IoCs/APT/micropsia_apt_c_23.md at master · jeFF0Falltrades/IoCs

By jeFF0Falltrades

Archived: 2026-04-06 00:05:14 UTC

MICROPSIA (APT-C-23)

Reporting

- https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/
- https://research.checkpoint.com/apt-map/
- https://www.clearskysec.com/micro-kasper/

YARA

```
rule micropsia_2018 {
 meta:
    author = "jeFF0Falltrades"
    hash = "4c3fecea99a469a6daf2899cefe93d9acfd28a0b6c196592da47e917c53c2c76"

 strings:
    $gen_app_id = { 53 31 DB 69 93 08 D0 68 00 05 84 08 08 42 89 93 08 D0 68 00 F7 E2 89 D0 5B C3 } /
    $get_temp_dir = { 68 00 04 00 00 8d 44 24 04 50 8b c7 e8 [4] 8b e8 55 e8 [2] fe ff } // 0x0042C6
    $str_install_appid = "ApppID.txt" wide ascii nocase

 condition:
    2 of them
}
```

Sample Hashes

```
 effa0e01adad08ae4bc787678ce67510d013a06d1a10d39ec6b19e2449e25fbd
26594039f3e5e1f3d592cb4b0f274891397c94b4ca63c7d3b43c1853c48e7281
c96138fd93b18e5a1682f6d4405e724b88058e4d57a4e9566ff96a87a560bc18
33e901018808514def3c2d71ae54c1f38ea25675243a815937af3ada0de25808
4c3fecea99a469a6daf2899cefe93d9acfd28a0b6c196592da47e917c53c2c76
0732672e4274ba03e58cadceadf18c8ccb4ee6b7b643b96aff1675e708f1c514
e36c51f19362447881e3953271fe1da835f2919a50e9e761f4ccffe3d52b23a7
```

```
fe90cb8d549481833bf72ff7f9e1fdad72e5b886cfa52033771bbb0034b23c32
ae254ab021632cb583071079b2be8af62ccfc232c687a515a716ea17bfa0db9b
```

Delivery URLs

```
https[:]//tinyurl[.]com/7412593655 --> https[:]//uc4688d6b7cd62aec5fe2018c3d1[.]dl[.]dropboxusercontent[.]com/
```

Source: https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/micropsia_apt_c_23.md