Beat: Technology

Adversarial Threat Report April 2022

Cyber Threat Alert from OTX Alienvault

New York City, 07.04.2022, 18:45 Time

OTX Alienvault - Adversarial Threat Report - April 2022
CREATED 2 HOURS AGO by AlienVaultPublic TLP: White
Cyber espionage actors typically target people across the internet to collect intelligence, manipulate them into revealing information, and compromise their devices and accounts. Researchers identified a group of hackers from Iran, known in the security industry as UNC788, that targeted people in the Middle East, including Saudi military, dissidents and human rights activists from Israel and Iran, politicians in the US, and Iran-focused academics, activists and journalists around the world.

Sources:
https://otx.alienvault.com/adversary/UNC788/pulses | https://duo.com/decipher/meta-disrupts-two-iranian-threat-groups

* ADVERSARY: UNC788

* INDUSTRIES: Energy, Finance, Government, NGO

* TARGETED COUNTRIES:
United States of America, Canada, Germany, United Arab Emirates, Norway, Iceland, Israel, India, Azerbaijan, Saudi Arabia, Brazil, Ukraine, Nigeria, Cameroon, Gambia, Zimbabwe, Congo

* MALWARE FAMILY: HilalRAT

* ATT&CK IDS:
T1102 - Web Service, T1017 - Application Deployment Software, T1498 - Network Denial of Service, T1499 - Endpoint Denial of Service, T1192 - Spearphishing Link, T1566 - Phishing, T1021 - Remote Services, T1081 - Credentials in Files, T1119 - Automated Collection

TAGS:
HilalRAT, Meta, Facebook, NGOs, Geopolitical conflict, UNC788, VMware

Excerpt from a report by Dennis Fisher posted on Duo.com:

"Meta has disrupted two separate cyberespionage groups from Iran that were using a variety of tactics on its platforms to target academics, activists, journalists and other victims. One of the groups, which has not been previously identified, was impersonating legitimate companies and used a complex network of fake personas across Facebook, Telegram, and other platforms to entice victims.

The disruptions are part of Meta’s efforts to remove malicious and inauthentic behavior from its platforms, and the company regularly takes down disinformation, cyberespionage, and other operations. In its most recent Adversarial Threat report, released Thursday, Meta said that the newly identified group from Iran was targeting companies in the energy, maritime, semiconductor, and telecom industries in several countries, including the United States, Israel, Russia, Canada, and others. The unnamed group relied on phishing and extensive social engineering tactics to target victims in those industries. One of the group’s key tactics was to spoof the domains of legitimate companies and also create a network of fake recruiting firms."

Article online:
https://www.uspa24.com/bericht-20399/adversarial-threat-report-april-2022.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement):

Exemption from liability:
The publisher shall assume no liability for the accuracy or completeness of the published report and is merely providing space for the submission of and access to third-party content. Liability for the content of a report lies solely with the author of such report.

Editorial program service of General News Agency:
UPA United Press Agency LTD
483 Green Lanes
UK, London N13NV 4BS
contact (at) unitedpressagency.com
Official Federal Reg. No. 7442619