Date：2019/11/06

【Cyberattack Warning】 Lemon_Duck PowerShell malware cryptojacks enterprise networks

Subject: Lemon_Duck PowerShell malware cryptojacks enterprise networks

- Description:
  - 　TWCERT received cyber intelligence, hacker using Lemon_Duck PowerShell compromise through EternalBlue SMB exploitation. Avoiding the security mechanism, hack in the terminal system then spread and run the malware, it will brute-force attack the MS-SQL service or deploy pass-the-hash attack.
  - The propagation method are listed below:
    1. EternalBlue: Compromise through SMB exploitation
    2. USB & Network Drives: The script writes malicious Windows *.lnk shortcut files & malicious DLL files to removable storage connected to infected machines, and to mapped network drives (CVE-2017-8464)
    3. Startup files: The script writes files to startup locations on the Windows filesystem (such as the Start Menu's Startup folder) to execute during reboot
    4. MS-SQL Server brute-forcing – The script tries a variety of (really bad) passwords that might be used by the SQL Server "SA" user account.
    5. Pass the Hash attack – Leverages the NTLM hashes from the table shown above.
    6. Execution of malicious commands on remote machines using WMI.
    7. RDP Bruteforcing
  - Source of attack come from:
    - Potential C2:
      27.102.107.41
    - Potential Brute Force:
      113.140.80[.]197 - Port Scanning/Brute force (CN)
      120.253.228[.]35 - Port Scanning/Brute force port 3389 (CN)
      112.133.236[.]187 - Brute Force port 445 (India)
      58.62.125[.]245 - Brute Force port 445/Port Scanning (CN)
    - Potential Scanning:
      58.221.24[.]178 - Port Scanning (CN)
      221.4.152[.]250 - Port Scanning port 1433 (CN)
      182.140.217[.]226 - Port scanning (CN)
      1.202.15[.]246 - Port scanning port 3389 (CN)
  - Additionally the following are potential host indicators:
    - Scheduled task named Rtsa
    - Listening port of 65529
    - Service with a randomly generated name
    - Mutexes within PowerShell called LocalIf and LocalMn
- Impact platform: All Windows versions
- Recommended practices:
  1. Install the Windows SMB security update.

2. Disable the SMBv1 protocol.
3. Use strong passwords.
4. Install the Windows CVE-2017-8464 vulnerability related security update.
5. Suggested to block those listed IPs above.

Network System Division
Computer and Communication Center

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20191106_02

Last update: **2019/11/11 11:57**