International Journal of Management, IT & Engineering
Vol. 10 Issue 06, June 2020,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Cybersecurity & COVID 19

Rishit Mishra

Abstract

With the world being caught in the middle of a pandemic and trying their best to fight the COVID 19 virus, a new concern is emerging – Cybersecurity. With the wide spread panic of the virus threat actors are using this opportunity to exploit the situation. As companies adapt to a changing model with more and more employees working remotely cybersecurity is becoming one of the key questions the companies need to answer. With more and more employees being outside the organisations network and using their own network, concerns over the safety of the organisations data and increased risk of compromise is something organisations need to think about. In this paper we discuss what types of attacks have been happening and how we can protect ourselves from these attacks.

Keywords:

Security
Cybersecurity
Malware
Phishing
Risk
Vulnerability

Author correspondence:

Rishit Mishra
Email: rmishra1907@gmail.com

1. Introduction

With the COVID 19 pandemic spreading like wildfire across the world almost all organisations within the world moved their employees to a remote access or a telecommuting option. Embracing this new normal comes with additional set of challenges as corporate servers are becoming more vulnerable to cyber attacksand companies should be thinking about taking additional precautionsto ensure their organization is ready to handle this from move a security standpoint and think about getting their employees are trained and aware.

2. Phishing Attacks

Google recently reported almost 18 million phishing scams were being reported everyday related to COVID 19. That is in addition to millions of phishing scams that get reported everyday. A research noted almost 667% hike in phishing attacks in the last couple of months. So what is Phishing?

Phishing is a form of social engineering. In social engineering the attacker interacts with the human by using his social skills and tries to obtain information that can compromise the information of an organization or its IT/computer systems. Phishing attacks use different methods such as email, malicious websites etc. to gain information which is mainly achieved by posing a trustworthy organization.

Different types of attacks have been seen going around the globe and these attacks are becoming more and more sophisticated as the day goes by.Threat actors are using the current situation and the exploiting the human need for information.Below are some of the attacks that have been observed

1. **Alerts** – In these attacks email apprears to be sent from reputed organisations like WHO and CDC informing about cases in your area and provides a link which you can click to find more information about these cases. Once you click on the link it installs the malware in the background on your system which compromises your data and the security of your system.

*Master's in Management Information Systems from Texas A&M University, USA

2. **Fake Stimulous check emails** – With more and more people eagerly waiting to receive their stimulous checks in this grave unemployment situation cybercriminals are sending notes like the below with the intent of capturing the user's data and exploiting them.

Figure 1 – Example phising email

3. **Coronavirus possible cure emails** – This email spoofs the address of the World Health Organisation (WHO) and says that they have solution for this disease and urges the user to forward it to all their friends and contacts. Once the user opens the malicious attachment it installs Agent Tesla malware. Agent Tesla is known to exploit known MS Office vulnerabilities CVE-2017-11882 and CVE-2017-8570. Through the CVE-2017-11882 vulnerability the attacker basically runs the arbitrary code to install the Agent Tesla malware and the exploiting CVE-2017-8750 downloads the payload which logs the user's key strokes and steals the user's sensitive data. Below mentioned is the attack chain.

Figure 2 – Agent Tesla Attack Chain

3. Exploiting Remote Access Vulnerabilities

As organisations prepare for a new normal and more and more organisations see workers working remotely, there has been growing risks and concerns over the organizations ability to scale and secure these remote communications. Lot of organizations did not have a remote model and were forced to deploy these remote networks, VPN's and the related IT infrastructures within a very short span of time. Malicious attackers take advantage of these last-minute mass movements in the hope that either the set up was not done accurately or misconfiguration was performed so they can exploit a known vulnerability within the system.Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) both noticed increased activities as actors were observed scanning known vulnerabilities in exisitingVPN products such as Citrix, Pulse Secure etc.

Some organisations have faced the challenges where being unable to procure enough hardware or IT equipment were forced to have their employees connect to the company's network using their personal devices. Now this imposes a two-fold challenge. Primarily the organisations are not aware of the extent of security like firewall, antivirus software that is installed in the employee's own computer and if it has already been compromised before or not.

Secondly given the nature of this sudden move to the remote model organisations were unable to dedicate enough time to train employees on the do's and don't of working remotely and how security needs to be considered leaving and their data at risk of an attack. Also as employees continue to work remotely, people are eager to venture out to change their environment and head over to café's or places with free wifi connections which puts the organisations systems at a greater risk when the user is trying to access it using an insecure network.

4. How to protect against these risks?

Cybersecurity is always evolving, and the threat actors are constantly adjusting their strategies in response to the mitigations that are developed. But there are certain things that we can always do to keep ourselves safe and secure from these types of attacks.

Phishing

- Avoid emails from unknown sources which contain a generic greeting as phishing emails are more likely not to use your exact name
- Keep a watchful eye on spelling mistakes and grammatical errors within these phishing emails
- Check on the address from which the email is sent or the link/URL they want you to click. Often this can be a very easy way to know if it's a fake.
- Be wary of online requests that ask you to provide your personal information such as SSN, login credentials, credit card details etc. over the email.
- Ensure to report any breach or suspicious activity/email to your organizations IT team so appropriate action can be taken

Remote Connectivity

- Ensure network devices, VPN's and devices which are being used to remote connect into the work environements are on the latest softwre versions and configurations.
- Ensure VPN connections which are setup are tested and IT teams are readily available in case any cybersecurity activities as required
- If possible, implement Multi factor authentication (MFA) for all VPN connections which increases security.
- If MFAcannot be implemented, implement strong password requirements

5. What to do if you have become a victim?

The best way to protect yourself from these attacks is to prevent them from happening. But in case you have fallen a victim to these what can you do next:

- Change the passwords for all the accounts you think that might have been compromised and those which might have similar or same passwords
- If credit card information was compromised inform the financial institution and cancel the credit card
- Update your devices malware and anti spyware software and run a full scan.
- Keep an eye on any unexepected activities on your accounts like login at an unexpected time or from an unknown country
- Wherever possible either set up multifactor authentication and if not try to ensure you have strong/compex passwords which cannot be broken down by brute force or dictionary attacks.

6. Conclusion

The paper presents an overview of the cybersecurity risks that are being seen during COVID 19 and how you can keep yourself safe from those. As security attacks become more sophisticated it is imperative that we keep ourselves aware and upto date with the latest trends in security and try to stay one step ahead of the attackers.

References

[1] https://www.us-cert.gov/ncas/alerts/aa20-099a
[2] https://www.jdsupra.com/legalnews/cybersecurity-risks-increasing-during-38481/
[3] https://www.wandera.com/signs-youve-been-phished/
[4] https://www.cisomag.com/researchers-uncover-agent-tesla-malware-abusing-ms-office-vulnerabilities/
[5]https://www.infoblox.com/wp-content/uploads/threat-intelligence-report-agent-telsa-infostealer-use-coronavirus-themes-v2.pdf
[6] https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html
[7] https://www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams
[8]https://security.berkeley.edu/news/scammers-are-exploiting-coronavirus-fears-phish-users
[9] https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020