

പ്രസ്താവന

റാൻസംവെയർ എന്നാൽ എന്താണ് ?

റാൻസംവെയർ ഒരു ഉപദ്രവകാരിയായ സോഫ്റ്റ്‌വെയർ ആണ്. അത് നമ്മുടെ കമ്പ്യൂട്ടറിലെ ഫയലുകളെ **encrypt** ചെയ്തു നമുക്കു ഉപയോഗിക്കാൻ പറ്റാത്ത രീതിയിൽ ആക്കി മാറ്റും. എന്നിട്ട് ആ കമ്പ്യൂട്ടർ അഥവാ മൊബൈൽ അഥവാ സെർവറിനെ തിരിച്ചു പഴയ രീതിയിൽ ആക്കി മാറ്റാൻ ആയി കാശ് ആവശ്യപ്പെടും . അടുത്തിടെ **Wannacry** എന്ന പേരിൽ ഒരു ഭയാനകമായ റാൻസംവെയർ ലോകം മുഴുവനും ബാധിച്ചു കൊണ്ടിരിക്കുകയാണ് . ലോകം ഇന്ന് വരെ കണ്ടതിൽ വെച്ച് ഏറ്റവും വലിയ റാൻസംവെയർ അറ്റാക്ക് ആണ് ഇത് . ഇന്ത്യയിലും ഇത് ബാധിച്ചിട്ടുണ്ട് .

Wannacry റാൻസംവെയർ എന്നാൽ എന്താണ് ?

Wannacry റാൻസംവെയർ വിൻഡോസ് കമ്പ്യൂട്ടറിനെ ആണ് അറ്റാക്ക് ചെയ്യുന്നത്. ഇത് **WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY** എന്നിങ്ങനെ പല പേരുകളിലായി പടരുന്നുണ്ട് .വിൻഡോസിൽ ഉള്ള **SMB** യിലെ ഒരു സെക്യൂരിറ്റി ലൂപ്ഹോൾ വഴിയാണ് ഇത് പടരുന്നത് . **Eternal Blue** എന്ന് പേരുള്ള ഒരു **vulnerability** ആണ് ഇതിനായി ഉപയോഗിക്കുന്നത് . വിൻഡോസ് **10** നു മുന്നേ ഉള്ള **MS17 -010** എന്ന സെക്യൂരിറ്റി വുൾനീറബിലിറ്റിയുടെ പാച്ച് അപ്ഡേറ്റ് ചെയ്യാത്ത എല്ലാ വിൻഡോസ് വേർഷനിലും ഇത് ബാധിക്കാവുന്നതാണ്. ഒരു കമ്പ്യൂട്ടറിൽ ഇത് ബാധിച്ചാൽ അതിലെ എല്ലാ ഫയലുകളും അത് **encrypt** ചെയ്യും. അതിനു ശേഷം **countdown** ഉള്ള ഒരു പോപ്പ് അപ്പ് കാണിക്കും. അതിൽ ഹാക്കറിനു നൽകേണ്ട **300\$** എങ്ങനെ നൽകണമെന്നും , അത് കൊടുത്തില്ലെങ്കിൽ ഫയലുകൾ ഡിലീറ്റ് ചെയ്യുന്ന തീയതിയും യൂസറിനെ കാണിക്കും. ഇത് കൂടാതെ **doublepulsar** എന്ന ഒരു **backdoor** ഉം അതിൽ ഇൻസ്റ്റാൾ ചെയ്യും.

Wannacry റാൻസംവെയർ എങ്ങനെ പടരുന്നു ?

Eternalblue എന്ന സെക്യൂരിറ്റി വുൾനീറബിലിറ്റി മുഖാന്തരം ആണ് ഇത് പരക്കുന്നത്. ഇന്റർനെറ്റിൽ ഉള്ള അനാവശ്യമായ ലിങ്ക് ക്ലിക്ക് ചെയ്യുന്നതിലൂടെയും, അറിയാത്ത ആളുകൾ അയച്ചു തരുന്ന ഇമെയിൽ അറ്റാച്ച്മെന്റ് വഴിയും ഇത് പരക്കും. ഇത് കൂടാതെ ഒരു നെറ്റ്‌വർക്കിൽ സ്വന്തമായി പടർന്നു പിടിക്കാനും ഉള്ള കഴിവ് ഇതിനുണ്ട്. ആദ്യം നെറ്റ്‌വർക്കിലെ കമ്പ്യൂട്ടറുകളെ ഇത് സ്കാൻ ചെയ്തു **eternalblue** എന്ന സെക്യൂരിറ്റി വീഴ്ച ഉണ്ടോ എന്ന് നോക്കുന്നു. ഉണ്ടെങ്കിൽ അത് വഴി ആ കമ്പ്യൂട്ടറിൽ റാൻസംവെയർ കയറ്റുന്നു. അതിനു ശേഷം ഇത് വീണ്ടും തുടർന്ന് നെറ്റ്‌വർക്കിലെ ബാക്കി ഉള്ള കമ്പ്യൂട്ടറിനെ കൂടി നശിപ്പിക്കുന്നു.

ഇത് തടയാൻ എന്ത് ചെയ്യണം ?

- മൈക്രോസോഫ്റ്റ് പുറത്തിറക്കിയ സെക്യൂരിറ്റി അപ്ഡേറ്റ് ആയ **MS17-010** എത്രയും പെട്ടെന്നു തന്നെ അപ്ഡേറ്റ് ചെയ്യണം.
- വിൻഡോസ് **NT**, വിൻഡോസ് **2000**, വിൻഡോസ് **XP** എന്നിവ പ്രൊഡക്ഷൻ എൻവിറോണമെന്റിൽ നിന്നും മാറ്റണം.
- **139, 445 , 3389** തുടങ്ങിയ പോർട്ടുകൾ ഫയർവാളിൽ തടയണം.
- അനാവശ്യമായ ലിങ്കുകൾ ക്ലിക്ക് ചെയ്യുന്നത് നിർത്തുക.
- അറിയാത്ത ആളുകൾ അയച്ചു തരുന്ന ഇമെയിൽ അറ്റാച്ച്മെന്റ് തുറക്കാതിരിക്കുക.
- വിൻഡോസിൽ ഉള്ള **SMB disable** ചെയ്യണം.
- സോഫ്റ്റ്വെയർ എല്ലാത്തന്നെ അപ്ഡേറ്റ് ചെയ്തു വെക്കണം
- ബ്രൗസറിൽ ഒരു പോപ്പ് ബ്ലോക്കർ വെക്കണം
- തുടർച്ചയായി ബാക്കപ്പ് എടുക്കണം
- നല്ല ഒരു ആന്റി വൈറസും, ആന്റി റാൻസംവെയർ സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്യണം.
- ഇത് കൂടാതെ താഴെ പറഞ്ഞിരിക്കുന്ന ലിസ്റ്റ് പ്രകാരമുള്ള ഐ.പി അഡ്രസ്സ്/ ഡൊമെയിൻസ്/ഫയൽ നെയിംസ് എന്നിവ ഫയർവാൾ/ ആന്റി വൈറസ് ഉപയോഗിച്ച് തടയണം.

IP address

16.0.5.10:135

16.0.5.10:49

10.132.0.38:80

1.127.169.36:445

1.34.170.174:445

74.192.131.209:445

72.251.38.86:445

154.52.114.185:445

52.119.18.119:445

203.232.172.210:445

95.133.114.179:445

111.21.235.164:445

199.168.188.178:445

102.51.52.149:445

183.221.171.193:445

92.131.160.60:445

139.200.111.109:445

158.7.250.29:445

81.189.128.43:445

143.71.213.16:445

71.191.195.91:445

34.132.112.54:445

189.191.100.197:445

117.85.163.204:445

165.137.211.151:445

3.193.1.89:445

173.41.236.121:445

**217.62.147.116:445
16.124.247.16:445
187.248.193.14:445
42.51.104.34:445
76.222.191.53:445
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
217.79.179.177:9001
213.61.66.116:9003
212.47.232.237:9001
81.30.158.223:9001
79.172.193.32:443
38.229.72.16:443**

Domains:

- **iuqerfsodp9ifjaposdfjhgosurijfaewrwegwea[.]com**
- **Rphjmrpwmfv6v2e[dot]onion**
- **Gx7ekbenv2riucmf[dot]onion**
- **57g7spgrzlojinas[dot]onion**
- **xxlvbrloxvriy2c5[dot]onion**
- **76jdd2ir2embyv47[dot]onion**
- **cwwnhwhlz52maq7[dot]onion**

File Names:

- **@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.eky
- 00000000.res
- C:\WINDOWS\system32\taskdl.exe

റാൻസംവെയർ സ്കൂൾ
കേരളാ പോലീസ് സൈബർ ഡോം