citizenlab / **malware-signatures**

Branch: master ▾ **malware-signatures** / malware-families / **bangat.yara**

Find file Copy path

Te-k Move rules and update IOCs 6d10393 on Nov 17, 2016

1 contributor

45 lines (38 sloc) 1009 Bytes

```
private rule BangatCode : Bangat Family
{
    meta:
        description = "Bangat code features"
        author = "Seth Hardy"
        last_modified = "2014-07-10"

    strings:
        // dec [ebp + procname], push eax, push edx, call get procaddress
        $ = { FE 4D ?? 8D 4? ?? 50 5? FF }

    condition:
        any of them
}

private rule BangatStrings : Bangat Family
{
    meta:
        description = "Bangat Identifying Strings"
        author = "Seth Hardy"
        last_modified = "2014-07-10"

    strings:
        $lib1 = "DreatePipe"
        $lib2 = "HetSystemDirectoryA"
        $lib3 = "SeleaseMutex"
        $lib4 = "DloseWindowStation"
        $lib5 = "DontrolService"
        $file = "~hhC2F~.tmp"
        $mc = "~_MC_3~"

    condition:
       all of ($lib*) or $file or $mc
}

rule Bangat : Family
{
    meta:
        description = "Bangat"
        author = "Seth Hardy"
        last_modified = "2014-07-10"

    condition:
        BangatCode or BangatStrings
}
```