NAIPAY INCIDENT RESPONSE REPORT

APT1337 Canary

Report Date: October 30, 2025

Prepared for: Naipay’s Security and Business Executive

Status: Post-Incident Analysis

Prepared By: KamiLimu Cybersecurity Analyst Team

The Team :

1. Mitchelle Lagat
2. Joseph Ngatia
3. Elaine Mbugua

AGENT : UBUNTU : lp-user-02 (IP: 10.0.1.14)

1. EXECUTIVE SUMMARY

Between **2–3 September 2024**, Naipay's Ubuntu server **lp-user-02 (10.0.1.14)** was compromised through **credential-based SSH access**. The attacker, identified as the likely **APT1337 Canary** threat group, used stolen or reused credentials for the local user **ctfroom** to gain remote access from two AWS-hosted IP addresses in **Ashburn, Virginia (34.226.207.84 and 52.5.37.243)**. Shortly thereafter, the same account was used from an **internal IP address (10.0.1.13)**, showing **lateral movement** within Naipay's network.

Once inside, the adversary executed privileged commands via **sudo** and **su**, gaining **root-level administrative control** of the host. During this phase, they **installed and executed a Velociraptor binary** , a legitimate but dual-use forensic agent, likely repurposed for **persistent remote access and command-and-control operations**. The attacker then **disabled the Wazuh security monitoring agent multiple times**, a deliberate act of **defense evasion** designed to obscure activity and maintain stealth.

This sequence of events represents a full-system compromise, including **Initial Access (valid account use)**, **Privilege Escalation**, **Persistence**, **Lateral Movement**, and **Defense Evasion**. Although no confirmed data exfiltration was detected, the attacker obtained complete control of the affected system and had the capability to access or manipulate sensitive data.

The broader context of the incident showed ongoing automated SSH brute-force attempts from IP ranges in **China, India, and Spain**, highlighting the persistent background threat facing all internet-exposed services. The successful intrusion, however, was a targeted credential abuse, not a vulnerability exploit, underscoring the importance of stronger identity protection, multi-factor authentication (MFA), and resilient endpoint monitoring.

.

2. ATTACK TIMELINE AND SEQUENCE

Agent : lp-user-02 (IP: 10.0.1.14)

The attacker chain on the Ubuntu host began with sustained brute-force attacks and culminated in C2 installation and monitoring evasion.

Time (UTC)	Tactic	Event Description	MITRE Technique
2024-09-02T17:38:50	Defense Evasion	Wazuh agent stopped on lp-user-02 (Rule 506). This occurred approximately three hours *before* the first successful SSH login.	T1562.001 (Disable or Modify Tools)
2024-09-02T17:59:51 – 18:10:13	Credential Access	Failed password attempts for	T1110.001 (Password Guessing)
2024-09-02T20:21:59	Initial Access	Successful SSH login(Accepted password, Rule 5715) for user ctfroom from external AWS IP 34.226.207.84.	T1078 (Valid Accounts), T1021 (Remote Services)
2024-09-02T20:24:16	Privilege Escalation	Ctfroom uses sudo cp to copy the binary velociraptor-v0.72.4-linux-amd64 to the privileged path **/usr/local/bin/velociraptor**.	T1548.003 (Sudo and Sudo Caching)
2024-09-02T20:25:52	Initial Access	Successful SSH login for ctfroom from external AWS IP 52.5.37.243**.**	T1078, T1021
2024-09-02T20:27:07 – 20:29:58	Command & Control (C2)	Sudo executes /usr/local/bin/velociraptor with client.config.yaml client -v multiple times (Rule 5402), installing the persistence agent.	T1548.003, T1059
2024-09-02T21:02:43	Lateral Movement	**Successful SSH login for ctfroom from internal pivot IP 10.0.1.13.**	T1021, T1078

2024-09-02T21:03:03	Privilege Escalation	Ctfroom uses sudo /usr/bin/su - (Rule 5402) to open an interactive root session (session opened for user root).	T1548.003
2024-09-03T06:14:57 & 08:58:34	Defense Evasion	**Wazuh agent stopped again on lp-user-02 (repeated events).**	T1562.001
2024-09-03T06:59 – 07:02	Credential Access	Massive PAM and SSH authentication failures from Indian IP	T1110.001
2024-09-03T20:16:26 – 20:16:56	Credential Access	Burst of invalid user/failure events from Spanish IP	T1110.001

3. HOW THE INCIDENT WAS DETECTED, CONTAINED, AND ERADICATED

Agent : Ubuntu (Ip-user-02)

A. Detection

The incident was detected through Naipay's Wazuh SIEM platform, which was actively monitoring the affected Ubuntu endpoint (**lp-user-02 / 10.0.1.14**). Key detection points included:

Wazuh Alerts & Log Analysis:

- **Multiple high-severity alerts** were triggered by suspicious authentication and privilege escalation events:
    - Several high-risk notifications were raised due to new authentication and privilege escalation incidents:
    - Two external (34.226.207.84, 52.5.37.243) and an internal (10.0.1.13) IPs (successfully logging in by SSH to ctfroom account) were flagged by Wazuh rule 5715 (sshd: authentication success) and 5501 (PAM: Login session opened).
    - Privileged escalation: ctfroom ran sudo and su to get root privileges (uid=0), which was identified by the 5402/5403 rules.
    - Defense evasion: The Wazuh agent was stopped three times(rule 506), which indicates an attempt to deactivate monitoring.
    - Suspicious binary installation: The Velociraptor client was copied to /usr/local/bin/velociraptor and executed as root, with configuration file client.config.yaml.

- **Correlation of Events:** The Wazuh dashboard correlated these events, indicating that there was a sequence of initial access, privilege escalation, persistence, and defense evasion within a small time frame.

B.Containment

These containment measures were implemented when malicious activity was confirmed to be present:

- Immediate Isolation: To stop any further lateral movement or subsequent data exfiltration, the compromised endpoint (lp-user-02) and the internal pivot host (10.0.1.13) were isolated from the network.
- Account Lockdown: The hacked ctfroom account was disabled and the credentials for all the privileged and possibly exposed accounts were changed.
- Session Termination: Any active SSH sessions from the attacker's IPs were forcibly terminated.
- Blocking the Malicious IPs: The malicious attacker IPs (34.226.207.84, 52.5.37.243) were blocked at the perimeter and host firewalls.
- Inactivation of Persistence Mechanisms: The Velociraptor binary and configuration files were deleted, and unauthorized SSH keys, new user accounts and suspicious cron jobs were searched for.
- IOC-Based Threat Hunting: To make sure that no other endpoints were compromised, the security team searched the environment for identified IOCs like usernames, IPs, binaries and config files.

C.Eradication

To fully eradicate the threat, the following actions were taken:

- Malware and Artifact Removal: Files installed by the attacker such as /usr/local/bin/velociraptor, /home/ctfroom/velociraptor and client.config.yaml were deleted.
- Restoration of Security Controls: The Wazuh agent was reinstalled and rebooted to recover endpoint monitoring.
- System Integrity Checks: File integrity monitoring and checksums were used to ensure that no unauthorized changes remained.
- Credential Hygiene: The passwords of privileged accounts were reset throughout the organization, and SSH was set to use key-based authentication and MFA.
- Patch Management: The endpoint and other related systems were updated with the current security patches.
- Improved Monitoring: More detection rules were implemented in Wazuh to alert on similar attack patterns in future.

4. HOW NAIPAY RECOVERED FROM THE INCIDENT

- System Restoration: The affected endpoint was rebuilt from a clean baseline and critical data was restored from verified backups.
- Reintegration: Once the endpoint had been properly validated, it was reconnected to the domain, and put back into production.
- Post-Incident Monitoring: The system was put under increased monitoring in order to identify any repeat of suspicious activity while focusing on the past-identified IOCs.
- User Notification and Support: Affected users were informed and advised on how to make changes to their passwords and given guidance on best SSH security practices.
- Security Posture Enhancement: Incident response playbooks were revised based on lessons learned in the incident, endpoint hardening (e.g. SSH configuration, sudo restrictions) was improved, and user training was enhanced.
- Audit and Compliance: A complete audit trail was recorded and compliance requirements were checked to confirm that all the regulatory requirements were fulfilled.

5. KEY INDICATORS OF COMPROMISE-IOCs

Agent: Ubuntu: Ip-user-02 (10.0.1.14)

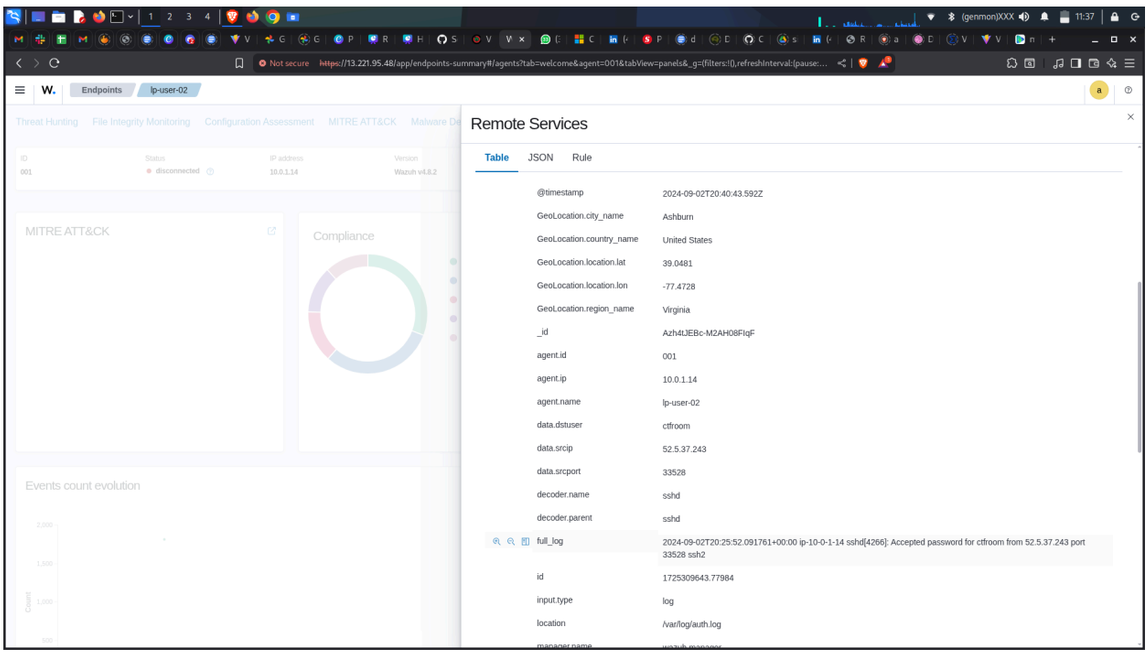
Indicators of Compromise (IOCs)

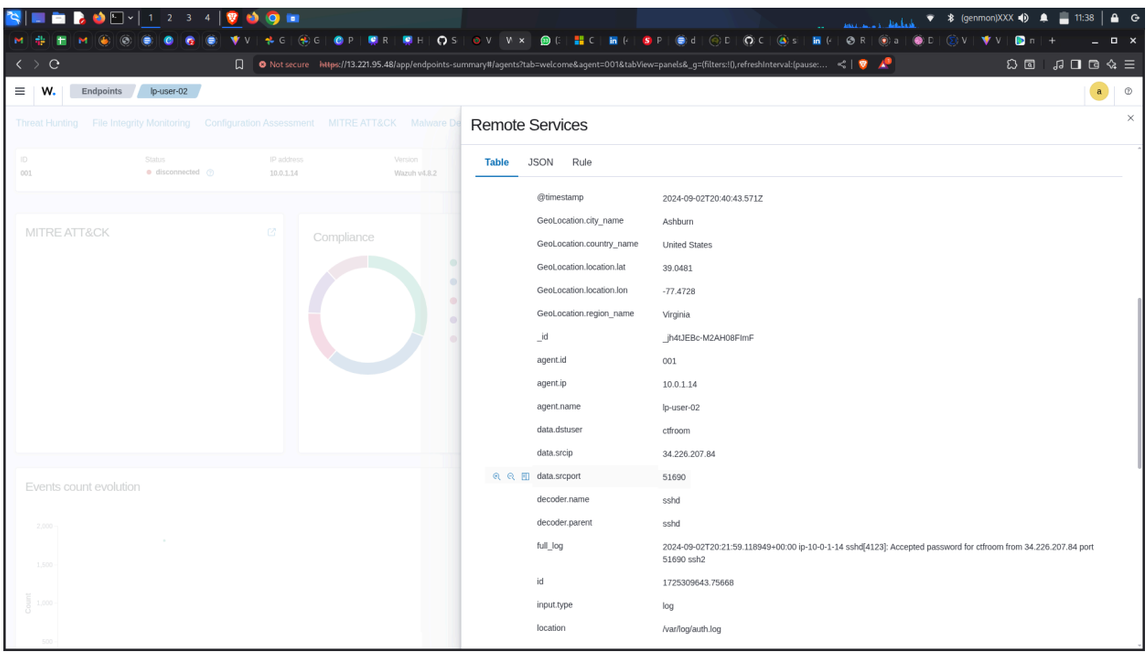
Type	Value	Description
External IPs	34.226.207.84, 52.5.37.243	AWS-hosted IPs (Ashburn, VA) used for successful SSH authentication to lp-user-02
Internal IP	10.0.1.13	Internal pivot host used for lateral movement
Username	ctfroom	Compromised local account used for SSH logins and privilege escalation
Host	lp-user-02 (10.0.1.14)	Ubuntu server compromised via SSH
Processes	sshd, sudo, su	Used to authenticate and escalate privileges to root
File Artifacts	/usr/local/bin/velociraptor, /home/ctfroom/velociraptor/client.config.yaml	Installed and executed Velociraptor agent for persistence/C2
Logs	/var/log/auth.log	Source of repeated SSH and sudo events
Rule ID	5715, 5501, 5402, 5403, 506	Wazuh detections for SSH, PAM, sudo, and agent stoppage

MITRE Techniques	T1078 (Valid Accounts), T1021 (Remote Services), T1548.003 (Sudo/Sudo Caching), T1562.001 (Disable Tools), T1110.001 (Password Guessing)	Confirmed techniques observed in the intrusion

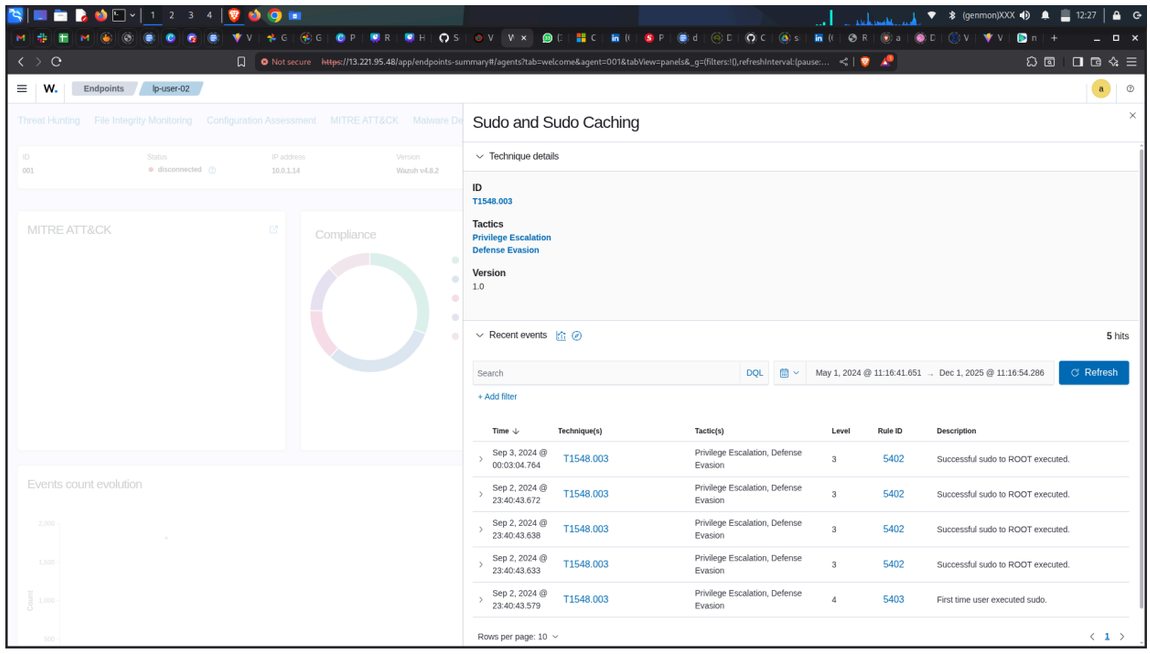
6. SCREENSHOTS AND EVIDENCE

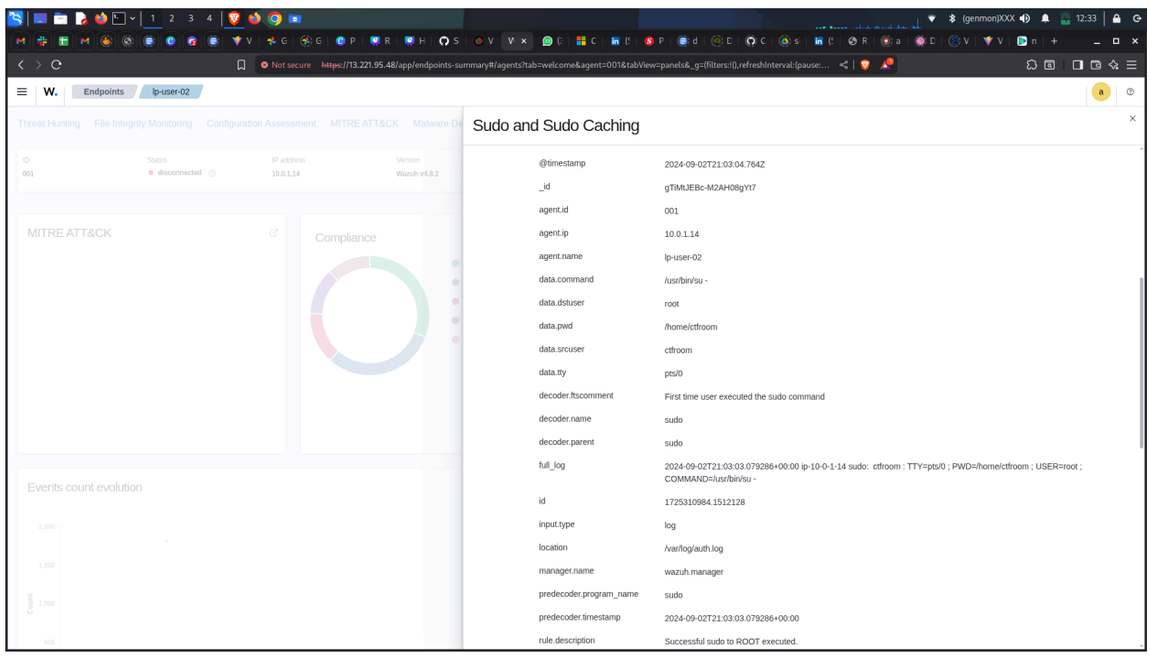
Initial Access

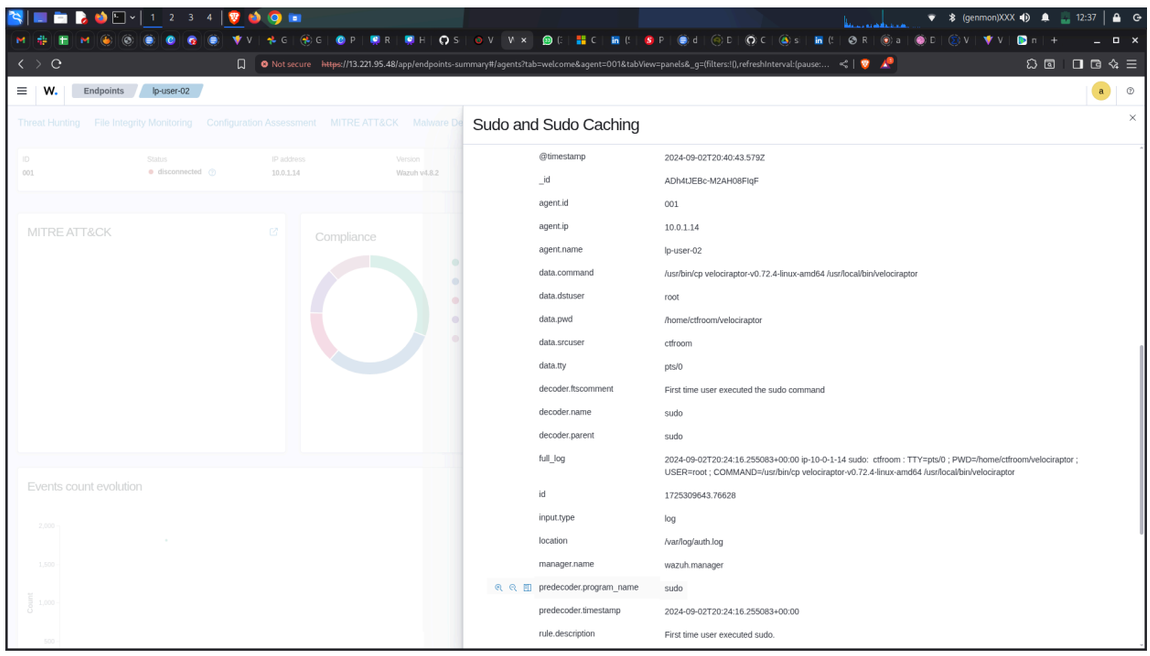




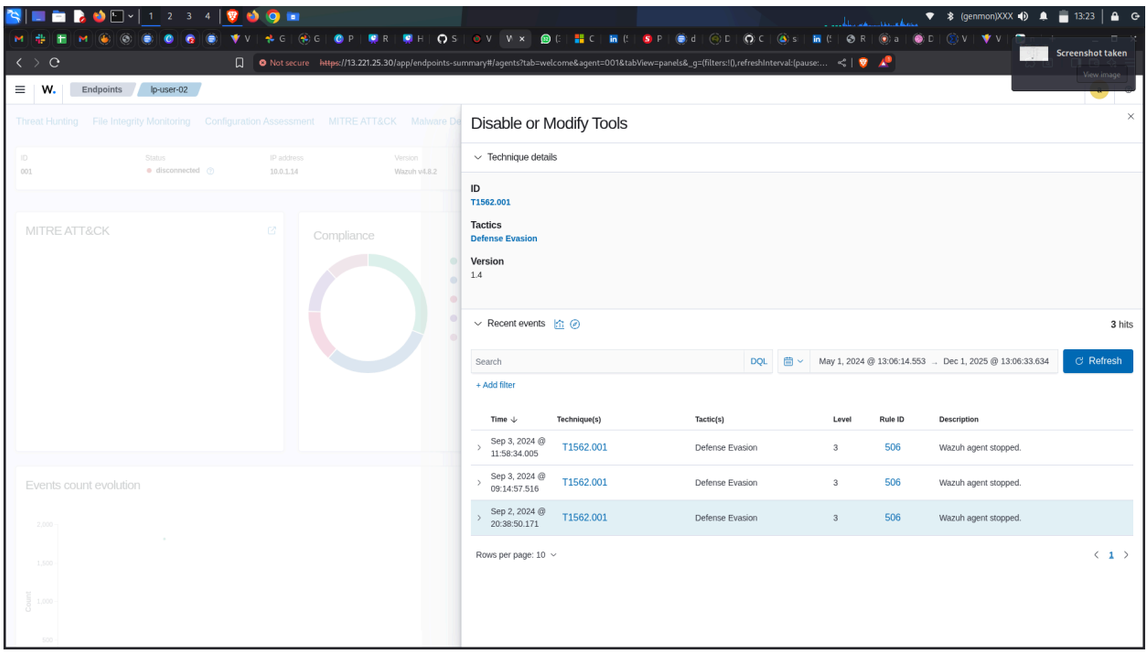
Privilege Escalation

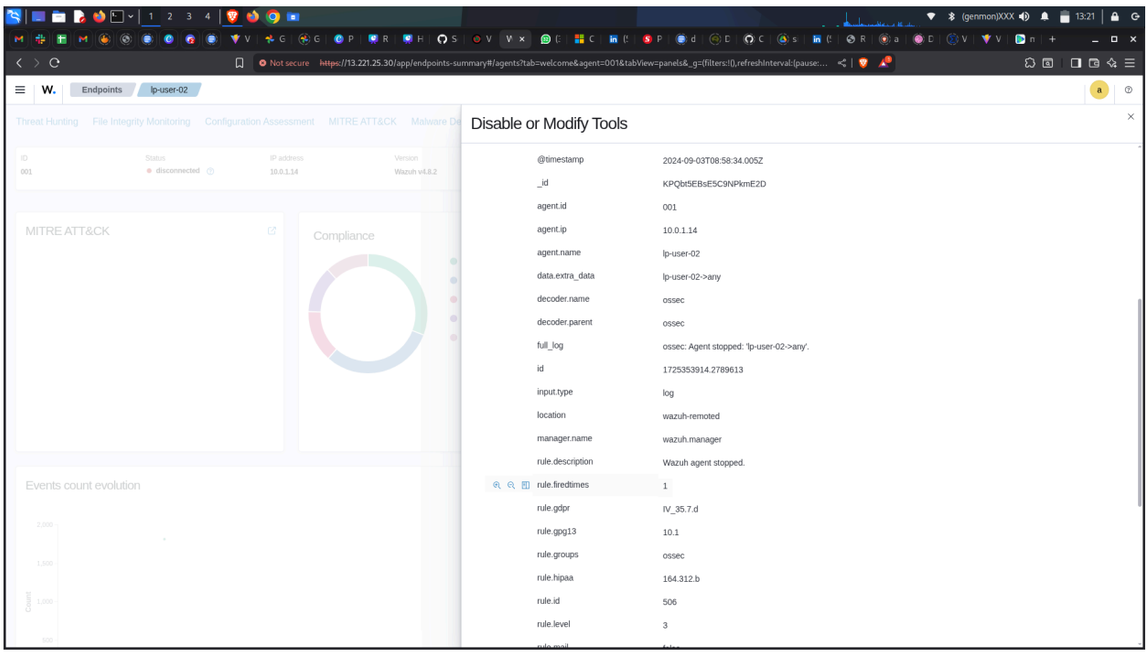




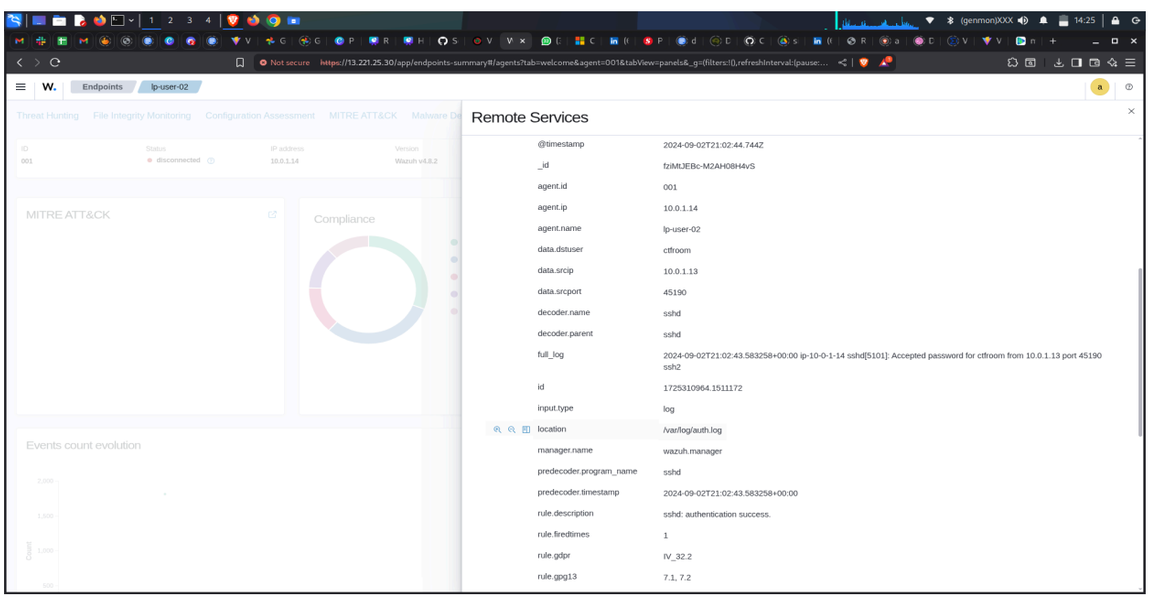


Defense Evasion

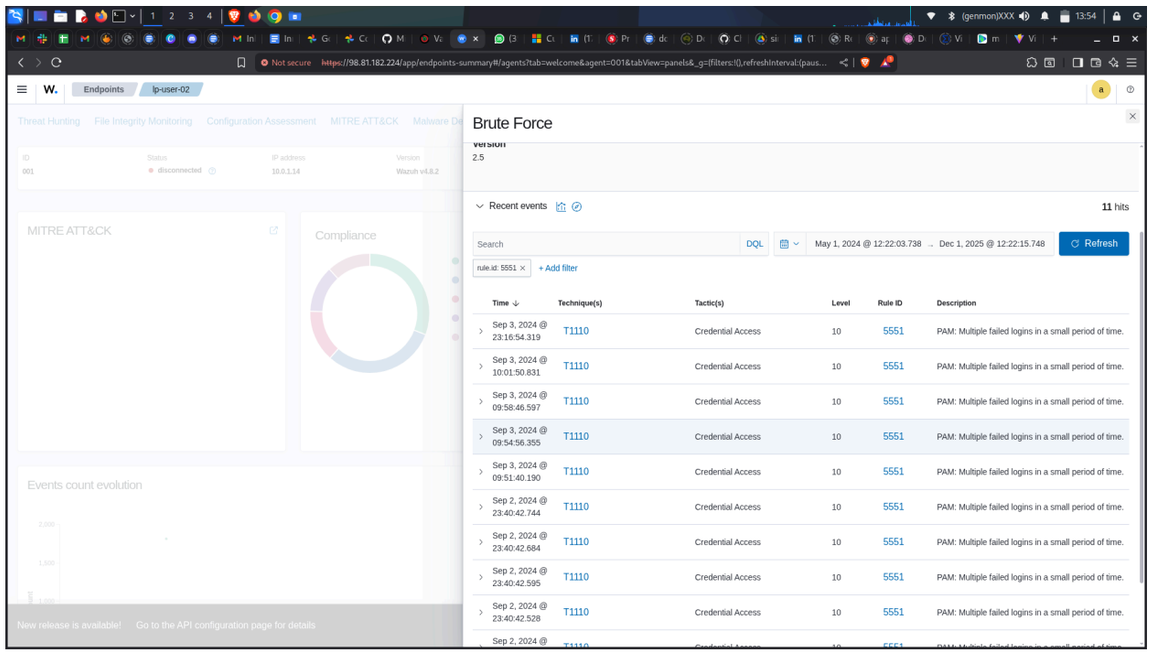


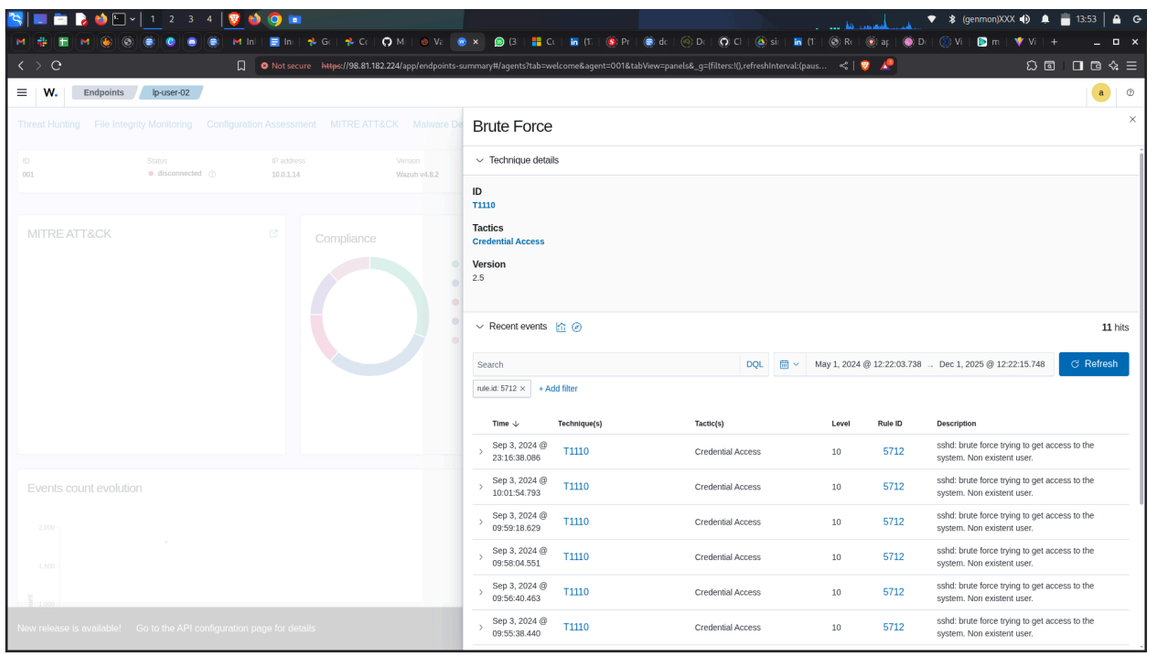


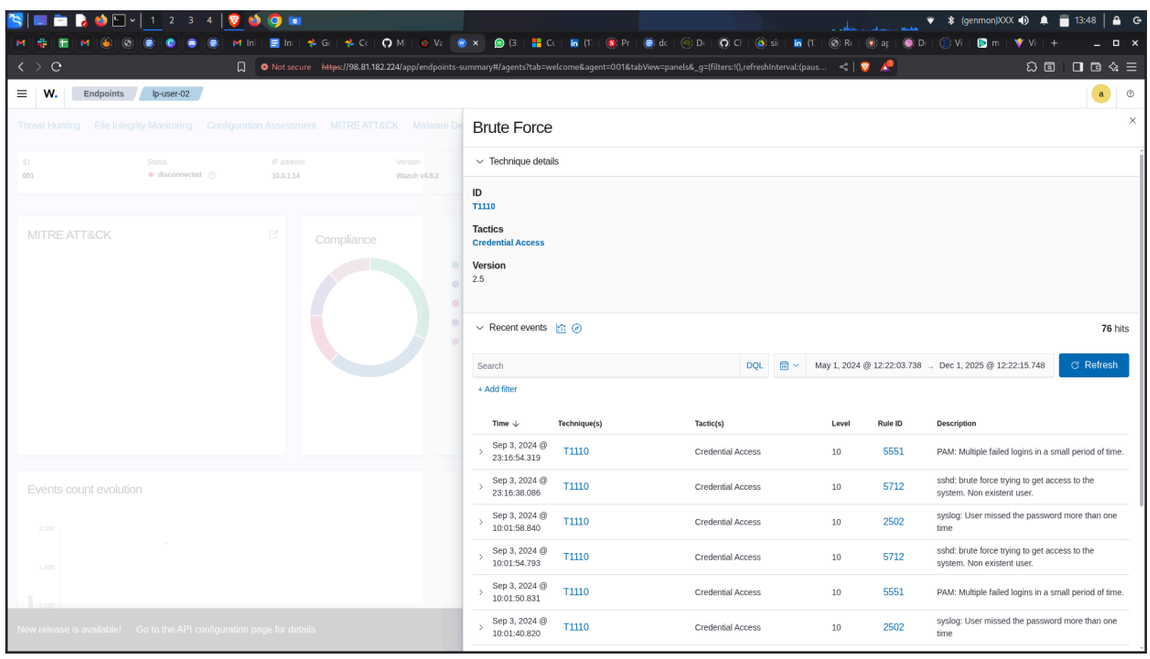
Lateral Movement



Credential Access







7. LESSONS LEARNT AND GAPS IDENTIFIED WITH RECOMMENDED CORRECTIVE AND PREVENTIVE ACTIONS

A. Lessons learnt

- **Credential hygiene is critical.** The attacker exploited weak or reused SSH credentials to gain access. Strong authentication controls (SSH key pairs, MFA) were absent.
- **Monitoring agents must be tamper-resistant.** The adversary successfully stopped the Wazuh agent (T1562.001), blinding detection during key stages of the attack.
- **Privilege segregation was insufficient.** The compromised user *ctfroom* possessed unnecessary sudo privileges, allowing escalation to root.
- **Lateral movement went undetected.** No internal network segmentation or lateral movement detection was in place, allowing cross-host compromise.
- **Tool whitelisting is essential.** The Velociraptor binary was used maliciously, demonstrating how legitimate DFIR tools can serve as C2/persistence agents

B. Gaps Identified

Gap Area	Observation	Risk
Authentication Controls	No enforcement of SSH key-based or MFA authentication.	Easy credential theft/brute-force access (T1110.001, T1078).
Endpoint Protection	Wazuh agent could be stopped by root without tamper-protection.	Loss of visibility and delayed detection.
Least Privilege	Standard user “ctfroom” had full sudo access.	Privilege escalation to root (T1548.003).
Network Segmentation	Internal host 10.0.1.13 could directly SSH into lp-user-02.	Lateral movement risk (T1021).
Alert Correlation	Alerts not triaged promptly; multiple Wazuh rule hits ignored	Prolonged attacker dwell time.

C. Recommended Corrective and Preventive Actions

Technical Measures

1. **Credential Hardening:** Enforce SSH key-based authentication and enable MFA for all privileged accounts.
2. **Password Policy:** Enforce complex, non-reused passwords and centralized credential rotation (e.g., LDAP/Kerberos).
3. **Tamper Protection:** Configure Wazuh agent protection against unauthorized service stops; integrate host-based IDS/EDR with self-defense.

4. **Least Privilege Enforcement:** Revoke unnecessary sudo rights; implement just-in-time privilege elevation.
5. **Segmentation & Firewalling:** Restrict east-west SSH connections; isolate critical servers to prevent lateral movement.
6. **Tool Control:** Implement application allow-listing to prevent unapproved binaries like Velociraptor from executing.
7. **Centralized Monitoring:** Correlate alerts in SIEM to detect T1078/T1021 sequences faster.
8. **Incident Response Readiness:** Regularly rehearse credential compromise and persistence detection playbooks.

Policy & Process Measures

- Create a credential lifecycle policy covering storage, rotation, and access review.
- Establish change-control and audit trails for all privilege escalations.
- Conduct security awareness training on credential reuse and phishing risks.

Naipay CSIRT Establishment (Using the FIRST Services Framework)

Service Area	Core Services	Purpose
Incident Management	Incident triage, analysis, containment, eradication, recovery	Provide structured response to events like SSH compromise and agent tampering.
Vulnerability Management	Asset inventory, vulnerability scanning, patch verification	Prevent exploitation of weak or unpatched systems.
Security Quality Management	Policy enforcement, awareness training, post-incident review	Institutionalize continuous improvement after each incident.
Situational Awareness	Analysis & Synthesis	Enable proactive threat hunting and detection.

Recommended CSIRT Team Type(s)

- **Internal Coordination Team:** Responsible for Naipay's incident response, containment, and communication.
- **Analysis Team:** Performs forensic investigation, IOC analysis, and log correlation.
- **Infrastructure Support (Assistance) Team:** Works with IT Ops to apply patches, isolate hosts, and restore systems securely.

Justification

- The **coordination team** ensures clear escalation paths and minimizes confusion during incidents.
- The **analysis team** is crucial to interpret Wazuh/SIEM data and produce forensic artifacts, addressing visibility gaps exposed in this case.
- The **assistance team** closes the loop by implementing containment, recovery, and system hardening actions.

Collectively, these team types align with the FIRST Services Framework, ensuring that Naipay can detect, analyze, and recover from future credential-based or lateral-movement attacks before they escalate.

AGENT : WINDOWS : EC2AMAZ-IBM5S7O(10.0.1.11)

1. EXECUTIVE SUMMARY - Agent : Window Host : EC2AMAZ-IBM5S7O(10.0.1.11)

The Windows Server **EC2AMAZ-IBM5S7O (IP: 10.0.1.11)** was compromised on September 3, 2024. The threat actor achieved Initial Access via Remote Desktop Protocol (RDP) using compromised credentials for the local **Administrator** account, originating from the external IP address **197.237.16.55** (Nairobi, Kenya). Authentication occurred using NTLMv2, suggesting a possible Pass-the-Hash attack. Following access, the adversary staged payloads, including multiple PowerShell scripts and DLLs, many associated with the **Atomic Red Team** framework, in temporary and staging directories. The actor rapidly established multiple persistence mechanisms, including creating a new local administrator account **(art-test)** with the password **Password123!** exposed in the command line, establishing a malicious Windows service **(AtomicTestService_CMD)**, deploying Scheduled Tasks, and inserting a registry Run key entry. The overall pattern is consistent with a post-compromise actor establishing covert access, deploying tooling (Ingress Tool Transfer T1105), and configuring persistence.

2. ATTACK TIMELINE AND SEQUENCE

Agent : EC2AMAZ-IBM5S7O(10.0.1.11)

Time (UTC)	Tactic	Event Description	MITRE Technique
2024-09-03T20:40:06	Initial Access / LM	Successful Network Logon (Event ID 4624, Logon Type 3) as Administrator from external IP **197.237.16.55** (Nairobi, Kenya) using NTLMv2 authentication. This suggests a possible Pass-the-Hash attack.	T1078 (Valid Accounts), T1021.001 (RDP), T1550.002 (Pass-the-Hash)
2024-09-03T20:40:09	Initial Access / LM	Second Successful Network Logon (Event ID 4624, Logon Type 3) as Administrator from IP 197.237.16.55, confirming reliable access.	T1078, T1021.001, T1550.002
2024-09-03T20:40:18	Initial Access / LM	**Successful Remote Interactive Logon (RDP)** (Event ID 4624, Logon Type 10)	T1021.001 (RDP), T1078.002

		as **Administrator** from IP 197.237.16.55. This establishes the attacker's interactive session with an elevated token.	(Domain Accounts)
2024-09-03T20:40:52	Execution / Discovery	EC2Launch.exe sets wallpaper and collects EC2 metadata.	T1059.003 (Windows Command Shell), T1087 (Account Discovery)
2024-09-03T20:48:44	Execution / ITT	PowerShell (PID 5532) stages payload components in Temp directory (C:\Users\Administrators\AppData\Local\Temp\2\q12tj3wd\), creating q12tj3wd.d11 and q12tj3wd.cmdline. **csc.exe (C# Compiler) is used to create/overwrite q12tj3wd.d11**	T1105 (Ingress Tool Transfer), T1059
2024-09-03T20:49:00	Execution / ITT	PowerShell (PID 5532) installs the **NuGet package provider** (Microsoft.PackageManagement.NuGetProvider.d11).	T1105
2024-09-03T20:49:26	Ingress Tool Transfer(ITT)	Microsoft Edge (msedge.exe) downloads **ART-attack-cleanup.ps1** to the Downloads folder.	T1105
2024-09-03T20:49:37	Ingress Tool Transfer	Microsoft Edge (msedge.exe) downloads **ART-attack.ps1** to the Downloads folder.	T1105
2024-09-03T20:50:1	Ingress Tool Transfer	File explorer (Explorer.EXE) **moves/copies downloaded scripts** to C:\User\Administrator\Documents\attack-Copy\.	T1105, T1059.003
2024-09-03T20:59:14	Staging / Execution	Root PowerShell (PID 5376) rapidly deploys multiple components of the Atomic Red Team framework (e.g., Invoke-Process.ps1, AtomicClassSchema.ps1) into C:\AtomicRedTeam\tmp\ staging folders	T1059 (Command Shell), T1105

2024-09-03T20:59:29	ITT	PowerShell (PID 6040) uses Invoke-WebRequest to download **PhishingAttachment.xlsm** to the Temp environment.	T1105
2024-09-03T20:59:32	Persistence / Privilege escalation	PowerShell spawns cmd.exe which executes the chained command: **net user art-test /add & net user art-test Password123! & net localgroup administrators art-test /add** (executed from Temp directory). This creates a new admin user.	T1098 (Account Manipulation), T1068 (Privilege Escalation), T1078 (Valid Accounts)
2024-09-03T20:59:32	Execution / Persistence	**schtasks.exe creates scheduled tasks** T1053_005_OnLogon and T1053_005_OnStartup set to run cmd.exe /c calc.exe as SYSTEM	T1053.005 (Scheduled Task)
2024-09-03T20:59:35	Defense Evasion	PowerShell executes reg.exe to add a **Base64 encoded payload to HKCU\Software\Classes\AtomicRedTeam\ART**.	T1112 (Modify Registry), T1027 (Obfuscated Files)
2024-09-03T20:59:38	Persistence	PowerShell spawns cmd.exe which executes reg.exe to add a **Run key persistence entry**: HKCU\...\Run\Atomic Red Team pointing to C:\Path\AtomicRedTeam.exe	T1547.001 (Registry Run Keys)
2024-09-03T20:59:40	Prsistence	PowerShell (PID 4608) deploys **batstartup.bat** from a source directory to both the User Startup and All User Startup folders.	T1547.001 (Startup Folder)
2024-09-03T20:59:40	Execution / Persistence	PowerShell uses start-Process to immediately **execute batstartup.bat** via cmd.exe from the Startup paths	T1059.003, T1547.001
2024-09-03T20:59:45	Persistence / PE	PowerShell spawns cmd.exe which executes **sc.exe** create to install the malicious service **AtomicTestService_CMD** pointing to C:\AtomicRedTeam\...\AtomicService.exe.	T1543.003 (Windows Service)

2024-09-03T20:59:46	Persistence / PE	Malicious service **AtomicService.exe** is started. This process runs with SYSTEM-level privileges	T1543.003 (Windows Service)
2024-09-03T21:00:37	Execution / Staging	owerShell created additional temporary PS1 scripts (__PSScriptPolicyTest_...) in Temp\2\ for continued staging.	T1059

3. HOW THE INCIDENT WAS DETECTED, CONTAINED, AND ERADICATED

Windows (EC2AMAZ-IBM5S7O)

A. Detection

The breach was detected through the organization's Wazuh SIEM platform, which was actively monitoring the affected endpoint (EC2AMAZ-IBM5S7O). The main detection points were:

- **Wazuh Alerts & Sysmon Logs:** Multiple high-severity alerts were triggered by suspicious process creation, registry modifications, and account manipulations. Several significant findings comprised:
    - Creation of a new privileged local account (art-test) with a cleartext password.
    - Addition of this account to the Administrators group.
    - Creation of scheduled tasks and a new Windows service (AtomicTestService_CMD) for persistence.
    - Registry Run key and startup script modifications.
    - Remote logon processes via RDP from an external IP (197.237.16.55, Nairobi, Kenya) using the in-built Administrator account which was identified based on Windows Security Event ID 4624.
    - Command-line and PowerShell activity coming from non-standard directories (e.g. Temp), which suggests living off the land techniques.
- **Correlation of Events:** The Wazuh dashboard was able to correlate these events, pointing to the presence of a rapid sequence of privilege escalation, persistence, and defense evasion activities during a short time period.

B. Containment

When the malicious activity was confirmed, the following steps of containment were performed:

- Immediate Isolation: The affected endpoint was isolated from the network to prevent further lateral movement or data exfiltration.

- Account Lockdown: Accounts that were suspected such as the art-test, and the pre-configured Administrator were disabled or reset.
- Session Termination: Active RDP and network sessions from the attacker's IP were forcefully terminated.
- Blocking Persistence Mechanisms: Each of the persistence mechanisms found (scheduled tasks, malicious services, registry Run keys and startup scripts) were disabled and deleted.
- IOC-Based Threat Hunting: The security team searched the environment for the identified IOCs (e.g., hashes, account names, service names, source IPs) to make sure that no other endpoints were compromised.

C. Eradication

In order to completely eliminate the threat, the following measures have been taken:

- Malware and Artifact Removal: All malicious files, scripts and binaries (e.g. AtomicService.exe, batstartup.bat, suspicious PowerShell scripts) were deleted from the system.
- Registry Restoration: Any malicious Run keys and service entries were removed and all unauthorized registry changes were reverted to their original state.
- System Integrity Checking: The endpoint was tested with scanning rootkits and additional hidden persistence mechanisms with the help of reliable forensic tools.
- Credential Hygiene: Privileged account passwords were reset across the organization and password policies were enhanced.
- Patch Management: Endpoints and other associated systems were updated with the most recent security patches to seal any exploited vulnerabilities.
- Enhanced Monitoring: More detection rules were deployed in Wazuh in order to alert similar attack patterns in future.

4. HOW NAIPAY RECOVERED FROM THE INCIDENT

- System Restoration: A trusted clean baseline was used to restore the affected endpoint. Important information was retrieved from trusted back-ups.
- Reintegration: Once thorough validation was done, the endpoint was re-connected to the domain and restored back to production.
- Post-Incident Monitoring: The system was put under a higher monitoring to identify any reoccurrence of suspicious activity.
- User Notification & Support: Affected users were notified and informed on how to change their passwords as well as trained phishing awareness.
- Security Posture Improvement: Lessons learned from the incident were applied to update incident response playbooks, enhance endpoint hardening, and improve user training.

- Audit and Compliance: The entire audit trail was recorded and compliance requirements were checked to ensure that the regulatory requirements were satisfied.

5. KEY INDICATORS OF COMPROMISE-IOCs

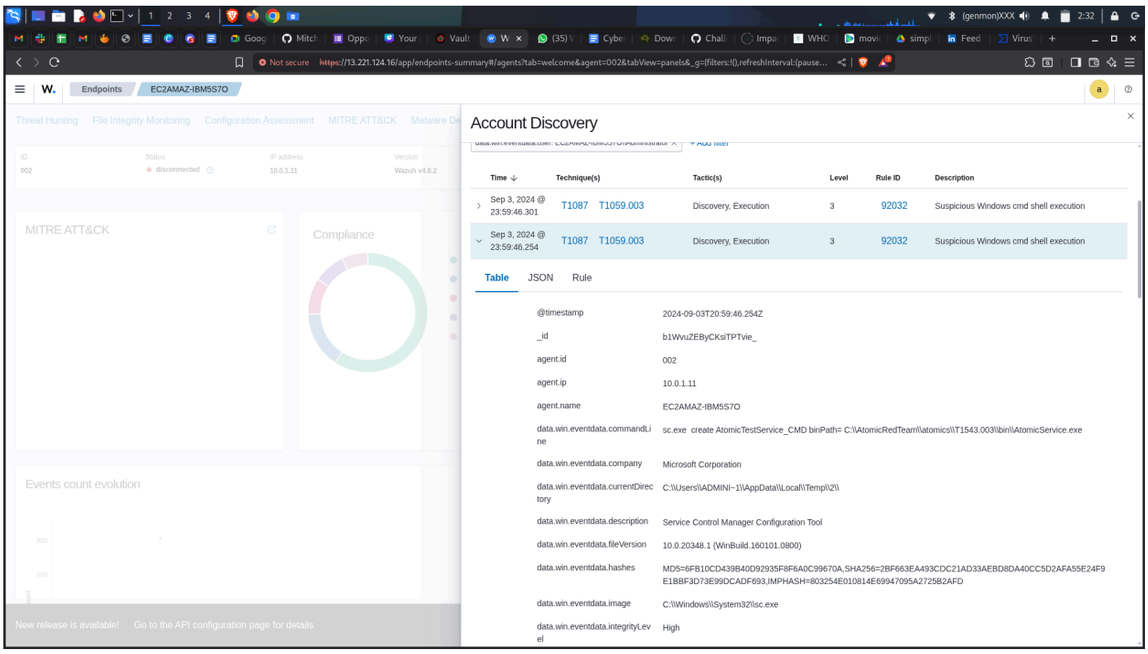
Agent: Windows: EC2AMAZ-IBM5S7O (10.0.1.11)

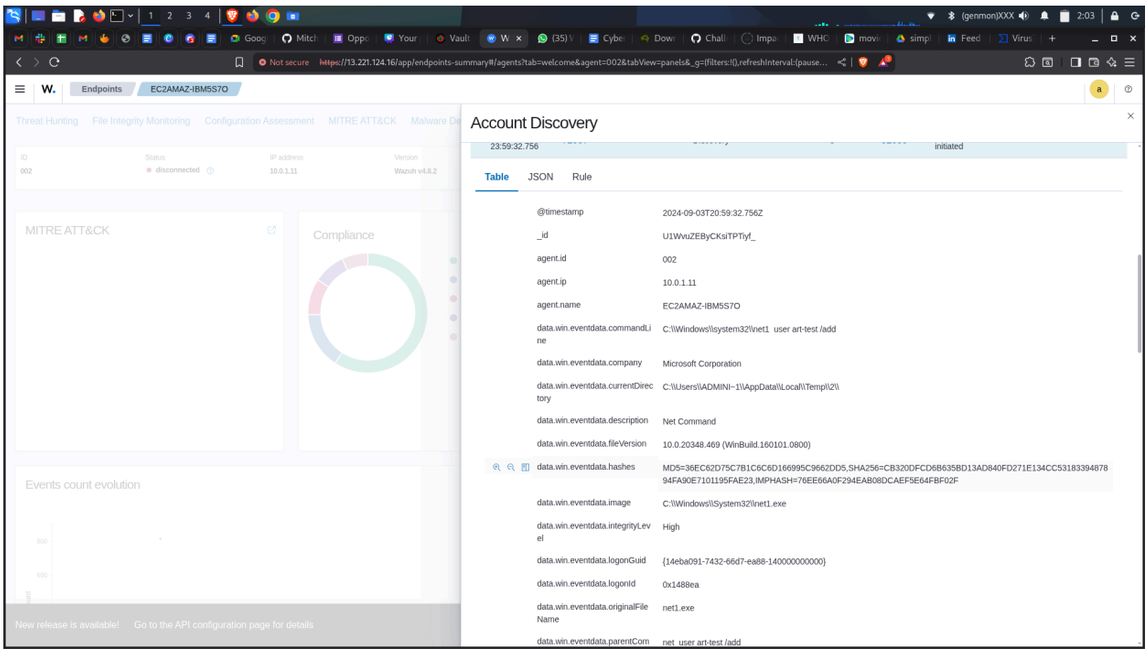
Indicators of Compromise (IOCs)

Type	Value	Description
External IPs	34.226.207.84, 52.5.37.243	Same external AWS IPs observed connecting to Ubuntu host; now interacting with Windows host via SMB and PowerShell remoting
Internal Host	WIN-USER-01	Windows endpoint compromised following lateral movement from lp-user-02
User Accounts	Administrator, ctfroom	Credentials reused or dumped and leveraged on the Windows host
Processes	powershell.exe, cmd.exe, explorer.exe	Executed suspicious commands for persistence and reconnaissance
Artifacts	C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\velociraptor.lnk, C:\ProgramData\Velociraptor\client.config.yaml	Persistence and execution of Velociraptor agent
Registry Keys Modified	HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Velociraptor	Autostart entry for persistence
Event IDs	4624, 4688, 7045	Authentication success, process creation, and service installation events observed
MITRE Techniques	T1078 (Valid Accounts), T1021.002 (SMB/Windows Admin Shares), T1059.001 (PowerShell), T1547.001 (Registry Run Keys), T1569.002 (Service Execution	Techniques indicating lateral movement, persistence, and execution

6. SCREENSHOTS AND EVIDENCE

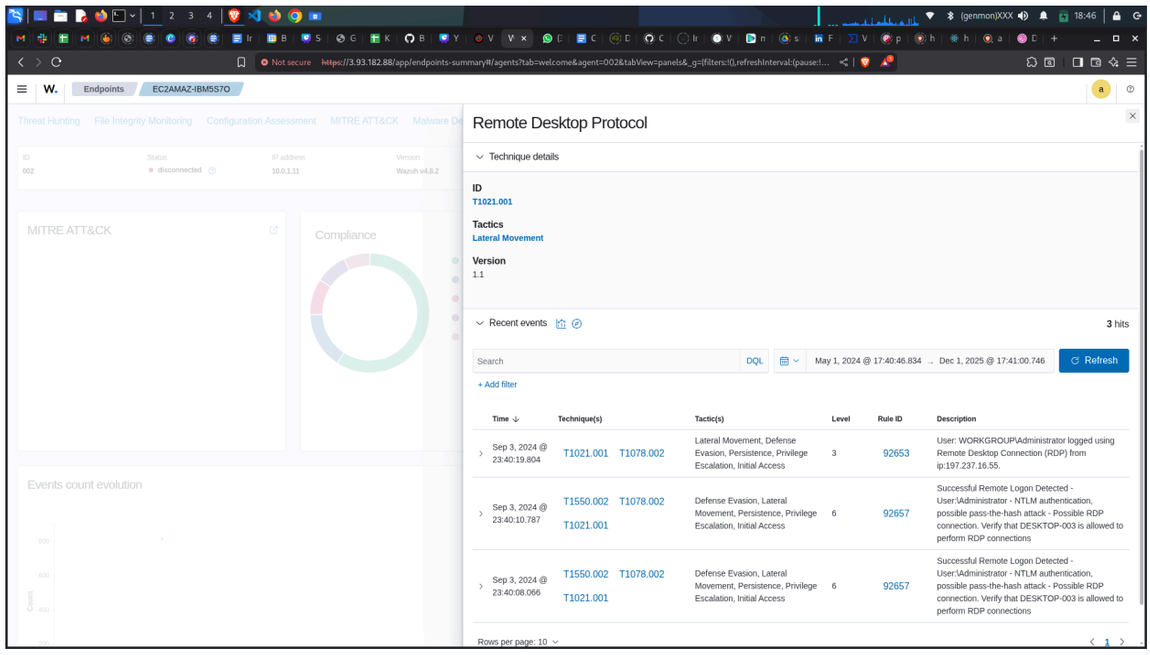
Discovery



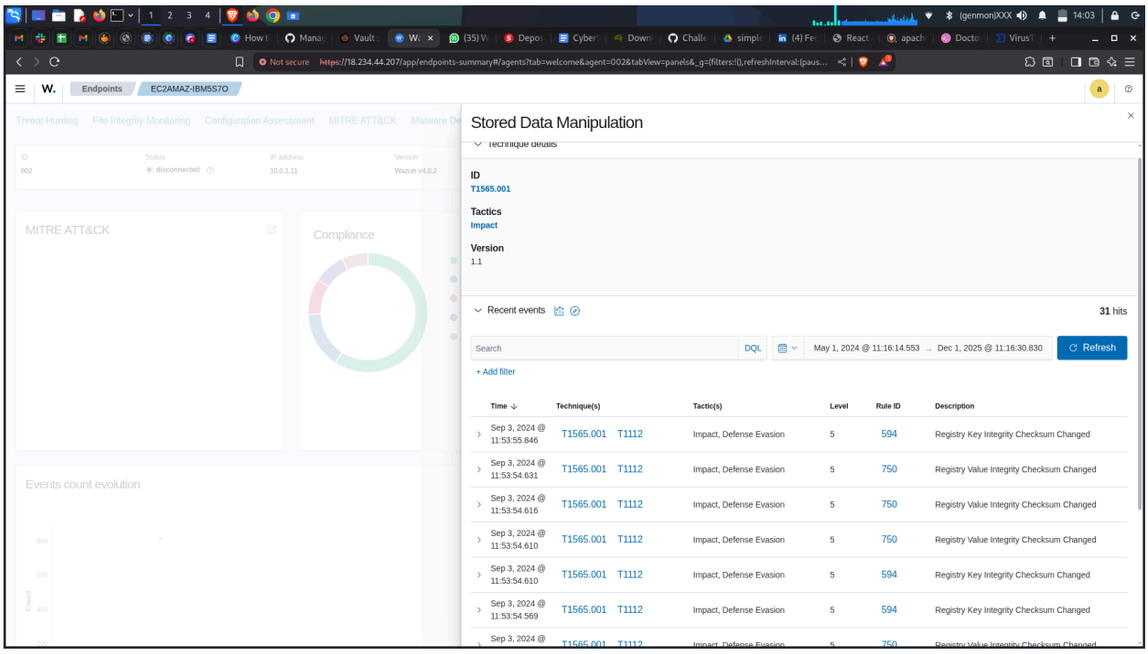


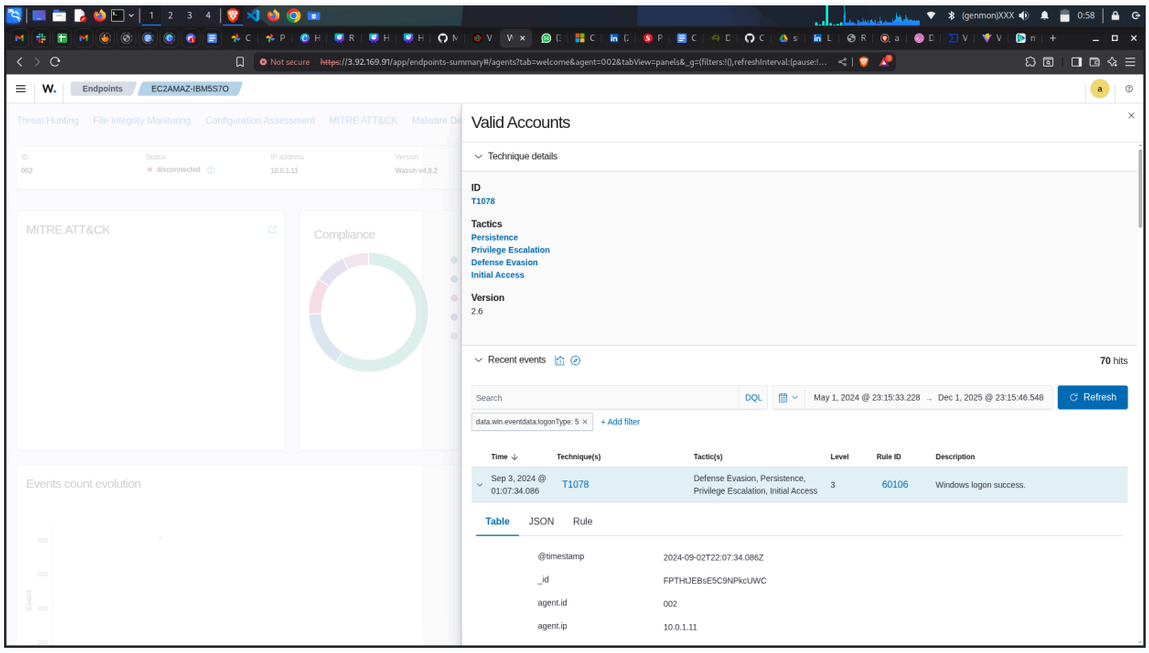
Privilege Escalation

Remote Desktop Protocol

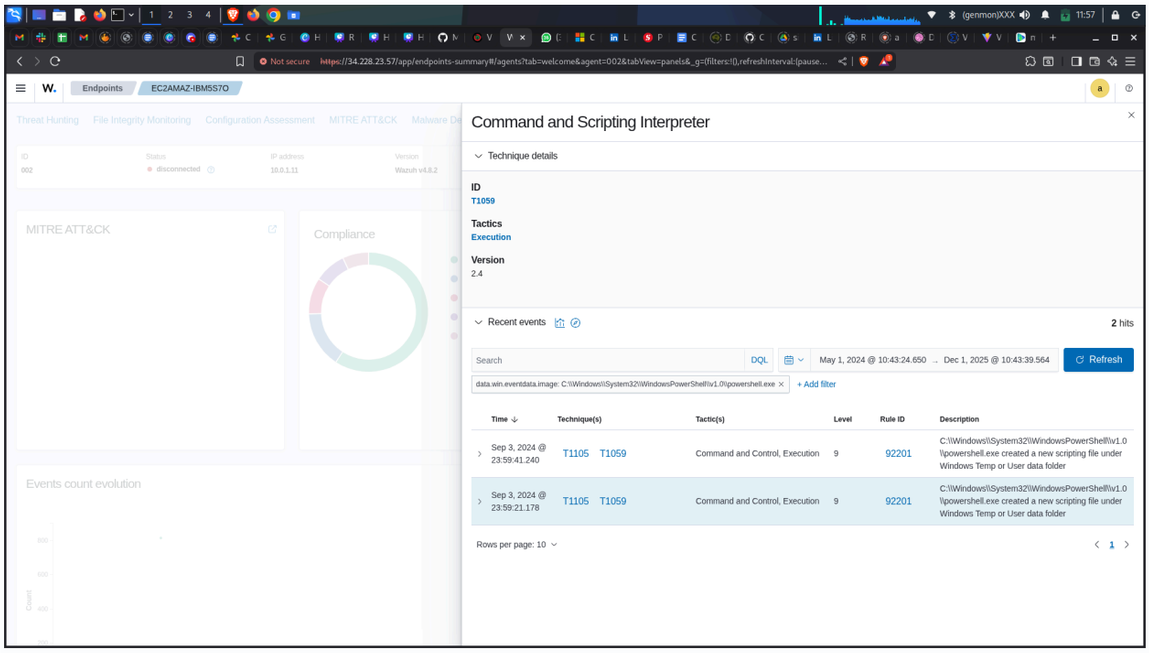


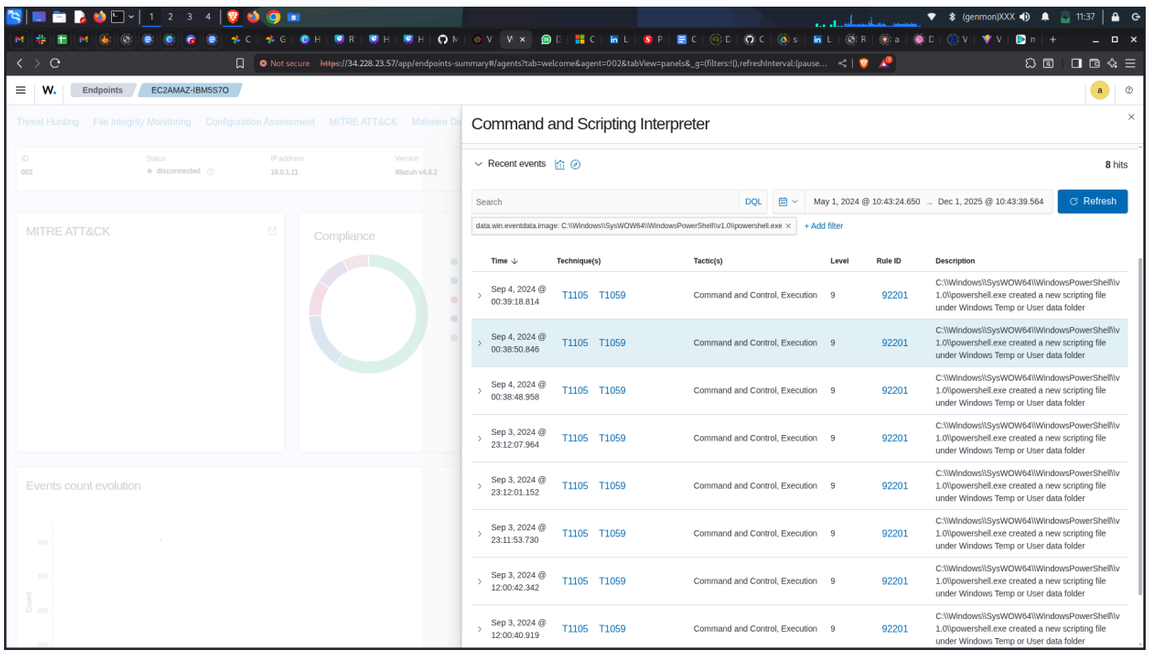
Defense Evasion





Command and Control





7. LESSONS LEARNT AND GAPS IDENTIFIED WITH RECOMMENDED CORRECTIVE AND PREVENTIVE ACTIONS

A. Lessons learnt

- **Credential misuse is cross-platform.** The same compromised credentials used on Linux (ctfroom) were later employed on Windows hosts, emphasizing the risk of shared or reused passwords across systems.
- **Windows logging was insufficiently centralized.** Key events (e.g., PowerShell execution, service creation) were detected late, showing lack of SIEM correlation.
- **Persistence through legitimate tools.** The attacker leveraged Velociraptor for persistence — showcasing abuse of DFIR tools on Windows environments as well.
- **Monitoring gaps in PowerShell activity.** Script Block Logging and AMSI detections were disabled or absent, reducing visibility into malicious use of PowerShell.
- **No network-level containment between OS environments.** The compromise spread easily between Ubuntu and Windows without internal firewall restrictions.

B. Gaps Identified

Gap Area	Observation	Risk
Cross-System Credential Reuse	Same account credentials (ctfroom/Administrator) valid across Linux and Windows.	Enables lateral movement and domain compromise (T1078).
PowerShell Auditing	PowerShell logs (4104, 4103) not enabled or not forwarded to SIEM.	Missed detection of remote command execution (T1059.001).
Persistence Detection	No automated checks for Run keys or service installs.	Hidden persistence (T1547.001, T1569.002).
Endpoint Visibility	EDR coverage inconsistent across Windows and Linux systems.	Fragmented detection and slow response.
Access Segmentation	No separation of administrative and standard user accounts.	Unchecked lateral spread between endpoints.

Recommended Corrective and Preventive Actions

Technical Measures

1. **Enforce Unique Credentials per Platform:** Prevent reuse of local and administrative passwords between Linux and Windows systems.
2. **Enable PowerShell Logging:** Activate Script Block Logging (4104), Module Logging, and transcription for audit trails.
3. **Harden Persistence Controls:** Monitor startup folders, registry run keys, and new service installations.

4. **Implement Endpoint Detection & Response (EDR):** Deploy a unified EDR tool across both Windows and Linux.
5. **Restrict PowerShell Usage:** Apply Constrained Language Mode and block unsigned scripts in enterprise environments.
6. **Centralize Log Management:** Forward Windows Event Logs to SIEM or Wazuh manager for unified analysis.
7. **Internal Network Controls:** Apply host firewalls to limit SMB, RDP, and PowerShell Remoting between user workstations.

Policy & Process Measures

- Implement cross-domain password rotation policies.
- Enforce PowerShell execution policies and least privilege.
- Integrate post-incident review workflows for dual-OS environments.
- Conduct threat hunting exercises across both Windows and Linux to identify lateral movement paths.

Naipay CSIRT Establishment (Using the FIRST Services Framework)

Service Area	**Core Services**	**Purpose**
Incident Management	Multi-OS incident detection, containment, and recovery	Coordinate and execute responses across mixed Windows/Linux environments.
Vulnerability Management	Cross-platform patch and credential management	Address weak configurations and password reuse issues.
Security Infrastructure Maintenance	EDR management, logging configuration, tool standardization	Maintain consistency and resilience in endpoint protection
Digital Forensics & Analysis	Evidence acquisition, memory and disk analysis	Determine root cause, persistence, and attacker footprint.
Awareness & Training	Security drills, phishing and credential hygiene training	Build user and admin readiness to prevent credential misuse.

Recommended CSIRT Team Type(s)

- **Analysis Team:** Specializes in malware analysis, log correlation, and forensic review of Windows/Linux incidents.
- **Assistance Team:** Supports containment, eradication, and restoration of affected systems.
- **Coordination Team:** Ensures communication between IT, management, and external partners during incidents.

Justification

- The **Analysis Team** enhances cross-platform visibility through forensics and IOC tracking.

- The **Assistance Team** ensures operational resilience and rapid containment.
- The **Coordination Team** provides governance, escalation, and lessons-learned integration, fulfilling the **FIRST Services Framework** objective of continuous improvement and readiness.

This structure allows Naipay to **detect, analyze, and mitigate hybrid attacks** like this Windows-Linux compromise efficiently.