Caveo Information Systems Ltd
Clifden Court, Ellis Quay
Dublin 7
D07 EV81, Ireland
Tel: 01 466 1188
www.caveosystems.com

URGENT
THREAT ADVISORY – WCRY RANSOMWARE

12th May 2017

Following the large scale attacks of the WanaCrypt0r Ransomware, please find below a brief summary about the threat and the vulnerability it targets.

Threat Known Names:

- Wanna Decryptor
- WanaCrypt0r 2.0
- WannaCry

What You Should Know

- The WannaCry ransomware encrypts files on endpoints and appends the affected files with the file extension ".WCRY", ".WNRY".

- The attack leverages an SMBv2 remote code execution exploit, codenamed ETERNALBLUE, against Microsoft Windows that was made available in the Shadowbrokers dump in mid-April of this year.

- Windows patch vulnerability that it targets https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.

- The current recommendation is to ensure that the updates cited in the Microsoft Security Bulletin Summary for March 2017 are installed on endpoints, and monitor news outlets for updates.

Analysis on the WannaCry Ransomware

- From McAfee Labs
  - https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
  - https://securingtomorrow.mcafee.com/executive-perspectives/wannacry-old-worms-new/
  - https://kc.mcafee.com/corporate/index?page=content&id=KB89335

McAfee DAT - Recommendation

- VirusScan Enterprise – v**8527**
- Endpoint Protection 10.x - **2978**

Mitigation Actions

- Access Protection Rules for VSE
  - Create rules to block New File Creation and Execution of the following Extension Name
    - *.WCRY
    - *.WNCRYT
    - *.WNRY
  - Rule to block Registry Key creation
    - HKLM - /Software/WanaCrypt0r

- Perimeter Firewall – Block OUT/IN Traffic from the following IP Address Lists
  - 197.231.221.221:9001
  - 128.31.0.39:9191
  - 149.202.160.69:9001
  - 46.101.166.19:9090
  - 91.121.65.179:9001
  - 2.3.69.209:9001
  - 146.0.32.144:9001
  - 50.7.161.218:9001
  - 217.79.179.177:9001213.61.66.116:9003
  - 212.47.232.237:9001
  - 81.30.158.223:9001
  - 79.172.193.32:443
  - 38.229.72.16:443

- Web Gateway – Block
  - Rphjmrpwmfv6v2e[dot]onion
  - Gx7ekbenv2riucmf[dot]onion
  - 57g7spgrzlojinas[dot]onion
  - xxlvbrloxvriy2c5[dot]onion
  - 76jdd2ir2embyv47[dot]onion
  - cwwnhwhlz52maqm7[dot]onion

- Names of Detected Infected Files
  - @Please_Read_Me@.txt
  - @WanaDecryptor@.exe
  - @WanaDecryptor@.exe.lnk
  - Please Read Me!.txt (Older variant)C:\WINDOWS\tasksche.exe
  - C:\WINDOWS\qeriuwjhrf
  - 131181494299235.bat
  - *176641494574290.bat*
  - 217201494590800.bat
  - [0-9]{15}.bat #regex
  - !WannaDecryptor!.exe.lnk
  - 00000000.pky

- 00000000.eky00000000.res
- C:\WINDOWS\system32\taskdl.exe

I hope the information will provide with you with a better understanding on the WannaCry Ransomware and the immediate remediation actions that you can take.

If you require any further assistance, please don't hesitate to contact Caveo Systems team at Support@CaveoSystems.com anytime.

Kind regards,
Brian See