Defensive Security Project

Virtual Space Industries (VSI)

Security Operations Center

- Ruth Ann Abrams - Russell Glober -
- Geovanni Herrera - Chris Nnaji -
- Ryan Nonn - Angus Ritchie -

Scenario - Security Operations Center (SOC) Overview

- Why Are We Here?
  - March 25, 2020 attack
- Current Environment
  - Increased risk for cyber-attacks (e.g. rumors about JobeCorp)
  - Monitoring Tool, Reports, and Alerts
- Attack Analysis
- Attack Summary
- Remediation Recommendations

Why Are We Here?

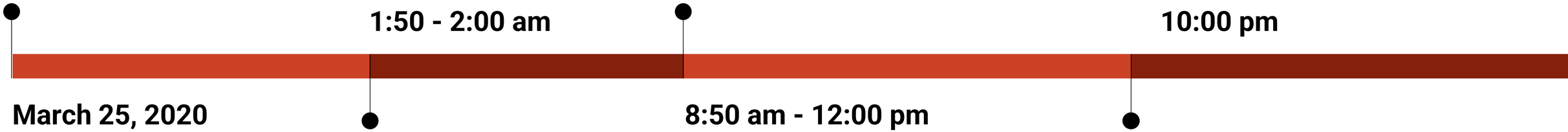
March 25, 2020 Attack Timeline

Pre-Attack Baseline
HTTP Posts: 30
Deleted accounts: 4,726
Password reset requests: 7 per hour

Attack 2: Brute Force and Access Gain

Password reset requests from NY IP: 1,296

User_j removed User_e from system security access at 11:55:50
User_j gained system security access by remote interactive logon at 11:58:42 am.



Attack 1: DDoS
User accounts locked out from
1 am to 2 am
Drop in deleted accounts at 2 am

HTTP POST = high of 785

Attack 3: Possible File Injection
Ukrainian IPs in Kyiv and Kharkiv
POSTing to /VSIAccount_logon.php

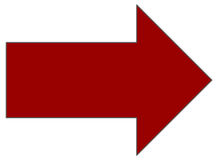
POST activity = high of 864
URI hits = high of 1,323

Current Environment

Splunk Enterprise Security

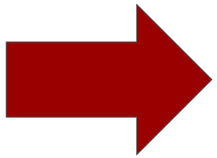
Application used to analyze large data sets, detect malicious network activity, and respond to threats quickly and accurately

- Real-Time Dashboards
- Threshold-Triggered Alerts



How we knew we were being attacked

- Custom Reports



How we analyzed what happened

Website Monitoring (Splunk Add-on)

- Monitors websites to detect downtime and performance problems
- Uses a modular input that can be set up easily (in five minutes or less)
- Provides excellent presets for the dashboard
  - Uptime Calculation
  - Status Monitoring
  - Email Outage Alerting
  - Change History
- Monitors real-time network activity and alerts to potential DDoS attacks such as occurred on March 25, 2020 at 08:59:00 pm
  - Greater than 3,000 HTTP response codes were generated by the Apache web server in a one-minute time span (indicative of a DDoS attack).

Logs Analyzed

1 Windows Logs

The Windows Server holds the intellectual property of the VSI next-gen program.

Operating system activity is recorded in the Security Log to track activity and keep a record of Server events.

This helps to identify unwanted actions (e.g., unauthorized access to privileged files).

2 Apache Logs

The Apache Log server contains the modules that deliver VSI web content through our webpages.

The modules include security measures such as password authentication and other features.

Monitoring Reports & Alerts

Reports — Windows

Designed the following Windows Server Reports:

Report Name	Report Description
Windows Activities	Tracks the success and failure of activities in Windows
Severity Count & Percentage	Displays the count and percentage of severity in Windows
Signatures & Signature IDs	Provides all signatures used and gives associated signature IDs

Alerts — Windows

Designed Failed Windows Activity Alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows Activity Alert	More than 10 failed Windows logins	7	When the number of failed logins is > 10

Failed Windows Activity Alert

Our threshold was set at the max number of failures in the baseline data. The minimum number of failed logins was 2, the average was 7, and the maximum was 10. The historical data did not exceed 10.

Windows Server

Alerts — Windows

Designed Successful Logon Alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logon Alert	Successful logins greater than 15	10	> 15 successful logins per hour

JUSTIFICATION:

Our threshold was set our tolerance level below the max number in the baseline data. The minimum number of failed logins was 8, the average was 13, and the maximum was 21 (which was an outlier).

Alerts — Windows

Designed User Account Deletion Alert:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Account Deletion Alert	Deleted user accounts exceed max threshold	11	User account deletion exceeds 20

JUSTIFICATION:

The threshold was set our tolerance level due to the wide range in the baseline data. The minimum number of deleted user accounts was 5, the average was 11-12, and the maximum was 22.

Reports — Apache

Designed the following Apache Server Reports:

Report Name	Report Description
Count of HTTP Methods	Counts the HTTP Methods during time frame
Count of HTTP Response codes	Number of completed HTTP requests by response code
Hourly International Activity (excluding USA)	Activity from countries other than the United States
Top 10 Referrer Domains	Top domains from which visitors came to our website

Alerts — Apache

Designed the following Apache Alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly International Activity	Number of attempts per country per hour	14 - 110	> 110

JUSTIFICATION: In pre-attack data, baseline = min of 14 and max of 110. The threshold was set at the max.

Alerts — Apache

Designed the following Apache Alerts:

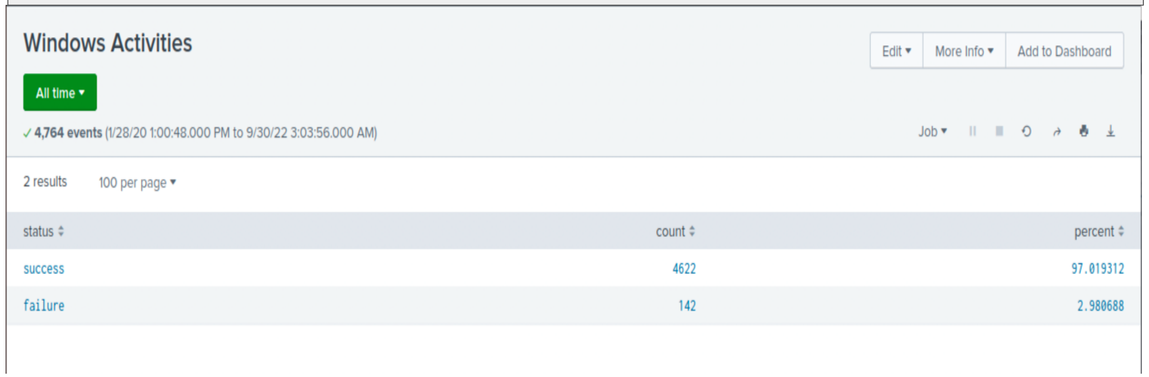
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly HTTP POST Method	Number of POST processes above threshold	< 6	> 6

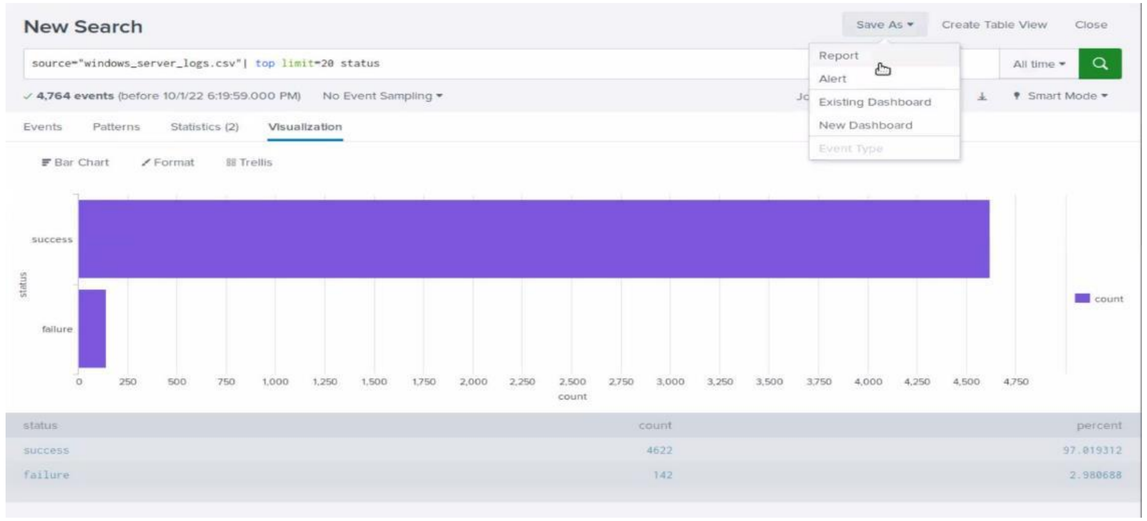
JUSTIFICATION: The baseline ranged from 0 to a max of 7. The threshold was set greater than 6.

Attack Analysis

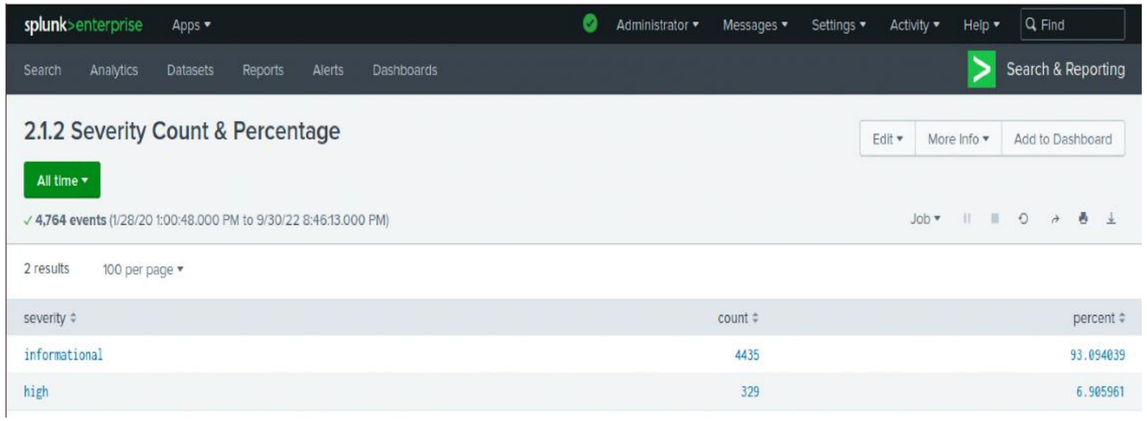
Pre-Attack Images of Reports — Windows

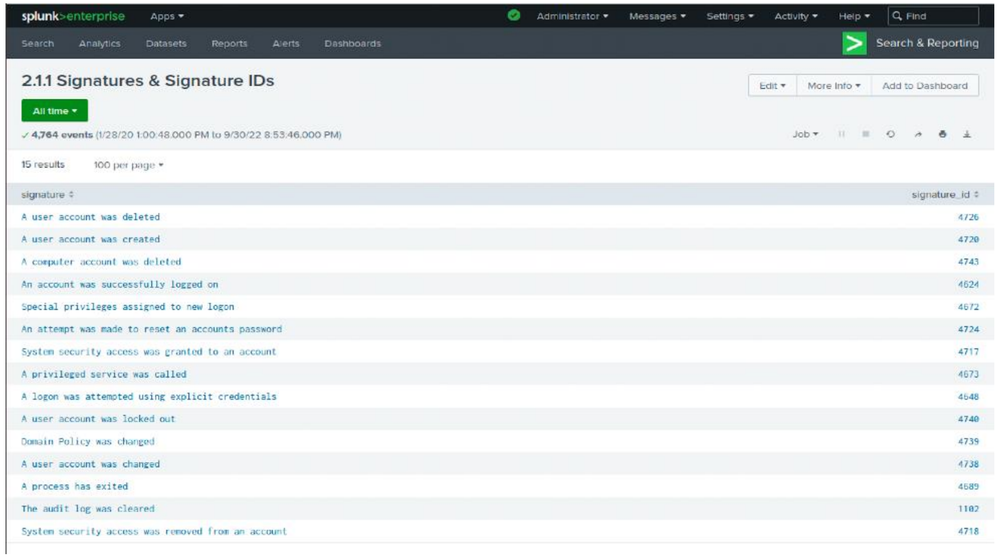
Pre-Attack Windows Activities



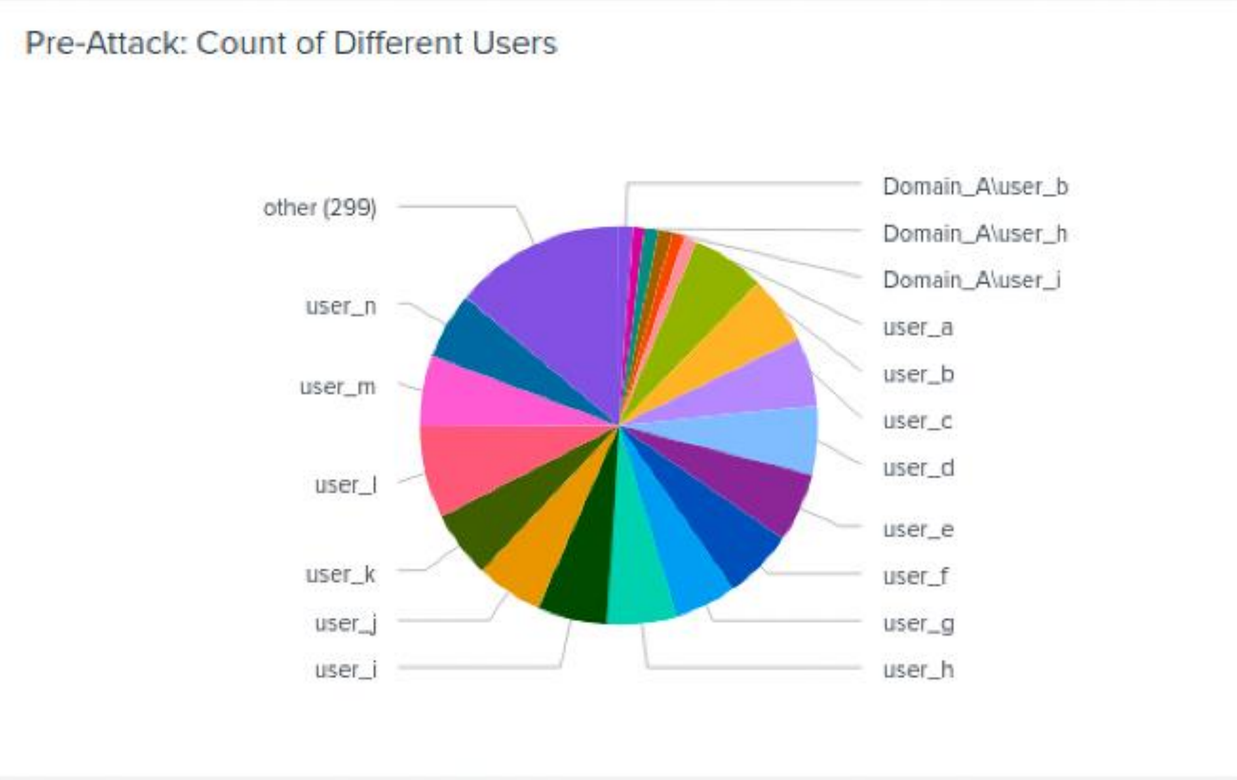


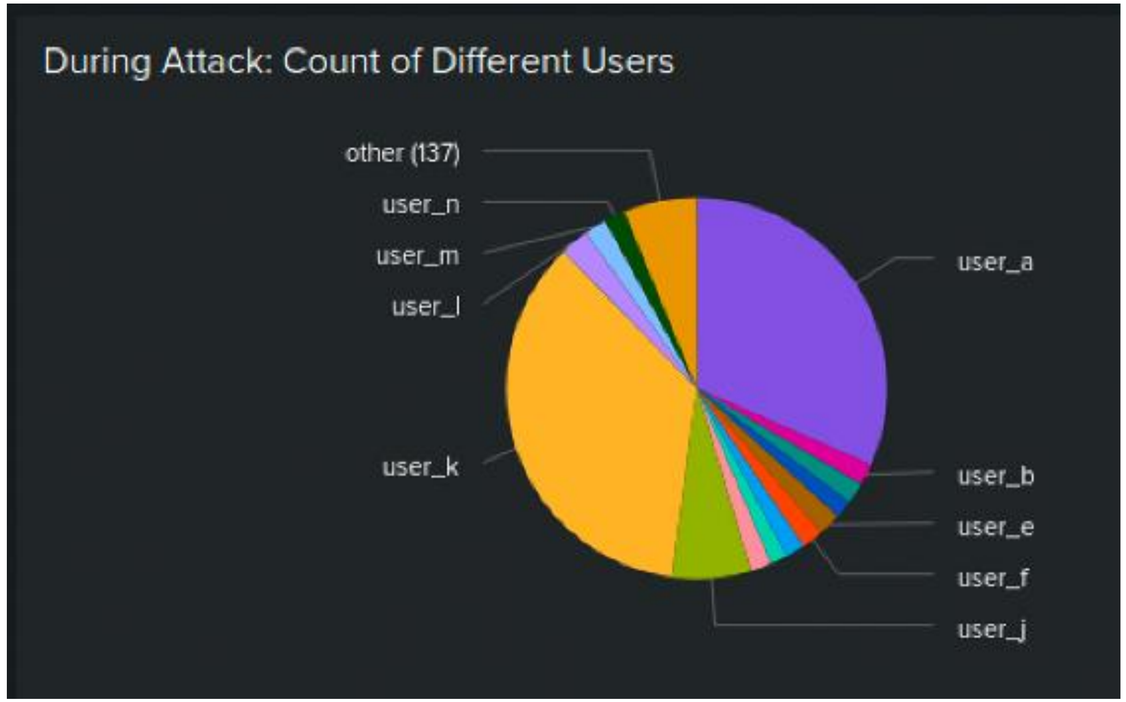
Pre-Attack Severity Count & Percentage



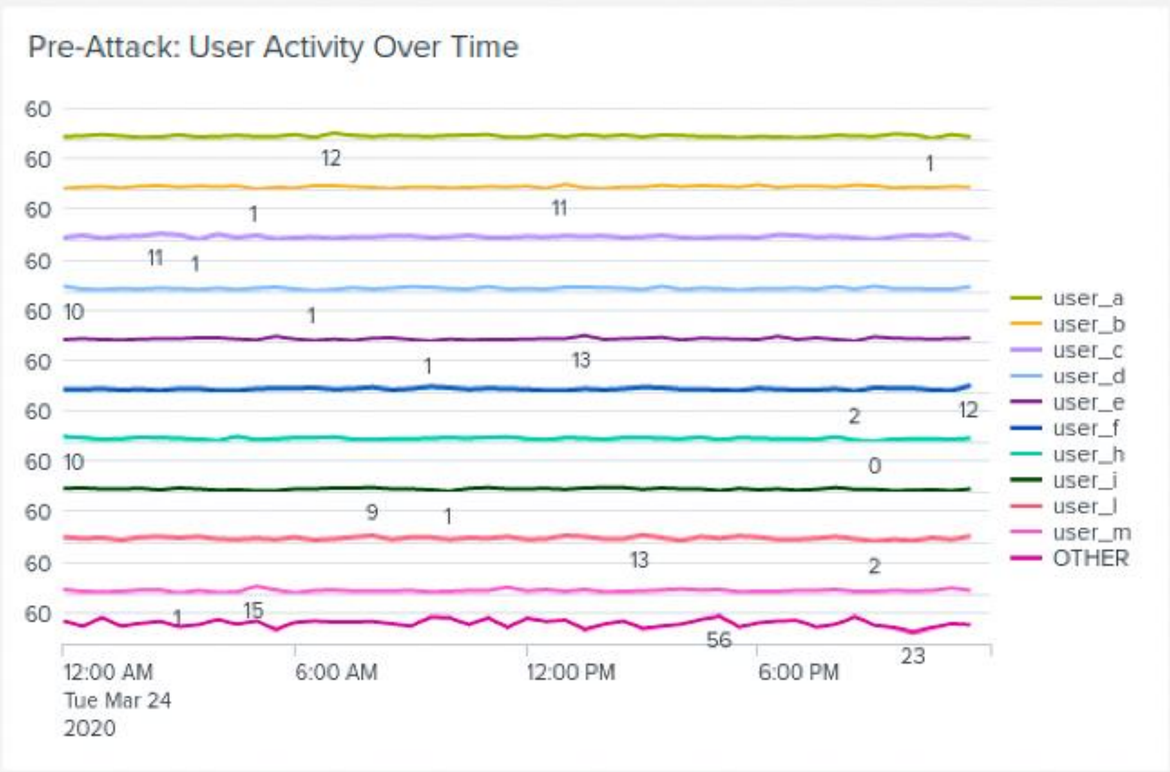


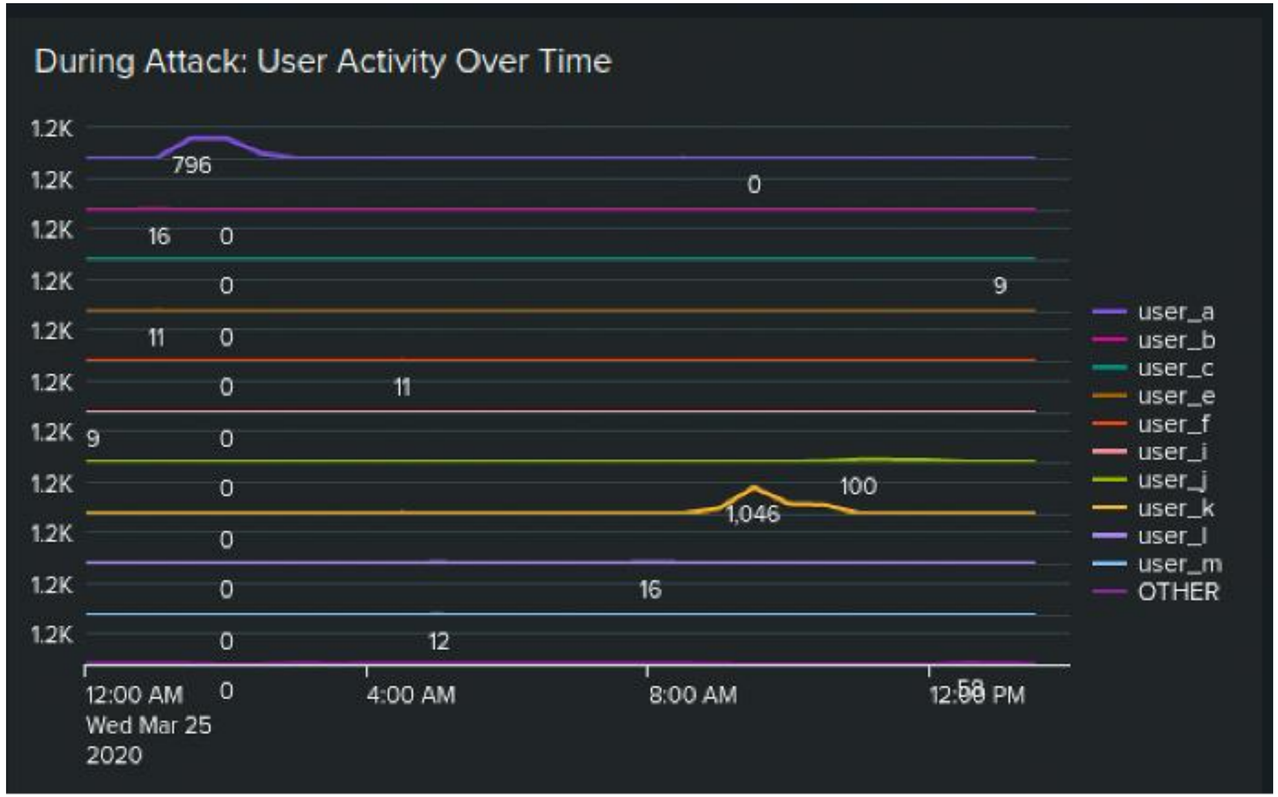
Windows Server Dashboard – Pre- and During Attack



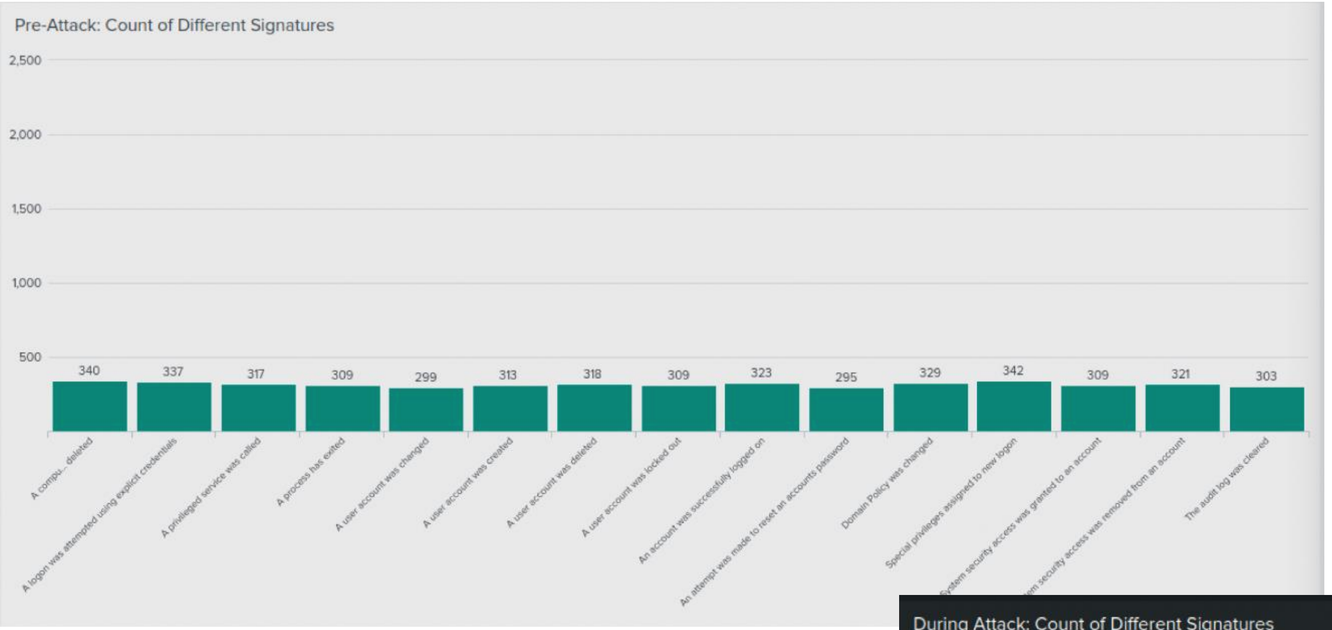


Windows Server Dashboard – Pre- and During Attack



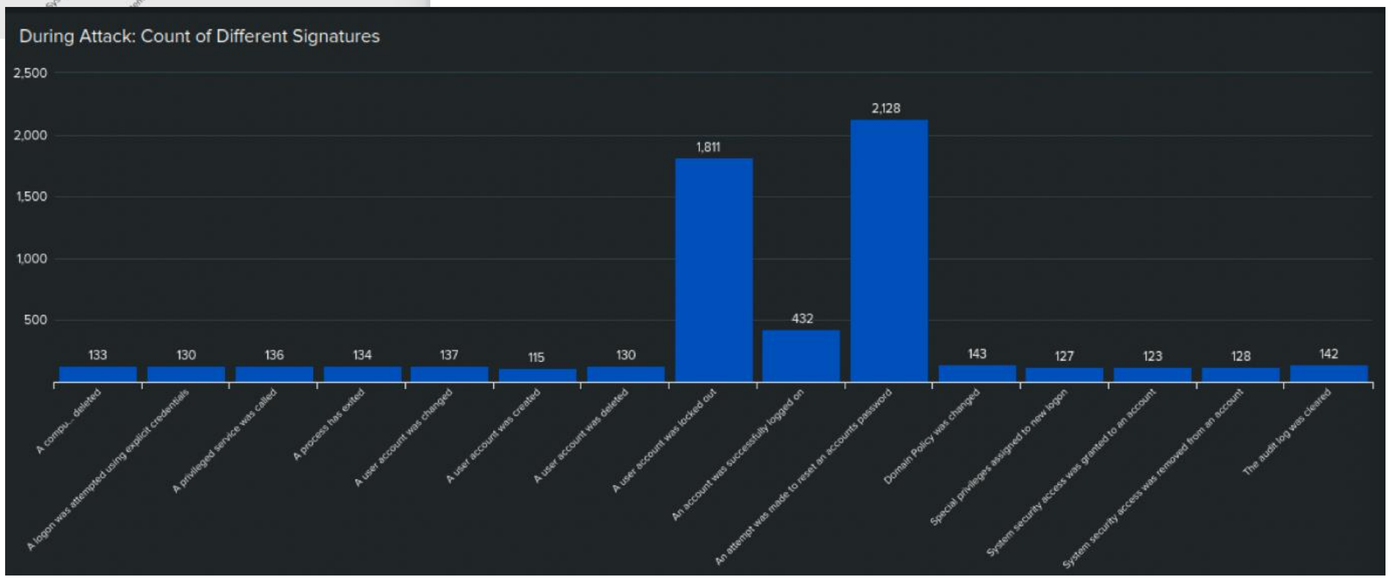


Windows Server Dashboard – Pre- and During Attack

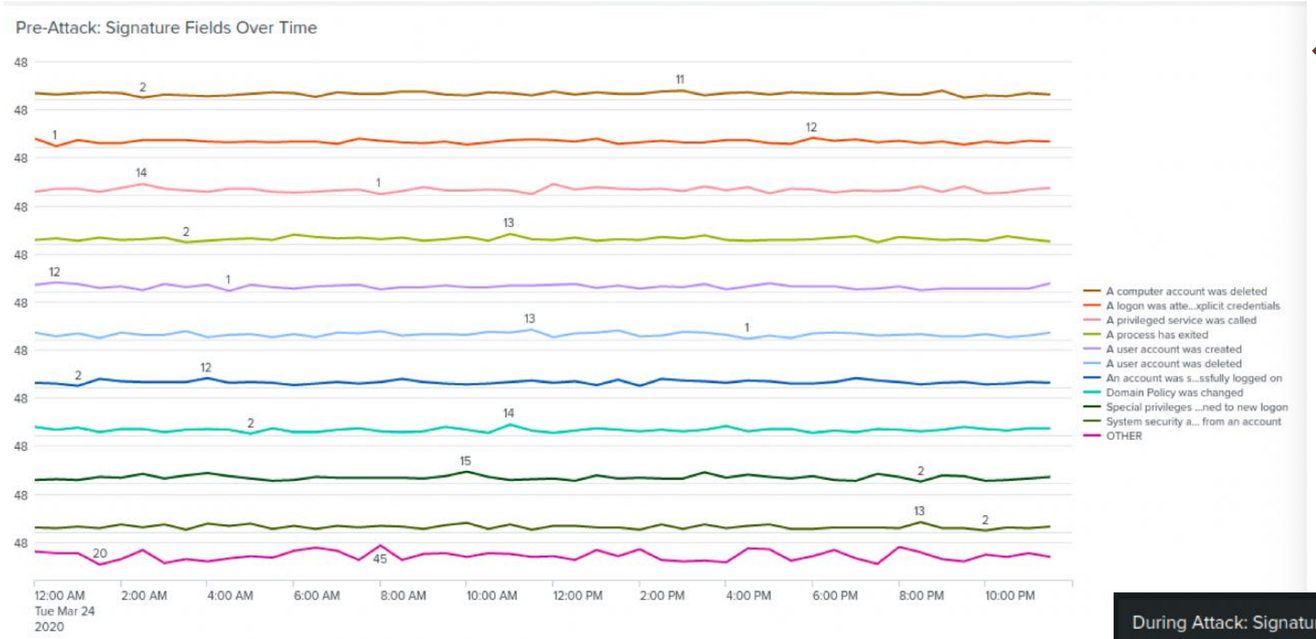


⬅ Pre-Attack Signature IDs
Baseline amount of user actions (e.g., requesting password resets, account lockouts, account logins).

During Attack Signature IDs ➡
Spike in user actions (account lock-outs and password reset requests)



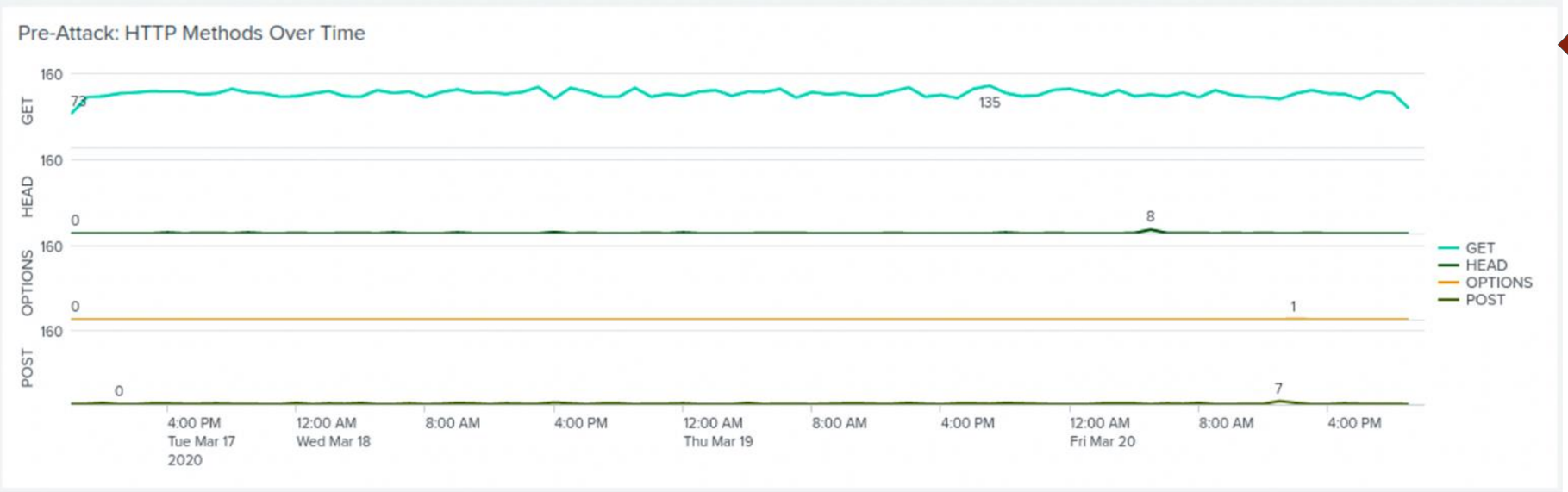
Windows Server Dashboard – Pre- and During Attack



⬅ Pre-Attack Signature Fields Over Time
Baseline of exact time of actions requested

During Attack Signature fields ➡
Spike in account lockouts from 1:30am to 2:30am and the password reset requests from 9:30am to 10:30am.

Apache Server Dashboard – Pre- and During Attack

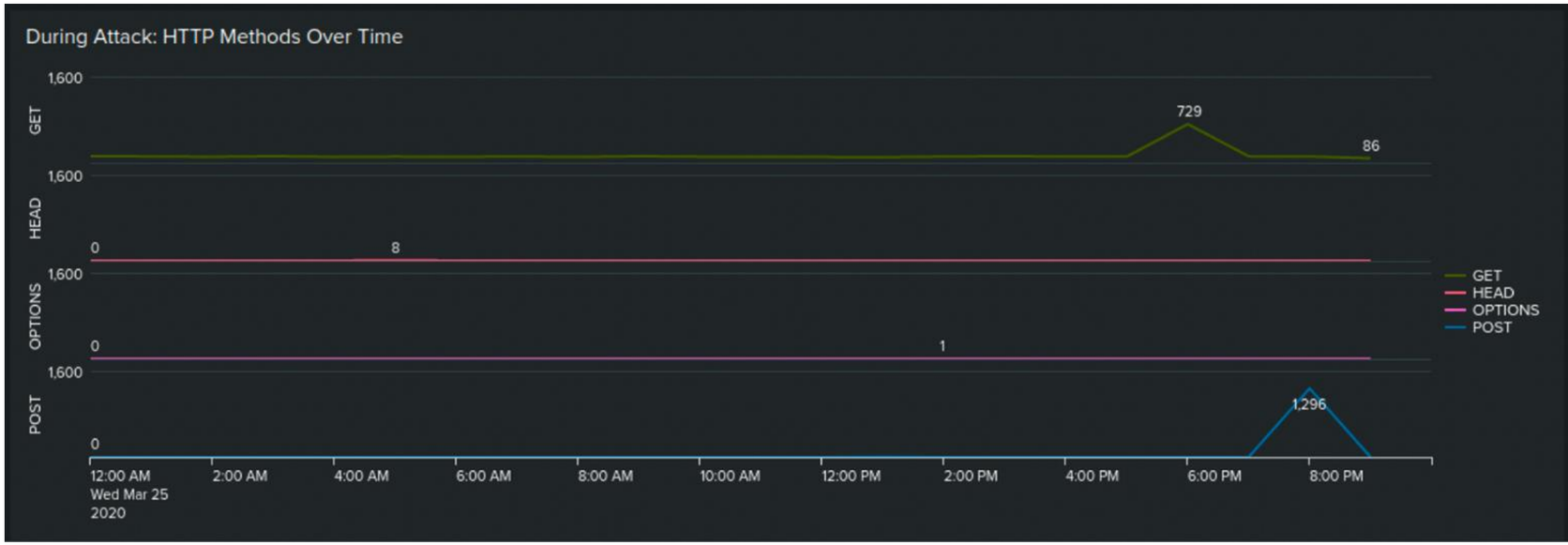


⬅ Pre-attack
HTTP Methods

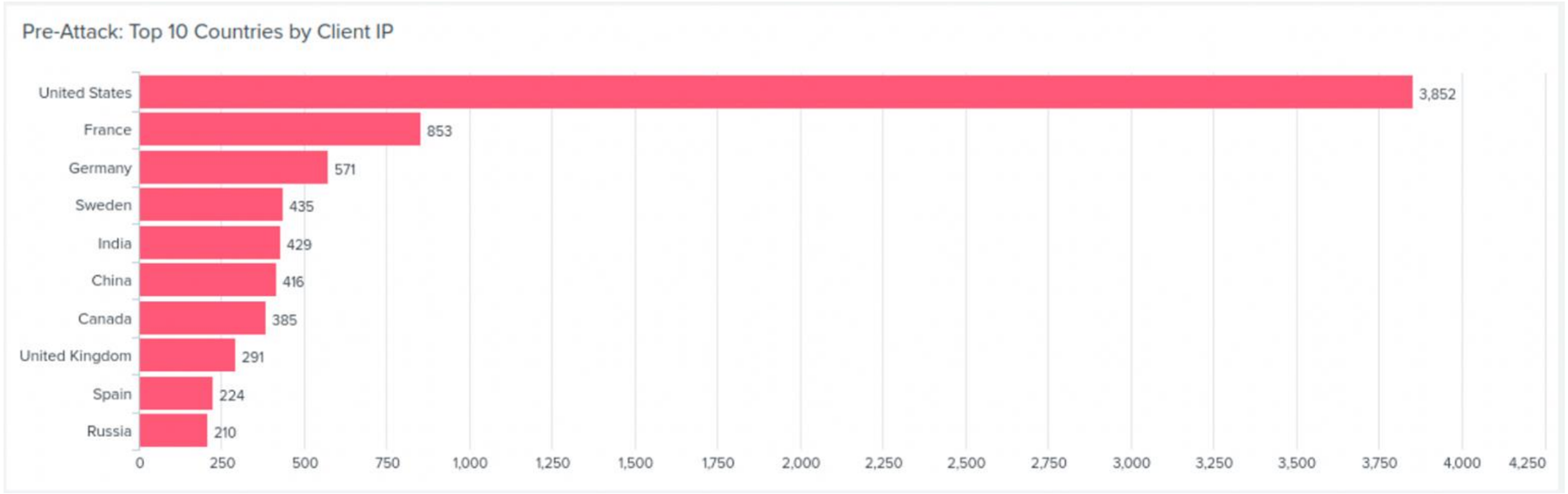
Baseline HTTP method activity over time. The data is relatively consistent with very few spikes in data.

During Attack ➡
HTTP Methods

This image shows the spike from 5:30pm to 6:30pm in GET posts and a spike 7:00 pm to 8:30pm in POST reponses.



Apache Server Dashboard – Pre- and During Attack

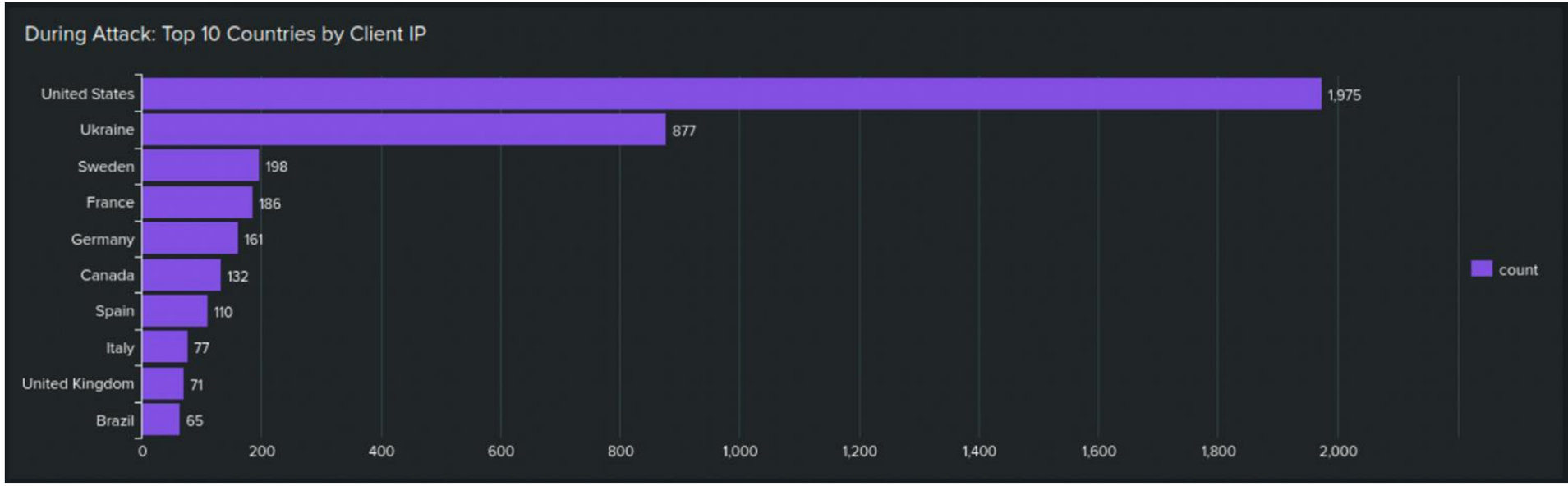


⬅Pre-Attack
Top 10 Countries

Top 10 countries that visited the site. United States, France and Germany are the top countries.

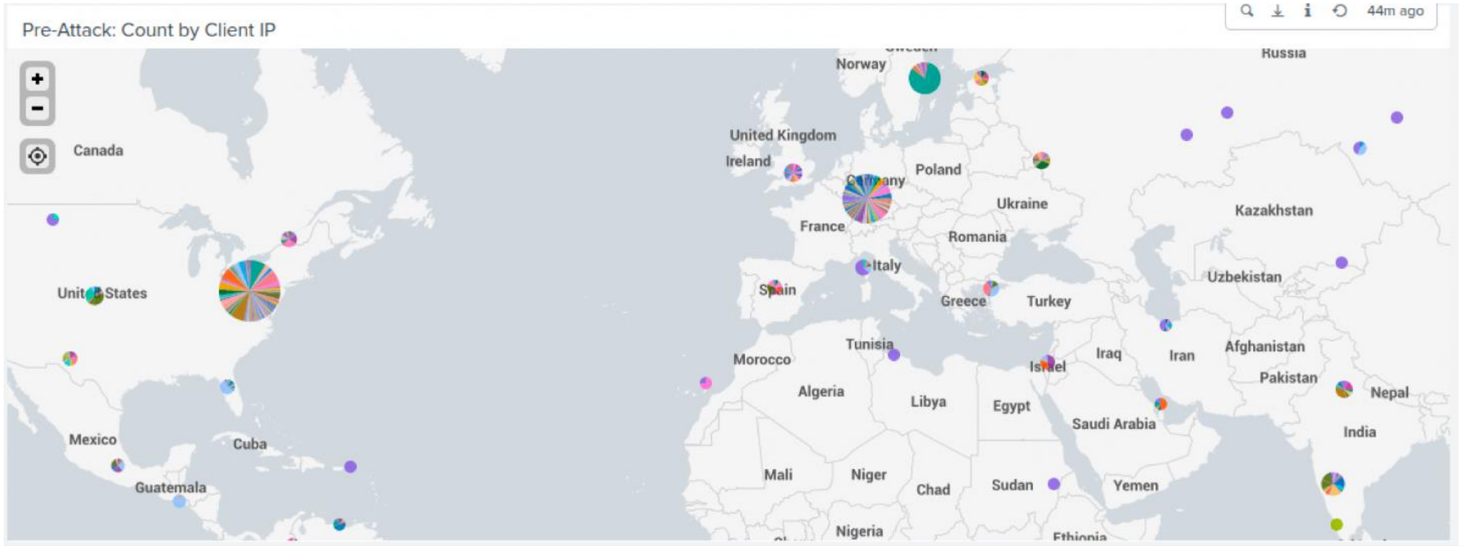
During Attack➡
Top Countries

The spike in country activity from the United States and Ukraine.



As we can see in charts A and B, there was an abnormal increase in traffic coming from Ukraine during the attack (210> to 877).

Apache Server Dashboard – Pre- and During Attack

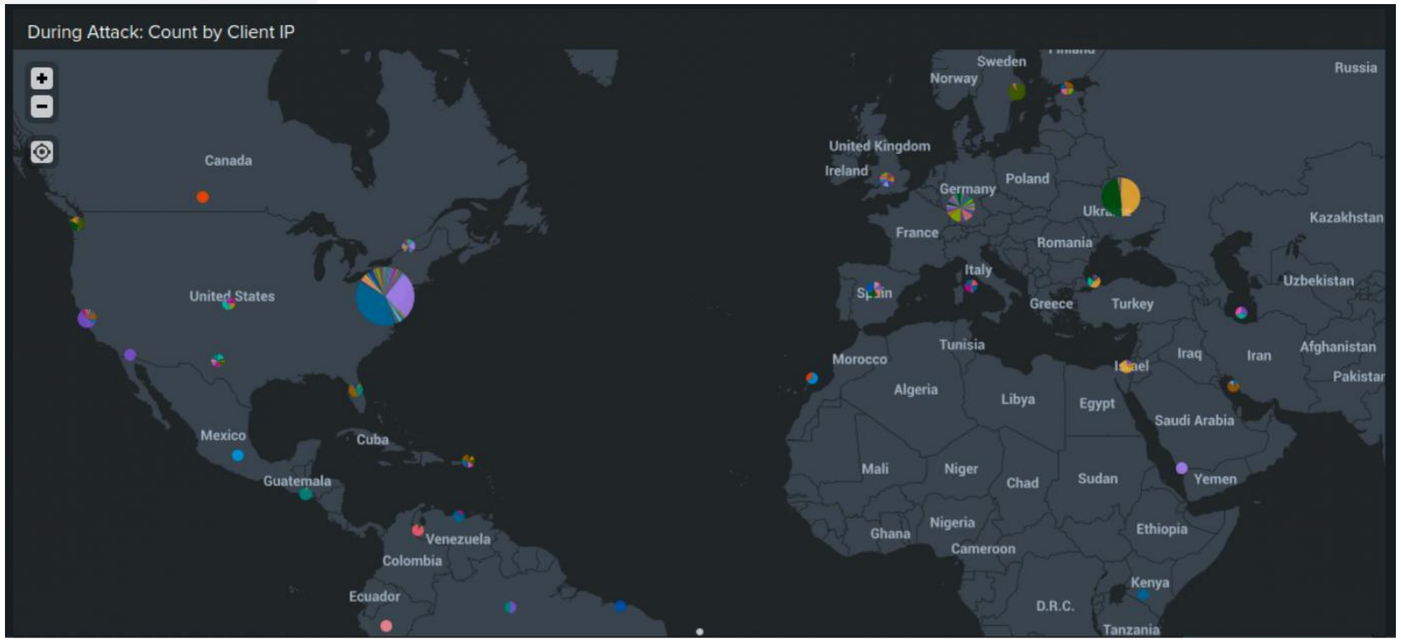


⬅ Pre-Attack

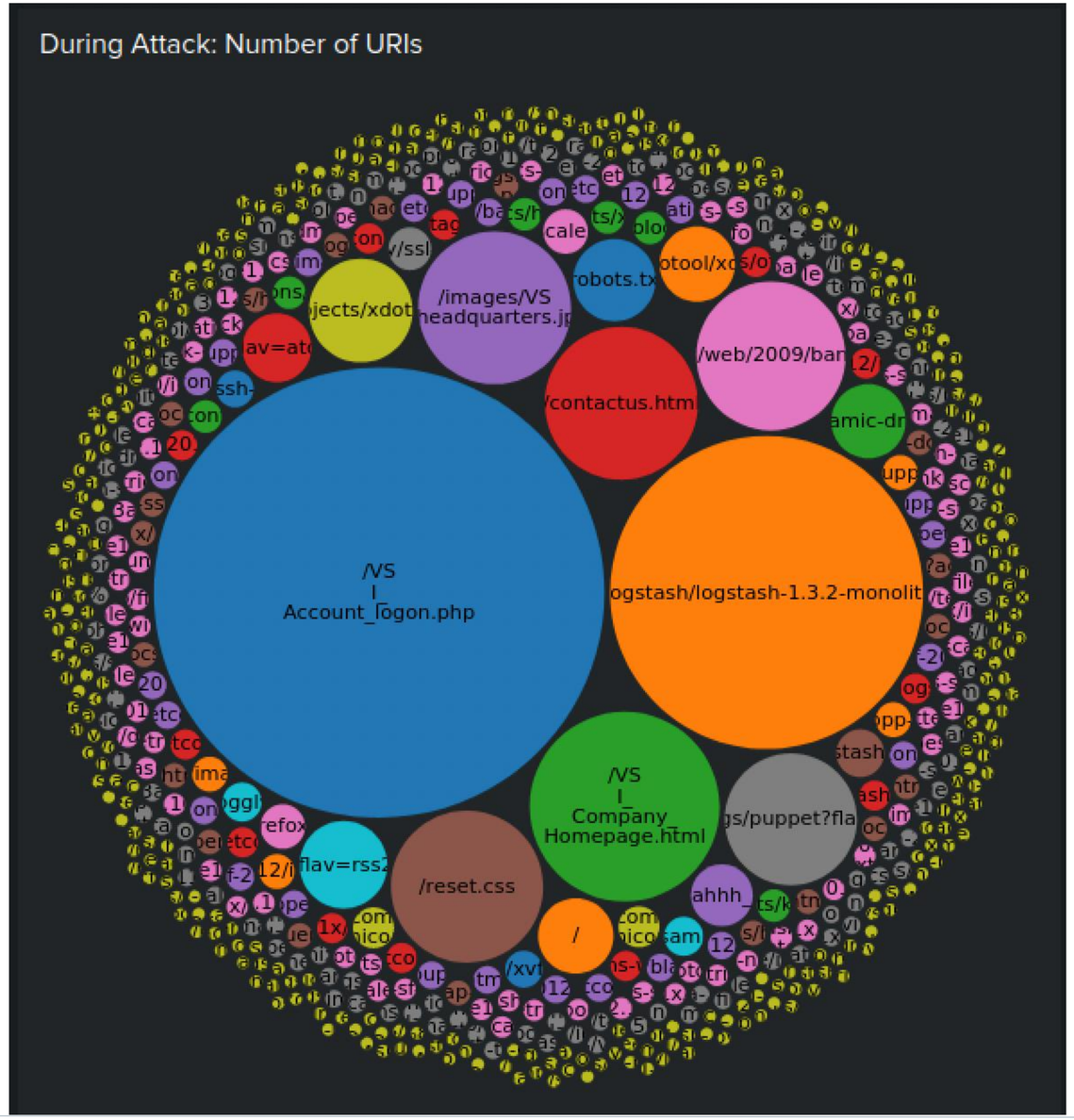
Top 3 Client IP origins located in the US, Germany and Sweden.

During Attack ➡

Top 3 Client IP origins located in the US, Ukraine and Germany



Apache Server Dashboard – Pre- and During Attack



Attack Summary

Attack Summary

Attack 1 - Denial of Service & Compromise

- At 1:50am on March 25, 2020, VSI experienced an extreme spike in successful logins of 785 (vs a baseline of 30) at abnormal times from IP addresses 194.105.145.147, 194.146.132.138, and 79.171.127.138, indicating a Distributed Denial of Service (DDoS) Attack
- At 2 am, the attacker(s) deleted several crucial accounts, likely hiding evidence of their malicious activities

Attack 2 - Persistence & Privilege Escalation

- From 9:20 am - 11 am, a series of password resets occurred (Windows log ID_4724)
- User_j removed User_e from system security access at 11:55:50 am
- User_j gained system security access by remote interactive logon at 11:58:42 am

Attack Summary (continued)

Attack 3 (DDoS and Possible .php Injection)

- At 8:05:59 pm, 1,296 HTTP POST requests came in from three different IP addresses indicating a Slow POST attack
  - 194.105.145.147 (Kyiv, Ukraine) – 438 requests
  - 194.146.132.128 (New York, NY) – 432 requests
  - 79.171.127.34 (Kharkiv, Ukraine) – 432 requests
- At 10pm, activity spiked from baseline of 85 to 877 events (including 864 logon attempts)
- An increase in GET requests that could imply a Slow GET attack
- URI data also shows potentially suspicious behavior due to the main files changing - a possible .php file injection (/VSIAccount_logon.php)

Remediation Recommendations

Remediation Recommendations – Windows Server

- Upgrade authentication schemes
  - Enable lockout of user accounts after multiple failed logins
  - Implement Multi-Factor Authentication (MFA)
  - Password resets should require a special code
  - Internal users should access
  - Conditional access to trusted devices with geolocation

- Isolate targets

- Lockout offending IPs
  - Protocols such as ICMP, can be limited to allow listed internal IP addresses, ensuring functionality while potentially limiting DDoS attacks

Remediation Recommendations – Windows Server

- Harden Windows Server
  - Set rate limits on routers
  - Enable timeouts on unused connections
  - Block unused ports on servers and firewalls
  - Detect and drop spoofed packages
  - Maintain up-to-date security configurations
  - Patch & upgrade software promptly and conduct maintenance

- DDoS protection and response vendors
  - Example: Akamai’s DDoS security and monitoring

Remediation Recommendations – Apache Server

- HTTPS:
  - Enable SSL on Apache Server via Mod_SSL to redirect to HTTPS

- GeoBlocking
  - Blocklist suspicious IP addresses and/or from originating countries (e.g., Ukraine) if allowed by business constraints

- Limit HTTP requests
  - Block an IP address after 5 consecutive POST requests to the logon.php page and/or logstash page (to prevent brute force attacks)

- Employ Detection/Network Management tool & Web Application Firewall
  - Mod_evasive/Mod_Security

Questions?