Exploit Research and Presentation

Andrew Maddox

University of Advancing Technology

Author Note

This paper was prepared for NTS330, taught by Aaron Jones.

Abstract/Structure

This paper goes over a malware also known as ransomware. Ransomware affects many businesses in the modern-day industry as well as individuals. Business mitigation and prevention in my opinion will be a large part of keeping these from affecting corporate communities.

Opening paragraph: Goes over the information about the malware and the small pieces vital to understand the rest of the information.

Main information: The main information involving the malware discussed and the details of such.

Ransomware: This section goes over ransomware as a whole and the versions and types it contains.

Risk to organization: This goes over the current risk assessment to the organization itself and what risk these involve.

Mitigation to risk: This goes over how to mitigate the problem at hand and better prepare workers and staff to not be affected by the ransomware.

Opening Paragraph

The malware I will be talking about involves business security financial and the current systems integrity. Ransomware is a large security risk in business nowadays as unsuspecting workers can download or possibly trigger an attack of sorts. This exploit is serving as a risk to business security and stands as a financial threat if good tactics to prevent this, like backups have not been placed. With our current system the integrity involving a ransomware attack would not be substantial and that is one of the actions that will be taken.

# Main information

Ransomware is a form of malware and has many purposes with different demands and actions. Most of malware is caused by social engineering ploys commonly tricking people to download a file from an email which is a big threat to businesses with susceptible workers. Ransomware attacks can be posed as multiple fear inducing personas such as the FBI or an important business person etc.

Ransomware

Ransomware comes in many different forms and serves many purposes and those will be covered here.

1: Scareware is a version of ransomware commonly carried out by tech support scams or other scams that involve pop up messages or something to provoke fear with a supposed solution. These scareware tactics usually involve a fee to get the ransomware “removed”. In these situations, there are usually empty threats and many popups but essentially the integrity of the files are safe and secure. The current software that is employed by network security experts in specific businesses will never request more money in the way these scammers request it.

2: Screen locking ransomware involves a complete lock down of a computer itself. This ransomware will completely block you from use of anything for the common user. These will commonly include a message speaking as if it is from the FBI or some official organization. Usually a scare tactic used by these are a mention of illegal activity detected on your personal computer. This supposed illegal activity can include cybercrimes like child pornography or piracy. This is a much more complex attack then scareware and controls many aspects.

3: Encrypting ransomware involves files and is probably the biggest threat to companies and individuals. Encrypting ransomware means a scrap of a system entirely most of the time because the files themselves have been compromised. This attack cannot be easily solved by any security software or system restore unless a backup is involved but there is still no guarantee. Once the files have been compromised with this attack there is little to no solution and serves as a big problem to business computers when they become compromised.

The Risk Ransomware Poses to Organizations

Ransomware poses a large risk to the organization itself as many workers are susceptible and can cause issues in the system and to personal computers. The majority of workers in the building uses a personal computer during work hours which means the number of devices susceptible to attacks is very high. These attacks can cause minimal to catastrophic damage depending on what system is compromised and who receives it. If a higher up like the CEO, CIO, or CISO with access to multiple systems computer gets compromised it is a bigger threat to the business then a simple machine. If the mainframe or something beyond that gets attacked or compromised the whole system in turn is compromised especially if a mainframe server is affected. If a full system or server is compromised with an encryption the data is basically trashed and is not good for the business.

Presentation on How to Mitigate the Risk

Steps the business could take to mitigate the risk of possible attacks or vulnerabilities due to lack of policy and mitigation practices.

1: A policy and run down or class for current workers to attend including information about ransomware and how to prevent it. Most likely the class will be taught by the head of IT or the IT department as they are most the most familiar with the current system and how it performs. The class would be mandatory for all workers and would contain vital information for them to properly keep systems secure.

2: Email security needs to be a core component and a large portion of monitoring for the IT department. If the IT department sets parameters or overviews certain suspicious emails running through it would mitigate possible attacks or compromises. Among monitoring traffic and many other security aspects IT plays a large part in business security.

3: Reference sheet. References sheets as to what emails to respond to and what are company emails and what are non-company emails is a good tool to have. The email reference sheet would be created in collaboration with the IT department along with regulations that usually indicate whether the emails are trusted.

4: Demographic. Hiring demographic plays a big part into whether workers are susceptible to many of these vulnerabilities. Commonly a younger demographic is more aware and statistically less likely to fall for phishing scams etc. Studies show that “more than 2 million different infections in the last year, focusing on the ten U.S. cities with the highest median age and the ten cities with the lowest median age. Their data showed that the infection rates in the “older” cities was 161% higher than in the “younger” cities”. It seems fair that all recruitment and choosing of certain people for jobs should not be solely based on this but as a mitigating factor it’s a fair point.

References

Ironcore. (2018, December 12). 7 Security Trends Shaping Intrusion Detection Technology. Retrieved from https://bricata.com/blog/trends-intrusion-detection/ -exploited-to-download/

Ransomware - What Is It & How To Remove It. (n.d.). Retrieved from <https://www.malwarebytes.com/ransomware/>

Raposo, K. (2015, July 27). Study shows older people are more susceptible to malware attacks. Retrieved from <https://knowtechie.com/older-people-are-more-susceptible-to-malware-attacks-according-to-recent-report-126/>