Files

20a569f

Go to file

.github
GPO
RaccineGUI
data_samples
images
reg-patches
robot-tests
scripts
sigma
source
tests
yara
in-memory
ext-vars-test.yar
gen_powershell_invocation.yar
gen_raccine_kills.yar
gen_ransomware_command_lin...
mal_darkside.yar
mal_emotet.yar
mal_exchange_cryptominer.yar
mal_revil.yar
other_0xa9five_poc.yar
powershell_loaders.yar
ryuk-commandlines.yar
.gitignore
LICENSE
README.md
Raccine.aps
Raccine.ico
Raccine.sln
build_dist.bat
explore.bat
install-raccine.bat

Raccine / yara / gen_ransomware_command_lines.yar

Neo23x0 fsutil usn deletejournal 8b673ef · 3 years ago History

Code Blame 62 lines (59 loc) · 2.73 KB Raw

```
rule ransomware_command_lines
{
    meta:
        description = "This is a rewrite of the formerly hard-coded program plus comman
        last_modified = "2021-07-26"
    strings:
        $e_vssadmin = "vssadmin" fullword nocase
        $e_wmic     = "wmic" fullword nocase
        $e_wbadmin  = "wbadmin" fullword nocase
        $e_bcdedit  = "bcdedit" fullword nocase
        $e_powershell  = "powershell" fullword nocase
        $e_diskshadow  = "diskshadow" fullword nocase
        $e_fsutil = "fsutil" fullword nocase

        $p_delete       = "delete" fullword nocase
        $p_shadows      = "shadows" fullword nocase
        $p_shadowstorage= "shadowstorage" fullword nocase
        $p_resize       = "resize" fullword nocase
        $p_shadowcopy   = "shadowcopy" fullword nocase
        $p_catalog      = "catalog" fullword nocase
        $p_quiet        = "-quiet" nocase
        $p_quiet2       = "/quiet" nocase
        $p_backup1      = "backup" nocase fullword
        $p_backup2      = "systemstatebackup" nocase fullword
        $p_recoveryenabled   = "recoveryenabled" fullword nocase
        $p_ignoreallfailures = "ignoreallfailures" fullword nocase
        $p_win32_shadowcopy = "win32_shadowcopy" fullword nocase
        $p_ps_version   = "-version" nocase
        $p_ps_version2  = "/version" nocase
        $p_ps_enc       = "-e" nocase
        $p_ps_enc2      = "/e" nocase
        $p_fsutil_usn   = "usn deletejournal" nocase
        $p_ps_cmds1     = "JAB"
        $p_ps_cmds2     = "SQBFAF"
        $p_ps_cmds3     = "SQBuAH"
        $p_ps_cmds4     = "SUVYI"
        $p_ps_cmds5     = "cwBhA"
        $p_ps_cmds6     = "aWV4I"
        $p_ps_cmds7     = "aQBlAHgA"
        $p_ps_cmds8     = "cwB"
        $p_ps_cmds9     = "IAA"
        $p_ps_cmdsa     = "IAB"
        $p_ps_cmdsb     = "UwB"
    condition:
            (
                ( $e_vssadmin and $p_delete and $p_shadows)
                or ( $e_vssadmin and $p_delete and $p_shadowstorage)
                or ( $e_vssadmin and $p_resize and $p_shadowstorage)
                or ( $e_wmic and $p_delete and $p_shadowcopy)
                or ( $e_wbadmin and $p_delete and $p_catalog and 1 of ($p_quiet*))
                or ( $e_wbadmin and $p_delete and 1 of ($p_backup*))
                or ( $e_bcdedit and $p_ignoreallfailures)
                or ( $e_bcdedit and $p_recoveryenabled)
                or ( $e_diskshadow and $p_delete and $p_shadows)
                or ( $e_powershell and $p_win32_shadowcopy)
                or ( $e_powershell and 1 of ($p_ps_version*))
```

```
57                  or ( $e_powershell and 1 of ($p_ps_enc*) and 1 of ($p_ps_cmds*))
58                  or ( $e_fsutil and $p_fsutil_usn )
59              )
60
61      }
```