|  |  |
| --- | --- |
| Cyber Intel Advisory  January 03, 2020 – IA2020-0101  **Potential for Cyber Attacks Following Strikes Against Senior Iranian Military Official** | |
| ***Insert your logo here  and contact information at the bottom of the paper*** |  |

**(U//FOUO) TLP: GREEN** The MS-ISAC assesses that Iran is highly-likely to retaliate against the United States and its interests following the airstrikes early Friday, killing a prominent Iranian military official. This assessment is based on historical Iranian retaliatory efforts. Iran specializes in asymmetric warfare and its response will highly likely be physical or cyber in nature, targeting U.S. interests globally. If tensions continue to escalate, this response will likely include cyber attacks against U.S. critical infrastructure.

**(U//FOUO) TLP: GREEN** The Iranian regime possesses advanced and highly capable cyber tactics, techniques, and procedures. While DHS assesses there are currently no specific, credible threats against our homeland, it anticipates an Iranian cyber response to the U.S. is likely to involve destructive malware with intent to disrupt U.S. critical infrastructure.1 Specifically, DHS assesses that Iranian cyber threat actors (CTAs) are likely to use pre-established access to U.S. critical infrastructure to launch destructive wipers (malware designed to eliminate files on systems and make them unrecoverable) against targets.2,3 Iranian cyber actors historically have been observed relying on tactics such as [password spraying](https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-password-attacks/) to gain initial access, then maintaining persistence through surreptitious means.

**(U) TLP: GREEN** Trusted third parties have provided reports of pro-Iranian, anti-American defacements against guidebook websites for U.S. cities. These guidebook websites are not government run, but rather provide basic information within respected localities.

**(U) TLP: GREEN** MS-ISAC will maintain a period of heightened monitoring as the situation develops and asks membership to report any anomalous activity to the MS-ISAC.

**RECOMMEDATIONS:**

* MS-ISAC has recommends SLTT governments remain vigilant of potential DDoS attacks and wipers as these are known tactics of Iranian APT groups.
* Maintain heightened log monitoring and awareness for suspicious activity on networks, especially those related to critical infrastructure
* SLTT governments should evaluate third party access to their networks and, if relevant, consider having a conversation with their Managed Service Providers (MSPs) to ensure appropriate steps are being taken to mitigate risk.
* Evaluate and manage third-party risks from the supply chain and vendors
* Keep all systems up-to-date and apply appropriate [patches](https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-patching/) when necessary.
* Ensure backups of systems are current and stored offline (CIS Control 10)
* Implement and maintained hardened configurations of systems (CIS Control 5)
* MS-ISAC members should ensure they have current disaster recovery plans (DRP) For more information regarding DRPs read the [DRP cybersecurity spotlight.](https://www.cisecurity.org/spotlight/cybersecurity-spotlight-disaster-recovery-plan-drp/)

**SOURCES:**

1. <https://content.govdelivery.com/accounts/USDHS/bulletins/274591b>
2. <https://threatpost.com/iran-targeting-u-s-with-destructive-wipers-warns-dhs/145950/>

3 <https://www.wired.com/story/iran-apt33-industrial-control-systems/>

*The information provided above is intended to increase the security awareness of an organization’s end users and to help them behave in a more secure manner within their work environment. Organizations have permission and are encouraged to brand and redistribute this advisory in whole for educational, non-commercial purposes. For more information regarding potential cyber threats please visit the Center for Internet Security website at CISecurity.org*

**(U) TLP:** **GREEN** The MS-ISAC is interested in your comments - an anonymous feedback [survey](https://www.surveymonkey.com/r/MSISACProductEvaluation) is available.

**(U) TLP:** **GREEN** The information in this document is current as of January 03, 2020. Citations and more information regarding potential cyber threats are available by contacting:

|  |  |
| --- | --- |
| ***Entity 1***  ***Telephone (###-###-####) · email***  ***URL*** | ***MS-ISAC*** *866-787-4722* ***·*** *SOC@cisecurity.org*  [*www.cisecurity.org*](http://www.cisecurity.org) |