**Review of Iranian Threat Groups and Techniques**

The Department of Homeland Security (DHS) is reporting that Iran is highly likely to retaliate against the United States and its interests following the airstrikes that killed a prominent Iranian military official. There are several Iran-based threat groups that posses advanced and highly capable cyber tactics, techniques, and procedures. While there are no specific, credible threats identified, DHS reports that Iranian cyber threat actors (CTAs) are likely to attack critical infrastructure through the use of malware wipers. Historically they have used password sprayers to gain initial access. Current reports indicate that pro-Iranian actors have defaced several American websites with anti-American messages.

Iran does not have the same strengths as Russia or China when it comes to cyber capabilities. For Iran, that means aiming at easier targets in the broader non-governmental sector. Even if they go after State, Local, Tribal, and Territorial (STLL) networks, non-government networks could be used as beachheads or used as lateral targets resulting in collateral damage.

The following is a short description of currently known Iran-based threat groups and the techniques they employ throughout the cyber kill chain as identified in the MITRE ATT&CK matrix.



**APT33** is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.

|  |  |  |  |
| --- | --- | --- | --- |
| TECHNIQUES | | | |
| Brute Force | Commonly Used Port | Credential Dumping | Data Compressed |
| Data Encoding | Execution Guardrails | Exfiltration Over Alternative Protocl | Exploitation for Client Execution |
| Exploitation for Privilege Escalation | Network Sniffing | Obfuscated Files or Information | PowerShell |
| Registry Run Keys / Startup Folder | Remote File Copy | Scheduled Task | Spearphishing Link |
| Standard Application Layer Protocol | Standard Cryptographic Protocol | Uncommonly Used Port | User Execution |
| Valid Accounts |  |  |  |

**APT39 (Chafer)** is an Iranian cyber espionage group that has been active since at least 2014. They have targeted the telecommunication and travel industries to collect personal information that aligns with Iran's national priorities.

|  |  |  |  |
| --- | --- | --- | --- |
| TECHNIQUES | | | |
| Connection Proxy | Credential Dumping | Data Compressed | Network Service Scanning |
| Registry Run Keys / Startup Folder | Remote Desktop Protocol | Remote Services | Scheduled Task |
| Scripting | Shortcut Modification | Software packing | Spearphishing Attachment |
| Spearphishing Link | System Network Configuration Discovery | System Owner/User Discovery | User Execution |
| Valid Accounts | Web Shell |  |  |

**Charming Kitten** is an Iranian cyber espionage group that has been active since approximately 2014. They appear to focus on targeting individuals of interest to Iran who work in academic research, human rights, and media, with most victims having been located in Iran, the US, Israel, and the UK. Charming Kitten usually tries to access private email and Facebook accounts, and sometimes establishes a foothold on victim computers as a secondary objective. The group's TTPs overlap extensively with another group, Magic Hound, resulting in reporting that may not distinguish between the two groups' activities.

|  |  |  |  |
| --- | --- | --- | --- |
| TECHNIQUES | | | |
| Command-Line Interface | PowerShell | Query Registry | Registry Run Keys / Startup Folder |
| Standard Application | Layer Protocol | System Information Discovery | System Owner/User Discovery |

**CopyKittens**is an Iranian cyber espionage group that has been operating since at least 2013. It has targeted countries including Israel, Saudi Arabia, Turkey, the U.S., Jordan, and Germany. The group is responsible for the campaign known as Operation Wilted Tulip.

|  |  |  |
| --- | --- | --- |
| TECHNIQUES | | |
| Code Signing | Data Compressed | Data Encrypted |
| Hidden Window | PowerShell | Rundll32 |

**Group5** is a threat group with a suspected Iranian nexus, though this attribution is not definite. The group has targeted individuals connected to the Syrian opposition via spearphishing and watering holes, normally using Syrian and Iranian themes. Group5 has used two commonly available remote access tools (RATs), njRAT and NanoCore, as well as an Android RAT, DroidJack.

|  |  |  |
| --- | --- | --- |
| TECHNIQUES | | |
| File Deletion | Input Capture | Obfuscated Files or Information |
| Screen Capture | Software Packing | Uncommonly Used Port |

**Leafminer** is an Iranian threat group that has targeted government organizations and business entities in the Middle East since at least early 2017.

|  |  |  |  |
| --- | --- | --- | --- |
| TECHNIQUES | | | |
| Brute Force | Create Account | Credential Dumping | Drive-by Compromise |
| Email Collection | File and Directory Discovery | Network Service Scanning | Obfuscated Files of Information |
| Redundant Access | Remote System Discovery | Scripting |  |

**Magic Hound** is an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia.

|  |  |  |  |
| --- | --- | --- | --- |
| TECHNIQUES | | | |
| Account Manipulation | Command-Line Interface | Commonly Used Port | Credential Dumping |
| Data Compressed | Email Collection | Files and Directory Discovery | File Deletion |
| Hidden Window | Input Capture | Obfuscated Files or Information | PowerShell |
| Process Discovery | Registry Run Keys / Startup Folder | Remote File Copy | Screen Capture |
| Scripting | Spearphishing Attachment | Spearphishing Link | Spearphishing via Service |
| Standard Application Layer Protocol | System Information Discovery | System Network Configuration Discovery | System Owner/User Discovery |
| Uncommonly Used Port | User Execution | Web Service |  |

**OilRig** is a suspected Iranian threat group that has targeted Middle Eastern and international victims since at least 2014. The group has targeted a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East. It appears the group carries out supply chain attacks, leveraging the trust relationship between organizations to attack their primary targets. FireEye assesses that the group works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.  This group was previously tracked under two distinct groups, APT34 and OilRig, but was combined due to additional reporting giving higher confidence about the overlap of the activity.

|  |  |  |  |
| --- | --- | --- | --- |
| Accoutn Discovery | Automated Collection | Brute Force | Command-Line Interface |
| Commonly Used Port | Compiled HTML File | Credential Dumping | Credentials in Files |
| Custom Command and Control Protocol | Deobfuscate/Decode Files or Information | Exfiltration Over Alternative Protocol | External Remote Services |
| Fallback Channels | File Deletion | Indicator Removal from Tools | Input Capture |
| Network Service Scanning | Obfuscated Files or Information | Password Policy Discovery | PowerShell |
| Process Discovery | Query registry | Redundant Access | Remote Desktop Protocol |
| Remote File Copy | Remote Services | Scheduled Task | Screen Capture |
| Scripting | Spearphishing Attachment | Spearphishing Link | Spearphishing via Service |
| Standard Application layer Protocol | Standard Cryptographic Protocol | System information Discovery | System Network Configuration Discovery |
| System Network Connections Discovery | System Owner/User Discovery | System Service Discovery | User Execution |
| Valid Accounts | Web Shell | Windows Management Instrumentation |  |