos suma (atitikmuo Bitcoin elektronine valiuta).
3. Specialistai atkreipė dėmesį į tai, kad idealiomis sąlygomis, ataka nebūtų turėjusi galimybių pasireikšti, kadangi Microsoft, keletą savaičių prieš ataką (kovo mėnesį), išleido pažeidžiamumą ištaisantį saugumo atnaujinimų paketą. Deja, daugelis organizacijų laiku neįsidiegė minėto saugumo atnaujinimų paketo arba naudojo jau nebepalaikomas Windows operacines sistemas.

Vykdant ataką, išnaudojamai SMBv1 ir SMBv2 protokolo pažeidžiamumai., kuriuos operacinė sistema naudoja bylų dalinimuisi tinkle.

WannaCry programinis kodas buvo sukurtas paveikti neatnaujintas Windows 7 ir Windows Server 2008 (arba senesnes ir nepalaikomas) versijas, tuo tarpu, pasak Microsoft, darbo stotys naudojančios Windows 10 operacines sistemas nėra paveikiamos šio pažeidžiamumo.

Užkrato vektorius yra kirminas (angl. worm), plintantis pasinaudojant SMB protokolo pažeidžiamumu. Pilnai atnaujintos Windows operacinės sistemos yra atsparios šiam kirminui, tačiau gali būti paveiktos kitais būdais (per elektroninį paštą, USB laikmenas, kitos programinės įrangos pažeidžiamumus).

Jei nors vienas kompiuteris yra pažeidžiamas vietiniame tinkle, žalinga programinė įranga automatiškai išplinta pasinaudodama SMB protokolu, prievadais 137 ir 138 UDP, ir 139 ir 445 TCP. Itin svarbu paminėti, kad **neatnaujinti** kompiuteriai ir tinklai su atvirais SMB protokolo prievadais, pasiekiamais iš interneto, gali būti tiesiogiai užkrėsti be jokio pristatymo mechanizmo.

Techninės pasekmės, užsikrėtus „WannaCry“ virusu:

Kenkėjiška programa užšifruoja ir panaikina prieigą prie dokumentų, nuotraukų ir kitų asmeninių duomenų, o už prieigos grąžinimą prašo išpirkos, taip pat automatiškai plinta į kitas darbo stotis, nereikalaudamas jokių vartotojo veiksmų, išnaudodamas Microsoft Windows operacinės sistemos kritinį pažeidžiamumą.

„WannaCry“ naudoja sudėtingą šifravimo mechanizmą, sukurdamas individualų šifravimo raktą kiekvienai iš užšifruotų bylų, kas labai apsunkina arba panaikiną bet kokią galimybę susigrąžinti prieigą prie užšifruotų duomenų.

Bylų galūnės, formatai, kuriuos žalinga programinė įranga siekia užšifruoti:

- MS Office galūnės: .ppt , .doc , .docx , .xlsx , .sxi
- Specifiniai dokumentų formatai: .sxw , .odt , .hwp
- Archyvai, medijos failai: .zip , .rar , .tar , .bz2 , .mp4 , .mkv
- El. pašto ir el. paštų archyvų failai: .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
- Grafiniai failai: .vsd , .odg , .raw , .nef , .svg , .psd
- Virtualių mašinų failai: .vmx , .vmdk , .vdi

Rekomendacijos:

Visiems tinkle esantiems ir ypač prie interneto prijungusiems įrenginiams būtina ištaisyti *SMB* pažeidžiamumą, kuris yra prieinamas įdiegiant *Microsoft* saugumo atnaujinimą **MS17-010.** Atnaujinimai turi būti įdiegti **nedelsiant**.

Papildomi veiksmai:

- Nedelsiant diegti atnaujinimo paketus sistemose, apie kurių pažeidžiamumus pranešė gamintojas.
- Sistemoms, kurioms nėra išleista atnaujinimų arba jos nebėra palaikomos, rekomenduojama apriboti prieigą prie tinklo arba visiškai išjungti.
- Esant galimybei, apriboti prievadų 137 ir 138 UDP, 139 ir 445 TCP komunikacijas organizacijos tinkluose.
- Surasti sistemas, kurios potencialiai galėjo būti atviros grėsmei, izoliuoti, atnaujinti ar/ir išjungti.
- Reguliariai daryti atsargines duomenų kopijas.
- Atnaujinti antivirusines programas, kurios jau gali aptikti ir užkardyti šią kenkėjišką programą.

Jei užšifruojamos bylos, rekomenduojama pasidaryti atsarginę duomenų kopiją prieš išvalant kompiuterius, kadangi iššifravimo raktas gali būti prieinamas ateityje. Žinoma, tokių garantijų nėra, bet sėkmingai vykdomi tyrimai kartais suteikia žinių apie iššifravimo galimybes. Taip pat, perspėjame, kad apmokėjimas, norint išsipirkti duomenis, neužtikrina to, kad užpuolikas atsiųs iššifravimo raktą.

Grėsmių indikatoriai (angl. *IOC*):

Pagrindinis vykdomasis failas:
MD5 : d5dcd28612f4d6ffca0cfeaefd606bcf
SHA1 : cf60fa60d2f461dddfdfcebf16368e6b539cd9ba
SHA256:32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf
Vykdomasis failas #2 :
MD5 :84c82835a5d21bbcf75a61706d8ab549
SHA1 :5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
SHA256:ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Zip archyvas:
md5 :b576ada3366908875e5ce4cb3da6153a
sha1 :30f8820cf93a627c66195f0d77d6a409024c6e52
sha256 :5873c1b5b246c80ab88172d3294140a83d711cd64520a0c7dd7837f028146b80

Parsiunčiami failai:

MD5 hash:
d5dcd28612f4d6ffca0cfeaefd606bcf
7328f1762bb54d68a0cad0c8e4bdeb14
39b9b37296e087c78116b2ba74918d38
079d3d5ed0a2e80fc518592d0f864c83
18c6ae712e1df5558c4b20f00d28b675

19fa1cd356c1bb535c2c1b050feb04a6
328cbad33d86bc6a092d4f7674534f39
3e0020fc529b1c2a061016dd2469ba96
4fef5e34143e646dbf9907c4374276f5
5dcaac857e695a65f5c3ef1441a73a8f
7bf2b57f2a205768755c07f238fb32cc
7e6b6da7c61fcb66f3f30166871def5b
8495400f199ac77853c53b5a3f278f3e
84c82835a5d21bbcf75a61706d8ab549
8faa0a41369d47ff17ac62db567c19a6
ad4c9de7c8c40813f200ba1c2fa33083
c17170262312f3be7027bc2ca825bf0c
f351e1fcca0c4ea05fc44d15a17f8b36

SHA1 hash:
cf60fa60d2f461dddfdfcebf16368e6b539cd9ba
4f507c08e4beb55039ccfaea9da9791e3bef9e7f
85d62fe8416943fe5f0e2b59f1bfc91607281e46
00f699cf9bbc0308f6e101283eca15a7c566d4f9
1a032d94d635cebd3246e41fe1bde7a38c4664ab
24fe98a174733ba17a1bf0c83c843b33ac53a726
3297ae295f029906a8d6c22321bc5a4ebb4aeb79
45356a9dd616ed7161a3b9192e2f318d0ab5ad10
47a9ad4125b6bd7c55e4e7da251e23f089407b8f
5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
7b10aaeee05e7a1efb43d9f837e9356ad55c07dd
911334d91fa249c8502b5e95cd5397d00e7b84be
be5d6279874da315e3080b06083757aad9b32c23
c3a91c22b63f6fe709e7c29cafb29a2ee83e6ade
d1af27518d455d432b62d73c6a1497d032f6120e
f19eceda82973239a1fdc5826bce7691e5dcb4fb
f832e0be698a3642644a1624e849b14a16c6a7f2
7d36a6aa8cb6b504ee9213c200c831eb8d4ef26b

SHA256 hash:
32f24601153be0885f11d62e0a8a2f0280a2034fc981d8184180c5d3b1b9e8cf
d92bec1998162668e1c98ffe74e8d84181272176258d4938a01c4892abae11bc
60a2c085ef37d633b178a2936caa41a7b7522a5f48b2dca72ef33263950f48c2
1027a9dd100726339a4bb335b58788feda15ccfeb553e78061caff2bb4a1f6a4
2ca2d550e603d74dedda03156023135b38da3630cb014e3d00b1263358c5f00d
402751fa49e0cb68fe052cb3db87b05e71c1d950984d339940cf6b29409f2a7c
4a25d98c121bb3bd5b54e0b6a5348f7b09966bffeec30776e5a731813f05d49e
4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
6bd686a756f23cddf49f4c17e4285ec7377742b456e38445f3a1d169b1310284
97ebce49b14c46bebc9ec2448d00e1e397123b256e2be9eba5140688e7bc0ae6
b66d05df85ef1a8ee7045b091641ff8bff7d0a097e44eda98655797b8620518e
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
c1931f33f1587427ea0e0d3c749144218766561de295688cef229c68cb38a7f9
c694f564500a728f8f21b6ccede18264d141fffd7481489c5d4c839683ae17db
d5e0e8694ddc0548d8e6b87c83d50f4ab85c1debadb106d6a6a794c3e746f4fa
e18fdd912dfe5b45776e68d578c3af3547886cf1353d7086c8bee037436dff4b
ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
1be0b96d502c268cb40da97a16952d89674a9329cb60bac81a96e01cf7356830

Registrų įrašai:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\pvbvdjax716
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\pvbvdjax716
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mssecsvc2.0

Veikla tinkle:

taskhsvc process listening on localhost:9050

Sukuriami failai ir jų direktorijos:
Užšifruotų failų galūnės pakeičiamos į .WNCRY
C:\ProgramData\pvbvdjax716\tasksche.exe
C:\ProgramData\pvbvdjax716*

Mutex:
MsWinZonesCacheCounterMutexA
MsWinZonesCacheCounterMutexA0

Vykdomojo failo pavadinimas:
@WanaDecryptor@.exe

Kontroliuojančios tarnybinės stotys (*Tor* tinkle):
57g7spgrzlojinas.onion
76jdd2ir2embyv47.onion
cwwnhwhlz52ma.onion
gx7ekbenv2riucmf.onion
sqjolphimrr7jqw6.onion
xxlvbrloxvriy2c5.onion

Killswitch domenai, kuriuos kenksmingas kodas tikrina prieš pradėdamas veikti:
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Pažeidžiama 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 2003
- Microsoft Windows XP

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/78351/wannacry-ransomware-used-in-widespread-attacks-all-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
8. https://www.trustwave.com/Resources/SpiderLabs-Blog/WannaCry--We-Want-to-Cry/
9. CCDOE bulletin: WannaCry Campaign: Potential State Involvement Could Have Serious Consequences

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*