CS 373 Summer 2019

Week 8 Write Up

Kirsten Wollam

Messaging Security

People are always the weak link in security, and that makes messaging a sure target. We often associate old folks that are not tech savvy with getting hit by phishing and spam, but as threats get more and more sophisticated, even the most security aware can have a hard time distinguishing a threat from something legitimate.

The basic form of malicious messaging is called phishing. This involves sending the user a message that asks them to do something, a call to action, that entices the user to go to a malicious link or provide personal information that can be used for malicious intents.

Spear phishing is a specific form of phishing that is targeted at an individual at an organization specifically. This sort of attack takes significantly more time, but can be extremely lucrative if targeted at the correct individuals.

Another popular method to get spam out in the world more effectively is snowshoe spam. With this the idea is to spread out the IP addresses that are sending the spam to avoid a spike in traffic over a single IP and avoid getting blacklisted. This can be very hard to detect if spread out over enough IP addresses, and is a constant problem for detection currently. One major way that this is achieved is through bot nets. A bot net is a group of machines that have been compromised and can be used for malicious deeds. If the malicious actor can get the bot net installed on many machines, they can then use that bot net to send the phishing emails out undetected. In reality malicious actors will create a bot net software package that they sell to people who wish to use if. These come and go over time as they are successfully deployed and then either cracked down on by law enforcement or go silent to avoid further detection. Bot nets originally started surfacing around 2010. That was the heyday for bot nets and the people running them, like Rustock, could

make $100000 a week.

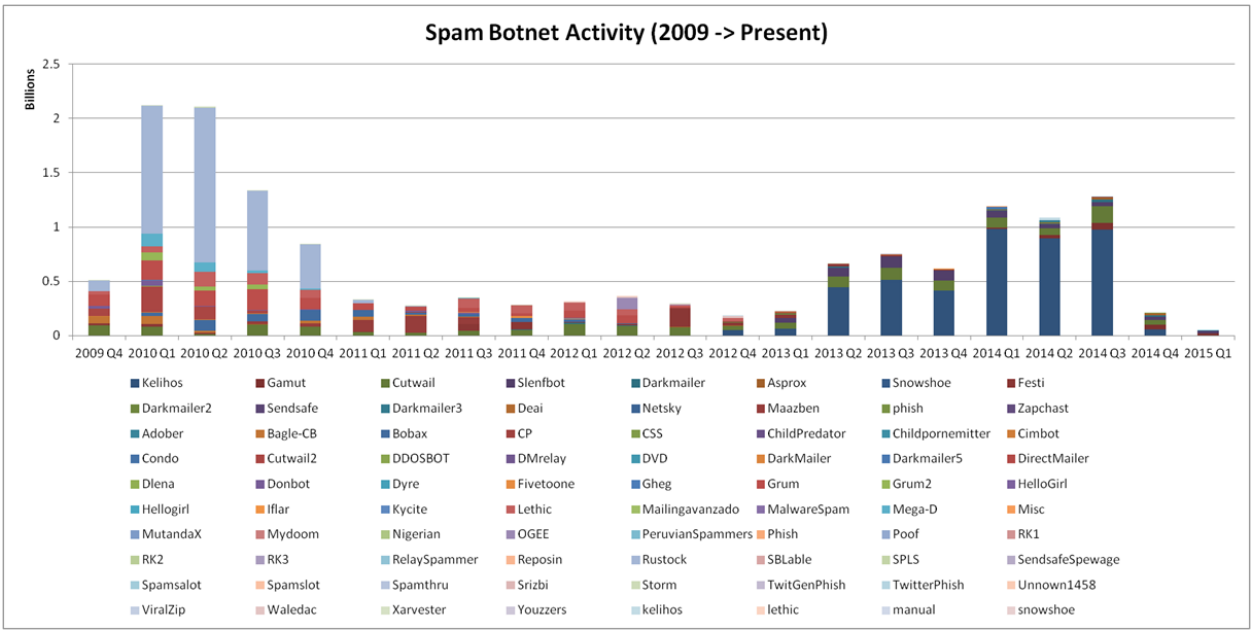

Figure 1 - W8L1 Messaging Security slide 14

Because we are so vulnerable to spam and phishing, there are many safety precautions that have been developed. With a billion messages to block a day these methods need high precision, and also must avoid false positives. Generally a false positive is seen as much worse than letting a spam message through since it blocks a user from getting legitimate mail they may be waiting for.

Antimalware must therefore parse out the good from the bad. this is done in a few ways, but generally starts with gathering key information out of knowns spam messages and grouping it so that it can be aggregated into valuable rules.

This is a balance between human input and automation. Humans can only process so much information and cannot meet the scale required, but are also better and catching spam and specifically filtering out false positives.

There are two main strategies used in protecting from spam:

reputation driven – IP, messages, URL

Realtime blackhole list (RBL), and other blacklist, eg spamhaus

content driven – common strings, message attributed

Heuristics – define rules for sorting, like a string match or regex or more complicated features sorting.

Bayesian filtering – based on statistics to calculate bad strings or other features and then used to classify