KOS-CERT
NJESIA NACIONALE PER SIGURI KIBERNETIKE
NATIONAL COMPUTER SECURITY UNIT
NACIONALNA JEDINICA ZA KOMPJUTERSKU BEZBEDNOST

MASAT PËR MBROJTJE NGA WANNACRY RANSOMWARE

Në lidhje me kampanjën e përhapjes së programit me qëllim të keq *WannaCry ransomware*, KOS-CERT rekomandon masat e përgjithshme proaktive dhe reaktive të cilat duhet të ndermirën me qëllim të parandalimit ose reagimit në rast të infektimit.

Duhet të theksohet se janë të rrezikuar të gjithë Sistemet Operative të bazuara në Windows në të cilët nuk janë instaluar arnimet e sigurisë.

Masat proaktive

1. Përditësimi i Sistemit Operativ Windows me arnimin e sigurisë që ofrohet nga Microsoft me reference MS17-010,
2. Përditësimi i Sistemeve Operative të Windows për të cilat normalisht me nuk ofrohet mbështetje e këto sisteme janë: Windows XP, Windows 8, Windows Server 2003, Referohuni ne linkun: Customer Guidance for WannaCrypt attacks,
3. Përditësoni ueb shfletuesin me versionin e fundit,
4. Përditësimi i mjeteve softuerike të antivirusit dhe antimalware,
5. Deaktivizimi i SMBv1 (Server Message Block) protokollit përmes hapave të dokumentuara ne artikullin Microsoft Knowledge Base Article 2696547,
6. Bllokimi i trafikun SMB në hyrje në portin 445 dhe portin 139 në Router dhe Firewall
7. Kontrollimi i të gjithë fajllave ekzekutiv në hyre të infrastrukturës Ueb/Proxy
8. Analizoni se cilat sisteme në rrjetin e brendshëm mund të jenë subjekt për tu sulmuar në mënyrë që ti izoloni, përditësoni ose ç'kyqni.
9. Ndani ose izoloni ato sisteme në rrjetin e brendshëm që nuk kanë mbështetje dhe arnime të sigurisë.

Address: Rr.Bedri Pejani No. 23, 10 000 Prishtinë, Republika e Kosovës
Phone: +381 38 200-28563; Fax: + 381 38 212 399;
E-mail: info@kos-cert.org; web-site: www.kos-cert.org

10. Trajtoni të gjitha mesazhet e dyshimta të postës elektronike që përmbajnë ndonjë pjesë me qellim të keq ose ndonjë URL.

11. Njoftoni të gjithë shfrytëzuesit për kujdes gjatë hapjes së mesazheve nga posta elektronike
12. Kontrolloni statusin e të dhënave nga backup në lidhje me integritetin dhe sigurinë e tyre
13. Kufizimi i qasjes në porte të panevojshme për përdoruesit fundore.

Masat reaktive

1. Pagesa për shërbimin nuk rekomandohet (pasi që nuk garanton kthimin e të dhënave). Po ashtu nuk rekomandohet edhe ndonjë tentim për ta kontaktuar atakuesin.
2. Izolimi ç'kyqja e Sistemit nga rrjeta (mos harroni edhe lidhjet Wireless nëse ekzistojnë), në mënyrë që të ndërpritet përhapja e mëtutjeshme e programit me qellim të keq.
3. Në raste të infektimit të sistemit dhe enkriptimit te të dhënave, rekomandohet që të dhënat e enkriptuara të ruhen për të ardhmen nëse dekriptimi gjendet, edhe pse për këtë nuk ka garanci,
4. Preferohet instalim i pastër i Sistemit Operativ dhe kthimi i te dhënave nga backup nëse ekziston, si dhe përditësimi i sistemit me arnimet e fundit të sigurisë.

Udhëzimet e sigurisë

1. Në përgjithësi, mbrojtja më e mirë kundër kësaj forme të sulmit është magazinimi i shpeshtë dhe i besueshëm backup (eng. Backup) dhe ruajtjen ne një vend të ndare nga kompjuteri nga i cili janë krijuar.
2. Pajisja në të cilën behet backup në asnjë forme nuk duhet të jetë e lidhur në rrjete pasi që ransomware tenton ti enkriptoj të dhënat edhe në Hard Disk që mund të jete i lidhur me ndonjë sistem përmes rrjetës.

Address: Rr.Bedri Pejani No. 23, 10 000 Prishtinë, Republika e Kosovës
Phone: +381 38 200-28563; Fax: + 381 38 212 399;
E-mail: info@kos-cert.org; web-site: www.kos-cert.org

Me shume info për këto mund ti gjeni në linqet e mëposhtme:

Reference:

[1]http://cert.europa.eu/static/SecurityAdvisories/2017/CERT-EU-SA2017-012.pdf

[2]https://circl.lu/pub/tr-41/

[3] 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

[4] https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacksall-over-the-world/

[5] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[6] https://blog.gdatasoftware.com/2017/05/29751-wannacry-ransomware-campaign

[7] https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/

[8] https://support.kaspersky.com/shadowbrokers

[9] https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targetsout-of-date-systems/

[10] https://intel.malwaretech.com/botnet/wcrypt

[11] https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacryptattacks/

[12] https://blog.comae.io/wannacry-new-variants-detected-b8908fefea7e

[13] https://www.ccn-cert.cni.es/en/updated-security/ccn-cert-statements/4485-nomorecry-tool-ccncert-s-tool-to-prevent-the-execution-of-the-ransomware-wannacry.html

[14] https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/

[15] https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis

Address: Rr.Bedri Pejani No. 23, 10 000 Prishtinë, Republika e Kosovës
Phone: +381 38 200-28563; Fax: + 381 38 212 399;
E-mail: info@kos-cert.org; web-site: www.kos-cert.org