

TryHackMe – BOTSV2 Advanced Investigation Report

Overview

This report documents a detailed investigation of the **BOTSV2 room on TryHackMe**, focusing on advanced threat hunting using **Splunk**. The investigation covered network traffic, user behavior, malware delivery, web vulnerability exploitation, ransomware activity, and account compromise events.

The main goals were to identify **malicious activity involving Amber Turing, Kevin Lagerfield, Mallory's MacBook (kutekitten), and Taedonggang APT behavior**, including file encryption, malware execution, and C2 communications.

All findings are fully supported by **Splunk searches**, filters, and event correlation across multiple sourcetypes.

Environment

- **Platform:** Kali Linux (Splunk Search & Reporting)
- **Splunk Index:** botsv2
- **Primary Sourcetypes:**
 - stream:http – HTTP/HTTPS traffic
 - stream:smtp – Email traffic
 - pan:traffic – Palo Alto firewall logs
 - osquery:* – Host-level OS and filesystem events
- **Target Domains:**
 - Primary: www.brewertalk.com
 - Competitor: www.berkbeer.com
- **Target Users:** Amber Turing, Kevin Lagerfield, Mallory

100-Series Challenges

Q1: Amber's Tor Browser Version

Objective: Identify the version of Tor Browser installed by Amber to anonymize web activity.

Methodology:

1. Filter events for Amber's activity using keyword search:

```
index=botsv2 amber tor
```

2. Look for **user agent strings** or download logs indicating Tor Browser installation.
3. Extract version number from the user agent string.

Evidence:

- Event showing Amber accessing Tor resources:

Mozilla/5.0 (...) Firefox/52.0 TorBrowser/7.0.4

Conclusion:

Tor Browser Version: 7.0.4

Q2: Brewertalk.com Public IPv4 Address

Methodology:

1. Filter HTTP traffic related to Brewertalk:

```
index=botsv2 sourcetype=stream:http brewertalk
```

2. Aggregate by destination IP to find public routable IPs:

```
| stats count by dest_ip
```

Evidence:

- Private IPs (e.g., 172.31.x.x) ignored
- Public IP observed: 52.42.208.228

Conclusion:

Public IPv4: 52.42.208.228

Q3: Vulnerability Scanner IP

Methodology:

1. Identify abnormal traffic from high-volume requests:

```
index=botsv2 sourcetype=stream:http http_host="www.brewertalk.com"
| search user_agent="*Nikto*" OR user_agent="*sqlmap*" OR
user_agent="*dirb*" OR user_agent="*nmap*"
| stats count by src_ip user_agent
```

Evidence:

- IP 45.77.65.211 appears repeatedly with Nikto scanning behavior.

Conclusion:

Scanner IP: 45.77.65.211

Q4: Targeted URI Path

Methodology:

- Focus on suspicious activity from the scanner IP:

```
index=botsv2 src_ip="45.77.65.211"
| stats count by uri_path
```

Evidence:

- /member.php observed repeatedly.

Conclusion:

Attacked URI Path: /member.php

Q5: SQL Function Abused

Methodology:

- Filter POST payloads targeting /member.php:

```
index=botsv2 src_ip="45.77.65.211" uri_path="/member.php"  
| table _time uri user_agent
```

Evidence:

- SQL injection payloads using:

```
updatexml(..., concat(...), ...)
```

Conclusion:

SQL Function: updatexml

Q6: XSS Cookie Value

Methodology:

1. Filter Kevin's HTTP traffic for likely XSS exfiltration:

```
index=botsv2 sourcetype=stream:http kevin  
| table _time src_ip dest_ip uri
```

2. Look for numeric-only cookie values in query strings.

Evidence:

- Cookie value transmitted: 1502408189

Conclusion:

Cookie Value: 1502408189

Q7: Malicious Brewertalk.com Username

Methodology:

- Identify POST requests creating user accounts on Brewertalk:

```
index=botsv2 sourcetype=stream:http brewertalk.com http_method=POST
| table _time uri form_data
```

- Look for usernames created with Kevin's stolen token.

Evidence:

- POST request data:

```
my_post_key=1bc3eab741900ab25c98eee86bf20feb
username=kIagerfield
password=beer_lulz
email=kIagerfield@froth.ly
```

Conclusion:

Malicious Username: kIagerfield

200-Series Challenges

These questions largely reference the same events and answers as 100-series questions:

Question	Answer
Tor Version	7.0.4
Brewertalk IP	52.42.208.228

Scanner IP	45.77.65.211
URI Path	/member.php
SQL Function	updatexml
XSS Cookie	1502408189
Malicious Username	klagerfield

300-Series Challenges (Mallory & MacBook Investigation)

Q1: Critical PowerPoint Encrypted File

Steps:

1. Identify Mallory's MacBook:

```
index=botsv2 mallory
```

2. Extract host field → kutekitten
3. Filter PowerPoint extensions:

```
index=botsv2 host="kutekitten" (*.ppt OR *.pptx)
```

Evidence:

- File encrypted by ransomware:

Frothly_marketing_campaign_Q317.pptx.crypt

Conclusion:

Encrypted PowerPoint: Frothly_marketing_campaign_Q317.pptx.crypt

Q2: Encrypted Movie File

Methodology:

1. Focus on same sourcetype as PowerPoint event.
2. Filter using encrypted file extension .crypt (example):

```
index=botsv2 host="kutekitten" sourcetype="osquery:file" *.crypt
```

Evidence:

- Encrypted movie file: GameOfThrones_S07E02.mkv.crypt

Conclusion:

Season & Episode: S07E02

Q3-Q7: USB Malware Delivery & C2 Analysis

Methodology:

1. Search for USB insertion & malware execution on kutekitten:

```
index=botsv2 kutekitten
```

2. Focus on Osquery events for user_folders, executable_hashes, USB_vendor fields.
3. External research via USB ID database confirms vendor.
4. Correlate timestamps for C2 communications after malware execution.

Evidence & Answers:

Question	Answer
USB Drive Vendor	Alcor Micro Corp.
Malware Programming Language	Perl
First Seen in Wild	2017-01-17
C2 Server 1 (FQDN)	eidk.duckdns.org
C2 Server 2 (FQDN)	eidk.hopto.org

400-Series Challenges (Amber & Competitor)

Q1-Q7: Competitor Investigation

Methodology:

1. Identify Amber's IP from pan:traffic logs:

```
index=botsv2 sourcetype="pan:traffic" amber
```

2. Filter HTTP traffic to competitor:

```
index=botsv2 IPADDR sourcetype="stream:HTTP" | dedup site | table site
```

3. Identify competitor using industry knowledge → www.berkbeer.com

4. Use SMTP logs to trace email communications with executive.

Evidence & Answers:

Question	Answer
Competitor Website	www.berkbeer.com
Executive Image	/images/ceoberk.png
CEO Name	Martin Berk
CEO Email	mberk@berkbeer.com
Second Employee Email	hbernhard@berkbeer.com
File Attachment Sent	Saccharomyces_cerevisiae_patent.docx
Amber's Personal Email	ambersthebest@yeastiebeastie.com

500-Series Notes

- Skipped in room; relevant to extended APT hunting and Splunk correlation exercises.
- Encouraged to implement in a **local Splunk instance** for hands-on exploration.

Observations & Correlations

- **Chained Attack Flow:**
 - Amber uses Tor for anonymity.
 - Brewertalk.com targeted by vulnerability scanner.
 - SQL Injection used on /member.php.
 - XSS exploited to steal Kevin's cookie.
 - Stolen CSRF token used to create malicious accounts.
 - Mallory's MacBook files encrypted by ransomware.
 - Taedonggang APT uses USB delivery and dynamic DNS C2.
 - Scheduled tasks maintain persistence (process.php).
- **Threat Intelligence Integration:**
 - Cross-reference malware hashes via **VirusTotal**, **Hybrid Analysis**, **Any.Run**.
 - Identify unusual file downloads
(`file_type == Microsoft Word Document (.docx)` or `file_type == Microsoft Word Document (.hwp)`).
- **Splunk Best Practices:**
 - Use dedup to remove duplicates.
 - Use stats count by FIELD to identify anomalies.
 - Combine sourcetype filters (`stream:http`, `osquery:file`, `stream:smtp`) for correlation.

Recommendations

1. **Network Monitoring:** Use Splunk dashboards to track unusual USB and file encryption activity.
2. **Email Security:** Monitor SMTP traffic for attachments and unusual recipient patterns.
3. **Threat Hunting Playbooks:** Create Splunk searches for SQL Injection, XSS, and CSRF activity.
4. **APT Detection:** Monitor dynamic DNS activity for early detection of C2 servers.
5. **Incident Response:** Correlate endpoint Osquery logs with network traffic to detect lateral movement.

Conclusion

This investigation illustrates **a multi-stage APT attack** combining:

- Tor usage for anonymity
- Automated web vulnerability scanning
- SQL Injection & XSS exploitation
- Cookie & CSRF token theft
- Spear phishing account creation
- Malware delivery via USB & ransomware encryption
- Dynamic DNS C2 communications

All findings are **fully traceable** in Splunk using the queries and filters detailed above, demonstrating **comprehensive threat hunting methodology** for academic, SOC, or incident response purposes.