Defensive Security Project
by: The Backdoor Bouncers

Table of Contents

This document contains the following resources:

01

Monitoring Environment

Windows and Apache Servers

02

Attack Analysis

Using Alerts and SOAR integrated efforts

03

Project Summary & Future Mitigations

SOC review with VSI for a complete and in-depth analysis of VSI's Window and Apache Servers

Monitoring Environment

splunk>enterprise

Scenario Setup with The Backdoor Bouncers

- The **Backdoor Bouncers** used **Splunk ES** to navigate and monitor the VSI threat landscape to hone in on potential breaches revealed to **VSI Enterprises**. **Jobecorp**, a rival company, is rumored to have unwanted access to **VSI** servers (Windows and Apache servers) in an attempt to remove **VSI Enterprises** from the marketplace. Through careful analysis of controlled times and flagged events, your friendly SOC Analyst Team at **Backdoor Bouncers** was able to employ **Splunk ES** to quickly detect, mitigate and create a Playbook for **VSI Enterprises** to block unwanted access to **VSI servers**.

splunk>enterprise

VSI

Splunk> CIM

Splunk Common Information Model (CIM) Add-on

1. It **normalizes data** across different sources by mapping fields to a common allowing **faster correlation** between logs from different systems.
2. **Splunk Enterprise Security** and **Splunk Security Essentials using CIM Setup in Splunk ES**allows users to configure data models, set index constraints, and manage acceleration settings, ensuring efficient data processing.
3. Leveraging normalized data from the **CIM** Add-on, this dashboard provides a comprehensive view of security incidents, facilitating efficient monitoring and response time for **VSI Enterprises!**

In Summary….**CIM** Allows **MORE** data to be synthesized in less steps!

Splunk Common Information Model - (CIM) Add-on

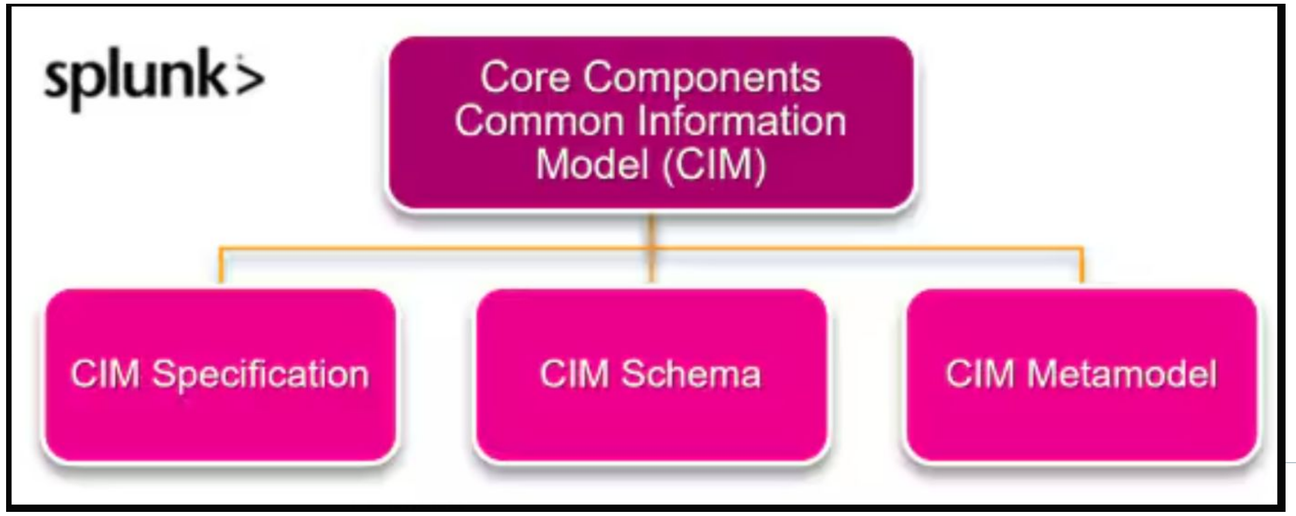
Palo Alto event

<180>May 6 16:43:53 paloalto.paseries.test LEEF:1.0|Palo Alto Networks|PAN-OS Syslog Integration|8.1.6|trojan/PDF.gen.eiez(268198686)|ReceiveTime=2019/05/06 16:43:53|SerialNumber=001801010877|cat=THREAT|Subtype=virus|devTime=May 06 2019 11:13:53 GMT|src=10.2.75.41|dst=192.168.178.180|srcPostNAT=192.168.68.141|dstPostNAT=192.168.178.180|RuleName=Test-1| usrName=admin\\user1|SourceUser=admin\\user1|DestinationUser=|Application=web-browsing

CIM Fields: user, src_ip, dest_ip

Jun 02 16:34:55 zscaler-nss: LEEF:1.0|Zscaler|NSS-FW|5.5|Drop|usrName=ADM\trole=Default Department\trealm=GCL->SBL-1\tsrc=10.11.12.13\tdst=10.44.68.1\tsrcPort=30553\tdstPort=53\tdstPreNATPort=30512\tsrcPreNATPort=234\tdstPostNATPort=2345\tsrcPostNATPort=332\tsrcPreNAT=10.17.15.14\tdstPreNAT=10.66.69.111\tsrcPostNAT=10.66.54.105\tdstPostNAT=10.17.15.14\ttsip=10.66.54.105\t\ttsport=0\t\tttype=GRE\tcat=nss-fw\tdnat=No\tstateful=No\taggregate=No\tnwsvc=HTTP\tnwapp=adultadworld\tproto=TCP\tipcat=Miscellaneous or Unknown\tdestcountry=United States\tavgduration=115\trulelabel=Firewall_Adult\tdstBytes=898\tsrcBytes=14754\tduration=0\tdurationms=115\tnumsessions=1

Zscaler event



Here are some examples of **CIM** fields and the build background of **CIM** that enables it to employ **LARGE** data sets between separate security systems and quickly report on threats.

Splunk Common Information Model - (CIM) Add-on continued…

The **CIM Specification** defines how data should be structured, labeled, and mapped to a **common data model**.

The **CIM Schema** is the **structured format** that defines how data fields are organized and named across different data models

The **CIM Meta** layer is the **metadata and definitions** that describe how **CIM** works within Splunk.

Enables cross-technology correlation – Normalize logs from different sources for unified analysis.

Improves Splunk ES functionality – Helps Enterprise Security dashboards and correlation searches function efficiently.

….so to Summarize, CIM Add-on Enhances Threat Detection & Investigation – Security analysts can query normalized fields across different log sources easily

Logs Analyzed

1 Windows Logs

Failed Windows Activities
Successful User Logins
Deleted Accounts
Analysis of Users (Signatures in System)

2 Apache Logs

HTTP Method Usage in System
Referrer Domain Analysis
International Access
URI focus analysis per User

Reports—Windows

Backdoor Bouncers designed the following reports:

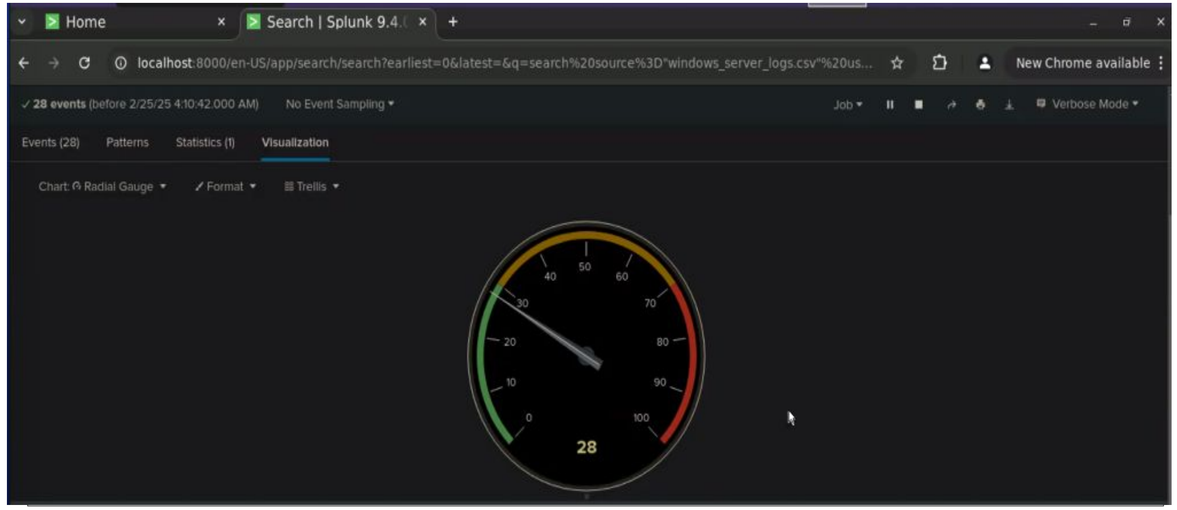
Report Name	Report Description
Signatures and IDs Report	Event Signatures and ID
Severity Levels	Showing Severity Levels and Percentage
Status of Success and Failures	Shows Comparison between the Two

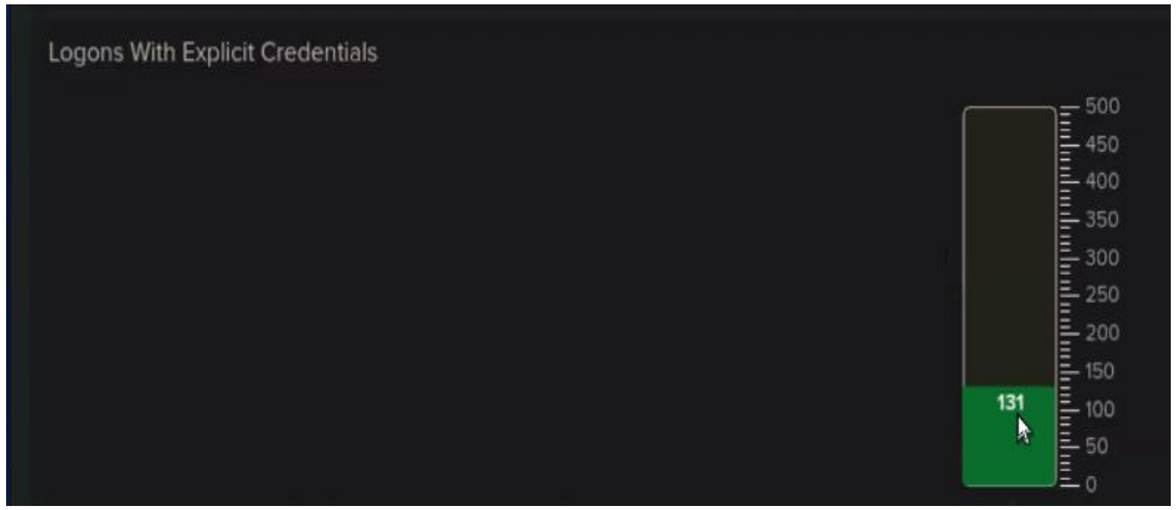
Windows Logs

splunk>enterprise

Images from Reports on Windows Server VSI Enterprise

Splunk ES showcases its **SOAR** potential for **VSI Enterprise** as Backdoor Bouncers collects Login information **INTEGRAL** to keeping **VSI Enterpise**'s information Safe!!





Alerts—Windows

Backdoor Bouncers designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Failed Activities in System	Trigger Action: Email to SOC for manual analysis of SOARs in place	6 event actions	35 event actions (6 total emails were generated to the SOC)

JUSTIFICATION: With the volume of Failed Activities in System, the baseline of the original data set suggested that **baseline was 6**. This accounted for the users traditionally introduced to the systems at VSI Enterprise. Upon analysis of the volume a few outliers were still observed encouraging the SOC Team to feel confident with **6 as the event action trigger** that would then send an Email to the SOC team for manual review of these entries and the better mitigation of potential network exposure.

Alerts—Windows

Backdoor Bouncers designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Successful Logins	Trigger Action: Email to SOC for manual analysis of SOARs in place	16 event actions	16 event actions (1 email was generated to the SOC)

JUSTIFICATION: With the volume of Successful User Logins, the baseline of the original data set suggested that **baseline was 16**. Upon analysis of the volume a few outliers or abnormalities were still observed encouraging the SOC Team to feel confident with **16 as the event action trigger** that would then send an Email to the SOC team for manual review of these entries and the better mitigation of potential network exposure.

Alerts—Windows

Backdoor Bouncers designed the following alerts:

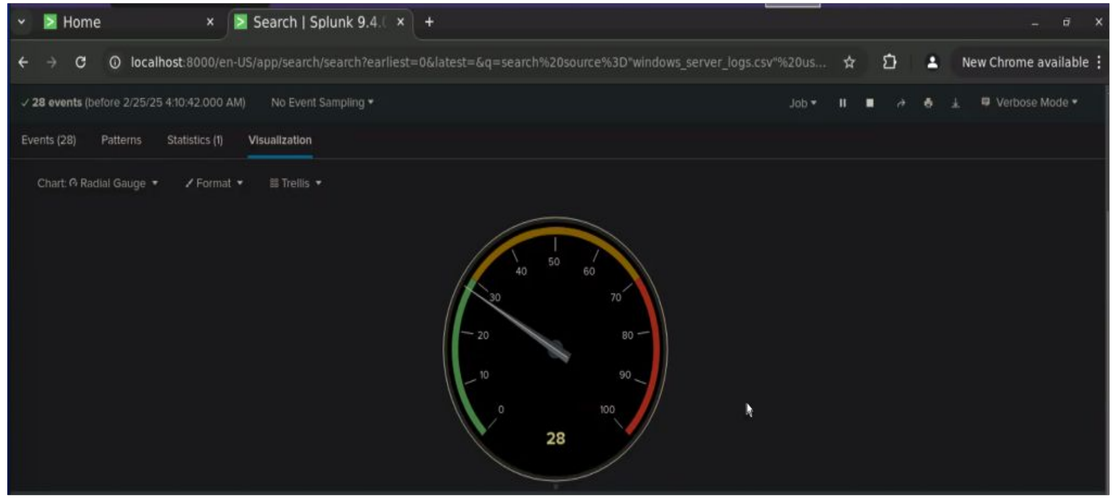
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alert Analysis for Deleted Accounts in System	Trigger Action: Email to SOC for manual analysis of SOARs in place	3 event actions	1 event actions (1 email was generated to the SOC)

JUSTIFICATION: With the volume of Deleted Accounts holding at 3 for the baseline group, Our SOC Team at **Backdoor Bouncers** moved forward with confidence. The results of the suspected attack do show logins per users in system. The graphs and charts provided help guide and pinpoint the users suspected of collusion with **Jobecorp** and should be evaluated further for information sourced for the following users: **user_c.**

Dashboards—Windows

Splunk ES custom displays your data in easy to view charts and graphs making it a business' first choice for protecting their network!

Keep your network safe from **Jobecorp** **with** **Backdoor Bouncers** team of experts that will walk you through the process and keep your data **SAFE!!!**



Apache Logs

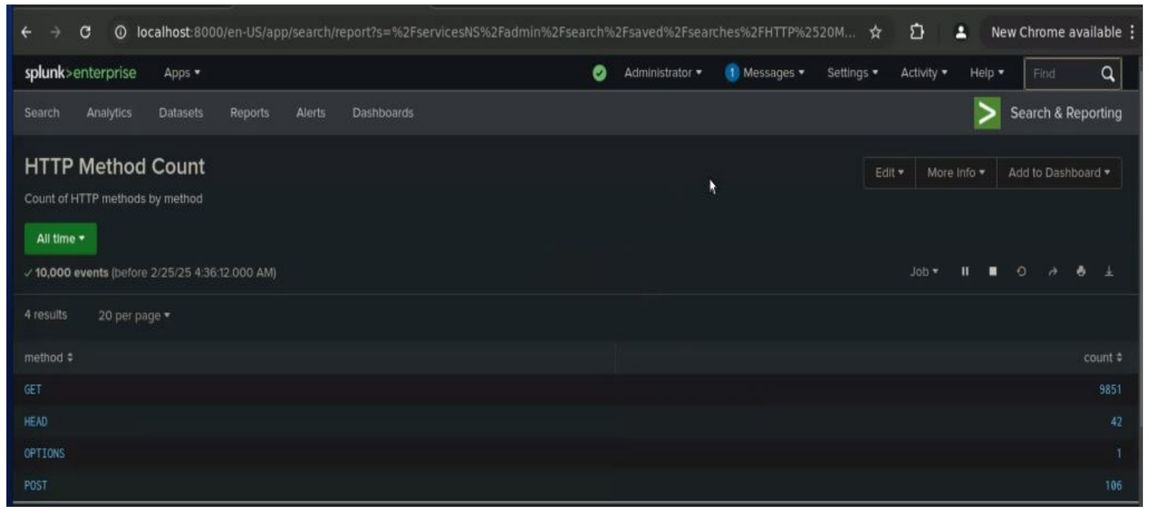
splunk>enterprise

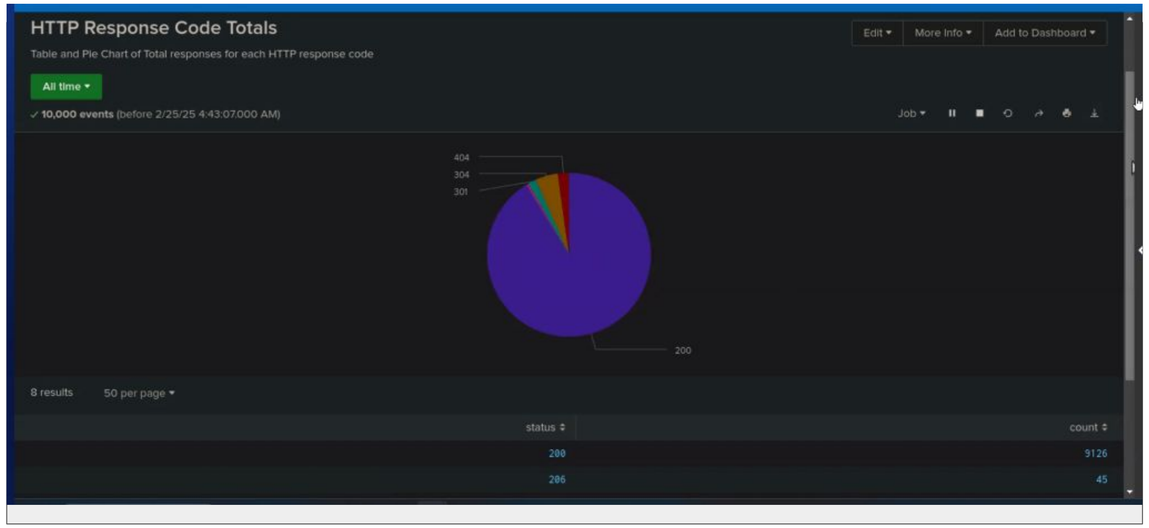
Reports—Apache

Backdoor Bouncers designed the following reports:

Report Name	Report Description
HTTP Method Count	Count of HTTP methods
Top VSI Domain Referrers	List of Top Domains that Refer Traffic to VSI Domain
HTTP Response Code Totals	Table and Pie Charts of Total responses

Images —Apache Report





To Prevent Threat Actors from accessing your network, you must **think like a Hacker!**

Our Trained Team of **SOC Analysts** found new areas of concern for **VSI Enterprise CRUCIAL** to network safety.

Alerts—Apache

Backdoor Bouncers designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Threshold for Non-USA Activity	Baseline threshold for Non-USA Activity	60	65

JUSTIFICATION: An analysis of the data showed a pattern of a general max of around 60. To effectively deter threats to the VSI Enterprise networks, we went with **65** as an alert threshold.

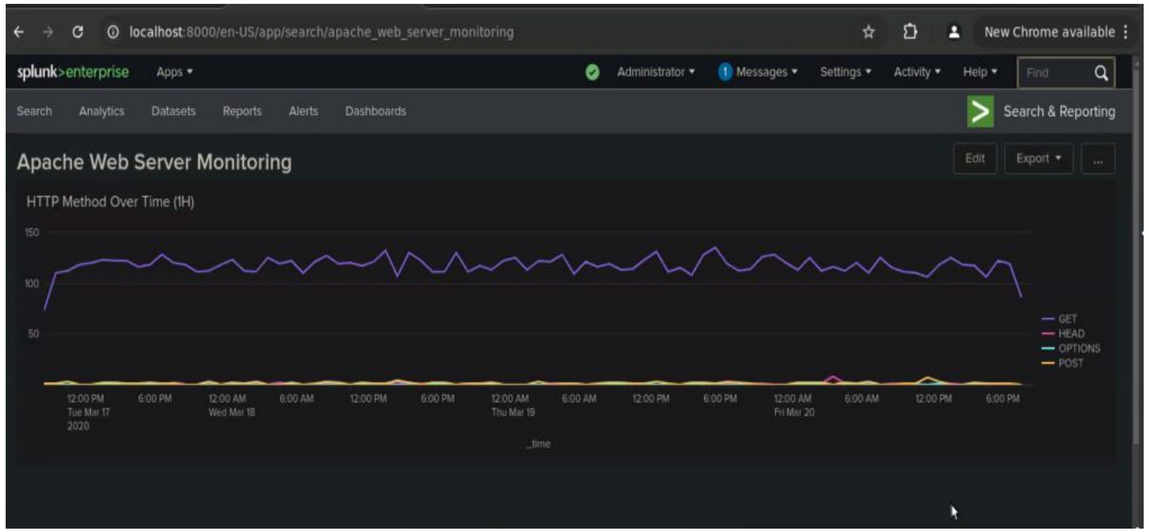
Alerts—Apache

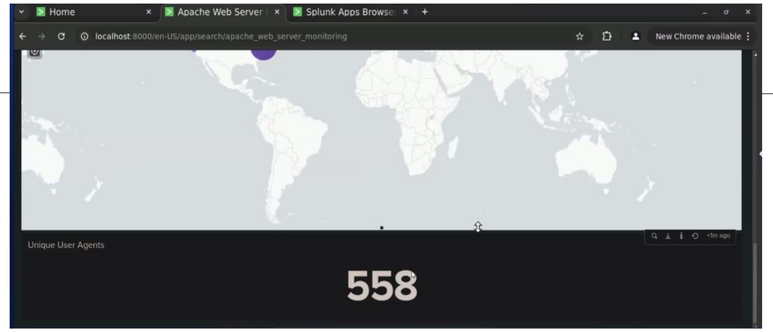
Backdoor Bouncers designed the following alerts:

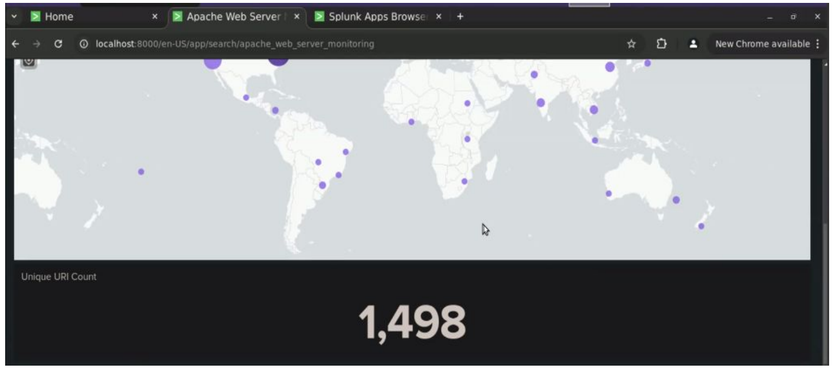
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP Post Method Threshold Exceeded	HTTP baseline hourly threshold for POST Method	3	4

JUSTIFICATION: There was an average of **3 posts per hour** and then when up to **4** for our threshold as there was very little variation, but with increasing threats on the horizon, Backdoor Bouncers approved **4** for the time until your next review.

Dashboards - Apache







International Usage of the Network is always a **CRITICAL** review item – These are selections from **VSI Enterprise**'s study.

```
source="apache_logs.txt" clientip="*" | iplocation clientip | geostats count
```

✓ **10,000 events** (before 2/25/25 5:15:01.000 AM) No Event Sampling

To Determine the right threshold, **Backdoor Bouncers** reviews Baseline data.

With **MORE** activity than ever, **VSI Enterprise** will need a focused solution for monitoring their network -

Choose **Peace of Mind!!**
Choose **Backdoor Bouncers**

Attack Analysis

splunk>enterprise

Attack Summary—Windows

Backdoor Bouncers findings from your reports when analyzing the attack logs.

- After further review of the attack logs Severity saw a pretty drastic increase in suspicious changes from **6%** **to** **20%**.
- Even though the failed activities saw a drop of 1.5% they did see a spike in activity around **8:00 AM MST** which triggered **6 emails to SOC**.
- Although we did not see a triggering event for successful created accounts, we did see a suspicious volume of deleted accounts linked to **user_c**.

Attack Summary—Windows

Backdoor Bouncers findings from your alerts when analyzing the attack logs. Were the thresholds correct?

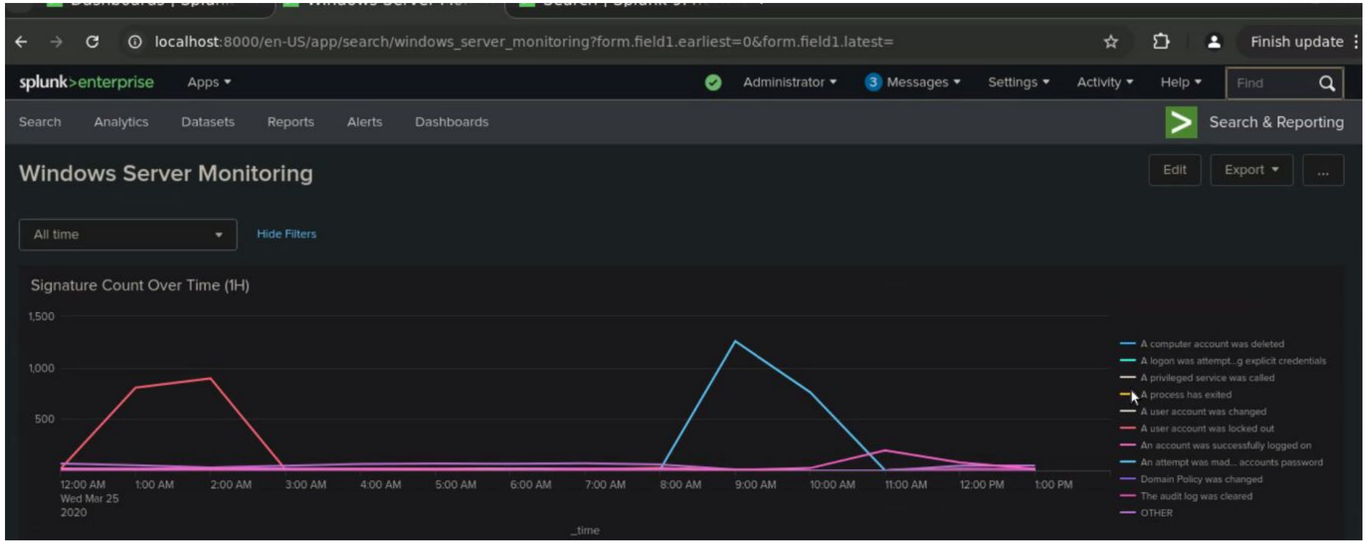
- Our alert was triggered and sent **6** emails to the SOC. This was due to increased activity around **8:00 AM MST** due to 35 events.
- Based off the findings, we could of raised the threshold to mitigate some of the extra data coming through.

Attack Summary—Windows

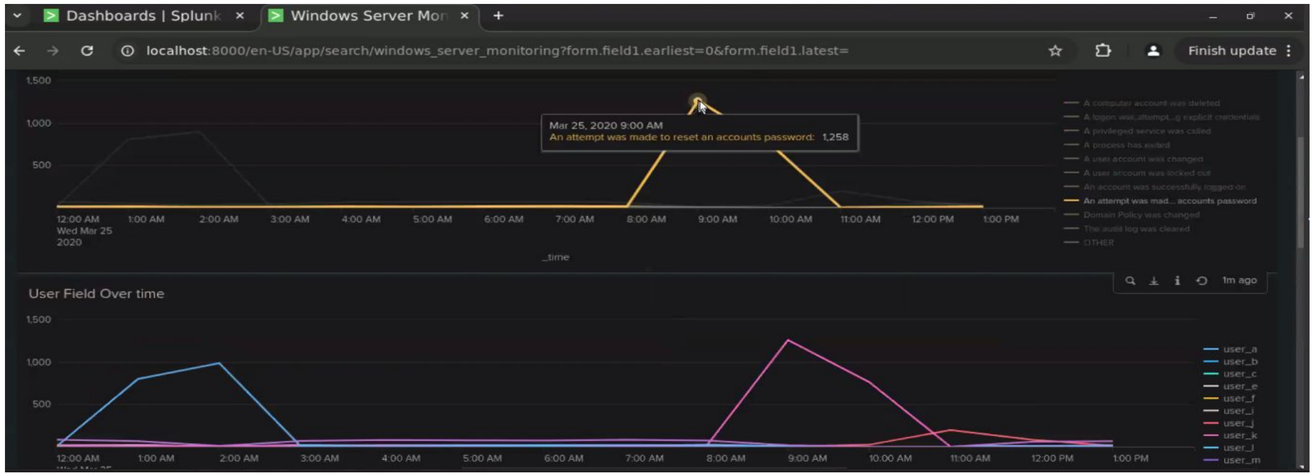
Backdoor Bouncers findings from your dashboards when analyzing the attack logs.

- When reviewing the dashboard for signatures, there was standout activity from **user_c** at **5:00 AM MST** which caused a logged trigger event. This was due to a deleted account at **5:00 AM MST** and a series of successful logins at **1:00 AM, 5:00 AM, 8:00 AM MST.**
- When reviewing the dashboard for users, there were three standout users that saw spikes in their volume **user_a, user_j,** and **user_k**. Our trained analysts saw abnormalities in user usage during the following hours: **1:00 AM, 2:00AM**, **9:30 AM, 10:30 AM and 11:45 AM MST.**

Screenshots of Windows Attack Logs



Backdoor Bouncers shows you who has access to your network - **Accountability!!**



Our Trained SOC Analysts are ready to source **VSI Enterprise**'s Future Cybersecurity needs -

As the Landscape Changes, **Change with Backdoor Bouncers!!**

Attack Summary—Apache

Backdoor Bouncers findings from your reports when analyzing the attack logs.

- When reviewing the **POST** method, we observed a large spike in activity. The large increase was about **12 times the normal amount**. This method is used to upload files and submit web forms.
- When reviewing the referrer domain report, we established a baseline of 3,000 but the attack data showed only 570, which is drastically less.
- We also saw changes in the HTTP response codes for **404** and **200**.

Backdoor Bouncers hosts yearly conferences after BootCon to encompass the updates most pertinent to Office Safety.

Call Today to schedule your company's review of this information, because McAfee Virus Scan doesn't catch what **Backdoor Bouncers** can!! Don't Hesitate - **Reserve your space today!!!**

Attack Summary—Apache

Backdoor Bouncers findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- Our threshold for international activity was set to 65 however, the event came back with over 800. We encouraged the SOC to increase the threshold to 70 due to this large number.
- Our threshold for HTTP **POST** was 4 and at **8:00 AM MST** we observed 1296 events which was able to trigger the email to the SOC.

Backdoor Bouncers hosts yearly conferences after BootCon to encompass the updates most pertinent to Office Safety.

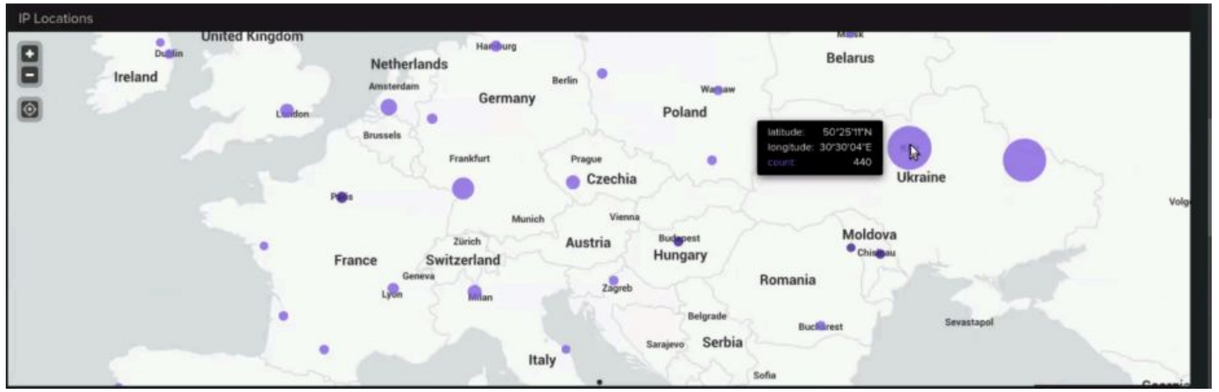
Call Today to schedule your company's review of this information, because McAfee Virus Scan doesn't catch what **Backdoor Bouncers** can!! Don't Hesitate - **Reserve your space today!!!**

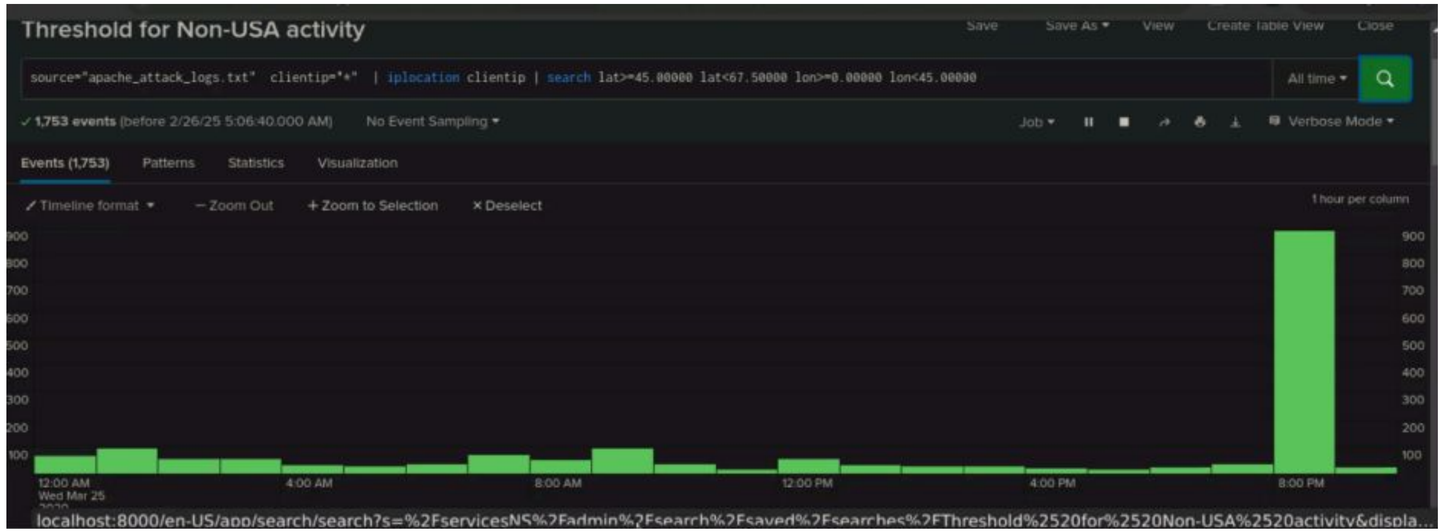
Attack Summary—Apache

Backdoor Bouncers findings from your dashboards when analyzing the attack logs.

- **Two spikes** in the data did stand out as abnormalities as collected for **POST** (1,296 events) and **GET** (729 events) at **6:00 PM MST (GET)** and **8:00 PM MST (POSTS).**
- The **GET** events were spiked in **Kiev, Ukraine** and jumped **10x**!
- Total URI changed by **55%** between the pool data and attack data.
- **Accountlogin.php** was hit with **1,323 events** in comparison to the baseline dataset.
- Based on the URI being assessed, we believe the attacker could of used either **Brute Force Attack or Password Spraying**.

Screenshots of Attack Logs





Additional Screenshots of Attack Log Dataset highlighting the spikes in activity

VSI Enterprise has most recently noted: **Kiev, Ukraine.**

Severity Level: CRITICAL

Summary and Future Mitigations

Project 3 Summary

- **What were your overall findings from the attack that took place?**

  After our review, we found that VSI suffered attacks on **March 25th** to both their Windows servers and Apache servers. These attacks most likely involved Brute Force Attacks and password spraying which occurred through multiple regions of the world.

- **To protect VSI from future attacks, what future mitigations would you recommend?**

  Strengthen Password Policies: Require strong policies across all departments such as length of password, use of special characters, and requiring regular password changes. As an extra layer of protection, we also recommend the use of **MFA, Network Segmentation along with the use of SOARs, SIEMS and Least Privilege Access.** Using these methods and ideals together we can monitor, mitigate and hopefully eliminate any potential leaks going further– Together We Can!!