Literature Review

Jordan Peters

March 1, 2020

I certify that all material in this dissertation which is not my own work has been identified.

Contents

1 Introduction

In 2010, a "worm" virus, one that spreads across and embeds itself into systems, infected approximately 100,000 systems [1] and caused exactly 984 nuclear centrifuges to repeatedly malfunction [2] over the span of at least 1 year [1]. It eluded detection by performing specific subroutines that would cause the equipment to only breakdown in such a way that it would cause no harm to people, and would make the scientists believe the equipment they were sold was just faulty and that they were unlucky. [2]

This virus was called Stuxnet, and its inception 10 years ago caused many researchers to become scared at the real-world implications that Stuxnet showed. [1] [2] Stuxnet proved that cybernetic attacks on critical infrastructures such as nuclear reactors are possible, and aren't just the type of attack that exists within the realms of theory or movie plotlines. [1] Stuxnet was of such high complexity and danger that security researchers at Symantec said they hope to never see anything like this again. [1]

How do attacks like these ever get remotely close to the systems that they target? What are their routes of intrusion? Was it difficult for the attackers to attack this way, or is it easy if you have the knowhow? This literature review aims to answer the question of how cybersecurity penetration is often orchestrated, and what researchers are attempting to do to analyse these attack vectors and deny infection altogether before catastrophy can be inflicted.

2 Literature Review

2.1 What do researchers know?

2.2 What do they not know?

2.3 What has been researched and what has not been researched?

2.4 Is the research reliable and trustworthy?

2.5 Where are the gaps in the knowledge?

3 Conclusion

Summary and conclusions to take forward.

4 Bibiliography

References

[1] N. Falliere, L. O. Murchu, and E. Chien, "W32. stuxnet dossier," *White paper, Symantec Corp., Security Response*, vol. 5, no. 6, p. 29, 2011. [Online]. Available: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-044.pdf

[2] P. W. Singer and A. Friedman, *Cybersecurity: What everyone needs to know.* oup usa, 2014. [Online]. Available: https://books.google.co.uk/books?id=B88ZAgAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false