Iran Cyber Threat Overview

InfraGard Jacksonville

PSA/TFO Kirby Wedekind
November 19, 2021

Agenda

- Timeline of Activity
  - 2013 – 2017
  - January 2020 – Present
    - Joint Advisory (11/17/21)
    - Indictment (11/18/21)
- Advanced Persistent Threats attributed to Iran

DDoS Targeting U.S. Financial Sector

- **Late 2011 to Mid-2013**
- In March 2016, the U.S. DOJ indicted seven Iranian actors employed by companies performing work on behalf of the Islamic Revolutionary Guard Corps (IRGC) for conducting DDoS attacks primarily targeting the public-facing websites of U.S. banks.
- The attacks prevented customers from accessing their accounts and cost the banks millions of dollars in remediation.

Unauthorized Access to New York Dam

- **August/September 2013**
- In March 2016, the U.S. DOJ indicted one Iranian actor employed by a company performing work on behalf of the IRGC for illegally accessing the supervisory control and data acquisition (SCADA) systems of the Bowman Dam in Rye, New York.
  - The access allowed the actor to obtain information regarding the status and operation of the dam
  - Remediation cost $30,000

Sands Las Vegas Corporation Hacked

- **February 2014**
- Cyber threat actors hacked into the Sands Las Vegas Corporation in Las Vegas, Nevada, and stole customer data, including credit card data, Social Security Numbers, and driver's license numbers
  - Sands Las Vegas Corporation's computer systems were wiped
- In September 2015, the U.S. Director of National Intelligence identified the Iranian government as the perpetrator of the attack in a Statement for the Record to the House Permanent Select Committee on Intelligence

Cyber Theft Campaign on Behalf of IRGC

- **2013 to 2017**
- In March 2018, the U.S. Justice Department indicted nine Iranian actors associated with the Mabna Institute for conducting a massive cyber theft campaign containing dozens of individual incidents, including “many on behalf of the IRGC.”
  - The thefts targeted academic and intellectual property data as well as email account credentials
- Campaign targeted “144 U.S. universities, 176 universities across 21 foreign countries, 47 domestic and foreign private sector companies, the U.S. Department of Labor, the Federal Energy Regulatory Commission, the State of Hawaii, the State of Indiana, the United Nations, and the United Nations Children’s Fund.”

Iranian APT Technique Mitigation & Detection

- Credential dumping
- Obfuscated files or information
- Data compressed
- Power shell
- User execution
- Scripting
- Registry run keys / startup folder
- Remote file copy
- Spearphishing link
- Spearphishing attachment

NCAS Alert AA20-006A
https://us-cert.cisa.gov/ncas/alerts/aa20-006a

Iran-Based Threat Actor Exploits VPN Vulnerabilities

- **Original release: September 15, 2020**
- **APT: Pioneer Kitten, Fox Kitten, PARISITE, UNC757**
  - Iran-based malicious cyber actor
  - Targeting US federal agencies & other US-based networks
  - Observed exploiting publicly known CVEs regarding Pulse Secure VPN, Citrix NetScaler, & F5 vulnerabilities
  - Exploited vulnerabilities to gain access to targeted networks
  - Maintained access within the successfully exploited networks for several months using multiple means of persistence
- **https://us-cert.cisa.gov/ncas/alerts/aa20-259a**

Pioneer Kitten

- Attack vector
  - Exploits unpatched vulnerabilities
  - Webshells
  - SSH Tunneling
  - VPN Exploitation
- Sells access to compromised systems and networks
- CVEs
  - CVE-2018-13379
  - CVE-2019-11510
  - CVE-2019-19781
  - CVE-2020-5902
- Goals:
  - Espionage
  - Financial gain
- Industries targeted:
  - Healthcare
  - Government
  - Technology
  - Defense
- Further reading:
  - https://www.crowdstrike.com/blog/who-is-pioneer-kitten/

Iranian Advanced Persistent Threat Actors Threaten Election-Related Systems

- **Original release: October 22, 2020**
- **APT: unattributed Iran-based malicious cyber actor**
  - Likely intent on influencing & interfering with the US elections to sow discord among voters & undermine public confidence in the US electoral process
  - Creating fictitious media sites & spoofing legitimate media sites to spread obtained U.S. voter-registration data, anti-American propaganda, and misinformation about voter suppression, voter fraud, and ballot fraud
  - Historically exploited critical vulnerabilities to conduct DDoS attacks, SQL injections attacks, spear-phishing campaigns, website defacements, and disinformation campaigns

https://us-cert.cisa.gov/ncas/alerts/aa20-296b

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

- **Original release: October 30, 2020**
- **APT: unattributed Iran-based malicious cyber actor**
  - Responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020.
    - Reference FBI FLASH message ME-000138-TT (10/29/2020)
  - FBI + CISA analysis identified targeting of US state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election
  - Tool used: Acunetix vulnerability scanner
- **https://us-cert.cisa.gov/ncas/alerts/aa20-304a**

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

- **Update!**
- On November 18, 2021, US DOJ indicted two Iranian nationals charged with cyber-enabled disinformation and threat campaign designed to influence the 2020 US Presidential election
- Emails sent to voters threatening violence if voters did not vote a certain way
  - Voter Threat Emails: Impersonated Proud Boys group
  - False Election Video: Metallica video
- Computer intrusions depicted in the False Election Video were simulated intrusions created by members of the conspiracy using their own server and data obtained from associated data exploitation

ICS Joint Security Awareness Report
Shamoon/DistTrack Malware

- **Original release: October 16, 2012; updated July 20, 2021**
- **APT: unattributed** (maybe Refined Kitten, Elfin, APT33)
  - Shamoon is information-stealing malware that includes a destructive module
    - Renders infected systems useless by overwriting the Master Boot Record (MBR), the partition tables, and most of the files with random data
    - Once overwritten, the data are not recoverable
- **7/20/21 Update:** USG attributes this activity to Iranian nation-state cyber actors. Iranian nation-state actors have been observed deploying Shamoon malware against industrial control systems.
- **https://us-cert.cisa.gov/ics/jsar/JSAR-12-241-01B**

Refined Kitten (APT33)

- Malware
  - SHAPESHIFT; DROPSHOT/Stonedrill
  - TURNEDUP; NANOCORE
  - ALFA Shell; NETWIRE
- Attack vector
  - Spearphishing
  - Recruitment-themed
  - Fake job descriptions & websites
  - Malicious .hta (HTML executable) files
- Other tools & methods
  - Brute-force attacks
  - Password spraying
  - Port 443
  - Mimikatz
  - FTP exfiltration
  - Command and control (C&C/C2)
  - Domain masquerading
- CVEs
  - CVE-2018-20250
  - CVE-2017-0213
  - CVE-2017-11774
- Goals:
  - Strategic Espionage
- Industries targeted:
  - Aviation
  - Petrol; Energy
- Further reading:
  - https://attack.mitre.org/groups/G0064/

Iranian Government-Sponsored APT Cyber Actors Exploiting MSE & Fortinet Vulnerabilities

- **Original release: November 17, 2021**
- **APT: unattributed**
  - FBI & CISA have observed this Iranian government-sponsored APT group
    - Exploit Fortinet vulnerabilities since at least March 2021
    - Exploit Microsoft Exchange ProxyShell vulnerability since at least October 2021
    - Gain access to systems in advance of follow-on operations, which include deploying ransomware
  - Scanning devices on ports 4443, 8443, and 10443 for Fortinet FortiOS vulnerability CVE-2018-13379
  - Enumerating devices for FortiOS vulnerabilities CVE-2020-12812 and CVE-2019-5591

Iranian Government-Sponsored APT Cyber Actors Exploiting MSE & Fortinet Vulnerabilities

- **Original release: November 17, 2021**
- **APT: unattributed**
  - In June 2021, exploited Fortigate appliance to access environmental control networks associated with a US-based hospital specializing in healthcare for children
    - Likely leveraged a server assigned to IP addresses 91.214.124[.]143 and 162.55.137[.]20—which FBI and CISA judge are associated with Iranian government cyber activity—to further enable malicious activity against the hospital's network
    - The APT actors accessed known user accounts at the hospital from IP address 154.16.192[.]70, which FBI and CISA judge is associated with government of Iran offensive cyber activity
  - As of October 2021, these APT actors have leveraged a Microsoft Exchange ProxyShell vulnerability—CVE-2021-34473—to gain initial access to systems in advance of follow-on operations

Rocket Kitten (APT35)

- Charming Kitten, Newscaster, Phosphorus, Saffron Rose, Ajax
- Malware
  - MAGIC HOUND
  - HAVIJ
- Attack vector
  - Social Engineering, Social Media Phishing, Spearphishing
  - Password Recovery Impersonation
  - SMS Spearphishing
  - Use of various social media platforms for the above
- Other tools & methods:
  - Two-Factor Authentication Defeat
  - Keylogging
  - Mimikatz
  - Microsoft Office vulnerability abuse
- Goals:
  - Strategic Espionage
- Industries targeted:
  - Military; Government; Defense Industrial Base
  - Media
  - Energy; Engineering; Telecommunications
  - Dissidents
- Further reading:
  - https://attack.mitre.org/groups/G0059/

Rampant Kitten

- Malware
  - Information stealing variants, primarily targeting KeePass and Telegram accounts of intended victims
  - Dharma ransomware
- Attack vector
  - Employ information stealers to target credentials, personal documents, SMS, and Telegram messages
  - An Android backdoor extracts two-factor authentication codes
  - Phishing pages masquerading as distributors of fake accounts
  - Bypassing two- and multi-factor authentication
- Other tools/methods: VPN exploitation
- CVEs
  - CVE-2019-11510
  - CVE-2019-19781
  - CVE-2020-5902
- Goals:
  - Strategic Espionage
- Industries targeted:
  - Government
  - Technology
  - Defense
- Further reading:
  - https://us-cert.cisa.gov/ncas/alerts/aa20-259a

References

- Shample, S (2020) Iranian APTs: An Overview. Middle East Institute. URL: https://www.mei.edu/publications/iranian-apts-overview. Accessed on Nov 18, 2021.
- Mandiant (2021) Advanced Persistent Threat Groups. URL: https://www.mandiant.com/resources/apt-groups. Accessed on Nov 18, 2021.
- DDoS targeting US Financial Sector. URL: https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged
- New York State Dam. https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

References

- Sands Casino Incident. URL: https://www.bloomberg.com/news/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas#p2
- CISA Potential for Iranian Response to US Military Strike. URL: https://us-cert.cisa.gov/ncas/alerts/aa20-006a
- Cyber Theft Campaign. URL: https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary

CISA
CYBER+INFRASTRUCTURE

For more information:
cisa.gov

Questions?
Email: Kirby.Wedekind@HQ.DHS.GOV
Phone: (202) 868-1361