Assignment 13: Ransomware

6 Steps

Kevin Durand

Introduction

When looking at the overall cyber operations that go into prevention and eradication of malware in a country or industry, there are a couple steps that a company can take. The first two steps, Pre-Planning and Preparation, are largely information-gaining steps to figure out the problems and the causes of those problems. The next two are dedicated to figuring out exactly what is attacking a system and containing it, these are the Identification and Containment sections of this process. Now that you know where the malware is and how it affects the system, you go into the Eradication mode, of getting rid of the malware. Usually after the system has been removed of the malware you go into a recovery mode, where you fix the system. Lastly you need to overview the system, see what has been learned and how to prevent things in the future.

Pre-Planning and Preparation

Based on the article by E&T, a lot of what needs to happen in regards to the problems the UK are facing, seem to be more of a prevention and social engineering problem. The main steps that would be most useful, in this case, would be in the preparation and prevention phase. In the article, we get a good look at what is causing these issues, "“Over half of employees working in retail don’t understand the cyber-security implications of poor password hygiene..." (E&T editorial staff); plainly it is visible that the preparation that would need to go into this would be to start teaching how to do better password hygiene. I would likely spend time sending out questionaires on password uses in the general public, then respond to those people with the goal of tracking down the malware being used.

Identification and Containment

Now that the source of the malware is identified, at least to the extent of we have a good understanding of how the malware is getting on the computers in the first place, we can go about figuring out what systems are on a computer. "The report also highlighted the threat of ‘Double Extortion’, a tactic used by gangs that involves the threat of leaking sensitive data online if victims refuse to pay..." (E&T editorial staff) tells CISA that we are looking for malware that is Ransomware that works with the help of a Worm or Rootkit, that allows the user into the system, probably as some sort of fake program on the user's computer. So we would then work to find out what exactly is being used, and then contain it to stop it from further doing damage. In addition we would eradicate the program.

Recovery and Review

This is largely the main point of what my team would do, while we have gotten rid of the malware on some users computers, their password practices may cause the issue to come back. What I would try to do is make sure that people are better about preventative measures. Since the public of the UK is involved, it is a lot harder to set down behaviors; as opposed to some retailers where company policy can prevent a lot of the issues. Doing classes and public announcements, we could inform the public why its been so easy for these attacks to happen and how to prevent them. Further than classes, we can engage with the general public, showing them exactly how their password practices can make it easier for malicious actors to gain access to their systems and data.

References

1. E&T Editorial Staff (2021, Nov. 12). *Ransomware is cyber-criminals' weapon of choice; UK retail facing barrage of attacks.* Engineering and Technology. https://eandt.theiet.org/content/articles/2021/11/ransomware-now-cyber-criminals-weapon-of-choice-as-uk-retailers-face-barrage-of-cyber-attacks/
2. Irwin, Luke. (2022, Oct. 5). *The 6 Phases of Cyber Incident Response Plan.* GRCI$_{\text{Law}}$. https://www.grcilaw.com/blog/the-6-phases-of-a-cyber-incident-response-plan
3. Baker, Kurt. (2022, Aug. 11). *The 12 Most Common Types Of Malware.* Crowdstrike. https://www.crowdstrike.com/cybersecurity-101/malware/types-of-malware/