Cybersecurity is an incredibly diverse field that, while important, is poorly understood by the layperson. Many aspects of the field are fairly arcane and difficult to parse if one is not fully engrossed in its myriad nuances and sometimes contradictory information. This is most easily portrayed by a recent and ongoing cyberattack that has been active since at least September of 2023. This attack is what is known as a "fake worker" scam, where a threat actor will pose itself as a seemingly legitimate employer and/or LinkedIn profile in order to distribute malware disguising itself as benign files. This specific attack set its sights upon aerospace workers; from airline workers to air defense employees. These attacks were specific to Israel, India, The United Arab Emirates, and other nations in the Middle East and Southern Asia.

This attack is attributed to a group within the Iranian government's cyberwarfare group Charming Kitten labeled as TA455 (Antoniuk, 2024). The attack involves the creation of various fraudulent job offers disseminated across the target countries on a number of different hosting platforms such as LinkedIn. This simplicity of deployment allows for the casting of a very, very wide net. The tactics utilized by TA455 is notably similar to North Korean cyberwarfare doctrine according to Clearsky, the organization who broke the news of this attack, and it is unclear whether or not TA455 is a North Korean group affiliating itself with Charming Kitten, or merely extremely similar cyber doctrines.

Once the victims were located and the documents distributed, the malware would install itself on the victims' machines. The malware in question is known as SnailResin, which activates a backdoor known as SlugResin. According to Microsoft Security Intelligence (MSI) SlugResin is a novel variant of the BrassBreaker backdoor that grants the C&C server of the threat actors access to the compromised device, allowing the easy installation of other malware types to scrape information such as banking details, personally identifiable information, and theft of

privileged credentials. This backdoor also grants the potential for a rolling compromise of devices connected on the same network as the initial victim. (*Microsoft* SlugResin Information)

This backdoor behaves like most common backdoors, attaching itself to a Trojan loader; in this case SnailResin, and installing itself from the ZIP containing the downloaded file. As it is installed, SlugResin creates a staging directory in order to fully deploy itself and mask itself as the legitimate "secur32.dll" file. This process creates numerous files in directories that are often looked over by ordinary users, deep in the %*LocalAppData%* directory, making it difficult to detect manually. Without the use of active virus scanning software, it is very likely to go unnoticed, especially due to the effort it takes to make itself inconspicuous. Now installed, it is simple for the threat actor who installed it to remotely access the computer, scrape data, and extract it to their home machines before covering their tracks.

While noted to have begun in 2023, the attack shows no signs of stopping even today. This fact leads to various complications for workers in the air industry in the affected regions, namely, how do they determine what is a real job posting and what is a fraudulent one? One of the numerous ways to determine this is to do research on every company that they find and are considering putting in for. A few simple steps would be to make note of the name, location, and date of posting. Say Company Z places a job posting on LinkedIn, the prospective worker could look up the name of Company Z to see if this is indeed their real LinkedIn page and then further determine if the other information provided is correct. Alternatively, Recruiters are a harder source to investigate as they are individual people rather than easily searchable companies. In this instance, as unpalatable as it may be, job seekers in affected regions should be advised to avoid any recruitment offers from individuals due to the risks that are posed by this attack.

In conclusion, the Iran-linked TA455 hacking group has planted various trojan accounts on sites like LinkedIn targeting air sector employees for unknown reasons. The attack involves the use of a fairly advanced backdoor called SlugResin which can potentially infect devices far beyond the initial compromised one. This backdoor is fairly difficult to detect due to it masking itself as a benign set of files in the deeper recess of a computer's OS. To defend themselves from this attack, it would be advisable for workers in affected regions to do research on the companies whose job offers they intend to follow up on and in general avoid recruiters

Microsoft. (n.d.). *Microsoft*. threat description - Microsoft Security Intelligence. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor%3AWin64%2FSlugResin.B%21dha&ThreatID=2147901124

Antonia, D. (2024, November 14). *Iran-linked group aims malware at aerospace industry through fake job recruiters*. Cyber Security News | The Record. https://therecord.media/iran-linked-hackers-aerospace-espionage-malware-fake-recruiters