AA20-006A: Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad

Technical Details

Iranian Cyber Threat Profile

Iran has a history of leveraging asymmetric tactics to pursue national interests beyond its conventional capabilities. More recently, its use of offensive cyber operations is an extension of that doctrine. Iran has exercised its increasingly sophisticated capabilities to suppress both social and political perspectives deemed dangerous to Iran and to harm regional and international opponents.

Iranian cyber threat actors have continuously improved their offensive cyber capabilities. They continue to engage in more "conventional" activities ranging from website defacement, distributed denial of service (DDoS) attacks, and theft of personally identifiable information (PII), but they have also demonstrated a willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks.

The U.S. intelligence community and various private sector threat intelligence organizations have identified the Islamic Revolutionary Guard Corps (IRGC) as a driving force behind Iranian state-sponsored cyberattacks–either through contractors in the Iranian private sector or by the IRGC itself.

Iranian Cyber Activity

According to open-source information, offensive cyber operations targeting a variety of industries and organizations—including financial services, energy, government facilities, chemical, healthcare, critical manufacturing, communications, and the defense industrial base—have been attributed, or allegedly attributed, to the Iranian government. The same reporting has associated Iranian actors with a range of high-profile attacks, including the following:

- **Late 2011 to Mid-2013 – DDoS Targeting U.S. Financial Sector:** In response to this activity, in March 2016, the U.S. Department of Justice indicted seven Iranian actors employed by companies performing work on behalf of the 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. [1]
- **August/September 2013 – Unauthorized Access to Dam in New York State:** In response, in March 2016, the U.S. Department of Justice 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. [2]
- **February 2014 – Sands Las Vegas Corporation Hacked:** 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.

According to a Bloomberg article from December 2014, the attack also involved a destructive portion, in which the 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. [3]

- **2013 to 2017 – Cyber Theft Campaign on Behalf of IRGC:** In response, 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. According to the indictment, the 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." [4]

Patterns of Publicly Known Iranian Advanced Persistent Threats

The following mitigations and detection recommendations regarding publicly known Iranian advanced persistent threat (APT) techniques are based on the MITRE ATT&CK Framework. [5]

Iranian APT Technique	Mitigation and Detection
Credential Dumping	Mitigation • Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication. • Consider disabling or restricting NTLM. • Ensure that local administrator accounts have complex, unique passwords across all systems on the network. • Limit credential overlap across accounts and systems by training users and administrators not to use the same password for multiple accounts. Detection • Windows: Monitor for unexpected processes interacting with Isass.exe. • Linux: The AuditD monitoring tool can be used to watch for hostile processes opening a maps file in the proc file system, alerting on the pid, process name, and arguments for such programs.
Obfuscated Files or Information	Mitigation

	• Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted. Detection • Windows: Monitor for unexpected processes interacting with Isass.exe. • Linux: The AuditD monitoring tool can be used to watch for hostile processes opening a maps file in the proc file system, alerting on the pid, process name, and arguments for such programs.
Data Compressed	Mitigation • Network intrusion prevention or data loss prevention tools may be set to block specific file types from leaving the network over unencrypted channels. Detection • Process monitoring and monitoring for command-line arguments for known compression utilities. • If the communications channel is unencrypted, compressed files can be detected in transit during exfiltration with a network intrusion detection or data loss prevention system analyzing file headers.
PowerShell	Mitigation • Set PowerShell execution policy to execute only signed scripts. • Remove PowerShell from systems when not needed, but a review should be performed to assess the impact to an environment, since it could be in use for many legitimate purposes and administrative functions. • Disable/restrict the WinRM Service to help prevent uses of PowerShell for remote execution. • Restrict PowerShell execution policy to administrators. Detection • If PowerShell is not used in an environment, looking for PowerShell execution may detect malicious activity. • Monitor for loading and/or execution of artifacts associated with PowerShell specific assemblies, such as System.

	Management.Automation.dll (especially to unusual process names/locations). • Turn on PowerShell logging to gain increased fidelity in what occurs during execution (which is applied to .NET invocations).
User Execution	Mitigation • Application whitelisting may be able to prevent the running of executables masquerading as other files. • If a link is being visited by a user, network intrusion prevention systems and systems designed to scan and remove malicious downloads can be used to block activity. • Block unknown or unused files in transit by default that should not be downloaded or by policy from suspicious sites as a best practice to prevent some vectors, such as .scr., .exe, .pif, .cpl, etc. • Use user training as a way to bring awareness to common phishing and spearphishing techniques and how to raise suspicion for potentially malicious events. Detection • Monitor the execution of and command-line arguments for applications that may be used by an adversary to gain Initial Access that require user interaction. This includes compression applications, such as those for zip files that can be used to Deobfuscate/Decode Files or Information in payloads. • Anti-virus can potentially detect malicious documents and files that are downloaded and executed on the user's computer. • Endpoint sensing or network sensing can potentially detect malicious events once the file is opened (such as a Microsoft Word document or PDF reaching out to the internet or spawning Powershell.exe) for techniques such as Exploitation for Client Execution and Scripting.
Scripting	Mitigation • Configure Office security settings enable Protected View, to execute within a sandbox environment, and to block macros through Group Policy. Other types of virtualization and application microsegmentation may also mitigate the impact of compromise. • Turn off unused features or restrict access to scripting engines such as VBScript or scriptable administration frameworks such as PowerShell. Detection

	• Examine scripting user restrictions. Evaluate any attempts to enable scripts running on a system that would be considered suspicious. • Scripts should be captured from the file system when possible to determine their actions and intent. • Monitor processes and command-line arguments for script execution and subsequent behavior. • Analyze Office file attachments for potentially malicious macros. • Office processes, such as winword.exe, spawning instances of cmd.exe, script application like wscript.exe or powershell.exe, or other suspicious processes may indicate malicious activity.
Registry Run Keys/Startup Folder	Mitigation • This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features. Detection • Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. • Monitor the start folder for additions or changes. • Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders. • To increase confidence of malicious activity, data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as network connections made for Command and Control, learning details about the environment through Discovery, and Lateral Movement.
Remote File Copy	Mitigation • Network intrusion detection and prevention systems that use network signatures to identify traffic for specific adversary malware or unusual data transfer over known tools and protocols like FTP can be used to mitigate activity at the network level. Detection • Monitor for file creation and files transferred within a network over SMB. • Monitor use of utilities, such as FTP, that does not normally occur.

	• Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server). • Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.
Spearphishing Link	Mitigation • Determine if certain websites that can be used for spearphishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. • Users can be trained to identify social engineering techniques and spearphishing emails with malicious links. Detection • URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. • Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.
Spearphishing Attachment	Mitigation • Anti-virus can automatically quarantine suspicious files. • Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity. • Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. • Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments in Obfuscated Files or Information. • Users can be trained to identify social engineering techniques and spearphishing emails. Detection • Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. • Detonation chambers may also be used to identify malicious attachments. • Solutions can be signature and behavior based, but adversaries may construct attachments in a way to avoid these systems.

	• Anti-virus can potentially detect malicious documents and attachments as they're scanned to be stored on the email server or on the user's computer.

References

[1] Department of Justice press release: Seven Iranians Working for Islamic Rev…
[2] Department of Justice press release: Seven Iranians Working for Islamic Rev…
[3] Bloomberg article: Now at the Sands Casino: An Iranian Hacker in Every Serv…
[4] Department of Justice press release: Nine Iranians Charged With Conducting …
[5] MITRE ATT&CK Framework
CISA Insights: Increased Geopolitical Tensions and Threats

Contact Information

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- CISAServiceDesk@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA homepage at http://www.us-cert.gov/.

Revisions

- January 6, 2019: Initial version