Nicholas Robertson

Article review 2

I'm taking a look at an article from the International Journal of Cyber Security Intelligence and Cybercrime. The article is titled Kerberoasting: Case studies of an attack on cryptographic authentication technology, and was written by Demers, D and Lee, Hannarae in 2022. It deals with the authentication program called Kerberos and how the program was hacked in multiple ways and how these hacks contributed to multiple different serious attacks.Kerberos being attacked and hacked is a big deal, because Kerberos is built in to some of the worlds most used operating systems from companies like Microsoft and Apple. The main point of this article is not only to inform the reader about Kerberos and how hackers use exploits and tactics to break through the program to infiltrate other, more important programs. But its main goal is to inform the reader on ways to combat it and steps that can be taken to keep companies safe. To begin with, while I was reading this article I couldn't help but notice that the vast majority of information that was being given out, was information that I had just learned throughout my time studying cybersecurity. Terms like NIST, HTTP, hashing and so on, but what I also found interesting and appreciated, was the fact that these terms were explained and detailed in order to make sure that the reader could follow along and understand the concepts without them having to take a full course in cybersecurity. As it goes on, it gives a brief history of what Kerberos is, who it's used and which companies use them, along with cryptography is and what the term Kerberoasting is. It's explained that Kerberoasting is a term used to signify an attack on Kerberos by "retrieving credentials of active directory service accounts without permission or escalation of privileges."(Kotlaba et al., 2020; Complex Knowledge: Kerberoasting Attacks Explained, 2021) So basically they steal credentials to gain approval or bypass the key authorization. This attack

can happen to anyone, and it can compromise anyones data in the process, but in the examples given to use later in the article, it seems that maily high profiled business and companies are the main target of these attacks. It is explained that weak passwords and phishing emails are usually how these people gain access or bypass Kerberos in the first place. It then goes on to give us case studies of different Kerberoasting attacks and how they affected different companies. These being Carbon spider, Wizard spider, Nobelium and Operation Wocao. Carbon and Wizard spider are both ransomware attacks, Operation Wocao being a Invoke-Kerberoast module to solicit credentials, and Nobelium being possibly the worst one with it being what they consider a cozybear. Being veritable undetected and feeding information gathered through a back door to the attackers. Besides the case studies there is practically no other form of research in this paper, besides the different protocols, and how kerberos was developed. After this, the article goes over the different methods, in which it can attack a person's system, mainly through human error. As stated before a common one is phishing email attacks and that's mainly the way attackers will implement these attacks, but along with the emails, there is a chance that it will contain a download link that will go to a google drive and will start to download Bazar malware if opened. It keeps going with different ways of how Kerberoasting attacks can be commenced like honeypots and lures for any potential hackers. In the end it gives you advice on how to be protected over attacks like this would be to properly train people in stronger password protection practices. They suggest passwords to be around thirty characters or more and should have a timeout sequence to prevent brute force attacks and to also change these passwords frequently to make it harder for hackers to decrypt your password. Finally the basic task of training employees/people in general to not open suspicious emails that could lead them into phishing attacks will also help too. The practice of social engineering plays a big role in these attacks and

the article seems to make it out as the be all and end all of how these attacks take place to begin with. I would say that this affects a lot of people mainly because of the sheer number of people who use either Microsoft or Apple in their day to day lives, having it be vulnerable to attacks would leave millions open to getting their data stolen. In conclusion I think this did a great job on explaining itself on how these attacks work and the method hackers use to commence these attacks. About the only thing I would criticize about this article is that in some sections of the article, it felt a little bloated with information and how it really didn't go into detail on how the average person can be affected by this. If they were to scale that down the technical jargon a little and include more examples of how this could affect the everyday person, it would be perfect.

Work cited:

"Kerberoasting: Case Studies of an Attack on a Cryptographic Authentica" by D Demers and Hannarae Lee (bridgew.edu)