Goldshire Network Traffic

WESTERN WASHINGTON UNIVERSITY

Justin Greene, Kenny Kettler, Elizabeth Schoen

CSCI 497L
Spring 2018
Dr. Michael Tsikerdekis

Introduction

Goldshire is a real, undisclosed city in Washington State, monitored by the Washington State Fusion Center. The network traffic we monitored was that of approximately 200 state, government, and private employees that opted into the program. Some notable features of Goldshire traffic are:

- Main policy violation Dropbox LAN sync broadcasts
- Possible Drive-By Download Attack investigated
- Created a Profile for which countries or groups are targeting Goldshire with Spearfishing and Mail Spam attacks

Spear Phishing and Mail Spam

Our team observed a huge volume of constant spam and presumably phishing attempts made to our local network. This spam originated mainly from three countries outside the United States. **Figure 3** shows the volume of this traffic over the span of April and May.

- While we did observe some spam out of the UK and the Ukraine, the bulk of our spam came from Seychelles, an archipelago off the coast of Africa
- On average our local web server received around 10,000 - 20,000 bytes of junk mail, spam, and potentially malicious files

Recommendation: Add the Seychelles IP to the local firewall, as it makes up more than 80% of the blacklisted traffic and likely none of it is legitimate.

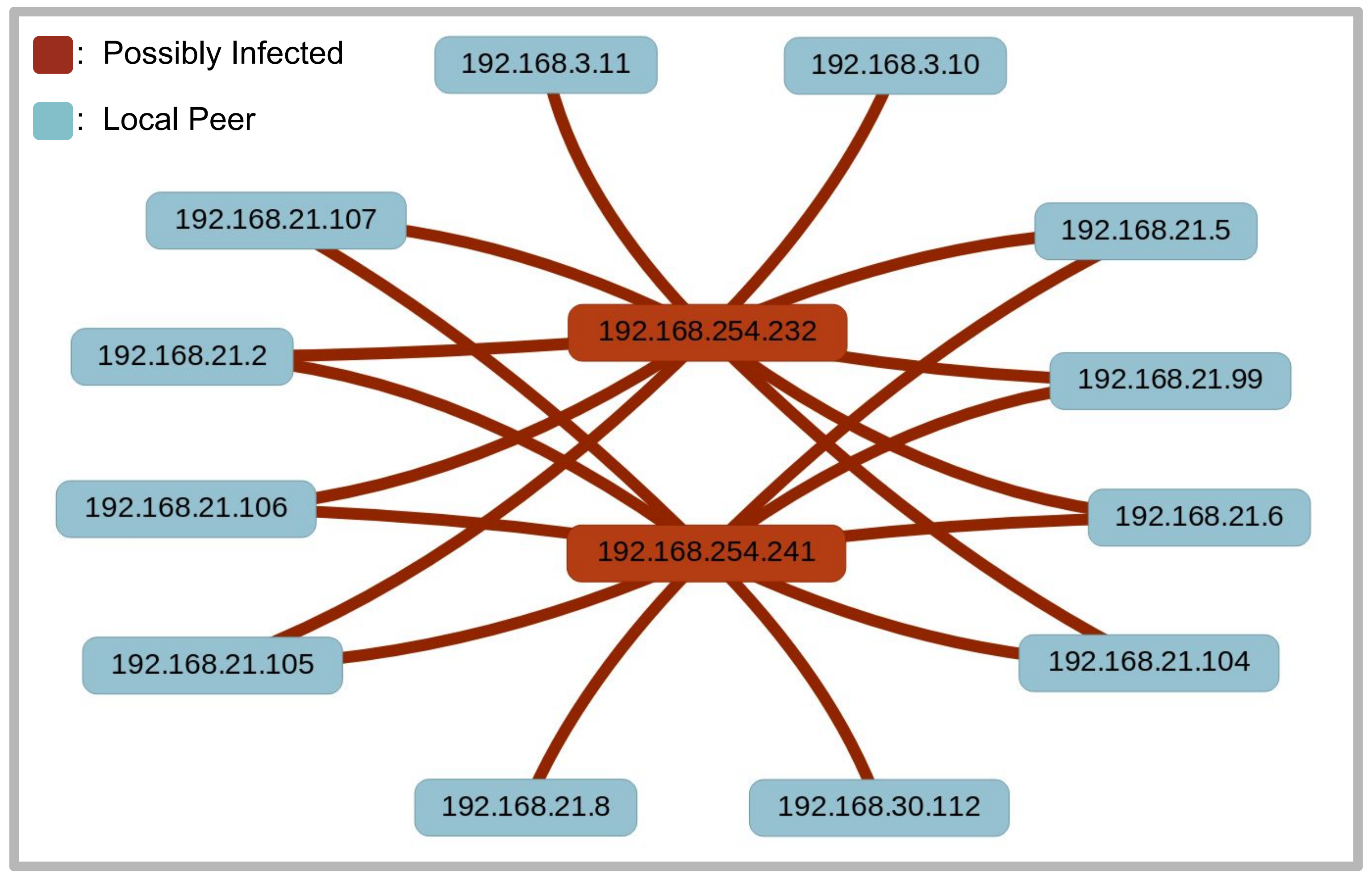

Figure 4. NetGraph showing local connections on ports 135 and 445 over a month

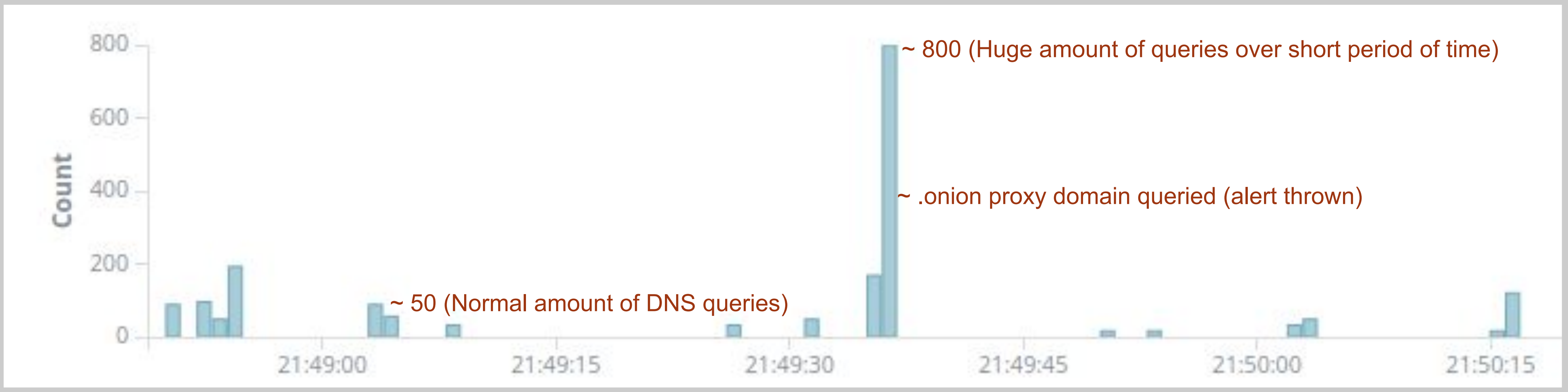

Figure 1, DNS Query volume Spike

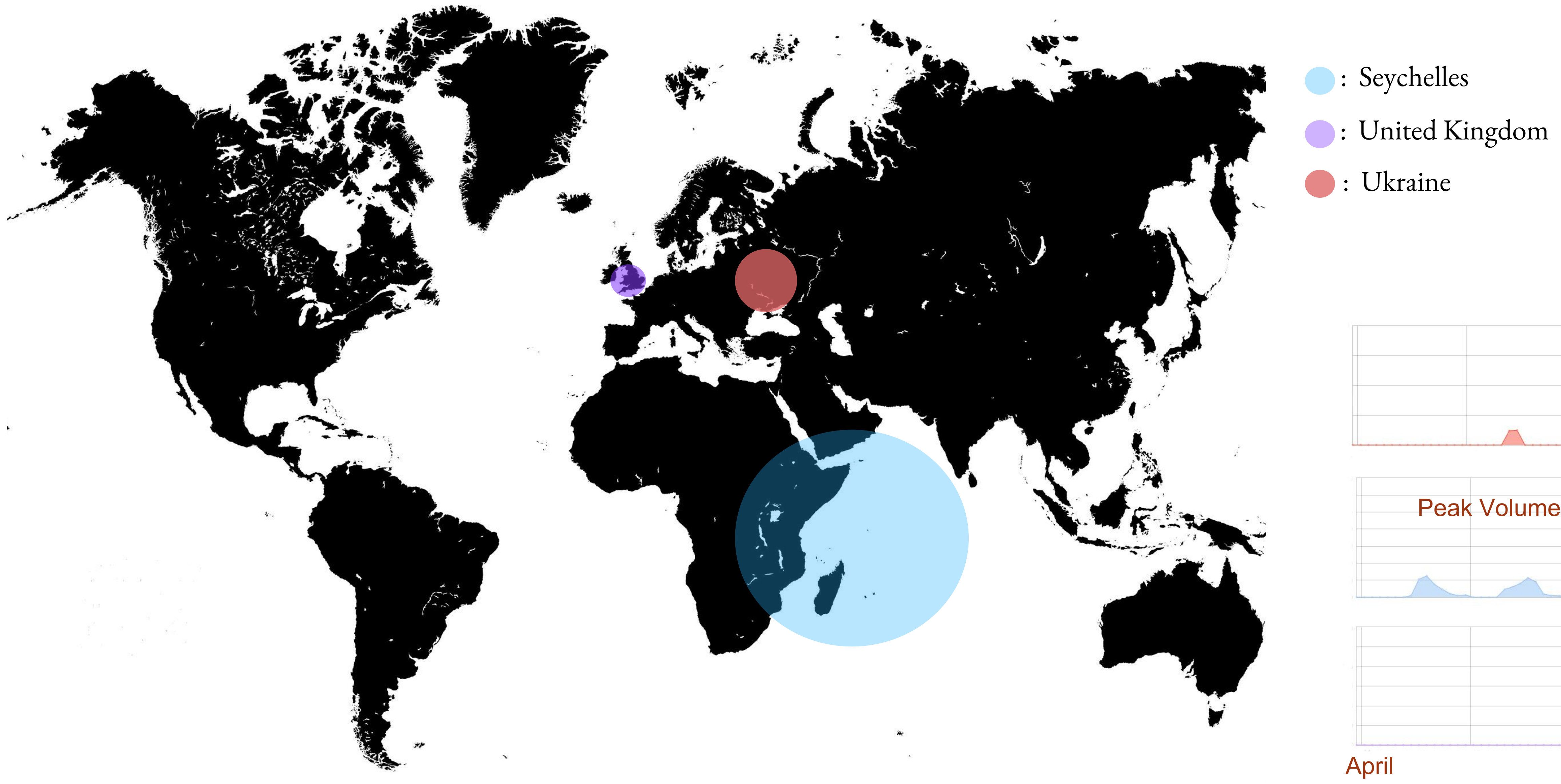

Figure 2, Map of Spearfishing and Mail Spam Attacks (Size of bubble indicates volume of traffic)

Potential Worm

Figure 4 shows the internal connections involving two suspicious machines. They exhibit worm-like behavior by contacting local computers in attempt to propagate through the network on unusual ports: 135 and 445. These ports are utilized by some Microsoft services, but not often by regular browsing computers.

- This is a large portion of our internal traffic, so the existence of it is strange
- The only other internal traffic our IDS captured involves software like Dropbox broadcasting over the network
- Brief investigations show the possibility of this worm originating from the aforementioned mail spam

Recommendation: If these services are not used, these machines need to be cleaned, ports must be closed, and the cause of the worm must be investigated.

Drive-By Download

Figure 1 shows the DNS queries of a local machine in Goldshire. This traffic was investigated because an alert was raised when our user made a request for a .onion proxy.

- Once the DNS volume was observed it became clear that our user was querying adult content and most likely navigated to a bad or compromised webpage
- We see superhuman browsing occur at 21:49:40 where over eight hundred domains are queried, including the .onion proxy that raised the alert
- It is possible the user was a victim of drive-by downloading, a popular method for infecting a machine with malware

Recommendation: The local machine should be cleaned and a domain based firewall could help prevent employees from browsing adult sites.

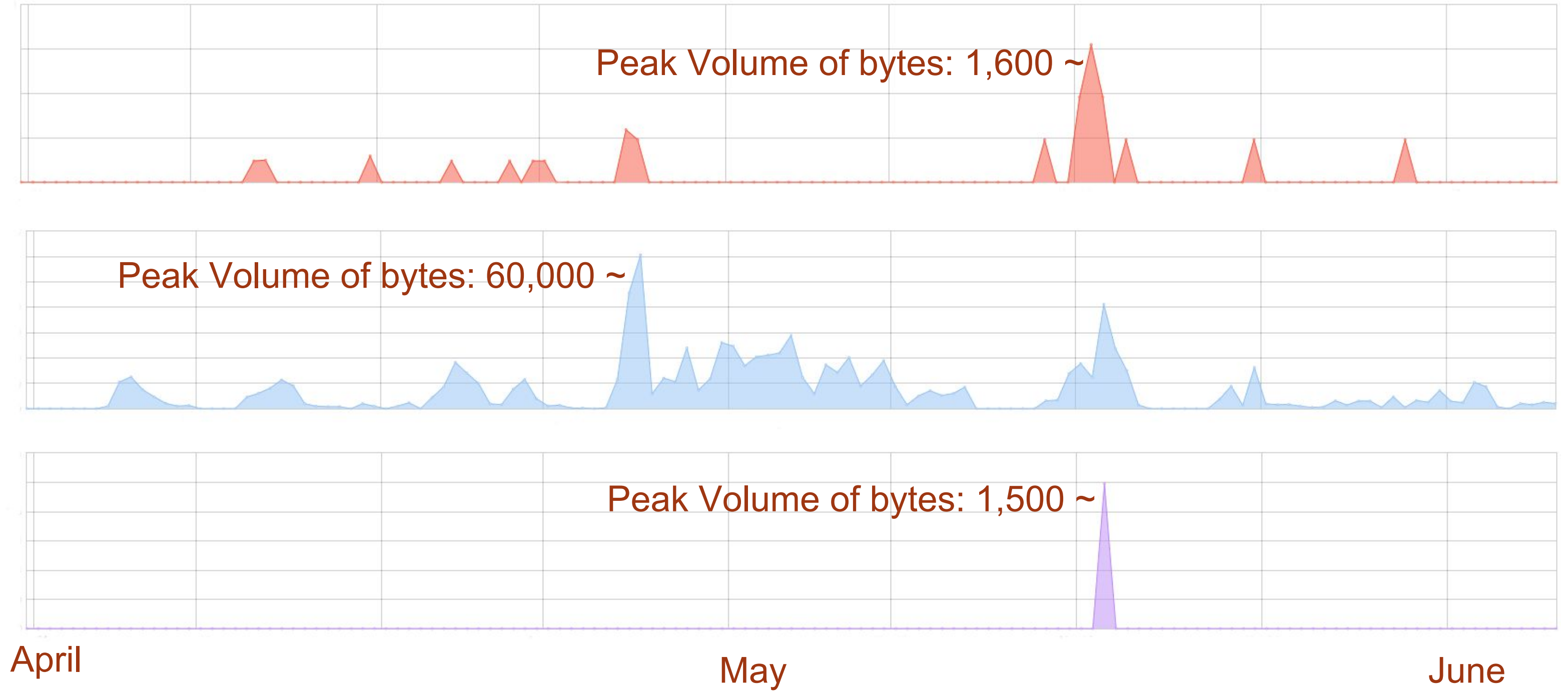

Figure 3, Volume of Spearfishing and Mail Spam Attacks in Bytes

Conclusion

Goldshire's Intrusion Detection System (IDS) setup was relatively ideal. Our team had access to alerts as well as traffic metadata such as source and destination IP and Port as well as the protocol. This information was more than enough to carry out in-depth investigations. During the duration of our network surveillance:

- 7 investigations were conducted by our team on suspicious activity observed, with 4 investigations leading to escalations to the Fusion Center
- Potential malware was observed either landing in our network or attempting to propagate via worm-like activity
- A potential infection was found by examining the DNS traffic after cross referencing the timestamps to an alert were a local machine made a query to a .onion proxy domain