Rewterz Threat Alert – Iranian APT Uses Job Scams to Lure Targets

rewterz.com/rewterz-news/rewterz-threat-alert-iranian-apt-uses-job-scams-to-lure-targets

November 18, 2019

Rewterz Threat Alert – Phishing Campaign Threatens an Automatic Password Change

November 18, 2019

Rewterz Threat Alert – Azorult Malware – Active IoCs

November 18, 2019

Severity

Medium

Analysis Summary

A phishing campaign is detected, luring its targets with fake job scams. The campaign is being linked to Iranian APT33. Indicators of compromise are given below, some of which have previously been used in other phishing campaigns as well. The motive of the campaign is still not known. Similar phishing campaigns have been previously launched to deploy Remote Access Trojans.

Impact

- Credential Theft
- Information Theft
- Unauthorized Remote Access

Indicators of Compromise

Domain Name

www[.]global-careers[.]org
dyn-intl[.]world-careers[.]org
global-careers[.]org
raytheonjobs.serveblog[.]net

Filename

JobDescription.zip
JobDescription.vbe

MD5

- 673510dd92eb812d70b017c27385d389
- 7c295c528fea9385a2e3165b683d1a46
- 24ccad79498d240f19bfd2fc144b875e
- af707c4f8e40f529e8a342259ee9c8ae
- 0efb36b6dd3493b7869e8da731eff77d

SHA-256

- e2b5900211088daf754d900ff7b229defe72bf6ae21efb53c966113a2b2b16b3
- 92e66acd62dfb1632f6e4ccb90a343cb8b8e2f4fb7c9bfa9ae0745db0748223b
- 6d76db96a544700a1fdcac810c7429aa64c22f249895d0a6e58d44809350fa69
- 14985711a5aa14c6cded0f21db544706ba845de89866e06c59a9151e7dafe19f
- ce0f7048903c6c2ee5357e8678247ae19666e91058060a3d38e09e49a94047b7

Source IP

208.91.197[.]91

URL

http[:]//fineksus[.]com/delp[.]exe

Remediation

- Block the threat indicators at their respective controls.
- Do not download and execute untrusted files.
- Do not respond to untrusted emails.