e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com

HOW A NEW HIRE CAN ACQUIRE CLASSIFIED DATA IN AEROSPACE INDUSTRY

Yelyzaveta Rachenko*1

*1Student, Department of Computer Science, A. N. Beketov University, Kharkiv, Ukraine.

https://orcid.org/0000-0002-8376-7308.

ABSTRACT

Professionals who are hired to be on an aerospace cybersecurity team are carefully vetted and undergo scrupulous background checks. But what if there was a way to acquire classified aerospace government data using a slow calculated method of becoming a team member first and hacking the needed department from the inside of a company? A method described in this paper shows the hypothetical steps which may be taken by a malicious hacker in order to get hired by a high-security organization. The steps are described in details in an attempt to understand the hacker's thinking. This piece is timely because the National Security Agency had released a new cybersecurity product on Jan 5th 2021[1] which contains instructions on how to prevent the event described in this paper.

Keywords: Aerospace, cybersecurity, team, recruitment, hire.

I. INTRODUCTION

The importance of cybersecurity has always been heightened in government agencies. Aerospace is a crucial part of the governmental system and thus is in need of utmost protection. National Security Agency helps protect cryptographic and communications intelligence and security in the United States of America, including parts of information in The National Aeronautics and Space Administration (NASA). Even though NASA has its own Cybersecurity & Privacy Division (CSPD) which is responsible for agency-wide safety of data, there might still be points where NASA or an identical agency is vulnerable. One way that such data is unsafe is if someone from the inside steals classified information which might put national security at risk depending on where the stolen information goes next. Usually, professionals who are hired to be on an aerospace cybersecurity team are carefully vetted and had already undergone careful background checks. This paper discusses one of the ways that a cybersecurity professional can get hired by any high-security agency and potentially steal classified data. The information in this publication is presented for the purpose so that such an event does not occur in real life.

II. METHODOLOGY

A possible method of how a cybersecurity professional can come up with the idea to acquire classified data from a governmental agency or a government party, what the process for a new hire in a government agency would be, and how soon the new hire would potentially get access to vital information, are presented in this paper. The theoretical research is done using the official publications posted on reputable governmental websites on the World Wide Web as well as published on paper in hard copy. For instance, some of the official websites mentioned in this paper are www.nsa.gov , www.nasa.gov , www.intelligencecareers.gov as well as others reputable websites. The reason why such a hypothetical topic was chosen is due to a higher number of cybersecurity attacks in the aerospace industry and on the United States as a whole. The hypothetical approach relies heavily on the information provided by official government websites and open to the public information. No classified information has been utilized in this publication.

III. MODELING AND ANALYSIS

This paper requires a theoretical approach aimed at developing models, theories, and hypotheses relevant to the space industry-specific hiring methods and if there are things that could be improved in these methods. The improvements in the recruitment method in the aerospace department of cybersecurity, as explained in this publication, are needed in order to prevent or at least lower the chance of a malicious hacker becoming a respected professional working in the company. The research investigated in this paper is driven by numerous theories, one of which is that it can be possible to get hired in a governmental agency within a short period of

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
Volume:03/Issue:01/January-2021 Impact Factor- 5.354 www.irjmets.com

time and, after passing all the background checks, get access to vital and at time even classified information.

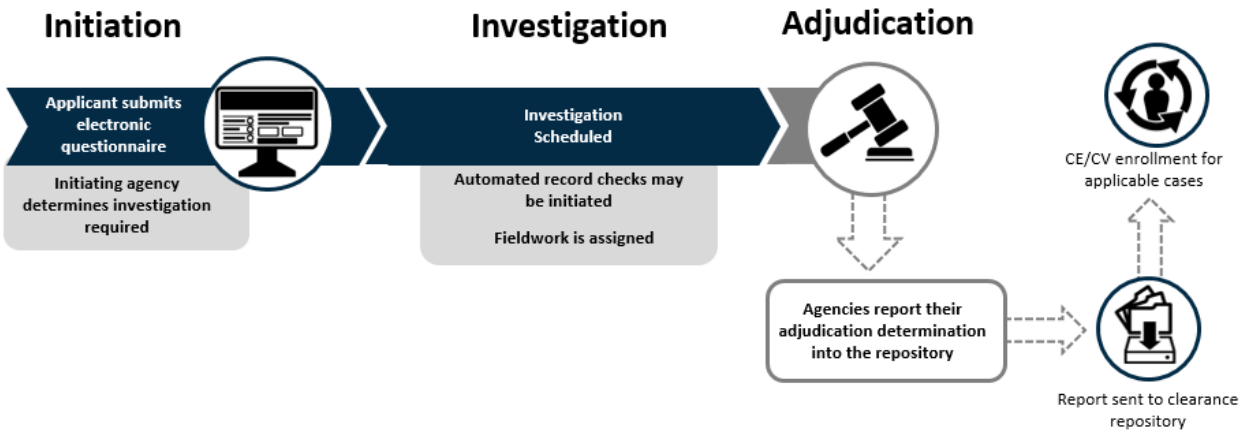

Fig.-1: An overview sample of the background investigations process [2].

IV. RESULTS AND DISCUSSION

The steps which would be taken by a cybersecurity professional in the aerospace industry who wishes to attain classified information are described below. The steps below are written under the hypothesis that the professional (Hacker) wishes to pose as someone who is interested in being recruited by any major organization, in this instance The National Aeronautics and Space Administration (NASA) which is an independent agency of the U.S. federal government responsible for aeronautics and space research as well as the civilian space program.

4.1 **Hacker gets a malicious offer**

Hacker gets an order to get a set of data from the International Space Station (ISS) or from NASA. Such a set of data is almost guaranteed to contain highly sensitive and even classified information. For instance, if we take the United States of America government as an example, then we can assume that the hacker gets an order to get some data from NASA. For instance, the payout amount to the hacker would be 10 million U.S. dollars and the time limit for the execution of the task is 1 year. What will the hacker do? For the sake of this example, let's name the hacker Hacker.

4.2 **Hacker does research**

Hacker researches how to get into the NASA system. Usually this has to be done from a computer which is connected to an encrypted (preferably private) VPN network (Virtual Private Network). The VPN network almost always has to be based in a different country. The reasoning behind it is that it is much harder for the United States government to get permission to search the quires (SQL or non-SQL, either way) and get a permit to search the computer's data from outside the U.S. It is allowed to confiscate a computer on foreign land by the U.S. government if that computer is believed to pose a national threat, such as a threat to national security. Another note is if with that VPN computer (which is supposedly overseas) the hacker also has a fake ID (Identification Document) linked to that computer which would not give out their real identity even in the case of the computer being confiscated. Such a move is usually done by more experienced hackers and might be easily overlooked by novice hackers which is exactly why it makes it more challenging for the agencies to catch more experienced professionals [3].

4.3 **Hacker realizes a different approach is needed**

After days or possibly weeks of researching and trying to break the encryption wall which is between Hacker and the NASA data Hacker wants, the hacker realizes that a hardware break-in might be needed. That hardware moment can be as much as simply being closer (distance-wise) to the NASA headquarters, being inside the NASA headquarters, being able to put a flesh drive / hard drive inside one of the NASA computers on-site, being able to create NASA login credentials, having access to one of NASA hard drives rooms, having access to reading NASA certified and classified protocols on how to decrypt certain codes and get through the encryption wall to

get the data needed [4]. There are ways to get the data needed which will not be mentioned in this paper for the sake of keeping this paper concise while giving all the necessary information.

4.4 **Hacker comes up with a new method - getting hired at the organization**

Hacker realizes that they are not sure what method they should use in order to acquire the data but they are positive that they need access to NASA headquarters. It is commonly thought that it is impossible for a hacker to get in NASA from the outside, so how can Hacker do it? If they are smart enough and have or able to acquire the needed credentials (such as a Bachelor's diploma, Master's diploma, a certain technical certificate, or some other type of a credential), they can apply for a job at NASA and slowly get access to whatever data they need [5]. With the 1 year time limit, it can be a challenge to raise on the career ladder quickly enough to get access to the needed data. However, it can be much easier for the hacker to steal data while being on the inside and using one of the company's computers.

4.5 **Hacker is a new hire at the company & after time passes, makes their move**

Hacker decides that they want to be a part of the NASA aerospace team. Hacker applied for a job available. NASA usually has plenty of analysts' jobs available with the need to hire new people. Hacker goes through the recruitment process just like everyone else - including thorough background checks [6]. Nevertheless, Hacker gets the job. Now Hacker is inside the NASA facility. It is important that Hacker does not do anything "out of the ordinary" in their first month or even a few first months. It would be the smartest for Hacker to wait until another new person is hired and then do something out of the ordinary. Naturally, all the suspicion will be shifted to the newest hired person [7]. Hacker might even put some evidence (fake proof) to add suspicion to the new hire. Hacker gets the data they need. This step has to be done without the NASA department suspecting anything. This step is approximately at the 6 month date on the 1 year deadline made by the person who hired Hacker for 10 million.

4.6 **Protecting the data acquired & Sharing the data with the buyer**

Hacker quietly backs up the data acquired on multiple computers with different VPN networks overseas. That way, even if NASA discovers that someone took the data [8], even if NASA gets permission (in other words, a warrant) to search a computer which is supposed to be located abroad, even if NASA finds the VPN network, even if NASA confiscates the data on that network [9], Hacker will have multiple backs ups of the data on different networks (all of them abroad, most likely).

Time passes. The investigation is closed. NASA is satisfied that the data has been recovered. The 1 year time mark is approaching. Hacker meets (in-person or virtually) with the payer, quietly handles them the data with no further suspicion from the police). Data Buyer pays Hacker 10 million and they part ways.

V. CONCLUSION

How was the event described successful? Timing was very important in this case.

Timeline of the event, from the idea to getting hired and acquiring classified data

Hacker gets hired (3-4 month time mark) but does not immediately take the data (they also might not have permission to see the data at this time and that is okay as of then). They wait until another employee is hired (5 month-5.5 month), then when Hacker acquires the data (6 month), the suspicion falls on the new employee or new employees. Hacker continues to work at NASA and monitors progress on the investigation. Once the investigation is closed and NASA is happy with the results, Hacker leaves the job (11 month). Hacker presents data to the Buyer (12 month).

The 6 steps in this publication described in details how a new hire can get access to classified information. First of all, the professional needs an idea and that idea or, in other words, offer can be presented by anyone with the means to pay and desire to get information they are not supposed to have. Again, this paper is written with the hope that such events do not happen in the future. Second of all, after the professional or Hacker does their research and realizes that they need to be inside the NASA facility (or inside any governmental facility) in order to attain the data needed, the person attempts to get hired at the facility. Even though thorough background checks are conducted, the professional still ends up being hired and with time acquires access to important and at times even classified information. In the given example, the hacker is an experienced cybersecurity professional in the aerospace industry, so they know how to come up with the most efficient timeline for their

actions. With a carefully planned out timeline, there are as least suspicions as possible and the hacker is able to do what they need without the organization's knowledge.

ACKNOWLEDGEMENTS

I would like to thank my Family for their unmeasurable support and love.

There will be another paper published in the nearest future describing in detail a path from a new hire to an employee with access to classified data ("Choosing An Aerospace Team Member with Cybersecurity Access to Classified Data out of Existing Team Members" - tentative name).

VI. REFERENCES

[1] NSA. (2021). Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2462345/nsa-releases-eliminating-obsolete-transport-layer-security-tls-protocol-configu/ .

[2] Defense Counterintelligence and Security Agency. (Retrieved 2021). Personnel Vetting, https://www.dcsa.mil/mc/pv/ .

[3] Rachenko, Y. (2018). The Struggles of Establishing a Secure Connection Over a Network of Satellites. National University Journal, p. 1, doi:10.6084/m9.figshare.13237886 .

[4] Rachenko, Y., Dotsenko N. (November 2020). "Enhancing the Efficiency of the Current Method of Establishing Team Members in Aerospace Communications." 4th International Scientific and Practical Conference; Boston, USA, BoScience Publisher, pp. 69-72, https://sci-conf.com.ua/wp-content/uploads/2020/11/FUNDAMENTAL-AND-APPLIED-RESEARCH-IN-THE-MODERN-WORLD-18-20.11.20.pdf

[5] The National Aeronautics and Space Administration (Retrieved 2021). Suitability Adjudication, NASA, https://www.nasa.gov/centers/nssc/suitability .

[6] Rachenko, Y., Dotsenko N. (January 2021). "Using a Computerized System to Determine the Most Suitable Job Skills for Aerospace Industry." 6th International Scientific and Practical Conference; Boston, USA, BoScience Publisher, pp. 69-72, https://sci-conf.com.ua/wp-content/uploads/2021/01/FUNDAMENTAL-AND-APPLIED-RESEARCH-IN-THE-MODERN-WORLD-20-22jan2021.pdf .

[7] Intelligence Careers. (Retrieved 2021). DEVELOPMENT PROGRAMS, NSA Intelligence Careers, https://www.intelligencecareers.gov/nsa/nsadevprograms.html .

[8] Johnson, K. (Retrieved 2021). Who Wants to Work With a Hacker?, U.S. Department of Defense, https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2082161/who-wants-to-work-with-a-hacker/ .

[9] Data Recovery. (Retrieved 2021). Data Recovery Services Provided to NASA, Data Recovery, https://datarecovery.com/clients/nasa/ .