**Chapter 2: The Rise and Fall of the Virtual Caliphate**

**By**

**Natnael Kebede**



**University of Dallas**

**2020**

This Paper Submitted in Partial Fulfillment of the Requirements for

CYBS 7359 – Penetration Testing and Vulnerability Assessment

Spring 2020

Presented to Dr. Renita Murimi

1. How have virtual communities altered the landscape of communities?

Virtual communities have altered the landscape of communities by establishing their continued and expanded presence through the internet and leaving the physical environment they once controlled. This technique allowed the virtual communities to satisfy their need for survival.

1. Research: early online communities

The history of online communities goes back to the 70s. Before the dawn of personal computers, a handful of specific individuals were holding online discussions via posted messages on bulletin boards. These boards were web applications that managed user-generated content. These message boards gave rise to early Internet forums that allowed individuals to post messages and comment on other messages. Eventually, small electronic mailing lists gave rise to forums that address specific topics. The forums, in turn, grew to multiple electronic communication means, with some of them consisting of millions of users. Due to these means, a sense of friendship grew among frequent visitors, and thus the first online communities appeared. Fast-forwarding to the 21st century, the popularity of online communities and community forums has skyrocketed (Ure, n.d.).

1. What are the barriers to entry for online participation?

The barriers to entry for online participation are identity, shared interests, and password requirements to access discussion pages.

1. Which disciplines could contribute to an understanding of cybersecurity?

The disciplines that could contribute to an understanding of cybersecurity include social and behavioral sciences. That is, effectively understanding cybersecurity requires an understanding of the human context. Social and behavioral sciences address this concern by providing us with the knowledge to address the interaction between humans and computer systems. The sciences also allow us to conduct research on vulnerable systems to enhance security controls.

1. What is the role that video sharing has played in formation of online communities, information dissemination and cybersecurity threats?

Video sharing has played a significant role in the formation of online communities by letting them access or upload video content. Supporters can access the content and share their ideas. Information can also be disseminated by sharing the link of the video content on forums. However, this technique also increased cybersecurity threats as it relies on targeted individuals who click on links that could be malicious.

1. Research: DDoS and a recent attack.

A distributed denial-of-service (DDoS) occurs when multiple machines are working together to attack a specific target. DDoS attackers often leverage the use of a botnet (a group of hijacked internet-connected devices to carry out large scale attacks). To make the attack possible, attackers take advantage of security vulnerabilities to control various devices using command and control software.

One of the recent DDoS attacks, and the largest one was that of GitHub’s, an online code management service. The servers of GitHub were hit by 1.3 Tbps of traffic that flooded them with 126.9 million packers of data each second. Unlike many recent DDoS attacks, the attackers used a strategy known as memcaching. The technique involves delivering a spoofed request to a vulnerable server that then floods a targeted victim with amplified traffic instead of botnets. The attack was the biggest recorded DDoS attack and took GitHub’s systems down for about 20 minutes (Felter, 2019).

1. How can you construct the profile of a hacker?

You can construct the profile of a hacker by carefully examining various circumstances. That is, one needs to study previous hacks, both successful and not, to understand the steps necessary. The hacker then creates a plan and find a way to enter a victim’s environment. To accomplish the entry, the hacker uses various techniques. Some of these include exploiting a vulnerability, launching malware, bypassing security controls, stealing a password, mapping a network, maintaining access, escalating privilege, or pursuing a DDoS attack (Long, 2012).

1. Research: Collective intelligence and its applications

Collective intelligence refers to a combined or group intelligence that emerges from the collaboration of various individuals with different backgrounds. Such type of intelligence is known to provide smarter decisions.

According to the author, collective intelligence mined from the internet was proved to be effective in decisions that exhibit coordination challenges, cognition calculations, and cooperation networks.

1. How can you use prediction to predict cybersecurity incidents?

We can use data-driven predictions that are generated from the increasing amount and complexity of cybersecurity attacks to predict future cybersecurity incidents. This mechanism involves utilizing research communities and industries that propose incident prediction schemes by using information from different data sources. Such sources include network data, social media data, data from webpages, and so on. Using the dataset, one can then apply machine learning techniques to analyze recent incident occurrences, make analysis, test existing security controls, and make a comprehensive summary that outlines what to expect soon.

1. When does the wisdom of experts fail?

According to the author, the wisdom of experts fails when they attempt to crowdsource questions. Such questions can be based on predictions to provoke the audience whose way of thinking has been unified by social media.

1. What is herding?

According to the author, herding refers to the tendency of large groups of people to behave the same way and even pursue a way of thinking that is similar.

1. What is the future of online behavior? Websites-> Forums -> Social Media -> Mainstream applications -> Encrypted apps -> ?

The future of online behavior on Websites, Forums, Social Media, and apps seems to exhibit cooperation among individuals. The cooperation, however, relies on a certain level of trust that the others in the group have already established. Additionally, individuals will continue to show behaviors that are horrible when compared to real-life interactions with strangers. This scenario arises from the fact that these communication means offer physical distance with relative anonymity and little reputational or punitive risk for bad behavior (Vince, 2018).

References

Felter, B. (2019). 5 of the Most Famous Recent DDos Attacks. Retrieved from https://www.vxchnge.com/blog/recent-ddos-attacks-on-companies

Long, L (2012). Profiling Hackers. SANS Institute Information Security Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864

Ure, C. (n.d.). A Short History of Online Communities. Retrieved from https://forumbee.com/article/q5hh79/short-history-of-online-communities

Vince, G. (2018). Evolution explains why we act differently online. BBC Future. Retrieved from https://www.bbc.com/future/article/20180403-why-do-people-become-trolls-online-and-in-social-media