

IoCs/APT/poshc2_apt_33.md at master · jeFF0Falltrades/IoCs

By jeFF0Falltrades

Archived: 2026-04-05 20:42:08 UTC

PoshC2 (specifically as used by APT33)

Reporting

- <https://malpedia.caad.fkie.fraunhofer.de/details/win.poshc2>
- <http://www.rewterz.com/rewterz-news/rewterz-threat-alert-iranian-apt-uses-job-scams-to-lure-targets>
- https://twitter.com/cti_marc/status/1194573048625729536

YARA

```
rule poshc2_apt_33_2019 {
  meta:
    author = "jeFF0Falltrades"
    desc = "Alerts on PoshC2 payloads which align with 2019 APT33 reporting (this will not fire o
    ref = "http://www.rewterz.com/rewterz-news/rewterz-threat-alert-iranian-apt-uses-job-scams-t

  strings:
    $js_date = /[datetime\]::ParseExact("\[0-9]+\[/[0-9]+\[/[0-9]+\]", "dd\MM\yyyy", \null/
    $js_crypt = "System.Security.Cryptography" wide ascii
    $js_host = "Headers.Add(\"Host\" wide ascii
    $js_proxy = "$proxyurl = " wide ascii
    $js_arch = "$env:PROCESSOR_ARCHITECTURE" wide ascii
    $js_admin = "[System.Security.Principal.WindowsBuiltInRole]::Administrator" wide ascii
    $hta_unescape = "%64%6f%63%75%6d%65%6e%74%2e%77%72%69%74%65%28%27%3c%73%63%72%69%70%74%20%74%
    $hta_hex = "202f7720312049455820284e65772d4f626a656374204e65742e576562436c69656e74292e446f77
    $hta_powershell = "706f7765727368656c6c2e657865" wide ascii

  condition:
    4 of ($js_*) or 2 of ($hta_*)
}
```

Sample Hashes

```
a fb46cd7278a77c fb28903bf221e68134f55032138850d6fefe70945dc8abfcf
fe94fc7b2c6b75c2b68ad75a6b7020acd9f76a22f522a80285549de2fc565e87
a40801441b60a3b0192e985265df655e34c94f9bee8346c0b62a8d3618ddf8cd
```

```
14985711a5aa14c6cded0f21db544706ba845de89866e06c59a9151e7dafe19f  
ce0f7048903c6c2ee5357e8678247ae19666e91058060a3d38e09e49a94047b7
```

Related Network IoCs

```
https[:]//213[.]227[.]155[.]25/babel-polyfill/6[.]3[.]14/  
world-jobs[.]org  
global-careers[.]org  
dyn-intl[.]world-careers[.]org  
raytheonjobs[.]serveblog[.]net
```

Source: https://github.com/jeFF0Falltrades/IoCs/blob/master/APT/poshc2_ap_33.md