Article Review: International Journal of Cybersecurity Intelligence & Cybercrime

Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology

Authors: D Demers & Hannarae Lee

Old Dominion University

Dr. Leigh Armistead CYSE 201S 23181

By: Sarah Vakos

Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology

In this article review for Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology by D Demers & Hannarae Lee, I will first go over how principles of social science relate to this article. The first principle of social science is relativism, it is defined as changes in one system can conduct changes in another system, the way decisions are made, how policies are managed, and how people share their experiences. The way that Kerberos operates for enterprises relates to other enterprises that use Kerberos and how they must keep up with its related attack, Kerberoasting. By sharing problems or reports of attacks from Kerberoasting is key to relativism because this how policies are managed from changes in a system. The next principle I will go over is objectivity and is defined as not having an opinion on a topic that is being studied to promote a non-bias research conclusion.

With the few case studies available from Kerberoasting, it might be hard to understand the full impact since other companies have not reported their experiences but with the information at hand scientists can work with what they have without thinking of ways of how they might have conducted the study better or having different approaches. The third principle is ethical neutrality and is defined as scientists having to follow ethical standards when they run their research. Ethical neutrality engages in this article where scientists must work with what they have to protect the rights of individuals or enterprises when reviewing case studies of Kerberoasting while respecting their decision-making so that they can empirically and objectively study the topic and have a full understanding. The research question of this article is figuring out how Kerberos works with its hypotheses focusing on the attack that stemmed off it, “Considering the devastating damage that can be caused by a successful Kerberoasting attack,

it is vital to understand not only how the attack works but how to defend against and mitigate attack attempts" (Demers & Lee, 2022).

This article's research methods include, "examining cases in which Kerberoasting has played a role in an attack or was used as a tool in an adversary's arsenal and review the outcomes" (Demers & Lee, 2022). By reviewing other case studies of this topic provides material to learn from to produce a full understanding and having data to produce a solution. Case studies in this article that I will go over are Operation Wocao, Carbon Spider and Nobelium. Data from Operation Wocao includes different incident response services to their clients, such as crisis management, technical investigations, and remediation. The analysis made from the Operation Wocao data was that in order to execute code on the system being attacked, Wocao used PowerSploit's Invoke Mimikatz module to try and extract Kerberos tickets from the system's memory (van Dantzig & Schamper, 2019).

Data from Carbon Spider was a two-part report from CrowdStrike and their use of ransomware. Analysis made from Carbon Spider was CrowdStrike was able to identify several Darkside campaigns that all utilized similar tools to achieve initial access (Loui & Reynolds, 2021). Once in, credentials are stolen and used to gain access into the system, stealing files and getting data from them to leak later. Data from Nobelium was based on the Microsoft Threat Intelligence Center (MSTIC) analysis of the attack against SolarWinds by an adversary called Nobelium by MSTIC (Demers & Lee, 2022). Phishing and spear phishing were used to steal credentials then searching through assets from a backdoor they built in. Analysis drawn from Nobelium was that it utilized Kerberoasting to obtain TGS tickets for Active Directory SPNs (Microsoft 365 Defender Research Team et al., 2021; Praetorian, 2022).

Empiricism is a concept from class that relates to this article and is defined as scientists studying behavior which is real to the five senses. In the article they review honey pots as an option to detect Kerberoasting attacks. Empiricism is related to honeypots due to being able to observe in real-time what a hacker is doing when they fall into the trap of a honeypot. With a honey pot that is enticing you can examine the hackers' actions once the account is live. Another concept from class that is related to this article is archival research. Archival research is defined as any record that is written or recorded and is used to conduct scientific efforts. This concept is related to the article since they use case studies to learn about Kerberos and Kerberoasting which are written records of experiments and research from other scientists or organizations.

Diversity is a concept we have discussed about in class; it is related to this article because there are a variety of distinct kinds of case studies all with different companies and organizations that studied and did experiments on Kerberoasting. There is also a diversity of how to detect and mitigate Kerberoasting attacks along with defense in depth as a policy implication for enterprises. The last concept is human factors and is defined as the field of psychology that uses psychological knowledge, including the principles of sensation and perception, to improve the development of technology as stated in module four of our class PowerPoint slides. Human factors are related to this article because of how enterprises can collaborate with each other with the data they have to improve technology and security of their systems to prevent Kerberoasting from occurring. By studying the factors related to being a human can influence the use of different projects and to producing a solution to protect the confidentiality, integrity, and availability of information.

Kerberoasting is related to the working class due to them being a consumer or a customer of businesses that contain their information and their shopping habits. This attack will often leak consumer information out to the public or to be sold to another party often times for identity fraud. This marginalized group is and can be impacted by this attack. Another marginalized group that is related to Kerberoasting is the elderly. Again, this type of group often shops online and has their data stored by businesses. Those businesses that use Kerberos are vulnerable to Kerberoasting which can affect the identities of the elderly.

Contributions to the study of Kerberoasting is for enterprises to share their breach reports from this attack. By coming together, sharing their experiences and what they did to prevent further attacks can help other companies that use Kerberos tremendously in protecting data. Microsoft Windows and Active Directory uses Kerberos so by checking and being updated by their reports and others that use Kerberos is a great deal of contribution because you can stay informed if any Kerberoasting attacks have occurred to be advised if you or your family's information has been leaked and to do everything you can to stop your information from getting into the hands of another.

References

Demers, D and Lee, Hannarae (2022) Kerberoasting: Case Studies of an Attack on a Cryptographic Authentication Technology, International Journal of Cybersecurity Intelligence & Cybercrime: 5(2), 25-39. Available at: https://vc.bridgew.edu/ijcic/vol5/iss2/3

van Dantzig, M., & Schamper, E. (2019, December 19). Operation Wocao: Shining a light on one of China's hidden hacking groups. Fox-IT. https://www.foxit.com/media/kadlze5c/201912_report_operation_wocao.pdf

Loui, E., & Reynolds, J. (2021, August 31). Carbon Spider embraces big game hunting, part 1. CrowdStrike. https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

Microsoft 365 Defender Research Team, Microsoft Threat Intelligence Center (MSTIC), & Microsoft Cyber Defense Operations Center (CDOC). (2021, January 20). Deep dive into the Soligate second-stage activation: From SUNBURST to TEARDROP and Raindrop. Microsoft Security. https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-tear-drop-and-raindrop/

Praetorian. (2022, March 8). Steal or forge Kerberos tickets: Kerberoasting. MITRE ATT&CK. https://attack.mitre.org/techniques/T1558/003/