DarkCloud Stealer Triage

c3rb3ru5d3d53c.github.io/malware-blog/darkcloud-stealer/

October 1, 2022

2022-10-01

3 min read

malware

Placeholder

> Protected with .NET Reactor

I obtained a sample of DarkCloud Stealer from @*James_inthe_box*, which is a 7zip compressed (fc55a2bd0a266b8eca264b9b74afff9d373746910035d18c901ac718b6c3948f). Once extracted, it results in the file FILENAME (3dbcb27a7f441b6f3d6e47d9ae69c69a1af582b3e5c0dce44642e5d0ad0cf566), which is packed with .NET reactor.

Persistence

Next, it establishes persistence with the command.

```
"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\jDDrSpcG" /XML
"C:\Users\admin\AppData\Local\Temp\tmp3332.tmp"
```

PE Injection

Once persistence is established, it will create the new process *RegSvcs.exe*, to perform PE injection. Next, it writes DarkCloud to this new process and resuming the thread.

DarkCloud Stealer

DarkCloud Stealer is written in Visual Basic.

String Decryption

- Function to Decrypt Key
- Function to Decrypt String
- Multiple Keys and Encrypted Strings

Stupid Ass VB Functions

Function	Description
rtcMidCharBstr	Get first character from string
rtcAnsiValueBstr	Get ascii char from BSTR

Decryption Routine (in-progress)

```
#!/usr/bin/env python

import sys

# reminder: add sanity/bounds checks

# second loop data [79, 2, 249, 45, 137, 239, 59, 183, 30, 108, 22, 55, 60, 0, 10, 35, 36,
159, 253, 24, 82, 216, 105, 235, 167, 68, 67, 236, 113, 201, 129, 5, 69, 199, 32, 135, 251,
52, 83, 132, 240, 160, 54, 165, 57, 176, 221, 120, 150, 78, 232, 88, 215, 126, 121, 17, 96,
62, 128, 107, 179, 172, 85, 70, 12, 241, 182, 97, 28, 173, 226, 207, 99, 16, 44, 162, 250, 91,
6, 64, 210, 243, 112, 227, 218, 116, 73, 244, 134, 81, 53, 7, 248, 111, 26, 170, 47, 198, 110,
77, 138, 41, 37, 148, 161, 40, 229, 8, 141, 13, 163, 72, 233, 1, 15, 149, 146, 145, 152, 123,
143, 51, 157, 186, 238, 168, 104, 246, 48, 144, 84, 122, 109, 255, 101, 155, 93, 20, 94, 180,
139, 147, 187, 130, 219, 46, 125, 213, 208, 142, 25, 230, 118, 223, 63, 23, 237, 92, 190, 49,
220, 193, 19, 214, 158, 95, 203, 184, 103, 194, 76, 71, 169, 39, 225, 31, 14, 3, 124, 178,
151, 153, 166, 212, 202, 90, 196, 242, 98, 33, 224, 197, 171, 117, 228, 29, 136, 211, 252,
102, 131, 4, 74, 234, 177, 205, 192, 254, 61, 100, 127, 50, 185, 191, 66, 27, 58, 80, 154,
174, 75, 38, 87, 21, 247, 114, 89, 204, 188, 195, 200, 156, 175, 140, 222, 86, 217, 181, 106,
209, 11, 245, 56, 34, 119, 189, 133, 43, 164, 231, 115, 9, 42, 18, 206, 65]

key = '5FF6E95651251C1B1875F6CCF66962'
ciphertext = 'OLICXaFwrQFFIPecOjalDht'

def decrypt(key, ciphertext):
    index = [x for x in range(0, 255 + 1)]
    tmp = ''
    while True:
        tmp += ciphertext
        if len(tmp) > 255: break
    tmp = tmp[:256]
    count = 0
    mod = 0
    while True:
        if 255 < count: break
        a = index[count] + mod
        c = a + ord(tmp[count]) & 0x800000ff
        if c < 0:
            c = (c - 1 | 0xffffff00) + 1
        mod = c
        b = index[count]
        index[count] = index[c]
        index[c] = b
        count += 1
    count = 0
    c = 0
    print(index)
    # ecx == tmp
    # iModifier = 0
    # for uCount in range(0, 255):
    #     al = index[uCount]
    #     uVar8 = edx + tmp[uCount] & 0x800000ff
    #     edx = tmp[uCount] + uVar8
    # return tmp

# ecx == values from 0 -> 255
# ecx+esi == *values 0 -> 255
```

```
result = decrypt(key, ciphertext)
print(result)
```

Indicators of Compromise

Type	Indicator	Description
SHA256	fc55a2bd0a266b8eca264b9b74afff9d373746910035d18c901ac718b6c3948f	DarkCloud Stealer 7zip
SHA256	3dbcb27a7f441b6f3d6e47d9ae69c69a1af582b3e5c0dce44642e5d0ad0cf566	DarkCloud Loader
SHA256	16c82a196dc8c41903a39bf00a01191f1a4357ed6861a7127ee7472f7fb565fc	DarkCloud Stealer (Unpacked)
SHA256	14b7a96e28f1bcfbf376992ee7dbf1a019dd41b1f4bb2b342772b092908d6008	DarkCloud Stealer Module? .NET?
SHA256	c4dd9ff9f514614ab4b4f7f6aee0e46e91aa91bcfe6f144d436b863024158c28	DarkCloud Stealer Module Loader

#lockbit #reversing #malware #analysis

Next Reversing Additional Lockbit 3.0 API Hashing