Cybersecurity and the Social Sciences (CYSE 201S)

School of Cybersecurity

Old Dominion University

Instructor: Diwakar Yalpi

Student: Charles Martin

February 17, 2024

Week 6 Journal Entry - Can you spot three fake websites and compare the three fake websites to three real websites, plus showcase what makes the fake websites fake?

Typo squatting is a cybercrime that criminals use to mimic real websites so that victims will go to the fake URL and then put in personal information or have them download malicious files. It can be a simple letter swap or misspelling, which cannot be easily noticed. There are three examples of such websites that try to be deceptive to reach these nefarious goals. One is notepads-plus-plus[.]org, which mimics notepad-plus-plus.org. (Toulas, 2022) Adding an “s” to Notepad makes it a completely different website where one hacker may have a file available for download filled with anything malicious to the victims. The website looks like the actual website, which is the case for all other sites. The victims would believe that they are downloading a notepad type of software, but instead, it could be something malicious. “The files from this site install the Vidar Stealer information-stealing malware, which has had its size inflated to 700MB to evade analysis.” (Toulas, 2022) Another one of these examples uses a different domain extension. www.torproject.org is imitated by www.tocproject.com. It is an easy mistake to click on the wrong website, but one that has severe consequences. “In this case, the website drops the Agent Tesla keylogger and RAT.” (Toulas, 2022) The last fake website I could find was the ethersmine.com malicious site, which is like the ethermine.org cryptocurrency site, which targets wallets and seed phrases. (Toulas, 2022)We must be vigilant about how we go to websites on the internet. If a website looks misspelled or gives off weird vibes, do more research and ensure that users go to the correct site before it is too late.

References

Toulas, B. (2022, October 23). *Typosquat campaign mimics 27 brands to push Windows, Android malware*. Retrieved from BleepingComputer: https://bleepingcomputer.com/news/security/typosquat-campaign-mimics-27-brands-to-push-windows-android-malware/?&web_view=true