**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: 3rd Short Response Paper for Modules 6-7 (Final)

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*You are the CISO at a firm that is experiencing so many problems with botnets activity and routing disruptions that you need help. Which avenues would you pursue to address these issues?*

The integrity of an organization’s network is analogous to the importance of blood running through the human body. If the blood is infected with a foreign agent if the blood is restricted in any way, if the blood is lacking some part of its built-in defenses, or if there is not enough blood flow to a certain part of the body, then the person can become sick, suffer injury or die. A network and the data in it mimic the circulatory system in many ways. The body has ways of dealing with and expects intrusions, a network should be the same. Being ready for and expecting intrusions might sound simple but it is the very thing that many organizations fail to do when they are defining their infrastructure. In the example given in the prompt, it seems like we are dealing with one of those networks, one that is not prepared for the fervent reality of botnets. Here are some clear steps to pivot out of the crisis.

#### Step One: “Shut It Down”

Shutting down the system is a painful thought. What about all the customers and potential loss of revenue? What if shutting down causes some sort of compliance issue, or alerts the news media or competition? By no means am I suggesting that the organization shut down any or all services without considering the cost and repercussions. The organization should carefully measure the cost of a network shut down and weigh that against the cost of potential data loss, lawsuits, and regulatory action. Maybe the malicious activity is only affecting certain services and not the whole network, in which case a partial shut down may be possible. Nevertheless, a pragmatic assessment of the cost should be conducted sans whatever emotion is linked with a complete shutdown. As a part of the deliberation, the organization should also be consulting with engineering on the effort and cost involved with resetting all the networking equipment to factory specs with the latest firmware. Almost all breaches that affect network hardware is because of bad configuration or failure to patch. Depending on the size of the organization this might have to happen in phases. At NASA I designed the cloud infrastructure for each campus so it could be destroyed and rebuilt in the space of 45 minutes. So there was never fear associated with bringing the entire system down. We designed it with the expectation that it should be taken down and rebooted quickly. As with any malicious activity, the worst should be assumed when taking precautionary steps. This is why resetting the networking hardware to wipe any potential implants from botnet activity is extremely important.

#### Step Two: “Grant Proper Permissions”

One of the reasons botnets are successful is because applications are open to receiving requests from anywhere. Mission-critical network services should be insulated from the public with layers of security in the form of permission checking. For example, a messaging infrastructure like Kafka could filter bad traffic and/or require “Proof of Work” from a new request before it touches the core API. Furthermore, the core application should be carefully configured to only accept requests from internal sources after the requests have been filtered, sanitized and verified. For example, AWS offers a service called Step Functions which a serverless State Machine. One huge benefit of this service is that is acts as the business logic for an application and can directly call AWS Lambdas ( serverless cloud functions ) that are verified by an ARN number. Verified the ARN before running the core services ensures that a bot can’t maliciously invoke the service.

#### Step Three: “Start a Malicious Curation Practice”

The next ( and probably not the last ) important step is to start a botnet detection practice that catalogs the fingerprints and signatures of botnets across the web. Having the botnet signatures in an accessible data store allows the security layer of the application to more effectively filter out the known malicious threats. Of course, this is also the work of a SIEM but there is no need for expensive software when most of the well-known threats have been publicly documented. Starting a catalog of your own allows for a great deal of control and flexibility of how you distribute and utilize this information throughout the system. Furthermore, SIEMs are often set up to experience the more serious activities of a breach then report them to the security team. Firewalls are built to keep big streams of requests out of private services. But both of these tools are often ineffective in protecting public services from requests that “look like” legitimate requests. A data store like Druid’s column base data store could filter out bad requests with subsecond efficiency, saving the organization time and money.

#### Summary

There is much more that could be done to protect the organization against botnets and much of it is very technical and therefore would have variations that depend on the type of business that was being attacked and the type of services that were being provided. However, by cleaning the equipment, resetting the way that services are exposed to the public and filtering the traffic based on known threats, an organization will have fought 95% of the battle in these three steps.