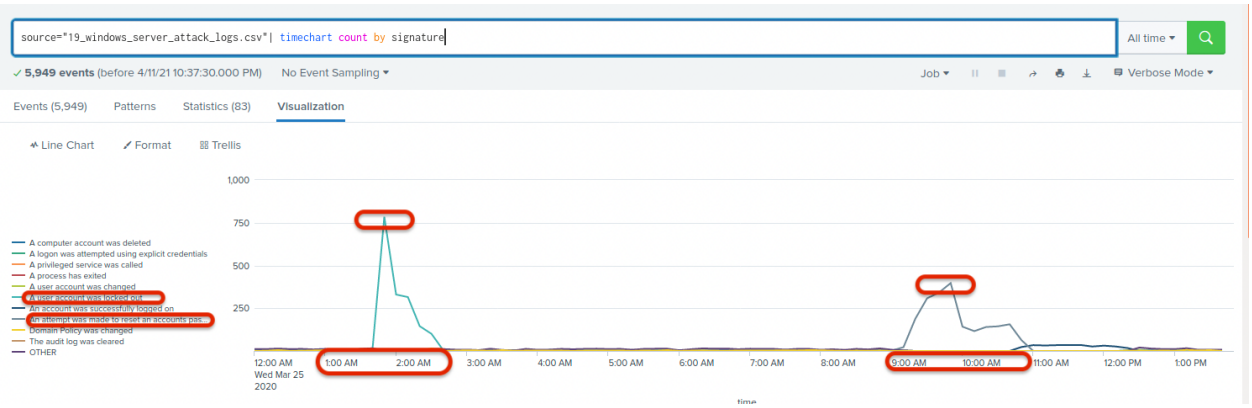
**Part 1: Windows Server Attack**
Note: This is a public-facing windows server that VSI employees access.

**Question 1**

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.




- Access Controls – Strong Passwords and Long Character Length Policy/Password changes every 90 Days/Multi-Factor/Account Lockout Threshold/Higher Levels of Encryption for Hashes, Captcha
- IPS to Monitor, Detect and Block suspicious activity, assess patterns from IP's, etc
- Firewall Rules -Whitelist and Blacklist, assess open ports
- System Scan to check for open ports visible externally, vulnerabilities, and patches of version that could be exploitable.
- Observer patterns associated with a specific userid, track the timeframes, add threshold alerts for that user, and track suspicious activity
- Supporting documentation:

https://www.okta.com/resources/whitepaper/okta-threatinsight/

- Process to determine if an IP Address is malicious:

**Brute force detection**
In the last X hours, Okta identifies a Y% failure rate for all logins originated from an IP address/set of IP addresses*
**IP address must cause at least Z # of failed logins*

**Question 2**

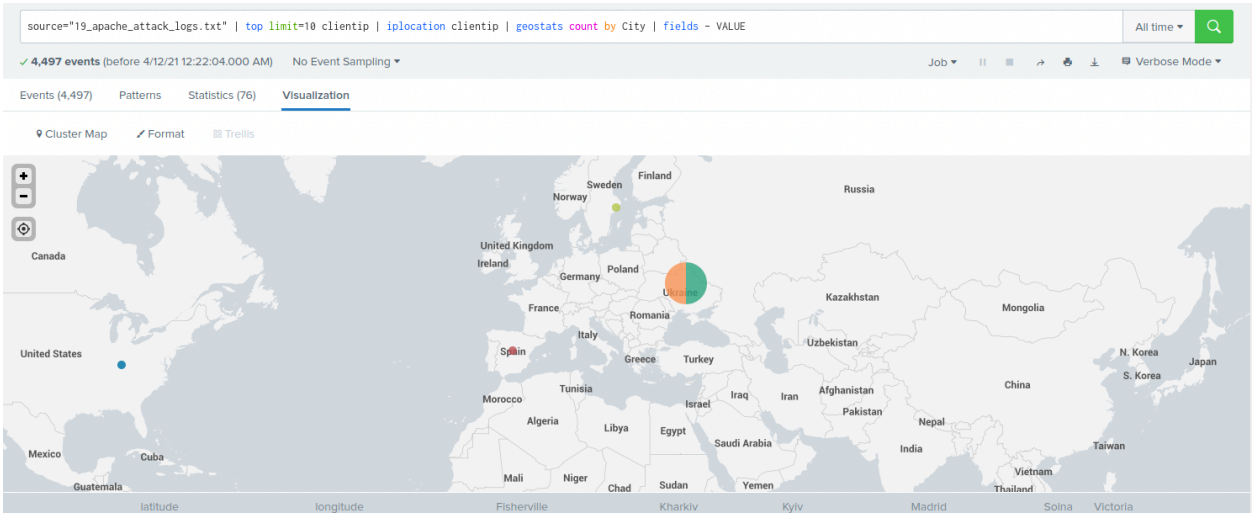
- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

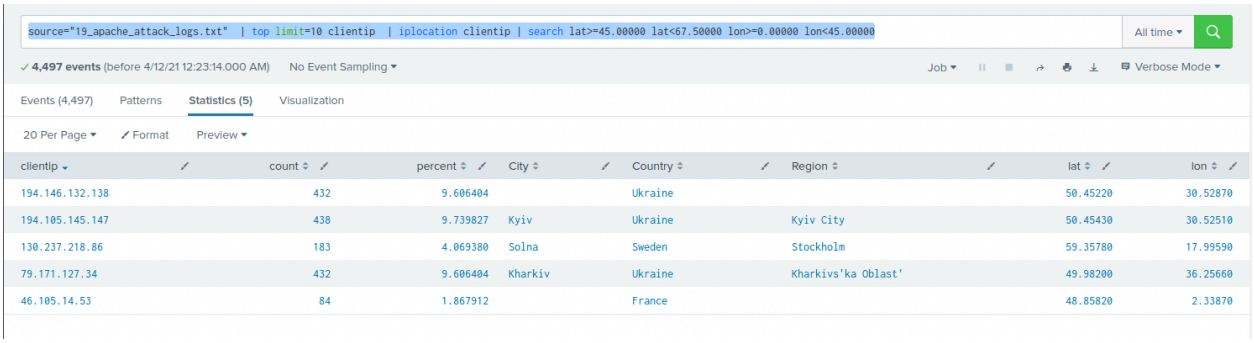
- Strong passwords and increase length of passwords, implement a tool similar to Captcha, monitor for increase traffic on the network and block the potentially suspicious IP address(es). Compare whitelisted ip_list compared to blacklist ip_list.
- Smart Firewall – Adjust to combinations of patterns, statistics, behavior to discern if the traffic is truly malicious

**Part 2: Apache Webserver Attack:**

## Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
    - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic map that justifies why you created this rule.




**Block All IP Address Traffic incoming and outgoing:**

194.146.132.138 #Ukraine
194.105.145.147 #Kyiv Ukraine Kyiv City
130.237.218.86 #Solna Sweden Stockholm
79.171.127.34 #Kharkiv Ukraine Kharkivs'ka Oblast'
46.105.14.53 #France

## Question 2

- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.

Firewall Monitoring, Smart Firewall or Next-Generation Firewall
Supporting Documentation:

NGFWs include the typical functions of traditional firewalls such as packet filtering,[2] network- and port-address translation (NAT), stateful inspection, and virtual private network (VPN) support. The goal of next-generation firewalls is to include more layers of the OSI model, improving filtering of network traffic that is dependent on the packet contents.

NGFWs perform deeper inspection compared to stateful inspection performed by the first- and second-generation firewalls.[3] NGFWs use a more thorough inspection style, checking packet payloads and matching signatures for harmful activities such as exploitable attacks and malware

Whitelisting
Packet filtering can prevent an IP spoofing attack since it is able to filter out and block packets that contain conflicting source address information.

- What other rules can you create to protect VSI from attacks against your webserver?
    - Conceive of two more rules in "plain english".

useragent

>100 Values, 99.978% of events

Selected Yes No

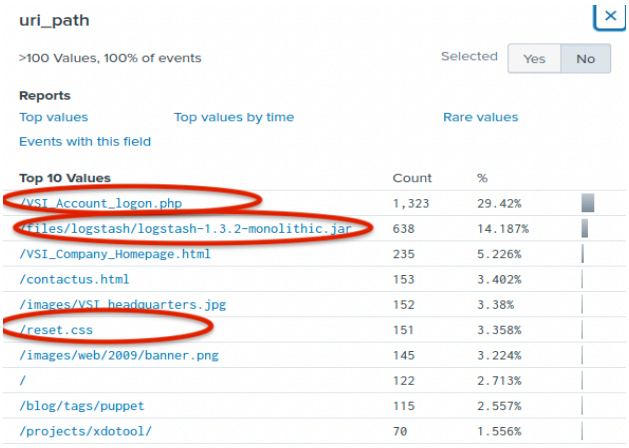
Reports

Top values Top values by time Rare values

Events with this field

| Top 10 Values | Count | % |
|---|---|---|
| Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.5072798778; InfoPath.1) | 1,296 | 28.826% |
| Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com) | 638 | 14.19% |
| Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 291 | 6.472% |
| Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36 | 183 | 4.07% |
| UniversalFeedParser/4.2-pre-314-svn +http://feedparser.org/ | 84 | 1.868% |
| Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:27.0) Gecko/20100101 Firefox/27.0 | 80 | 1.779% |
| Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) | 74 | 1.646% |
| Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 73 | 1.624% |
| Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0 | 72 | 1.601% |
| Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36 | 69 | 1.535% |

Microsoft » Infopath : Security Vulnerabilities
Opscode : Security Vulnerabilities
Chef Client can be used as Pentesting via Google Chrome




Appears the account login page utilizing "**php**" could have been exploited.
Appears the signature reset account could have been exploited due to **cross-site-scripting**
Elastic » Logstash » 1.3.2 : Security Vulnerabilities – **Exposes Credentials**
**Refer_Domains** is another element to assess for attacks susceptible to a cross domain referrer header leakage vulnerability.

Alert Any ICMP Flood Requests Above Threshold within Specific Timeframe (Seconds) Incoming Traffic
Alert Any TCP SYN Flood Requests Above Threshold within Specific Timeframe (Seconds) Incoming Traffic
Alert (useragent) uri_path *bot* *php* *css* requests Above Threshold withing specific timeframe (seconds)

**Guidelines for your Submission:**

In a word document, provide the following:

- Answers for all questions.
- Screenshots where indicated

Submit your findings in BootCampSpot