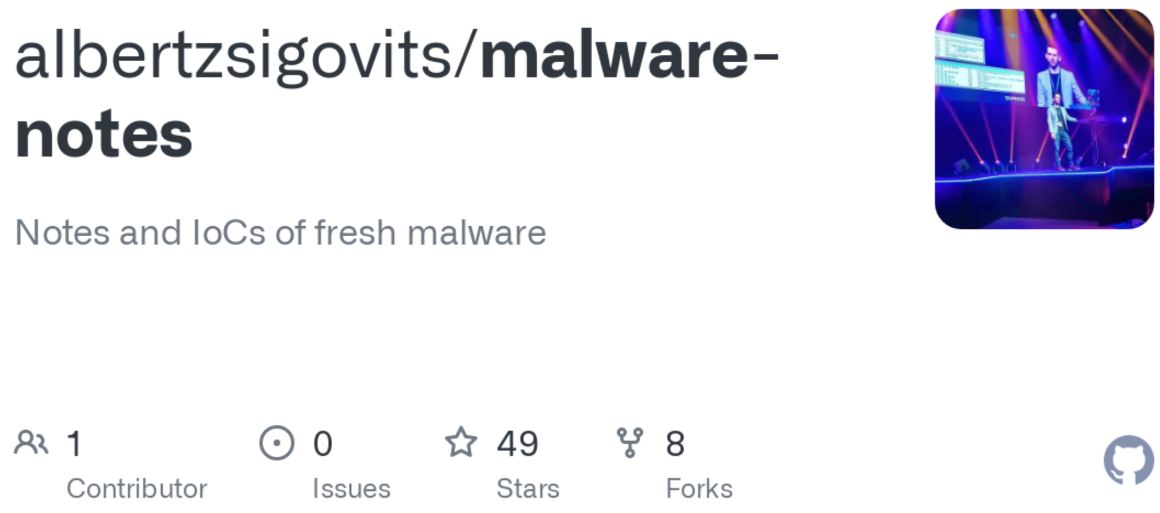
malware-notes/README.md at master · albertzsigovits/malware-notes · GitHub

github.com/albertzsigovits/malware-notes/blob/master/Ransomware-Windows-DarkBit/README.md

albertzsigovits


albertzsigovits/**malware-notes**

Notes and IoCs of fresh malware

master

Name already in use

A tag already exists with the provided branch name. Many Git commands accept both tag and branch names, so creating this branch may cause unexpected behavior. Are you sure you want to create this branch?

malware-notes/Ransomware-Windows-DarkBit/README.md

Cannot retrieve contributors at this time

DarkBit Ransomware

YARA rules:

```
rule ransomware_darkbit_ransomnote : windows ransomware darkbit {
    meta:
        author = "albertzsigovits"
        reference =
"https://twitter.com/vxunderground/status/1624814604936249345"
        date = "2023-02-13"
    strings:
        $note1 = "But, you can contact us via TOX messenger if you
want to recover your files personally." ascii wide
        $note2 = "All your files are encrypted using AES-256 military
grade algorithm." ascii wide
        $note3 = "They should pay for firing high-skilled experts."
ascii wide
        $tor =
"iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad.onion"
ascii wide
    condition:
        2 of ($note*) or $tor
}

rule ransomware_darkbit_windows_Strings : windows ransomware darkbit
{
    meta:
        author = "albertzsigovits"
        date = "2023-02-16"
        filetype = "pe"
        threat = "Ransomware.DarkBit.Windows"
        sha256 =
"9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff"
    strings:
        $goinf = " Go buildinf:"
        $mingw = "Mingw-w64 runtime failure:"
        $cgo = "_cgo_dummy_export"

        $rstr1 = "Rstrtmgr.dll"
        $rstr2 = "RmStartSession"
        $rstr3 = "RmRegisterResources"
        $rstr4 = "RmGetList"
        $rstr5 = "RmShutdown"
        $rstr6 = "RmEndSession"

        $cfg1 = "\"names\":"
        $cfg2 = "\"limits\":"
        $cfg3 = "\"extensions\":"
        $cfg4 = "\"processes\":"
        $cfg5 = "\"hostnames\":"

        $db1 = "\"darkbit.jpg\":"
        $db2 = "\"recovery_darkbit.txt\":"
        $db3 = "\"Darkbit\":"
    condition:
        uint16(0) == 0x5A4D
        and uint32(uint32(0x3C)) == 0x00004550
        and (
                ( $goinf and $mingw and $cgo and 2 of ($rstr*) and 3
of ($cfg*) )
                or
                ( 2 of ($cfg*) and 1 of ($db*) )
        )
}

rule ransomware_darkbit_windows_asm : windows ransomware darkbit {
    meta:
        author = "albertzsigovits"
        date = "2023-02-16"
        filetype = "pe"
        threat = "Ransomware.DarkBit.Windows"
        sha256 =
"9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff"
    strings:
        $gob1 = {
                    45 88 47 ??                // mov byte [r15 + 1],
r8b
                    90                        // nop
                    4C 8B 84 24 ?? ?? 00 00 // mov r8, qword [rsp +
0x88]
                    49 C1 E8 ??                // shr r8, 4
                    49 83 C7 ??                // add r15, 2
                    48 8B 44 24 ??            // mov rax, qword [rsp
+ 0x78]
                    4C 8B 8C 24 ?? ?? 00 00    // mov r9, qword [rsp
+ 0xb0]
                    48 89 D0                // mov rax, rdx
                    48 8B 94 24 ?? ?? 00 00    // mov rdx, qword [rsp
+ 0xc0]
                    4C 89 84 24 ?? ?? 00 00    // mov qword [rsp +
0x88], r8
                    41 ?? ?? ??                // and r8d, 0xf
                    49
        }

        $gob2 = {
                    48 89 84 24 ?? ?? 00 00    // mov qword ptr ss:
[rsp+D0],rax
                    48 89 5C 24 ??            // mov qword ptr ss:
[rsp+60],rbx
                    31 C0                    // xor eax,eax
                    48 8D 5C 24 ??            // lea rbx,qword ptr
ss:[rsp+44]
                    B9 ?? 00 00 00            // mov ecx,6
        }

        $wyhash = {
                    4D 8B 88 ?? ?? 00 00            // mov r9, qword
```

```
[r8 + 0xf0]
                    49 BA 2F 64 BD 78 64 1D 76 A0    // movabs r10,
0xa0761d6478bd642f
                    4D 01 D1                        // add r9, r10
                    49 BB DB 28 B4 A0 D1 7E 03 E7    // movabs r11,
0xe7037ed1a0b428db
                    4D 31 CB                        // xor r11, r9
        }

        $vss1 = {
                    48 8B 94 24 ?? ?? 00 00        // mov rdx,qword
ptr ss:[rsp+C8] [rsp+C8]:"delete"
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+138],rdx [rsp+138]:"delete"
                    48 8B 54 24 ??                // mov rdx,qword
ptr ss:[rsp+58]
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+140],rdx
                    48 8B 94 24 ?? ?? 00 00        // mov rdx,qword
ptr ss:[rsp+F0] [rsp+F0]:"shadows"
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+148],rdx [rsp+148]:"shadows"
                    48 8B 94 24 ?? ?? 00 00        // mov rdx,qword
ptr ss:[rsp+80]
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+150],rdx
                    48 8B 94 24 ?? ?? 00 00        // mov rdx,qword
ptr ss:[rsp+C0] [rsp+C0]:"/all"
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+158],rdx [rsp+158]:"/all"
                    48 8B 54 24 ??                // mov rdx,qword
ptr ss:[rsp+50]
                    48 89 94 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+160],rdx
                    48 89 84 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+168],rax [rsp+168]:"/Quiet"
                    48 89 9C 24 ?? ?? 00 00        // mov qword ptr
ss:[rsp+170],rbx
                    48 8B 84 24 ?? ?? 00 00        // mov rax,qword
ptr ss:[rsp+D0] [rsp+D0]:"vssadmin.exe"
                    48 8B 5C 24 ??                // mov rbx,qword
ptr ss:[rsp+60]
                    48 8D 8C 24 ?? ?? 00 00        // lea rcx,qword
ptr ss:[rsp+138] [rsp+138]:"delete"
        }

        $vss2 = {
                    48 BA CB BB 16 11 B4 B1 42     // mov
rdx,AD42B1B41116BBCB
                    48 89 94 24 ?? ?? 00 00         // mov qword ptr
ss:[rsp+B1],rdx
                    48 BA  6D A1 5B 11 15 7B 7B    // mov
```

```
rdx,7B7B15115BA16DAD
                    48 89 94 24 ?? ?? 00 00            // mov qword
ptr ss:[rsp+B8],rdx
                    48 BA 9D C8 65 70 D0 DC 2B C3    // mov
rdx,C32BDCD07065C89D
                    48 89 94 24 ?? ?? 00 00            // mov qword
ptr ss:[rsp+A2],rdx
                    48 BA C3 4D C5 3E 7D 70 0F 1E    // mov
rdx,1E0F707D3EC54DC3
                    48 89 94 24 ?? ?? 00 00            // mov qword
ptr ss:[rsp+A9],rdx
        }

    condition:
        uint16(0) == 0x5A4D
        and uint32(uint32(0x3C)) == 0x00004550
        and 3 of them
}
```

DarkBit diary:

```
SHA256:
9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff
Packer: None
Compile time: 2023-02-11 22:10:54
PEInfo: PE32+ executable (console) x86-64 (stripped to external PDB),
for MS Windows
Language: Golang (CGO)
Obfuscation: Gobfuscate
Hashing: Wyhash hash algorithm and wyrand PRNG
Ransomware Mutex: Global\dbdbdbdb

Ransomware Note: RECOVERY_DARKBIT.txt
SHA256:
fca050431ba94630d691a7d6cbdd491354c69f738b0d8e03b531173a741ad286

TOR:
hxxp://iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad[.]oni
on/support
TOX ID:
AB33BC51AFAC64D98226826E70B483593C81CB22E6A3B504F7A75348C38C862F00042
F5245AC
Telegram: DarkBitChannel
Twitter: DarkBitTW
```

DarkBit parameters:

```
-h | Help
-all | Run on all without timeout counter
-domain | Domain
-force | Force blacklisted computers
-list | List
-nomutex | Force not checking mutex
-noransom | No encryption
-password | Password
-path | Path
-t | Threads
-username | Username
```

VirusTotal perks:

```
vhash:0560b76d5555151c051d1az3f1d&z1
authentihash:8a1db8d4c117daa25ab31735b9866cb989907cf524fe2c052ffa9e67
f582c79c
imphash:9bcadd8ed34a63728178995d1b006421
ssdeep:"49152:S4mkYp+03HbhndpeoVK9/0cjXd77yg6PxHuy7vDKD12K5EKGHg1q14g
UynCLgIMk:UF31ed/XB7AbvbAEKGpTI7"
behaviour_files:"%HOMEPATH%\\recovery_darkbit.txt"
behaviour_files:"%HOMEPATH%\\appdata\\recovery_darkbit.txt"
behaviour:"Global\\dbdbdbdb"
behaviour:"\\Sessions\\1\\BaseNamedObjects\\Global\\dbdbdbdb"
```

Config template:

```
        "limits": [
                "limitMB": 25,
                "parts": 1,
                "eachPart": -1
            },
            {
                "limitMB": 1000,
                "parts": 2,
                "eachPart": 12000
            },
            {
                "limitMB": 4000,
                "parts": 3,
                "eachPart": 10000
            },
            {
                "limitMB": 7000,
                "parts": 2,
                "eachPart": 20000
            },
            {
                "limitMB": 11000,
                "parts": 3,
                "eachPart": 30000
            },
            {
                "limitMB": 51000,
                "parts": 5,
                "eachPart": 30000
            },
            {
                "limitMB": 1000000,
                "parts": 3,
                "eachPart": 1000000
            },
            {
                "limitMB": 5000000,
                "parts": 5,
                "eachPart": 1000000
            },
            {
                "limitMB": 6000000,
                "parts": 20,
                "eachPart": 10000000
            }
        ],
        "extensions": {
            "msilog": 1,
            "log": 1,
            "ldf": 1,
            "lock": 1,
            "theme": 1,
        "msi": 1,
        "sys": 1,
        "wpx": 1,
        "cpl": 1,
        "adv": 1,
        "msc": 1,
        "scr": 1,
        "key": 1,
        "ico": 1,
        "dll": 1,
        "hta": 1,
        "deskthemepack": 1,
        "nomedia": 1,
        "msu": 1,
        "rtp": 1,
        "msp": 1,
        "idx": 1,
        "ani": 1,
        "386": 1,
        "diagcfg": 1,
        "bin": 1,
        "mod": 1,
        "ics": 1,
        "com": 1,
        "hlp": 1,
        "spl": 1,
        "nls": 1,
        "cab": 1,
        "diagpkg": 1,
        "icl": 1,
        "ocx": 1,
        "rom": 1,
        "prf": 1,
        "themepack": 1,
        "msstyles": 1,
        "icns": 1,
        "mpa": 1,
        "drv": 1,
        "cur": 1,
        "diagcab": 1,
        "exe": 1,
        "cmd": 1,
        "shs": 1,
        "Darkbit": 1
    },
    "names": {
        "thumbs.db": 1,
        "desktop.ini": 1,
        "darkbit.jpg": 1,
        "recovery_darkbit.txt": 1,
        "system volume information": 1
    },
    "processes": [],
        "hostnames": [
                --- LIST OF TARGET HOSTNAMES ---
                ]
```

Ransom note:

```
Dear Colleagues,
We’re sorry to inform you that we’ve had to hack Technion network
completely and transfer “all” data to our secure servers.
So, keep calm, take a breath and think about an apartheid regime that
causes troubles here and there.
They should pay for their lies and crimes, their names and shames.
They should pay for occupation, war crimes against humanity,
killing the people (not only Palestinians’ bodies, but also Israelis’
souls) and destroying the future and all dreams we had.
They should pay for firing high-skilled experts.

Anyway, there is nothing for you (as an individual) to be worried.
That’s the task of the administration to follow up our instruction
for recovering the network.
But, you can contact us via TOX messenger if you want to recover your
files personally. (TOX ID:
AB33BC51AFAC64D98226826E70B483593C81CB22E6A3B504F7A75348C38C862F00042
F5245AC)

Our instruction for the administration:
All your files are encrypted using AES-256 military grade algorithm.
So,
        1. Don't try to recover data, because the encrypted files are
unrecoverable unless you have the key.
        Any try for recovering data without the key (using third-
party applications/companies) causes PERMANENT damage. Take it
serious.
        2. You have to trust us. This is our business (after firing
from high-tech companies) and the reputation is all we have.
        3. All you need to do is following up the payment procedure
and then you will receive decrypting key using for returning all of
your files and VMs.
        4. Payment method:
                Enter the link below

http://iw6v2p3cruy7tqfup3yl4dgt4pfibfa3ai4zgnu5df2q3hus3lm7c7ad.onion
/support
                Enter the ID below and pay the bill (80 BTC)
                        $TARGETID
You will receive decrypting key after the payment.

Notice that you just have 48 hours. After the deadline, a 30% penalty
will be added to the price.
We put data for sale after 5 days.
Take it serious and don’t listen to probable advices of a stupid
government.

Good Luck!
“DarkBit”
```