The Cyber Collective
Enhancing Security Mindfulness
www.thecyco.com

DANGERS OF TORRENTING TO BUSINESSES

April 2021

1.0. INTRODUCTION

Torrenting is the act of sharing content on a peer-to-peer (P2P) file-sharing network. P2P file sharing enables different users to connect for the purpose of exchanging files without uploading them to a server. These files are called torrents.

2.0. HOW TORRENTING WORKS

Torrenting does not enable the storage of files on a centralized server. However, the files are broken down into bits of data and saved in participating computers (peers) on a network to aid the file-sharing process. For instance, a P2P file sharing protocol like BitTorrent breaks down files into pieces and move them from uploaders to downloaders via a torrent client program. This program connects users to exchange data after reading all the information in the torrent file.

3.0. TORRENTING RISKS TO BUSINESSES

A report by BitSight in 2015 gave perspective and insight into how organizations interact with Peer-to-peer file-sharing networks such as BitTorrent. BitSight researched over 30,700 and discovered that 23 percent of these organizations interacted with BitTorrent for P2P file sharing. It was also discovered that 43 percent of torrented files contained malware.

From the above analysis, it can be deduced that a hand full of companies have employees that secretly use the company's network to download torrent files. Research has shown that the most downloaded files from P2P file sharing networks are movies and most of these movies are copyrighted, which makes this act illegal. In May 2020, Microsoft caught cybercriminals adding malware to "*John Wick 3*" and "*Contagion*" movie torrents in Spain, Mexico, and several American countries. Cybercriminals are evolving their attack methodologies daily and recently, one of the most common strategies is to attack individuals, businesses or organizations by embedding malware in 'free' movies, music, or applications. Malware such as Viruses, Worms, and Trojan-horses are harmful to enterprise endpoint devices and can disrupt the smooth running of a business.

Author: ***Segun Ebenezer Olaniyan***

The above mentioned risk is not the only risk torrenting poses to businesses and organizations, below are more of such risks:

i. **Ransomware:** These are malicious software designed to hold computers to ransom by blocking access to the data, information, and files contained on such computers until a stipulated amount is paid. ComputerWeekly reported in July 2020 that *EvilQuest* - a MacOS Ransomware - spreads through pirated versions of popular MacOS software products downloaded as torrents. This Ransomware can encrypt the victim's files; install a keylogger that monitors and record keystrokes made on the victim's computer, and steal any files found that relates to cryptocurrency wallets. Ransomware has cost enterprises billions of dollars and torrenting can expose an organization to this costly risk.

ii. **Data Infiltration:** Torrenting using an organization's endpoint devices can expose the entire organization to the risk of unauthorized access to sensitive business information. The sensitive information can include data about the company's stakeholders, financial records, employee records, etc. Whenever an employee downloads a torrent file from a P2P file sharing network using the company's computer, the company network information will be exposed and attackers can leverage this information to launch their attacks.

iii. **Legal Crisis:** The greatest risk of torrenting is that most torrent files contain copyrighted materials. Users who engage in torrenting copyrighted material are liable to face legal issues hence, if an employee uses an organization's device to download torrent files, the entire organization is at risk of facing legal charges or huge fines for illegal activities. Some Internet Service Providers now monitor torrent users' activities online and if caught downloading copyrighted torrent files, such an organization can be suspended from the ISP's services.

4.0. MITIGATING TORRENTING RISKS

So how can organizations keep employees from torrenting the business into a cyber attack?

i. **Blacklisting**

This is a security control model which explicitly defines prohibited activities and IP addresses and consequently authorizes anything that doesn't fit the definition to be blacklisted. Leveraging on firewalls is one of the most effective ways of implementing Blacklists as firewall blacklisting restrains access to and from flagged websites. Intrusion Detection or Prevention Systems (IDS or IPS) are also effective ways to implement blacklisting.

ii. Whitelisting

This security control model explicitly names or lists approved activities, connections, files, users, or applications. So an organization can create a concise list of acceptable websites, IP addresses, or applications and block access to any others not on that list. It tends to be a more effective security control measure than Blacklisting, as it is not too feasible to single out and blacklist EVERY known criminal address on the internet. Organizations can take advantage of whitelisting programs built into their systems, routers, and other endpoint and network appliances, or check here for more resources.

5.0. CONCLUSION

It is not enough for organizations to believe their information systems infrastructure is safe until the activities of all employees on the organization's network and endpoint devices are critically probed. Also, conducting regular cybersecurity awareness trainings for employees will enhance thier security mindfulness and induce security best practices.

REFERENCES

https://news.softpedia.com/news/employees-downloading-torrents-files-put-many-companies-at-risk-498056.shtml
https://www.techrepublic.com/article/microsoft-catches-cybercriminals-adding-malware-to-john-wick-3-contagion-torrents/
https://www.computerweekly.com/news/252485493/Mysterious-EvilQuest-macOS-ransomware-spreads-through-torrents
https://www.varonis.com/blog/ids-vs-ips/
https://www.springboard.com/blog/what-is-whitelisting/