Finding Malicious Malware using Twitter Scanner

Morgan Hamlin & Dr. Fredericks, Grand Valley State University

Introduction

Zoom has become an increasingly popular application. This has led to an increase in cyber-criminal activity. Cybercriminals have been utilizing social engineering tactics to persuade users to download compromising software. Their agenda is to gain access to sensitive information and exploit your system. I utilized a Python bot to find malicious malware posted on Twitter under the domain name of Zoom. This bot can scan and identify potential threats, with the idea being to bring awareness to phishing scams and help mitigate dangerous Zoom downloads on Twitter.

Further information

This was an observational study in which randomly selected tweets were pulled for data analysis within Twitter's API. A Python bot using search word zoom.us the bot looked for the keywords: download, update, and join us. Under each category the tweets were analyzed for the following categorical variables defined as;

Phishing Scam: A link requesting money and information beyond registration name and email.

Malicious Malware: A link with executable files or other automatic downloads.

Potential Threat: An automatic meeting link that has an exposed password.

Citations

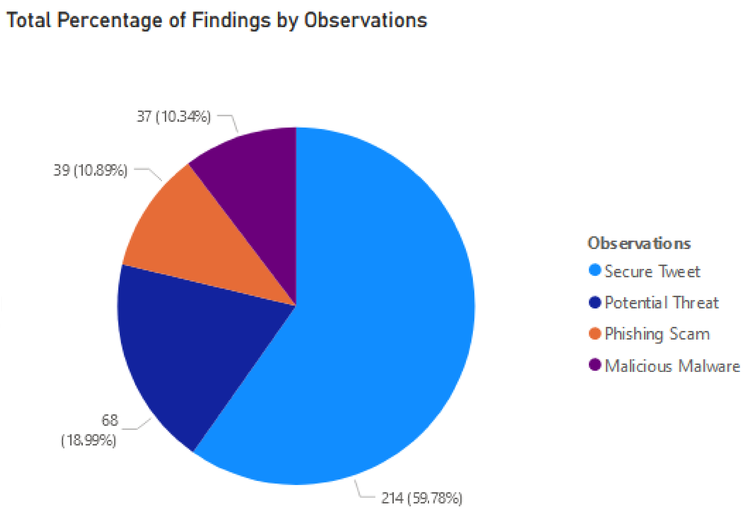
"Best Practices for Securing Your Zoom Meetings." *Zoom Video Communications, INC.*

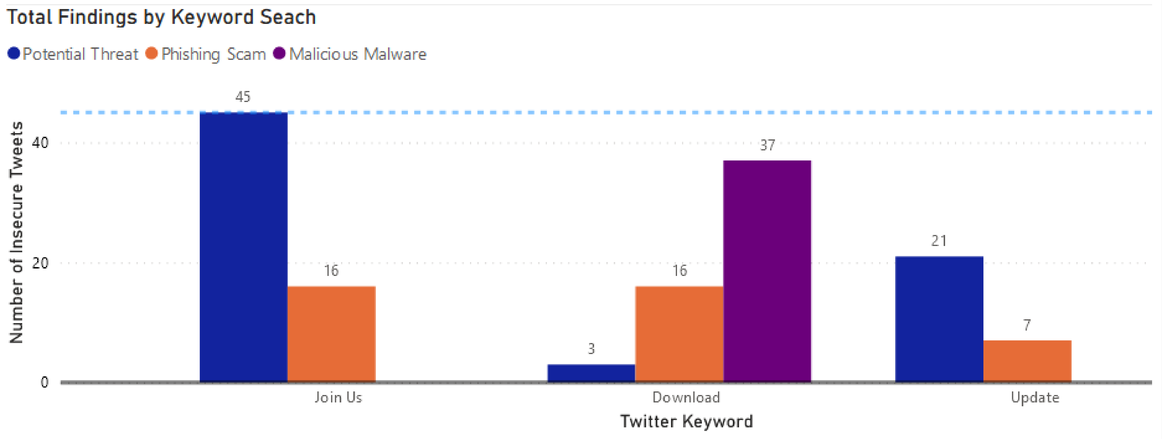
"About Account Security." *Twitter Help Center.* https://help.twitter.com/en/safety-and-security/account-security-tips

"Twitter Scanner." *Morgan Hamlin (2022)* https://github.com/morgan91-bit/TwitterScanner.git (2022).

Results

Out of 360 Tweet observations only 59.78% were considered secure. 18.99% were considered "Potential Threats", 10.89% were "Phishing Scams", 10.34% were "Malicious Malware". Over 40% of our tweet observations under the category zoom.us are considered insecure. Below you will notice, out of the 360 total observations, 120 per keyword, Join Us had the highest number of "Potential Threats" at 37% followed by "Update" with 17% and "Download" with .025%. "Download" was the only keyword that found "Malicious Malware" with 30% of its observations. "Phishing Scams" were even between "Join Us" and "Download" at 13% followed by "Update" with 0.05%.





Conclusions

People post Zoom meetings on Twitter, saying "Join us", "Download Now" or "Update your Zoom", my bot scans for those keywords and analyzes potential threats. Out of the total 320 tweets collected 40% were considered threats, out of that 40%, 10% was "Malicious Malware". This is a bigger issue then people think, it is affecting people without them knowing leaving people exposed and vulnerable. Most people scan social media sites without being aware of what links they are clicking and the consequences that can follow.

Malicious Malware Awareness

When it comes to malicious malware Twitter Help Center has good advice. "Many Twitter users post links using URL shorteners, like bit.ly or TinyURL, to create unique, shortened links that are easier to share in Tweets. However, URL shorteners can obscure the end domain, making it difficult to tell where the link goes to. In general, please use caution when clicking on links." (Twitter Help Center, 2022)

Phishing Scam Awareness

In addition, most of the phishing scams were observed to be under the use of Zoom's register feature. Before joining, a host would ask various questions beyond name and email such as your full address, college you attended, where you work, email, phone number, age, etc. all this data is collected and used by the host, not Zoom. In this case the host user can gains access to sensitive information and can exploit your system. Utilizing two factor authentication and maintaining awareness about the data you are giving to unknown sources is an important to your security.

Potential Threat Awareness

"Potential Threats" with 18.99% of the total observations, automatic links where the highest's threat. To give users more control over their meetings Zoom Video Communications Inc., is recommending users to use:

1. Turn on Your Waiting Room.
2. Don't Use Personal Meeting ID for public meetings.
3. Require a passcode to join
4. Only allow in registered or domain verified users.