BADAN SIBER DAN SANDI NEGARA

Jalan Harsono R.M. Nomor 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550
Telepon (021) 7805814, Faksimile (021) 78844104
***Website* : https://bssn.go.id, *E-mail* : humas@bssn.go.id**

INDICATOR OF COMPROMISE BRAIN CIPHER RANSOMWARE

RILIS : 27 JUNI 2024

No	*Indicator Of Compromise*	*Hash*	*File*	*Path*
1.	c60a0b99729eb6d95c2d9f8b76b9714411a3a751	SHA1	Win_old.exe	C:\User\itadmin\music\
2.	9c5698924d4d1881efaf88651a304cb3	MD5	Win_old.exe	C:\User\itadmin\music\
3.	935c0b39837319fda571aa800b67d997b79c3198	SHA1	Win.exe	Any Path
4.	448f1796fe8de02194b21c0715e0a5f6	MD5	Win.exe	Any Path

No	*Indicator Of Compromise*	*Hash*
1.	07612eed1e0341bcff08870f8a47df488318cee57bd1fb64709c0a5dc8635340	SHA256
2.	0ed5729655b3f09c29878e1cc10de55e0cbfae7ac344f574d471827c256cf086	SHA256
3.	1ddacee1d2593697027955716903 7a335b362f86c3797ded625d68077bd0145c	SHA256
4.	6e07da23603fbe5b26755df5b8fec19cadf1f7001b1558ea4f12e20271263417	SHA256
5.	917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2	SHA256
6.	eb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12	SHA256
7.	6c1b646e002e45688d750e5feb47fc3d6f514b77	SHA1

No	*Indicator Of Compromise*	*Hash*
8.	870865aad7c7cccafbca0c1f50f7eecaedbd4bf1	SHA1
9.	968c4ae64dcb71c9eeffd812ef38a69d5548b3bb	SHA1
10.	9cb96848386327410ca588b6cd5f6401	MD5
11.	deb2e0756d331362d57ad9fe408c4ff3	MD5
12.	eebb7935dfe2a521bd5253c7e4660fb4	MD5
13.	131.253.33.203	IPv4
14.	184.25.191.235	IPv4
15.	20.99.133.109	IPv4
16.	20.99.186.246	IPv4
17.	204.79.197.203	IPv4
18.	http://mybmtbgd7aprdnw2ekxht5qap5daam2wch25coqerrq2zdioanob34ad.onion	url
19.	brain.support@cyberfear.com	email

Yara Rules Based Signature Detection

```
rule braincipher_ransom {
    meta:
        description = "Detection rule for braincipher ransomware behavior
and known indicators"
    strings:
        $behavior1 = { 33 D2 4D ?? ?? 01 8B C7 FF C7 F7 F6 42 0F B? ?? ??
41 3? 4? FF 3B FB }
        $behavior2 = { 48 8? ?? E8 ?? ?? 00 00 FF D3 4C }
        $behavior3 = "auth_timestamp:" ascii
        $behavior4 = "auth_signature:" ascii
        $behavior5 = "&act=check" ascii
        $sha256_1 =
"07612eed1e0341bcff08870f8a47df488318cee57bd1fb64709c0a5dc8635340"
        $sha256_2 =
"0ed5729655b3f09c29878e1cc10de55e0cbfae7ac344f574d471827c256cf086"
        $sha256_3 =
"1ddacee1d2593697027955716903 7a335b362f86c3797ded625d68077bd0145c"
        $sha256_4 =
"6e07da23603fbe5b26755df5b8fec19cadf1f7001b1558ea4f12e20271263417"
        $sha256_5 =
"917e115cc403e29b4388e0d175cbfac3e7e40ca1742299fbdb353847db2de7c2"
        $sha256_6 =
"eb82946fa0de261e92f8f60aa878c9fef9ebb34fdababa66995403b110118b12"
        $sha1_1 = "c60a0b99729eb6d95c2d9f8b76b9714411a3a751"
        $sha1_2 = "935c0b39837319fda571aa800b67d997b79c3198"
        $sha1_3 = "6c1b646e002e45688d750e5feb47fc3d6f514b77"
        $sha1_4 = "870865aad7c7cccafbca0c1f50f7eecaedbd4bf1"
        $sha1_5 = "968c4ae64dcb71c9eeffd812ef38a69d5548b3bb"
        $md5_1 = "9c5698924d4d1881efaf88651a304cb3"
        $md5_2 = "448f1796fe8de02194b21c0715e0a5f6"
        $md5_3 = "9cb96848386327410ca588b6cd5f6401"
        $md5_4 = "deb2e0756d331362d57ad9fe408c4ff3"
        $md5_5 = "eebb7935dfe2a521bd5253c7e4660fb4"
        $ip1 = "131.253.33.203"
        $ip2 = "184.25.191.235"
        $ip3 = "20.99.133.109"
        $ip4 = "20.99.186.246"
        $ip5 = "204.79.197.203"
        $url =
"http://mybmtbgd7aprdnw2ekxht5qap5daam2wch25coqerrq2zdioanob34ad.onion"
        $email = "brain.support@cyberfear.com"

    condition:
        uint16(0) == 0x5A4D and
        uint32(uint32(0x3c)) == 0x00004550 and
```

```
        (
            any of ($behavior*) or
            any of ($sha256*) or
            any of ($sha1*) or
            any of ($md5*) or
            any of ($ip*) or
            $url or
            $email or
            pe.imphash() == "41fb8cb2943df6de998b35a9d28668e8"
        )
}
```

Yara Rules Based Behavior Detection

```
rule BrainCipher_Ransomware
{
    meta:
        description = "Identify Brain Cipher Ransomware samples found in the
wild"
    strings:
        // 8B75 0C             mov esi,dword ptr ss:[ebp+C]
        // AD                  lodsd
        // 35 FF5F0310         xor eax,10035FFF
        // 50                  push eax
        // E8 6FFEFFFF         call 00B85C24
        // 85C0                test eax,eax
        // 0F84 23010000     je 00B85EE0
        // 8B7D 08             mov edi,dword ptr ss:[ebp+8]
        // 83C7 04             add edi,4
        $1 = { 8b 75 0c ad 35 ff 5f 03 10 50 e8 6f fe ff ff 85 c0 0f 84 23 01 00
00 8b 7d 08 83 c7 04 }
        // 83C4 F4             add esp,FFFFFFF4
        // 56                  push esi
        // C745 FC 00000000     mov dword ptr ss:[ebp-4],0
        // C745 F8 00000000     mov dword ptr ss:[ebp-8],0
        // E8 46EDFEFF         call 00B81640
        // 8BC8                mov ecx,eax
        // 8D45 F4             lea eax,dword ptr ss:[ebp-C]
        // 50                  push eax
        // 51                  push ecx
        // FF15 2C57BA00         call dword ptr ds:[BA572C]
        // 8945 F8             mov dword ptr ss:[ebp-8],eax
        // 837D F8 00          cmp dword ptr ss:[ebp-8],0
        // 74 2B               je 00B9293B
        // 837D F4 02          cmp dword ptr ss:[ebp-C],2
        // 72 25               jb 00B9293B
        // 8B75 F8             mov esi,dword ptr ss:[ebp-8]
        $2 = { 83 c4 f4 56 c7 45 fc 00 00 00 00 c7 45 f8 00 00 00 00 e8 46 ed fe
ff 8b c8 8d 45 f4 50 51 ff 15 2c 57 42 00 89 45 f8 83 7d f8 00 74 2b 83 7d f4 02
72 25 8b 75 f8 }
        // 8BC1             mov eax,ecx
        // 33D2             xor edx,edx
        // F7F6             div esi
        // 8AC1             mov al,cl
        // 8A1417           mov dl,byte ptr ds:[edi+edx]
        // 025405 00        add dl,byte ptr ss:[ebp+eax]
        // 02D3             add dl,bl
        // 8A5C15 00        mov bl,byte ptr ss:[ebp+edx]
        // 8A541D 00        mov dl,byte ptr ss:[ebp+ebx]
        // 865405 00        xchg byte ptr ss:[ebp+eax],dl
        // 88541D 00        mov byte ptr ss:[ebp+ebx],dl
        // 41               inc ecx
        // 81F9 00030000     cmp ecx,300
        // 75 D6            jne 00B993AE
        // 5D               pop ebp
        // 33C9             xor ecx,ecx
        // 8B7D 0C          mov edi,dword ptr ss:[ebp+C]
        // BE 40000000      mov esi,40
        // 55               push ebp
        // 8B6D 10          mov ebp,dword ptr ss:[ebp+10]
```

```
        // 33C9             xor ecx,ecx
        // 8B7D 0C          mov edi,dword ptr ss:[ebp+C]
        // BE 40000000      mov esi,40
        // 55               push ebp
        // 8B6D 10          mov ebp,dword ptr ss:[ebp+10]
        $3 = { 8b c1 33 d2 f7 f6 8a c1 8a 14 17 02 54 05 00 02 d3 8a 5c 15 00 8a
54 1d 00 86 54 05 00 88 54 1d 00 41 81 f9 00 03 00 00 75 d6 5d 33 c9 8b 7d 0c be
40 00 00 00 55 8b 6d 10 }

    condition:
        uint16(0) == 0x5a4d and filesize < 170KB and ($1 or $2 or $3)
}
```