Raccine / yara / gen_ransomware_command_lines.yar

62 lines (59 loc) · 2.73 KB

Code Blame Raw

```
rule ransomware_command_lines
{
    meta:
        description = "This is a rewrite of the formerly hard-coded program plus command line combi
        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
```

```
27              $p_win32_shadowcopy = "win32_shadowcopy" fullword nocase
28              $p_ps_version   = "-version" nocase
29              $p_ps_version2  = "/version" nocase
30              $p_ps_enc       = "-e" nocase
31              $p_ps_enc2      = "/e" nocase
32              $p_fsutil_usn   = "usn deletejournal" nocase
33              $p_ps_cmds1     = "JAB"
34              $p_ps_cmds2     = "SQBFAF"
35              $p_ps_cmds3     = "SQBuAH"
36              $p_ps_cmds4     = "SUVYI"
37              $p_ps_cmds5     = "cwBhA"
38              $p_ps_cmds6     = "aWV4I"
39              $p_ps_cmds7     = "aQBlAHgA"
40              $p_ps_cmds8     = "cwB"
41              $p_ps_cmds9     = "IAA"
42              $p_ps_cmdsa     = "IAB"
43              $p_ps_cmdsb     = "UwB"
44          condition:
45                  (
46                      ( $e_vssadmin and $p_delete and $p_shadows)
47                      or ( $e_vssadmin and $p_delete and $p_shadowstorage)
48                      or ( $e_vssadmin and $p_resize and $p_shadowstorage)
49                      or ( $e_wmic and $p_delete and $p_shadowcopy)
50                      or ( $e_wbadmin and $p_delete and $p_catalog and 1 of ($p_quiet*))
51                      or ( $e_wbadmin and $p_delete and 1 of ($p_backup*))
52                      or ( $e_bcdedit and $p_ignoreallfailures)
53                      or ( $e_bcdedit and $p_recoveryenabled)
54                      or ( $e_diskshadow and $p_delete and $p_shadows)
55                      or ( $e_powershell and $p_win32_shadowcopy)
56                      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      }
```