Search Log Files

# Indicators of Compromise (IOCs)

In searching through our log files there are multiple indicators we are looking for, below is a list of some of the higher prioritized indicators that we look for:

* Unusual Outbound Network Traffic
* Anomalies In Privileged User Account Activity
* Geographical Irregularities
* Other Log-In Red Flags
* Swells in Database Read Volume
* HTML Response Sizes
* Large Numbers Of Requests For The Same File
* Mismatched Port-Application Traffic
* Suspicious Registry Or System File Changes
* DNS Request Anomalies
* Unexpected Patching Of Systems
* Bundles of Data In The Wrong Places
* Web Traffic With Inhuman Behavior
* Signs of DDoS Activity

## Detected Indicators

1. One indicator that we encountered is a user whose authentication was failing and then the password for the account was changed without any of us knowing. After the password was changed the user was logging on successfully. This could be a compromise to the user account and allow someone without the necessary privileges to access information that is precious to the company.
2. Another indicator that we encountered was that after observing the ports open on our Mail Server we noticed that a Telnet server service was running on port 23. Telnet is a very unstable protocol because it does not encrypt any information that is sent over a network connection, this includes user names and passwords.

## Mitigation/Prevention Techniques

1. In order to prevent user accounts from being compromised we change all user account passwords to a password that matches our strict policy. Additionally, once we detect any abnormalities in user account log-in attempts we test the user account log-in information by doing it ourselves. After ensuring that all account information is accurate and secure we continue to monitor our logs to detect any abnormalities.
2. In order to prevent any compromise through Telnet we close off the port completely because the Mail Server does not require the telnet service. After killing the service we also implement a rule in our firewall that prevents any access to port 23.

### Conclusion

After checking various resources such as Wireshark Traffic on our DC, hash files on our web servers, and viewing the logs on our Mail Server there haven't been any serious detection's of DDoS attacks, enhanced privileges or botnet commands. We will continue to monitor our resources to insure that all of our systems are stable.