DTrack

github.com/jeFF0Falltrades/IoCs/blob/master/APT/dtrack_lazarus_group.md

jeFF0Falltrades

jeFF0Falltrades/ **IoCs**

A collection of Indicators of Compromise (IoCs), most aligning with samples derived from the signatures in the YARA-Signatures repo

1 Contributor | 0 Issues | 27 Stars | 2 Forks

Utilized by North Korean APT "Lazarus Group"; Not to be confused with ATMDtrack

Reporting

YARA

```
rule dtrack_2020 {
    meta:
        author = "jeFF0Falltrades"

    strings:
        $pdb = "Users\\user\\Documents\\Visual Studio
2008\\Projects\\MyStub\\Release\\MyStub.pdb" wide ascii
        $str_log = "----------------------------- Log File Create...."
wide ascii
        $str_ua = "CCS_Mozilla/5.0 (Windows NT 6.1" wide ascii
        $str_chrome = "Local Settings\\Application
Data\\Google\\Chrome\\User Data\\Default\\History" wide ascii
        $str_tmp = "%s\\~%d.tmp" wide ascii
        $str_exc = "Execute_%s.log" wide ascii
        $str_reg_use = /net use \\\\[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.
[0-9]{1,3}\\C\$ \/delete/
        $str_reg_move = /move \/y %s \\\\[0-9]{1,3}\.[0-9]{1,3}\.[0-9]
{1,3}\.[0-9]{1,3}\\C\$\\Windows\\Temp\\MpLogs\\/
        $hex_1 = { d1 ?? 33 ?? fc 81 ?? ff 00 00 00 c1 ?? 17 }
        $hex_2 = { c1 ?? 08 8b ?? fc c1 ?? 10 }
        $hex_3 = { 81 0D [4] 1C 31 39 29 }
    condition:
        2 of them or $hex_3
}
```

Sample Hashes

```
3cc9d9a12f3b884582e5c4daf7d83c4a510172a836de90b87439388e3cde3682
bfb39f486372a509f307cde3361795a2f9f759cbeb4cac07562dcbaebc070364
51ac3966b48c91947de4ce51a90aee9deb730d86cedf8c863d9dcdf0fb322537
61c1b9afa2347c315a6b4628f9dff3ada6f8d040345402d4708881f05b1ec48b
ee9cd8decf752a47eefe24369a806976dce8ac2c29a8271c68bc407326fb19a9
791c59a0d6456ac1d9976fe82dc6b13f3e5980c6cfa2fd9d58a3cc849755ea9f
93a01fbbdd63943c151679d037d32b1d82a55d66c6cb93c40ff63f2b770e5ca9
a0664ac662802905329ec6ab3b3ae843f191e6555b707f305f8f5a0599ca3f68
c5c1ca4382f397481174914b1931e851a9c61f029e6b3eb8a65c9e92ddf7aa4c
b0bf63300fd4f6a0b1544663b6326c250086369b128d241287d150e6e6409fd8 (test
file)
1ba8cba6337da612d1db2cdfe1b44f6110741d91ba696a5b125ebd3e9b081ed7
4701cc722f03253fb332747f951fff4c4ff023e13096a7e090a22b95c70efbf3
```