Kaspersky recently reported that they recently analyzed spyware that was affecting Iranian IP addresses in the late autumn of 2018. According to them, an updated version of Remexi malware was used to spy on some people in Iran, of which some of the IP addresses belonged to foreign diplomats in the country. Remexi was originally associated with a group known as Chafer, whom have been active since 2014, and was used in 2015. The updated version that Kaspersky analyzed dated back to March 2018 and its capabilities included exfiltrating captured keystrokes, credentials, cookies/history, and screenshots through a legitimate Microsoft application called Background Intelligent Transfer Service, which was designed to enable background Windows updates. According to Denis Legezo, a security researcher at Kaspersky, he stated that, "..the people behind this spyware campaign look more like system administrators than sophisticated threat actors. They know how to code, but their campaign relies more on the creative use of tools that exist already."

Kaspersky found no concrete evidence that showed how Remexi was spread. They however found a correlation between Remexi and an execution of a PE compiled AutoIT script. Remexi is an issue within a larger one of a nation state such as Iran with its growing cyber focus and its general distrust of the western world. The theocratic government is seeking to consolidate its power and to maintain its dominance in its presence in the Middle East. This entices the question, what exactly would Chafer do with the stolen information? Could they be selling it to the Iranian government? This ethical dilemma also brings a wider societal and even international security issue, in which foreign diplomats could be faced with danger at any point in time for certain communications or of the like.

As this issue is fairly recent, the world has a responsibility to push back against this sort of espionage behavior in relation to the danger that foreigners have within the country. Countries with embassies within Iran's borders would probably up their security forces in the embassies, possibly send more IT professionals to thoroughly audit all machines, and there might even be some public pushback from some of the bigger countries such as Canada, France, or even Saudi Arabia. International media should focus on the ways to prevent this spyware from spreading to people's machines such as extra vigilance in phishing attempts, USB drop attacks, or even insider threats.

Sources:

https://www.symantec.com/blogs/threat-intelligence/chafer-latest-attacks-reveal-heightened-ambitions

https://securelist.com/chafer-used-remexi-malware/89538/

https://www.scmagazine.com/home/security-news/two-new-cyber-espionage-groups-targeting-isps-inside-iran/

https://www.theonlinecitizen.com/2019/02/01/chafer-cyberespionage-group-targets-embassies-with-updated-homebrew-spyware/

https://www.washingtonpost.com/news/global-opinions/wp/2018/06/07/with-no-skin-in-the-game-can-the-u-s-have-any-influence-on-iran/?utm_term=.a794c4c928fe