CYBERBULWORK

SOC REPORT

2025

Table of Contents

List of Tables

List of Figues

Executive Summary

This report provides a comprehensive overview of the recent cybersecurity landscape and incident response activities at CyberBulwork. Over the reporting period, the Security Operations Center (SOC) investigated and responded to a variety of threats, including sophisticated phishing campaigns, malware infections, unauthorized access attempts, and vulnerabilities in both endpoint and mobile device environments.

The SOC's investigations revealed that phishing remains a significant threat, with attackers employing social engineering tactics and impersonation to bypass technical controls and target employees. Multiple incidents involved malicious links and attachments, some of which were designed to deliver credential-stealing malware or remote access Trojans. The team's structured approach to email threat analysis, including sender verification, domain reputation checks, and header analysis, enabled the rapid identification and containment of these threats.

In addition to email-based attacks, the SOC responded to suspicious sign-in activity, identifying brute-force attempts and unauthorized access from foreign IP addresses. Swift action, including session revocation, credential resets, and the implementation of conditional access policies, helped to mitigate potential damage and prevent recurrence.

The report also details the analysis of malware samples, including PE32 droppers and AsyncRAT payloads, which demonstrated advanced persistence and data exfiltration techniques. The SOC's use of sandbox analysis, endpoint detection, and network monitoring was instrumental in uncovering the full scope of these threats and informing effective remediation strategies.

Vulnerability management was another key focus, particularly in response to the July 2023 Microsoft Patch Tuesday, which addressed over 130 vulnerabilities, including several actively exploited remote code execution flaws. The SOC implemented a phased patch management plan, comprehensive communication strategies, and real-time monitoring to ensure timely remediation and minimize business disruption.

Mobile device security was assessed, revealing that a significant portion of the organization's Android fleet was outdated and lacked Mobile Device Management (MDM) controls. The report outlines a clear roadmap for device updates, MDM implementation, and ongoing user education to address these risks.

Finally, the SOC enhanced its detection and response capabilities by deploying custom analytics rules and watchlists in Microsoft Sentinel, ensuring real-time identification of malicious

Incident Overview

During the reporting period, CyberBulwork's Security Operations Center (SOC) responded to a diverse set of cybersecurity incidents, including sophisticated phishing campaigns, malware infections, unauthorized access attempts, and critical vulnerabilities in both endpoint and mobile device environments. The following overview provides a comprehensive breakdown of these incidents, the tactics used by adversaries, and the investigative steps taken by the SOC.

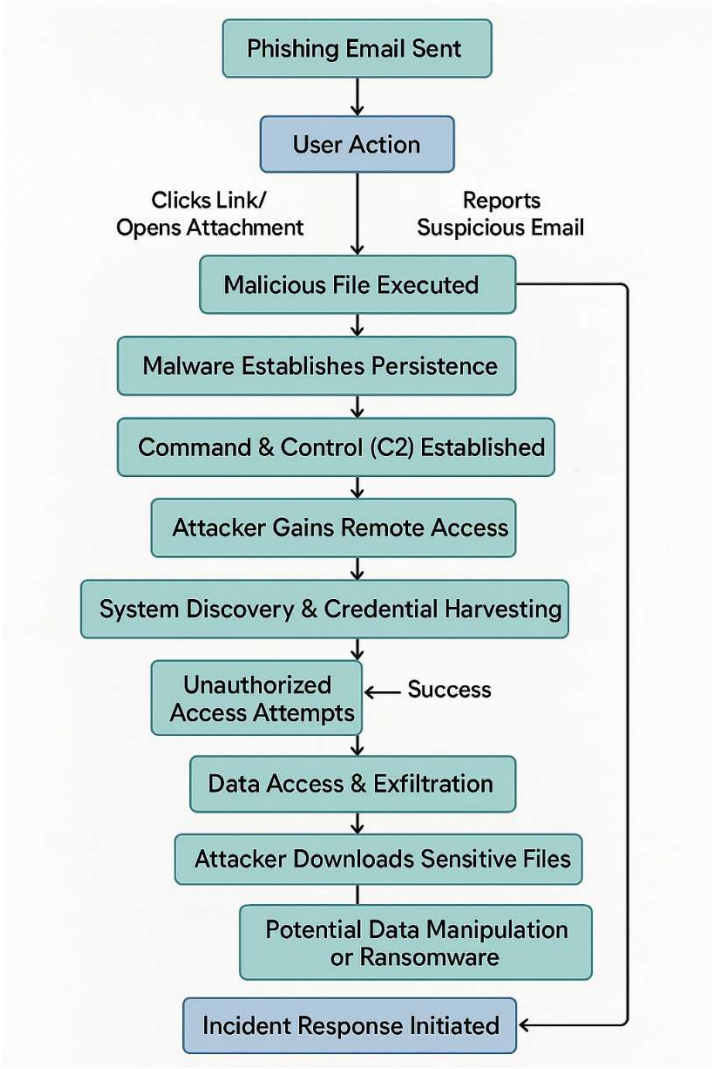


Figure 1: Incident Diagram

Phishing Campaigns and Email Threats

Nature of Attacks

Phishing remains a persistent and evolving threat. Attackers leveraged social engineering, impersonation, and well-crafted emails to bypass technical controls and target employees. The campaigns aimed to:

- Steal credentials via fake login pages or malicious links.
- Deliver malware through attachments or drive-by downloads.
- Manipulate users into executing harmful actions under the guise of legitimate business communications.

Notable Phishing Incidents

- Team-Building Scam:
  An email, seemingly from an internal address, invited staff to a "fun team-building activity" with a link to http://theannoyingsite.com. Analysis revealed suspicious JavaScript and browser manipulation, confirming it as a phishing attempt. Prompt user reporting prevented further compromise.
- Fake Adobe Update:
  An email impersonating Adobe support directed users to a masked link (https://updatedcadobe.blogspot.com/atom.xml). The sender's domain and IP were inconsistent with legitimate Adobe communications, and the domain had a history of phishing and malware distribution.
- Affiliate Marketing Graymail:
  An email from a personal Gmail account with an affiliate link was flagged. VirusTotal found no immediate threats, but the source and URL were logged for monitoring.
- Malicious Project Files:
  An email encouraged users to download "updated project files" from Google Drive. Security vendors flagged the file as malware, and the link was quarantined.
- Impersonated Code Review Request:
  An email from a non-corporate Gmail address requested a code review and linked to a suspicious pastebin-like site (https://wtools.io/paste-code/bOs4). VirusTotal flagged the URL as malicious.

Investigation and Response

The SOC followed a structured approach**:**

- Sender and Domain Verification: Checked for mismatches and reputation.
- Header Analysis: Inspected for spoofing and redirection.
- Content Review: Assessed for urgency, vague greetings, and suspicious links.

- User Reporting: Encouraged and acted on staff reports.
- Isolation: Blocked malicious senders and quarantined affected systems.

Key Takeaway

User vigilance and rapid escalation were critical in neutralizing these threats. Ongoing user education and technical controls (e.g., email filtering, sandboxing) proved effective.

Unauthorized Access and Account Compromise

Incident Summary

A notable incident involved suspicious sign-in activity for a UK-based user, Erwin Smith. The SOC detected multiple unauthorized login attempts from foreign IP addresses (China, Thailand, Bulgaria), indicating brute-force and credential-stuffing attacks.

Attack Pattern

- Multiple failed login attempts across Microsoft services (Exchange, Azure CLI, SharePoint).
- Successful access after several failures, followed by suspicious file downloads (e.g., updated_payroll.xlsx, vulnerability_report.xlsx).
- Use of different services to test credentials and evade detection.

Investigation Steps

- Log Analysis: Correlated sign-in and activity logs with IP geolocation.
- Behavioral Analysis: Flagged logins outside the user's normal pattern.
- Threat Intelligence: Identified IPs with poor reputations and prior abuse reports.

Response

- Immediate session revocation and credential reset.
- Notification of stakeholders and activation of crisis communication.
- Enhanced monitoring and conditional access policies.

Impact

The attacker's intent appeared to include financial manipulation and reconnaissance for further exploitation. Swift action prevented escalation.

Malware Infections and Advanced Threats

PE32 Dropper and AsyncRAT

- Initial Infection:
  A VIP user received a phishing email with a Catalogue.rar attachment containing a malicious diskpart.exe (SHA-256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa). The file was disguised as a legitimate Windows utility.
- Malware Behavior:
  - Created scheduled tasks for persistence ("Windows Update BETA").
  - Dropped files in system directories (e.g., MuiUnattend.exe).
  - Abused legitimate processes (schtasks.exe, werfault.exe, rundll32.exe) for stealth.
  - Connected to legitimate Microsoft services, likely as a precursor to C2 communication.
- AsyncRAT Payload:
  - Delivered via a ZIP archive, extracted and executed by WinRAR.
  - Established C2 communication with donzola.duckdns.org (IP: 192.169.69.26).
  - Exfiltrated system information and keystrokes.
  - Maintained persistence via registry modifications and encrypted config files.

Investigation and Containment

- Sandbox Analysis: Used ANY.RUN and VirusTotal to observe behavior.
- Network Monitoring: Tracked outbound connections and DNS queries.
- Forensic Review: Analyzed dropped files, registry changes, and memory dumps.
- Containment: Isolated affected hosts, removed malware, and blocked malicious domains.

Lessons

The use of legitimate processes and dynamic DNS for C2 highlights the sophistication of modern malware. Layered endpoint protection and rapid incident response were essential.

Vulnerability Management

Microsoft July 2023 Patch Tuesday

- Scope: 132 vulnerabilities, including 37 RCEs and 6 actively exploited flaws.
- Risks: Potential for system downtime, data breaches, and financial loss.
- Critical CVEs: Included Office and Windows HTML RCE, Outlook spoofing, SmartScreen bypass, and privilege escalation.

Response Strategy

- Asset Inventory: Identified and prioritized vulnerable systems.
- Testing: Deployed patches in a controlled environment before production rollout.
- Deployment: Used SCCM, WSUS, and Intune for phased rollout.
- Monitoring: Validated patch success and monitored for issues.
- Communication: Notified stakeholders and provided post-deployment updates.

Long-term Improvements

- Formalized vulnerability management program.
- Risk-based asset classification and patch prioritization.
- Automation of patch deployment and compliance reporting**.**

Mobile Device Security

Assessment

- 250 Android devices (50% of fleet) were outdated and lacked MDM controls.
- High-risk vulnerabilities (e.g., CVE-2023-26083, CVE-2021-29256) exposed devices to remote code execution and privilege escalation.

Immediate Actions

- Conducted device inventory and prioritized updates.
- Communicated urgency to users and provided support for updates.
- Isolated non-compliant devices where possible.

Long-term Strategy

- Recommended Microsoft Intune or ManageEngine MDM for centralized control.
- Established update policies, device lifecycle management, and user education.
- Planned for regular compliance reviews and policy refinement.

Enhanced Detection and Response

- Custom Analytics in Microsoft Sentinel:
  Deployed custom rules and watchlists for real-time detection of malicious domains, IPs, and file hashes.
- Alignment with MITRE ATT&CK:
  Ensured comprehensive coverage of tactics and techniques.
- Continuous Improvement:
  Regularly updated detection rules and watchlists based on threat intelligence and incident outcomes.

The incidents during this period demonstrate the evolving tactics of threat actors and the importance of a multi-layered defense. CyberBulwork's SOC effectively combined technical controls, user education, and structured response processes to detect, contain, and remediate threats. Ongoing investment in advanced detection, vulnerability management, and mobile security will further strengthen the organization's resilience.

Incident Timeline (MITRE ATT&CK Mapping)

The following timeline provides a detailed, step-by-step mapping of the major incidents at CyberBulwork to the MITRE ATT&CK framework. Each phase of the attack lifecycle is illustrated with specific tactics, techniques, and real-world evidence from the investigation, showing how adversaries progressed from initial access to exfiltration and how the SOC responded at each stage.

Date/Phase	MITRE ATT&CK Tactic	Technique/Sub-technique (ID)	Description & Evidence

Mar 11, 2024	Initial Access	Phishing: Spearphishing Link (T1566.002) Phishing: Spearphishing Attachment (T1566.001)	Attackers sent emails with malicious links (e.g., http://theannoyingsite.com) and attachments (Catalogue.rar containing diskpart.exe) to employees, aiming to trick users into clicking or opening files1[2][7].
Mar 11, 2024	Execution	User Execution (T1204)	A VIP user opened the malicious attachment, executing diskpart.exe disguised as a legitimate utility1.
Mar 11, 2024	Persistence	Scheduled Task/Job (T1053)	Malware created a scheduled task ("Windows Update BETA") using schtasks.exe to ensure persistence on reboot1[3][4].
Mar 11, 2024	Defense Evasion	Masquerading (T1036) Impair Defenses (T1562)	The malware used legitimate process names and abused Windows utilities (e.g., werfault.exe, rundll32.exe) to evade detection and blend in with normal system activity1[4].
Mar 11, 2024	Command and Control	Application Layer Protocol (T1071)	The AsyncRAT payload established C2 communication with donzola.duckdns.org over dynamic DNS, using encrypted channels to exfiltrate data and receive commands1[4].
Mar 11, 2024	Discovery	System Information Discovery (T1082)	The malware enumerated system and user information, preparing for further exploitation and exfiltration1[4].
Mar 11, 2024	Collection	Data from Local System (T1005)	The attacker searched for and collected files of interest, such as payroll and vulnerability reports, from the local system1[6].
Mar 11, 2024	Exfiltration	Exfiltration Over C2 Channel (T1041)	Sensitive files were exfiltrated to the attacker's infrastructure via the established C2 channel1[4].
Apr 9, 2025	Credential Access	Brute Force (T1110)	Multiple failed and then successful login attempts from foreign IPs (China, Thailand, Bulgaria) indicated brute-

			force and credential-stuffing attacks against Microsoft services15.
Apr 9, 2025	Lateral Movement	Valid Accounts (T1078)	After successful credential compromise, the attacker accessed additional services (SharePoint, Exchange) using the victim's credentials1.
Apr 9, 2025	Collection	Data from Information Repositories (T1213)	The attacker downloaded sensitive files (updated_payroll.xlsx, vulnerability_report.xlsx) from SharePoint and other repositories1.
Apr 9, 2025	Exfiltration	Exfiltration Over Web Service (T1567)	Downloaded files were exfiltrated through standard web protocols, blending with normal user activity1.
Ongoing	Impact	Data Manipulation (T1565)	The attacker attempted to modify payroll data, indicating a goal of financial manipulation1.
Ongoing	Defense Evasion	Indicator Removal on Host (T1070)	The malware and attacker actions included attempts to clear logs and remove traces of activity1.

Table 1: Incident Timeline

Timeline Narrative

1. **Initial Access (T1566.001/.002):**
   Attackers launched a coordinated phishing campaign, sending emails with both malicious links and attachments. These emails were designed to appear legitimate, leveraging social engineering to bypass user suspicion. Some emails impersonated internal staff or trusted brands, while others used urgency or business context to prompt action.
2. **Execution (T1204):**
   A targeted user executed the attached file, which was a PE32 dropper disguised as a Windows utility. This action initiated the infection chain, allowing the malware to run on the endpoint.
3. **Persistence (T1053):**
   To maintain access, the malware created scheduled tasks using schtasks.exe, a common persistence technique observed in both commodity and advanced threats. This ensured the malware would survive reboots and maintain a foothold in the environment.

4. **Defense Evasion (T1036, T1562):**
   The malware used legitimate process names and abused trusted Windows utilities to avoid detection by endpoint security tools. It also attempted to disable or bypass certain security controls.
5. **Command and Control (T1071):**
   AsyncRAT established encrypted communications with a remote C2 server using dynamic DNS, allowing the attacker to issue commands, exfiltrate data, and maintain control over the compromised system.
6. **Discovery & Collection (T1082, T1005, T1213):**
   The attacker and malware enumerated system information and searched for files of interest, including sensitive business documents and vulnerability reports, both on local systems and in cloud repositories.
7. **Credential Access (T1110):**
   Brute-force and credential-stuffing attacks were detected against Microsoft services, with multiple failed and then successful logins from suspicious foreign IPs. This allowed the attacker to escalate access and move laterally within the environment.
8. **Lateral Movement (T1078):**
   With valid credentials, the attacker accessed additional services, including SharePoint and Exchange, to further their objectives.
9. **Exfiltration (T1041, T1567):**
   Sensitive files were exfiltrated over the established C2 channel and via standard web protocols, making detection more challenging.
10. **Impact (T1565):**
    The attacker attempted to manipulate payroll data, indicating a financial motivation and the potential for business disruption.
11. **Defense Evasion (T1070):**
    Efforts were made to remove evidence of compromise, including log clearing and deletion of dropped files, to hinder investigation and response.

Visual Summary

MITRE Tactic	Key Techniques Used	Real-World Example from Incident
Initial Access	T1566.001, T1566.002	Phishing emails with links/attachments
Execution	T1204	User opens malicious attachment

Persistence	T1053	Scheduled task "Windows Update BETA"
Defense Evasion	T1036, T1562, T1070	Masquerading, log clearing, process abuse
Command and Control	T1071	AsyncRAT C2 via dynamic DNS
Discovery	T1082	System and user info enumeration
Collection	T1005, T1213	Payroll and vulnerability report files
Credential Access	T1110	Brute-force login attempts
Lateral Movement	T1078	Use of compromised accounts
Exfiltration	T1041, T1567	File downloads and C2 exfiltration
Impact	T1565	Payroll data manipulation

Table 2: MITRE ATT&CK Summary

This detailed mapping demonstrates how CyberBulwork's SOC tracked and responded to each stage of the attack lifecycle, using the MITRE ATT&CK framework to guide detection, investigation, and remediation efforts.

Response Actions

1. Detection and Initial Assessment

- **User Reporting:**
  Employees were encouraged and trained to report suspicious emails and activities. Multiple phishing attempts were flagged by vigilant staff, triggering rapid investigation.
- **Automated Alerts:**
  Security tools (CrowdStrike, Microsoft Sentinel, EDR) generated alerts for suspicious files, sign-in anomalies, and malware behaviors.
- **Triage:**
  The SOC classified incidents based on severity, potential impact, and affected assets, prioritizing VIP users and critical systems.

2. Investigation and Analysis

- **Email Threat Analysis:**

- Verified sender addresses, checked for domain mismatches, and analyzed email headers for spoofing.
- Used tools like VirusTotal, AbuseIPDB, and WHOIS to assess domain/IP reputation.
- Inspected email content for urgency, vague greetings, and suspicious links or attachments.
- Cross-checked reported IoCs against internal watchlists and threat intelligence feeds.

- **Malware Analysis:**
  - Detonated suspicious files in ANY.RUN and internal sandboxes to observe behavior.
  - Analyzed process trees, file drops, registry changes, and network connections.
  - Identified persistence mechanisms (e.g., scheduled tasks, registry modifications).
- **Unauthorized Access Investigation:**
  - Reviewed sign-in and activity logs for anomalous patterns (e.g., foreign IPs, brute-force attempts).
  - Correlated login events with user location and typical behavior.
  - Flagged and investigated downloads of sensitive files (e.g., payroll, vulnerability reports).
- **Vulnerability Assessment:**
  - Mapped assets against known CVEs from Microsoft Patch Tuesday and Android advisories.
  - Assessed exposure and prioritized systems for urgent remediation.

3. Containment

- **Email Threats:**
  - Quarantined malicious emails and attachments.
  - Blocked sender domains and URLs at the email gateway and firewall.
- **Malware Incidents:**
  - Isolated infected endpoints from the network to prevent lateral movement.
  - Disabled compromised user accounts and revoked active sessions.

- Blocked C2 domains and IPs (e.g., donzola.duckdns.org, duchessgarden.sn).

- **Unauthorized Access:**
  - Suspended affected accounts and reset credentials.
  - Implemented conditional access policies to restrict logins by geography and device.
- **Vulnerable Systems:**
  - Segmented unpatched or high-risk systems into isolated VLANs.
  - Limited external exposure and applied access control lists (ACLs).

4. Eradication

- **Malware Removal:**
  - Deleted all identified malicious files (e.g., diskpart.exe, MuiUnattend.exe, cred.dat).
  - Removed persistence mechanisms (scheduled tasks, registry keys).
  - Performed full-system and memory scans with updated AV/EDR signatures.
- **Credential Hygiene:**
  - Forced password resets for affected and at-risk users.
  - Reviewed and removed unauthorized access tokens and sessions.
- **Vulnerability Remediation:**
  - Deployed emergency patches to address actively exploited vulnerabilities.
  - Disabled or removed vulnerable services and software where immediate patching was not possible.

5. Recovery

- **System Restoration:**
  - Restored affected endpoints and servers from clean, verified backups.
  - Re-imaged systems where compromise could not be fully ruled out.
- **Service Validation:**

- Verified system and application integrity post-restoration.
- Conducted user acceptance testing to ensure business continuity.

- **Re-enablement:**
  - Gradually reconnected remediated systems to the network after thorough validation.
  - Monitored for signs of reinfection or residual attacker presence.

6. Communication

- **Internal Notification:**
  - Promptly informed IT, management, HR, and legal teams of incidents and response actions.
  - Activated the crisis communication plan for high-severity incidents.
- **User Updates:**
  - Provided clear instructions to affected users (e.g., password resets, device updates).
  - Thanked and reinforced the importance of user vigilance in reporting threats.
- **Stakeholder Briefings:**
  - Delivered regular updates to executives and department heads.
  - Documented incident details, impact, and remediation steps for compliance and audit purposes.

7. Post-Incident Review and Continuous Improvement

- **Lessons Learned:**
  - Conducted structured post-incident reviews with all stakeholders.
  - Identified gaps in detection, response, and user awareness.
  - Updated incident response playbooks and technical controls based on findings.
- **Awareness and Training:**
  - Delivered targeted security awareness sessions, especially for VIP users and high-risk departments.

    - Launched phishing simulation exercises to reinforce best practices.

- **Detection Enhancement:**
    - Refined custom analytics rules and watchlists in Microsoft Sentinel.
    - Integrated new IoCs and behavioral patterns into SIEM and EDR platforms.
- **Policy and Process Updates:**
    - Strengthened email attachment and link filtering policies.
    - Enhanced credential management and multi-factor authentication requirements.
    - Formalized patch management and mobile device security policies.

8. Specialized Response: Mobile Device Security

- **Short-Term Actions:**
    - Conducted a full inventory of Android devices, prioritized updates for those most at risk.
    - Communicated urgency to users and provided hands-on support for updates.
    - Isolated or replaced devices that could not be updated.
- **Long-Term Strategy:**
    - Selected and piloted an MDM solution (Microsoft Intune/ManageEngine).
    - Developed and enforced a comprehensive mobile device update and compliance policy.
    - Scheduled regular security reviews and user education for mobile device management.

9. Collaboration and Threat Intelligence Sharing

- **Internal Collaboration:**
    - Maintained open channels between SOC, IT, legal, and executive teams.
- **External Sharing:**
    - Shared IoCs and attack patterns with industry partners and threat intelligence platforms to bolster sector-wide defenses.

CyberBulwork's response actions were comprehensive, rapid, and multi-layered, leveraging both technical controls and human vigilance. The SOC's structured approach spanning detection, containment,

eradication, recovery, and continuous improvement minimized business impact, strengthened defences, and reinforced a culture of security awareness across the organization.

Indicators of Compromise (IoCs)

The Indicators of Compromise (IoCs) identified during CyberBulwork's recent incident investigations span email threats, malware infections, unauthorized access, and vulnerability exploitation. These IoCs are critical for threat detection, hunting, and response, and have been integrated into our SIEM and endpoint protection platforms for real-time monitoring and automated alerting.

Email Threats and Phishing Campaigns

Malicious Domains and URLs

- http://theannoyingsite.com
  Used in a phishing email disguised as a team-building activity; analysis revealed suspicious JavaScript and browser manipulation.
- https://updatedcadobe.blogspot.com/atom.xml
  Masqueraded as an Adobe update; flagged in threat reports for previous malware distribution.
- https://wtools.io/paste-code/bOs4
  Linked in a code review phishing email; flagged by 9 security vendors as malicious
- Google Drive-hosted binary (URL withheld for safety)
  Linked in a phishing email; flagged as malware by multiple vendor.

Suspicious Sender Addresses

- c6d90d5d-df87-11ee-a2fc-525400450766@azxmarket.com
  Used in a phishing campaign targeting VIP users with malicious attachments.
- jasonconrad099@gmail.com
  Source of affiliate graymail; monitored for patterns but not immediately malicious.

Malicious IPs Associated with Email Threats

- 209.85.215.170
  Originated phishing emails; poor reputation and history of abuse.

Malware Infections

Malicious File Hashes

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
  SHA-256 hash of diskpart.exe, a PE32 dropper disguised as a Windows utility, delivered via phishing email.
- b773ca84...exe
  Primary executable in a malware infection chain; used to spawn child processes and establish persistence.
- 1f3c7379dd29298aa24b3aa3a3113ed3051f4515bc3c016893e285d311a74202.zip
  AsyncRAT payload, enabling remote access and data exfiltration.

Dropped or Associated Malicious Files

- MuiUnattend.exe
  Dropped in %AppData%\Microsoft\Windows\MuiUnattend\ for persistence.
- cred.dat
  Encrypted configuration file dropped by AsyncRAT in %AppData%\WinRAR
- Catalogue.rar
  Archive containing the malicious diskpart.exe

Malicious Domains and C2 Infrastructure

- duchessgarden.sn
  Used to host and distribute malware; part of the phishing and malware delivery infrastructure.
- azxmarket.com
  Sender domain for phishing emails; associated with campaign automation..
- donzola.duckdns.org (IP: 192.169.69.26)
  AsyncRAT command-and-control (C2) server, leveraging dynamic DNS for resilience.
- gracefulinox.com
  Associated with phishing and malware campaigns.

Unauthorized Access and Account Compromise

Malicious IP Addresses

- 150.158.77.170 (China)
  Used in unauthorized sign-in attempts; flagged as malicious and reported for abuse.
- 124.120.140.202 (Thailand)
  Involved in suspicious login activity outside the user's normal location.
- 79.124.60.6 (Bulgaria)
  Used to download sensitive files after successful brute-force login.
- 117.50.0.178
  Source IP for phishing and malware delivery.

Files Accessed or Exfiltrated

- updated_payroll.xlsx
  Downloaded by attacker, likely for financial manipulation..
- vulnerability_report.xlsx
  Accessed to identify exploitable weaknesses in infrastructure.

Persistence and Evasion Techniques
Processes and Registry Artifacts

- Abuse of legitimate Windows processes:
  - schtasks.exe (for scheduled task creation, e.g., "Windows Update BETA")
  - werfault.exe, slui.exe, sppextcomobj.exe, rundll32.exe (for stealthy execution and privilege escalation)
- Registry modifications:
  - HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory (used by AsyncRAT to track extracted files)

Vulnerability Exploitation (Patch Tuesday and Mobile Devices)
High-Risk CVEs (Microsoft Patch Tuesday, July 2023)

- CVE-2023-36884 (Office/Windows HTML RCE)
- CVE-2023-35311 (Outlook Spoofing)
- CVE-2023-32049 (SmartScreen Bypass)

- CVE-2023-36874 (Error Reporting Privilege Escalation)
- CVE-2023-32046 (MSHTML Platform RCE)
- CVE-2023-35332 (Routing and Remote Access RCE)

Android Device Vulnerabilities

- CVE-2023-26083 (Android System RCE)
- CVE-2021-29256 (Qualcomm RCE)
- CVE-2023-2136 (Android Framework Privilege Escalation)

Integration into Detection and Response

1. SIEM Watchlists: All identified IoCs (domains, IPs, file hashes, URLs) have been added to Microsoft Sentinel watchlists and custom analytics rules for real-time detection and automated response.
2. Threat Intelligence Sharing: IoCs are shared with industry partners and threat intelligence platforms to enhance sector-wide defenses.
3. Continuous Updates: Watchlists and detection rules are regularly reviewed and updated based on new intelligence and incident outcomes.

Table 3:Summary Table of Key IoCs

Type	**Value/Description**	**Context/Threat Type**
File Hash	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa	PE32 dropper (diskpart.exe)
File Hash	1f3c7379dd29298aa24b3aa3a3113ed3051f4515bc3c016893e285d311a74202	AsyncRAT payload
Domain	duchessgarden.sn	Malware delivery/phishing
Domain	azxmarket.com	Phishing campaign
Domain	donzola.duckdns.org	AsyncRAT C2

IP Address	150.158.77.170 (China)	Unauthorized access
IP Address	124.120.140.202 (Thailand)	Unauthorized access
IP Address	79.124.60.6 (Bulgaria)	Data exfiltration
File	MuiUnattend.exe, cred.dat, Catalogue.rar	Dropped/persistent malware files
URL	http://theannoyingsite.com, updatedcadobe.blogspot.com/atom.xml, wtools.io/paste-code/bOs4	Phishing/malware delivery
CVE	CVE-2023-36884, CVE-2023-35311, CVE-2023-32049, etc.	Vulnerability exploitation

These IoCs form the backbone of CyberBulwork's threat detection and response strategy, enabling rapid identification, containment, and eradication of threats across the organization's digital estate

Further Actions

1. Proactive Threat Hunting and Continuous Monitoring

- **Ongoing Threat Hunting:**
    - Regularly search for new and related IoCs (domains, IPs, file hashes, registry changes) across all endpoints, servers, and cloud services.
    - Use advanced EDR and SIEM tools (e.g., Microsoft Sentinel, CrowdStrike) to automate detection and correlation of suspicious behaviors.
    - Monitor for lateral movement, privilege escalation, and persistence techniques mapped to MITRE ATT&CK.
- **Behavioral Analytics Expansion:**

- Refine and expand custom analytics rules in Microsoft Sentinel to detect advanced threats, including living-off-the-land techniques and unusual user behaviors.
- Integrate machine learning-based anomaly detection for early warning of novel attack patterns.

2. User Awareness and Training

- **Targeted Security Awareness Campaigns:**
  - Launch quarterly phishing simulation exercises, especially for VIPs and high-risk departments.
  - Provide regular, scenario-based training on identifying and reporting phishing, social engineering, and suspicious attachments.
  - Distribute security bulletins highlighting recent threats and lessons learned.
- **Feedback and Reporting Mechanisms:**
  - Encourage staff to report suspicious emails and activities via a dedicated channel.
  - Recognize and reward prompt reporting to reinforce a security-first culture.

3. Policy and Process Enhancement

- **Incident Response Playbook Updates:**
  - Review and update incident response procedures based on recent incidents and post-incident reviews.
  - Incorporate lessons learned into playbooks, including escalation paths, communication templates, and technical checklists.
- **Email and Attachment Policy Hardening:**
  - Enforce stricter controls on executable attachments and links, especially for VIP users.
  - Implement advanced email filtering and sandboxing for all inbound messages.
- **Credential and Access Management:**
  - Mandate multi-factor authentication (MFA) for all users, with hardware-based security keys for privileged accounts.

- Regularly review and tighten conditional access policies, especially for remote and high-risk logins.

4. Vulnerability and Patch Management

- **Accelerated Patch Deployment:**
  - Continue phased, risk-based patching for all critical and high-severity vulnerabilities, with special focus on systems exposed to the internet or handling sensitive data.
  - Automate patch compliance reporting and follow up on non-compliant endpoints.
- **Vulnerability Scanning and Asset Inventory:**
  - Increase the frequency of vulnerability scans and asset discovery.
  - Maintain an up-to-date inventory of all hardware, software, and mobile devices.
- **Exception and Risk Management:**
  - Document and track any patch exceptions, with compensating controls and risk acceptance sign-off.

5. Mobile Device Security and MDM Implementation

- **Immediate Device Update Campaign:**
  - Complete the update of all outdated Android devices, prioritizing those with critical vulnerabilities.
  - Provide hands-on support and troubleshooting for users facing update issues.
- **MDM Solution Rollout:**
  - Select and deploy a Mobile Device Management (MDM) solution (e.g., Microsoft Intune or ManageEngine).
  - Enforce device compliance policies, including mandatory updates, encryption, and remote wipe capabilities.
  - Pilot the MDM rollout with a subset of devices, then expand organization-wide.
- **BYOD Policy Review:**

- Update Bring Your Own Device (BYOD) policies to require enrollment in MDM and compliance with security standards.

6. Detection and Response Technology Enhancement

- **Watchlist and Rule Maintenance:**
  - Regularly update SIEM watchlists with new IoCs from threat intelligence and incident investigations.
  - Tune custom analytics rules for improved accuracy and reduced false positives.
- **Integration with Threat Intelligence:**
  - Share IoCs and attack patterns with industry partners and threat intelligence platforms.
  - Subscribe to sector-specific threat feeds for early warning of emerging threats.

7. Collaboration, Communication, and Compliance

- **Cross-Functional Collaboration:**
  - Maintain regular communication between SOC, IT, legal, HR, and executive teams for coordinated response and decision-making.
  - Conduct joint tabletop exercises to test incident response readiness.
- **Stakeholder and Regulatory Reporting:**
  - Ensure timely notification to management, compliance, and—if required—regulatory authorities in the event of significant incidents.
  - Document all actions, findings, and communications for audit and compliance purposes.

8. Post-Incident Review and Continuous Improvement

- **Structured Post-Incident Reviews:**
  - Hold debrief sessions after each major incident to identify what worked, what didn't, and where improvements are needed.
  - Track and implement agreed-upon action items, assigning clear ownership and deadlines.
- **Metrics and KPIs:**

- Monitor key performance indicators such as incident response times, patch compliance rates, and user reporting rates.
- Use these metrics to drive continuous improvement in security posture.

9. Strategic Initiatives

- **Zero Trust Security Model:**
  - Progressively implement Zero Trust principles, including continuous verification, least privilege, and micro-segmentation.
  - Enforce conditional access and device health checks for all remote and privileged access.
- **Automation and Orchestration:**
  - Expand the use of security automation for alert triage, incident response, and compliance reporting.
  - Integrate SOAR (Security Orchestration, Automation, and Response) tools where feasible.

These further actions will ensure CyberBulwork not only addresses the immediate aftermath of recent incidents but also builds a more resilient, proactive, and adaptive security posture. By combining technical controls, user engagement, process improvement, and strategic investment, the organization will be better equipped to defend against both current and emerging cyber threats.

Lesson Learned

1. **User Vigilance and Security Awareness Are Critical**
   - **Prompt User Reporting Prevents Escalation:**
     Multiple incidents were detected early because staff members reported suspicious emails and activities. For example, the “team-building activity” phishing email was escalated before any user clicked the malicious link, preventing a potential breach.
   - **Ongoing Training Is Essential:**
     Regular security awareness training and phishing simulations have proven effective. Users who received training were more likely to recognize and report phishing attempts, reducing the risk of credential theft and malware execution.

- **Feedback Loops Reinforce Good Behavior:**
  Acknowledging and rewarding staff for reporting threats encourages a culture of vigilance and shared responsibility.

2. **Structured, Multi-Layered Investigation Processes Work**

   - **Comprehensive Email Analysis:**
     The SOC's structured approach verifying sender authenticity, analyzing headers, checking domain/IP reputation, and cross-referencing IoCs enabled rapid identification and containment of phishing campaigns.

   - **Collaboration Across Teams:**
     Effective incident response required close coordination between IT, cybersecurity, management, and legal teams. This ensured swift containment, clear communication, and compliance with regulatory requirements.

   - **Playbook-Driven Response:**
     Following established incident response playbooks (aligned with NIST and MITRE ATT&CK) ensured that all critical steps detection, containment, eradication, recovery, and post-incident review were executed consistently.

3. **Technical Controls and Advanced Detection Are Indispensable**

   - **SIEM and EDR Are Game Changers:**
     The deployment of Microsoft Sentinel with custom analytics rules and watchlists, along with endpoint detection and response (EDR) tools, enabled real-time detection of malicious domains, IPs, and file hashes.

   - **Sandboxing and Threat Intelligence:**
     Detonating suspicious files in sandboxes (ANY.RUN) and leveraging threat intelligence feeds provided deep insights into malware behavior and attack infrastructure.

   - **Automation Accelerates Response:**
     Automated alerting, watchlist integration, and custom rules reduced response times and improved detection accuracy.

4. **Phishing and Social Engineering Remain Top Threats**

- **Attackers Are Sophisticated:**
  Phishing emails were highly targeted, using social engineering, impersonation, and urgency tactics to bypass technical controls and exploit human behavior.

5. **Technical Controls Alone Are Not Enough:**
   Even with advanced filtering, some phishing emails reached users. Human vigilance remains a necessary last line of defense.

6. **Credential and Access Management Must Be Strengthened**

   - **Brute-Force and Credential Stuffing Are Ongoing Risks:**
     Unauthorized access attempts from foreign IPs (China, Thailand, Bulgaria) highlighted the need for stronger authentication and monitoring.

   - **MFA and Conditional Access Are Essential:**
     Incidents demonstrated the importance of enforcing multi-factor authentication (MFA) and implementing conditional access policies to prevent unauthorized logins.

7. **Malware Can Evade Basic Defenses**

   - **Living-off-the-Land Techniques:**
     Malware samples abused legitimate Windows processes (e.g., schtasks.exe, werfault.exe, rundll32.exe) for persistence and stealth, making detection more challenging.

   - **Persistence Mechanisms Are Sophisticated:**
     Attackers used scheduled tasks, registry modifications, and encrypted configuration files to maintain access and evade removal.

8. **Vulnerability and Patch Management Are Business-Critical**

   - **Timely Patching Prevents Exploitation:**
     The July 2023 Patch Tuesday exposed over 130 vulnerabilities, including actively exploited RCEs. A phased, risk-based patch management approach minimized business disruption and reduced exposure.

   - **Asset Inventory and Prioritization Are Key:**
     Maintaining an up-to-date inventory of assets and prioritizing patching for critical systems and high-risk vulnerabilities is essential for effective risk management.

- **Testing and Rollback Procedures Reduce Risk:**
  Testing patches in a controlled environment and having rollback plans in place prevented system outages and ensured business continuity.

9. **Mobile Device Security Is a Growing Challenge**

- **Outdated Devices Are High-Risk:**
  50% of Android devices were outdated and lacked MDM controls, exposing the organization to critical vulnerabilities (e.g., CVE-2023-26083, CVE-2021-29256).

- **MDM Is No Longer Optional:**
  Implementing a Mobile Device Management (MDM) solution is necessary to enforce updates, monitor compliance, and enable remote wipe capabilities.

- **User Education for Mobile Security:**
  Users need clear guidance and support for updating devices and understanding mobile threats.

10. **Communication and Documentation Enhance Resilience**

- **Clear Stakeholder Communication:**
  Timely, transparent updates to management, IT, HR, and legal teams ensured coordinated response and minimized confusion.

- **Comprehensive Documentation:**
  Detailed incident records, including IoCs, response actions, and lessons learned, support compliance, audit readiness, and continuous improvement.

11. **Continuous Improvement Is Essential**

- **Post-Incident Reviews Drive Progress:**
  Structured debriefs after each incident identified gaps and informed updates to playbooks, policies, and technical controls.

- **Metrics and KPIs Guide Investment:**
  Tracking incident response times, patch compliance, and user reporting rates helps prioritize resources and measure progress.

- **Threat Landscape Is Evolving:**
  Regular review and adaptation of security strategies, controls, and training are necessary to stay ahead of emerging threats.

CyberBulwork's recent incidents have reinforced the importance of a holistic, layered security approach combining user education, technical controls, structured processes, and continuous improvement. By acting on these lessons, the organization will further strengthen its resilience against both current and emerging cyber threats.

Vulnerability Management

Vulnerability management at CyberBulwork is a structured, risk-driven process that ensures timely identification, assessment, remediation, and monitoring of security weaknesses across all IT assets, including endpoints, servers, applications, and mobile devices. The approach is both tactical (addressing immediate threats) and strategic (building long-term resilience), as demonstrated during the July 2023 Microsoft Patch Tuesday and the Android device security review.

1. **Risk Assessment and Asset Inventory**

   - **Asset Inventory:**
     All systems running Microsoft software and Android devices were catalogued using the CMDB and asset management platforms. Assets were classified by business criticality, data sensitivity, exposure to external threats, and regulatory requirements.

   - **Vulnerability Exposure Mapping:**
     Each asset was cross-referenced with the latest CVEs, especially those from Microsoft's July 2023 Patch Tuesday (132 vulnerabilities, 37 RCEs, 6 actively exploited), and Android advisories (e.g., CVE-2023-26083, CVE-2021-29256).

2. **Prioritization and Change Management**

   - **Risk-Based Prioritization:**
     Systems were prioritized for patching based on their criticality, exposure, and the severity of vulnerabilities. Special attention was given to internet-facing, high-privilege, and legacy systems.

   - **Change Management:**
     All patch deployments were subject to change advisory board (CAB) review, with documented impact assessments, rollback strategies, and communication plans to minimize business disruption.

3. **Testing and Staging**

   - **Patch Testing:**
     Patches were first deployed in a virtualized test environment simulating production, including various OS versions and business-critical applications. Checksums were used to verify patch integrity, and pre-deployment snapshots ensured rollback capability in case of failure.

   - **Compatibility and Stability Checks:**
     Testing focused on system stability, application compatibility, and endpoint behavior post-patching.

4. **Deployment and Remediation**

   - **Phased Rollout:**
     Deployment tools such as Microsoft Endpoint Configuration Manager (SCCM), Windows Server Update Services (WSUS), and Intune (for cloud endpoints) were used for a staggered rollout, scheduled during maintenance windows to reduce operational impact.

   - **Automated Compliance Reporting:**
     Patch compliance was tracked using SCCM reports and PowerShell scripts, ensuring all critical systems were updated and identifying any failures for immediate remediation.

5. **Post-Deployment Monitoring and Validation**

   - **Validation:**
     Post-deployment, systems were monitored to confirm successful patch installation, service continuity, and system reboots where necessary. Helpdesk tickets were tracked for any user-reported issues.

   - **Rollback Procedures:**
     The ability to revert patches using VM snapshots or CLI tools was maintained, ensuring rapid recovery from any patch-related failures.

6. **Vulnerability Isolation and Endpoint Hardening**

   - **Network Segmentation:**
     Unpatched or high-risk systems were isolated into dedicated VLANs or firewall zones, with restricted access via ACLs and limited external exposure.

- **Application Control and System Hardening:**
  Application whitelisting, attack surface reduction rules, and the removal of unnecessary services were enforced. Exploit protection features (such as DEP) were enabled, and least privilege principles applied.

7. **Mobile Device Vulnerability Management**

- **Immediate Update Campaign:**
  All Android devices were inventoried and prioritized for updates, with urgent attention to those one year or more out of date. Update clinics and support channels were established to assist users.

- **MDM Implementation:**
  A roadmap was developed for deploying Microsoft Intune or ManageEngine MDM, enforcing update policies, encryption, and remote wipe capabilities. BYOD policies were updated to require MDM enrollment and compliance.

8. **. Long-Term Program Improvements**

- **Formal Vulnerability Management Program:**
  A dedicated team and cross-functional committee were established, with clear roles, responsibilities, and KPIs. Policies were developed for scan frequency, remediation timelines, and exception management.

- **Standardized Patch Cycle:**
  A monthly patching schedule was implemented, aligned with vendor releases, and supported by standardized testing, approval, and emergency patch protocols.

- **Automation and Reporting:**
  Automated patch deployment and compliance reporting were expanded, with scripted techniques for complex systems and regular executive dashboards.

    - **Continuous Review:**
      Asset classifications and vulnerability prioritizations are reviewed quarterly, and the program is refined based on incident outcomes and threat intelligence.

9. **Communication and Stakeholder Engagement**

- **Pre-Deployment Notifications:**
  Stakeholders—including IT, compliance, and business leaders—were notified in advance of major patch cycles, with clear explanations of the risks, timelines, and expected impacts.
- **Technical Briefings:**
  IT and support teams received detailed patch notes, asset targeting lists, and escalation procedures for patch-related issues.
- **Post-Deployment Updates:**
  Confirmation emails and internal announcements summarized completed updates, resolved issues, and next steps, reinforcing transparency and accountability.

10. Metrics, KPIs, and Continuous Improvement

- **Performance Tracking:**
  Key metrics such as patch compliance rates, mean time to remediate (MTTR), and vulnerability recurrence are tracked and reported to leadership.
- **Post-Incident Reviews:**
  Lessons learned from patching incidents and vulnerability exploitation are incorporated into playbooks and future planning, driving continuous improvement.

CyberBulwork's vulnerability management program is risk-driven, highly structured, and continuously evolving. By combining asset inventory, risk-based prioritization, rigorous testing, phased deployment, and robust stakeholder communication, the organization ensures timely remediation of vulnerabilities while minimizing business disruption. The integration of automation, MDM, and continuous improvement practices positions CyberBulwork to proactively defend against both current and emerging threats.

Recommendations

Based on the analysis of recent incidents and the current security landscape at CyberBulwork, the following recommendations are made to further strengthen the organization's cybersecurity posture:

1. **Enhance Email Security Controls**
    - Implement stricter policies for email attachments, especially for executable content and archives.
    - Deploy advanced email filtering and sandboxing for all inbound messages, with heightened scrutiny for VIP users.
    - Regularly update and test phishing simulation exercises tailored to different user groups, including executives.
2. **Expand User Awareness and Training**
    - Continue regular, scenario-based security awareness training for all staff.
    - Recognize and reward prompt reporting of suspicious emails or activities to reinforce a culture of vigilance.
    - Distribute timely security bulletins highlighting new threats and lessons learned from recent incidents.
3. **Strengthen Access and Credential Management**
    - Enforce multi-factor authentication (MFA) for all users, with hardware-based security keys for privileged accounts.
    - Regularly review and update conditional access policies, especially for remote and high-risk logins.
    - Monitor for and respond to brute-force and credential-stuffing attempts using automated alerting.
4. **Advance Vulnerability and Patch Management**
    - Maintain a risk-based, phased patch management process, prioritizing critical and high-risk systems.
    - Automate patch deployment and compliance reporting where possible.

- Conduct regular asset inventories and vulnerability scans, with quarterly reviews of asset classifications and patch priorities.

5. **Implement Comprehensive Mobile Device Management (MDM)**
    - Deploy an MDM solution (such as Microsoft Intune or ManageEngine) to enforce update policies, encryption, and remote wipe capabilities.
    - Update BYOD policies to require MDM enrollment and compliance with security standards.
    - Provide ongoing user education and support for mobile device security.
6. **Enhance Detection and Response Capabilities**
    - Continue refining custom analytics rules and watchlists in Microsoft Sentinel for real-time detection of malicious domains, IPs, and file hashes.
    - Integrate new IoCs and behavioral patterns into SIEM and EDR platforms.
    - Expand the use of automation and orchestration for alert triage and incident response.
7. **Formalize and Test Incident Response Processes**
    - Regularly review and update incident response playbooks based on lessons learned from recent incidents.
    - Conduct cross-functional tabletop exercises to test readiness and improve coordination between IT, security, legal, and executive teams.
    - Document all incidents, actions, and outcomes for compliance and continuous improvement.
8. **Foster a Culture of Continuous Improvement**
    - Track key performance indicators (KPIs) such as incident response times, patch compliance rates, and user reporting rates.
    - Hold structured post-incident reviews to identify gaps and drive updates to policies, controls, and training.
    - Share threat intelligence and IoCs with industry partners to strengthen sector-wide defenses.

Conclusion

The findings of this report underscore the dynamic and evolving nature of the cyber threat landscape facing CyberBulwork. The organization's layered defense strategy combining technical controls, user education, and cross-functional collaborationhas proven effective in detecting and mitigating a wide range of threats.

Key lessons learned include the critical importance of ongoing user awareness training, the need for robust patch and vulnerability management processes, and the value of advanced detection technologies such as SIEM and endpoint protection platforms. The rapid response to phishing, malware, and unauthorized access incidents has minimized potential impacts and reinforced the organization 's resilience.

Looking ahead, CyberBulwork is committed to continuous improvement in its cybersecurity posture. This includes investing in advanced threat detection and response capabilities, expanding the use of automation, and regularly reviewing and updating incident response playbooks. The organization will also prioritize the implementation of comprehensive mobile device management, regular security awareness training, and a risk-based approach to vulnerability management.

By maintaining a proactive and adaptive security strategy, CyberBulwork is well-positioned to defend against current and emerging threats, safeguard its assets and data, and uphold the trust of its stakeholders.

Appendix: Attendance and Contribution

S/N	CLASS NAME	4/6 (Sun)	4/7 (Mon)	4/8 (Tue)	4/9 (Wed)	4/10 (Thu)	4/11 (Fri)	4/12 (Sat)	4/13 (Sun)	4/14 (Mon)	4/15 (Tue)	2/26 (Wed)
1	Ololade Elizabeth Adesagba	P	P	P	P	P	P	P	P	P	P	P
2	Oluwaseyi Adebayo	P	P	P	P	P	P	P	P	P	P	P
3	Muizz Babatunde Majeed	P	P	P	P	P	P	P	P	P	P	P
4	Dike Promise Chimamanda	P	P	P	P	P	P	P	P	P	P	P
5	Shado Peculiar Unini	P	P	P	P	P	P	P	P	P	P	P
6	Etinosa Imafidon	P	P	P	P	P	P	P	P	P	P	P
7	Daniel Owoeye-Wise	P	P	P	P	P	P	P	P	P	P	P
8	Alli-Balogun, Luqman Damilare	P	P	P	P	P	P	P	P	P	P	P
9	Motunrayo Sanusi	P	P	P	P	P	P	P	P	P	P	P

Work breakdown structure

S/N	Task Title	Task
1	Ololade Elizabeth Adesagba	Preparation phase incident play book, Suspicious Sign in mini report, Incidence playbook mini report, Custom alerts mini report, Team building email analysis, SOC report.
2	Oluwaseyi Adebayo	Team building email analysis, Containment phase of the Incidence Playbook.
3	Muizz Babatunde Majeed	Download updated project email analysis, Containment phase of the Incidence Playbook.
4	Dike Promise Chimamanda	SOC presentation slides
5	Shado Peculiar Unini	Remediation Phase of the Incidence Playbook, Important Adobe update email analysis and Meeting Minutes.

6	Etinosa Imafidon	Sprint Lead, Custom Alerts, Email Analysis using splunk, Post-Incidence phase of the Incidence playbook.
7	Daniel Owoeye-Wise	Sprint Lead, Vulnerability Management for the Patch Tuesday and Mobile Device management and the Detection phase of the Incidence play book.
8	Alli-Balogun, Luqman Damilare	Email Analysis Mini report, Remediation phase of the Incidence playbook, Sprint Lead.
9	Motunrayo Sanusi	Code Review email and Detection phase incident play book

Appendix: Mini Reports

Active Email Threats Investigation and Response

During an organisational investigation, five team members flagged a wave of phishing emails. Analysis revealed a coordinated effort by threat actors skilfully crafted to exploit human behaviour and extract sensitive data or trigger harmful actions. Designed emails were intended to manipulate recipients into divulging sensitive information or executing detrimental actions.

The analysis uncovered key tactics behind the phishing campaign, exposing both the attackers' sophistication and gaps in our defences. These insights enabled swift, targeted responses and strengthened our resilience against future threats.

This investigation highlights the vital role of ongoing awareness and user education in cybersecurity. Acting on these insights helps neutralise current threats while boosting our defence against future attacks.

Investigation Steps

Effective email threat investigation demands a structured approach. Here's a breakdown of the key steps:

1. **Initial Assessment**:
    - Check the sender's address for domain mismatches.
    - Check the subject line for urgency tactics.
    - Verify the source for authenticity.
2. **Check for Suspicious Content and review Links and URLs**:
    - Scrutinise the email body for vague greetings or errors.
    - Preview links for mismatched URLs.
    - Treat unexpected attachments as potential threats.
3. **Check for Domain and IP Reputation**:
    - Use tools like WHOIS to verify domain Ownership.
    - Check domain/IP reputation with tools like VirusTotal or AbuseIPDB for signs of malicious activity.
4. **Analyze email Headers**:

- Review email headers for spoofing or redirection clues.
- Verify SPF, DKIM, and DMARC results to confirm sender authenticity.

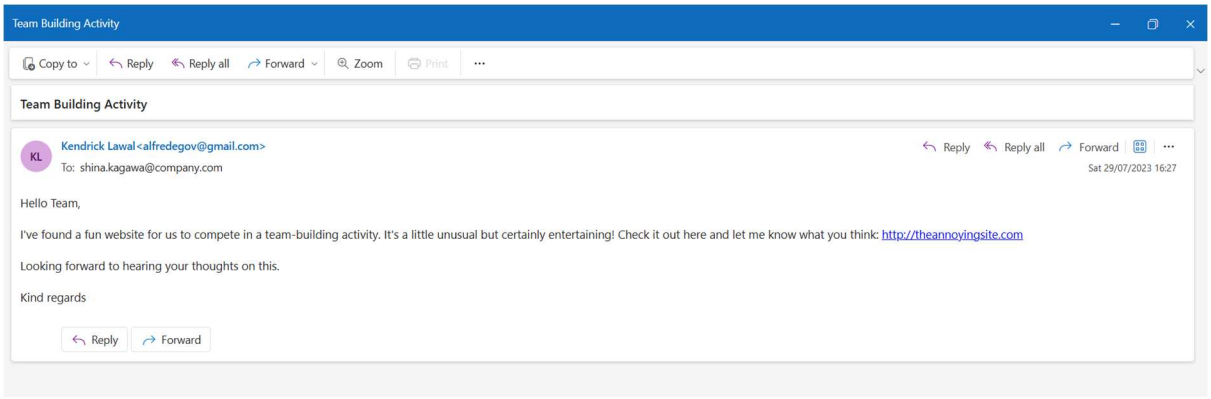
5. **Check for Branding Consistency**:
    - Cross-check branding, logos, and formatting against known legitimate emails to spot inconsistencies.
6. **Contact the Sender Directly**:
    - Verify the email using official contact details, not those provided in the message.
7. **User Reports and Patterns**:
    - Collect staff feedback on received emails and spot trends in subjects or sender addresses for common phishing patterns.
8. **Compare to Known Indicators of Compromise (IoCs)**:
    - Cross-check the sender, subject, URLs, and attachments against known indicators of compromise.
9. **Collaborate with IT/Cybersecurity Teams**:
    - Share findings with IT and cybersecurity teams for further analysis.
10. **Isolate and Respond**:
    - Isolate affected systems to contain the threat.
    - Block malicious senders.
    - Educate staff on recognising and reporting phishing attempts

Evidence and IoCS

Tool Used: AnyRunl, VirusTotal, AbuseIPDB.

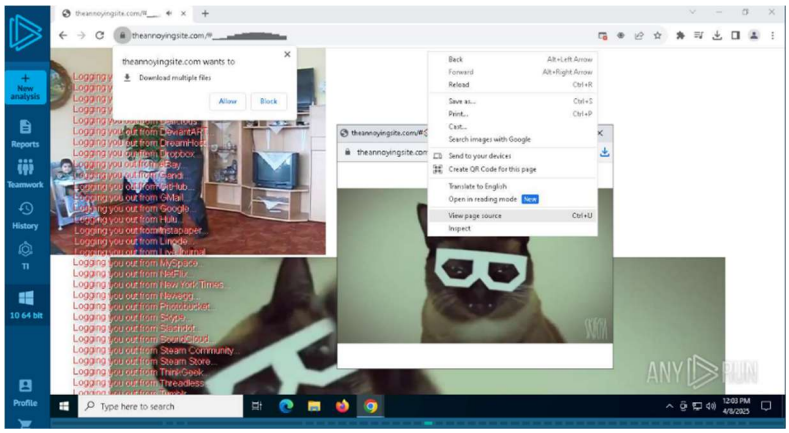
Team Building Activity

Below is the reported email.

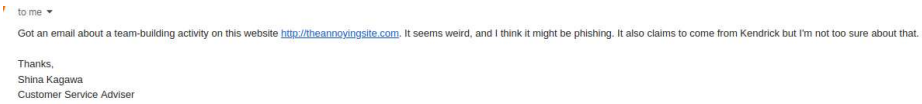


User Shina reported a suspicious email, seemingly from an internal address, promoting a 'fun team-building activity' with a link to http://theannoyingsite.com.

The email, posing as a casual team-building game, used social engineering to lower suspicion. The URL analyzed in Anyrun showed suspicious JavaScript, popups, potential browser manipulation, and no clear legitimate function.



Shina wisely avoided clicking the link and escalated the issue promptly.



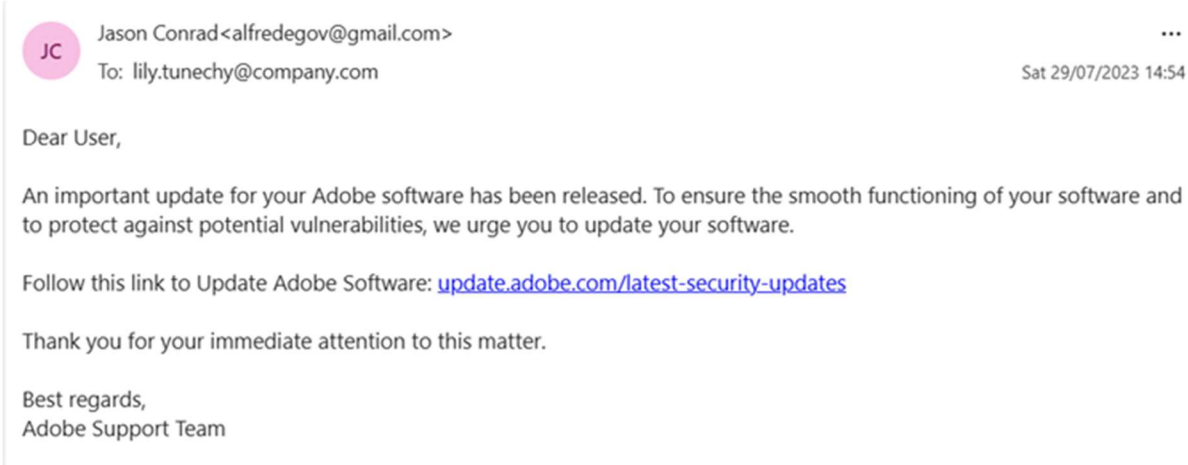
In conclusion, the email is malicious, with the domain hosting suspicious content, likely part of a broader phishing or exploit campaign.

Indicators of Compromise (IOCs)

Type	Value	Notes
Domain	theannoyingsite.com	Host of malicious content (JavaScript abuse, no HTTPS)
URL	http://theannoyingsite.com	Shared in phishing message
Email Subject / Body	Casual internal-style message promoting "fun website"	Likely crafted to bypass suspicion and filters

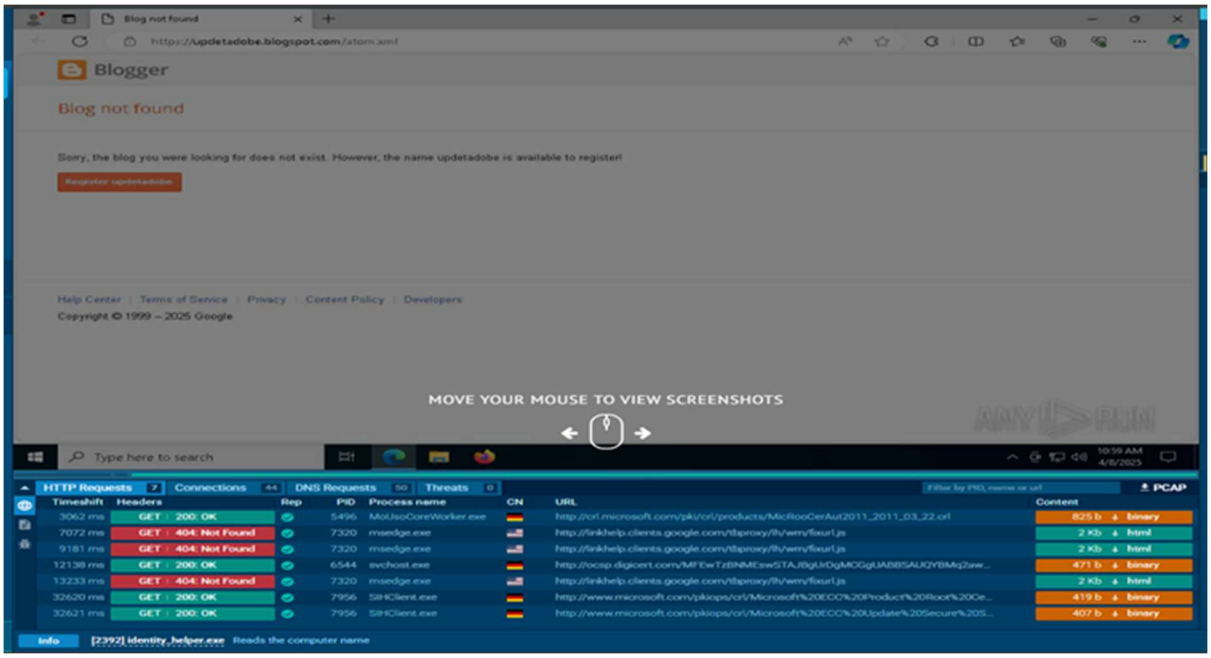
Important Adobe Update

Below is the reported email.



The URL 'update.adobe.com/latest-security-updates' is masked by a malicious custom domain. Hovering over the link reveals it leads to a blog, which is suspicious since official Adobe updates would direct to a legitimate download repository, not a blog.

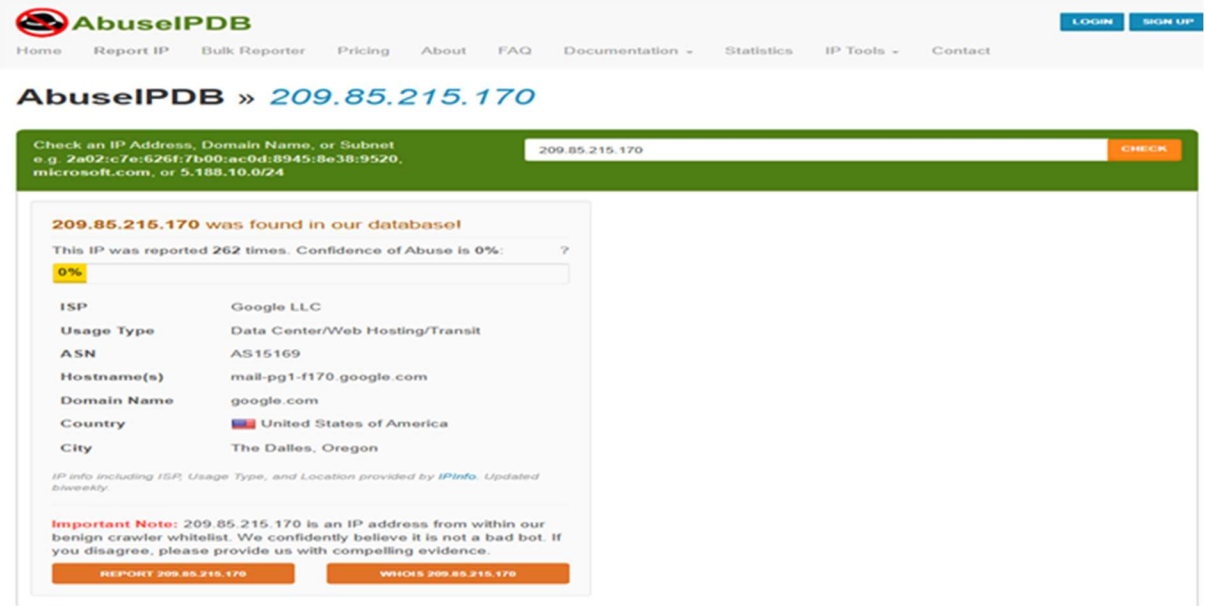
Further, AnyRun analysis revealed suspicious activity linked to 'https://updatedcadobe.blogspot.com/atom.xml,' which led to a 'Blog not found' error. Despite its inactivity, the URL's presence in threat reports suggests previous use in malware distribution.



The Email Header as shown below, further confirmed that this is an impersonation. Jason Conrad is being spoofed for malicious intent because the email sender's name and domain name are inconsistent. The email also originated from an IP address "209.85.215.170" hosted in Dallas, Oregon, USA.

```
X-IncomingTopHeaderMarker:
 OriginalChecksum:7D036766CC6B0C4B76FD67704E117ADE861572764533788FDA95A32178C5A000;UpperCasedChecksum:F36748904F7F
Received: by mail-pg1-f170.google.com with SMTP id 41be03b00d2f7-563c7aabf38so2778570a12.0
        for <lily.tunechy@company.com>; Sat, 29 Jul 2023 07:54:54 -0700 (PDT)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=gmail.com; s=20221208; t=1690642494; x=1691247294;
        h=to:subject:message-id:date:from:mime-version:from:to:cc:subject
         :date:message-id:reply-to;
        bh=ANyuEQ8svyteKchSYumFDap7xajbkXsKyGwQY4LPePk=;
        b=ZmaCxPOZ5Kj+6CUy7cPqg5B3fLAUwlGlw7NG+MwPuSduy9175KK91c6W+pnGEWvj7A
         WnPvXbFXKM9lG10gePapjOh7hqoDmkJnukVYW2I9lCUyt0Xv3ZfLM9dUWkYq+RztuCGq
         4m7DKJsZWiSQhxWbY2sydX1InAMej2EXF/ur8Dgiv8rG9p3yiVF4w3ZfPIf/Z7+EJgLH
         ZdQD1OuwpLXnQCcs4nyUhtjv1d+9qu4Sbgv/LviV+OpzTDFPPD8VfNNWHEiXIrEhOfRE
         DtPrlZo7UsL994o+ZMCZFHp67hSymnMnRNMxEA4v8knwKljhfxT5bR2yxzEvCeo8TlK5
         14Sw==
X-Google-DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=1e100.net; s=20221208; t=1690642494; x=1691247294;
        h=to:subject:message-id:date:from:mime-version:x-gm-message-state
         :from:to:cc:subject:date:message-id:reply-to;
        bh=ANyuEQ8svyteKchSYumFDap7xajbkXsKyGwQY4LPePk=;
        b=hFjWuzAkGSCiZUgc3VQi04YOBG+qd54u1C4cbWzobwN5A7GuJH39iuz/eof5+eKcWt
         w3yXJInqRd1wcar90ltRDLUgmM8Oa56c51Wiiozv1ZP2FhsgRlGSBducefkrFFguPEyl
         ehj4iwa6ZT0C+V735fcVOGG5RNNlTmWmUild2VPPHSYFOb56xhdnkLK7MWzDyaxDlR9a
         2Z3XhWOJt7a7XYDzgdzSdO23htoZxt71aQpriKywecdH4GAD1XcwkzaHdvJam1tSaCX0
         5/wsPoxLGTzJrBF7z9I1YdWUQI7k3LHTWHy0aNp2KwahM58AV4M6Es16bPbTp5Bbas35
         3O+Q==
X-Gm-Message-State: ABy/qLYWsrZnMM3Yc9zxYGFHyH+awLE5qLQt3W1601GPXbkGdFtl4YQu
        DS69v5t7DR3JxGP4Z+SUOPHwE7RhWk6NKp3qGvLuODphD7c34hF/
X-Google-Smtp-Source: APBJJlHBw6MXxh4JklBalUUPcIAwV+/X9bLbzrqtV/7qTJ3Z875G0Q91fHrc1qkiLBOy8x2bbrurBsjuM8oVAHN5rbA=
X-Received: by 2002:a17:90b:101:b0:268:ad94:3cf5 with SMTP id
 p1-20020a17090b010100b00268ad943cf5mr475568pjz.8.1690642493560; Sat, 29 Jul
 2023 07:54:53 -0700 (PDT)
From: Jason Conrad <alfredegov@gmail.com>
Date: Sat, 29 Jul 2023 15:54:42 +0100
Message-ID: <CAK+pMvdiJQ3+R93bCHF8P8UL1-bN=GJHxVhDCTPAy0egyxKFkg@mail.gmail.com>
Subject: Important Adobe Update
To: lily.tunechy@company.com
Content-Type: multipart/alternative; boundary="000000000000455b390601a16146"
X-IncomingHeaderCount: 13
Return-Path: alfredegov@gmail.com
X-MS-Exchange-Organization-ExpirationStartTime: 29 Jul 2023 14:54:54.7491
 (UTC)
```

The IP linked to the suspicious domain has a poor reputation, with numerous reports of phishing and fraud. A 0-confidence score highlights its consistent use for malicious activities.

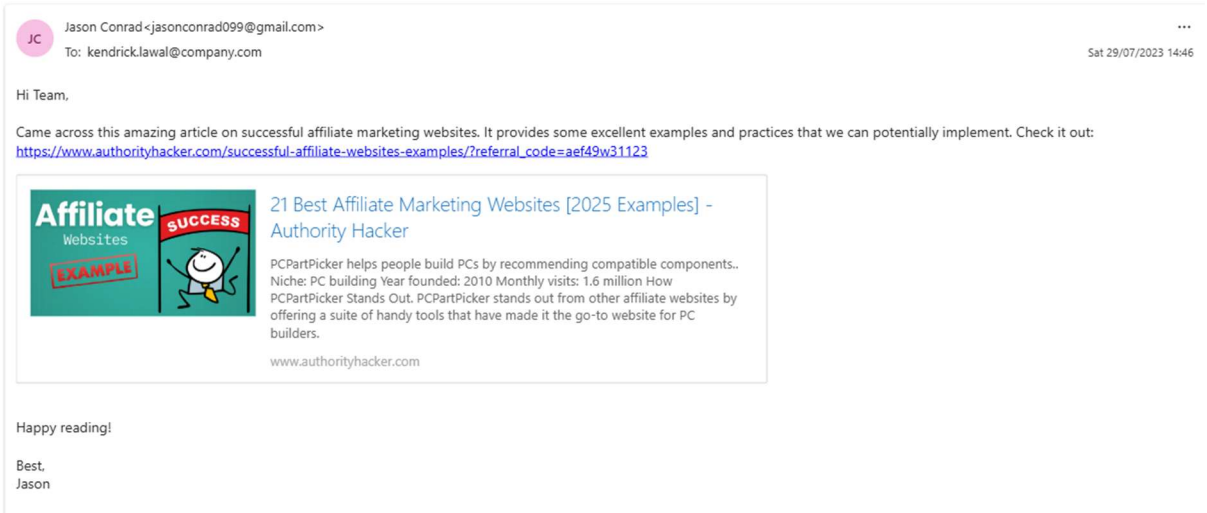


Indicators of Compromise (IOCs)

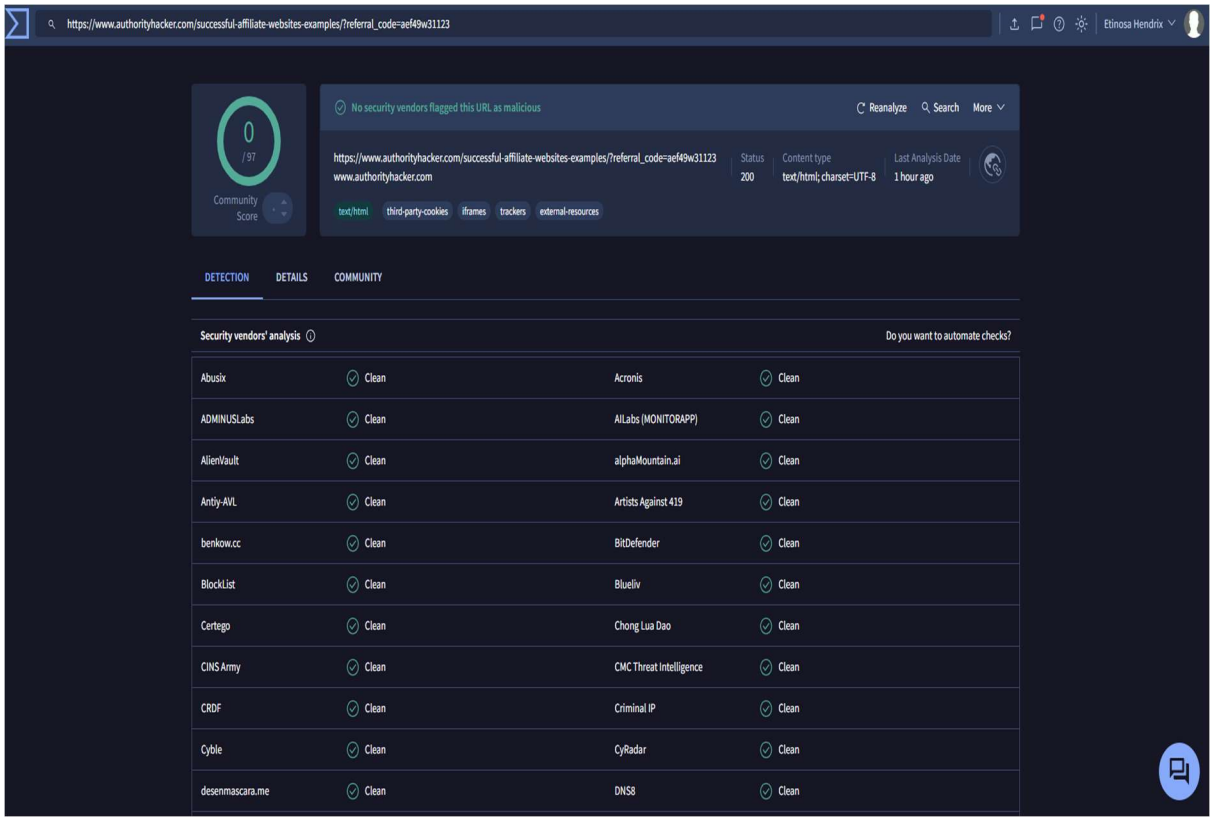
Type	Value	Notes
Domain	blogspot.com	Proactive detection and alerting through EDR/SIEM systems.
URL	https://updatedcadobe.blogspot.com/atom.xml	Feeding data into systems for threat intelligence and response.
IP Address	209.85.215.170	High-value forensic data for blocking and tracking threats effectively.
File Hashes	MD5, SHA256	Vital for incident response and identifying compromised files or systems.

Affiliate Marketing Best Practices

Below is the reported email.



An email from jasonconrad099@gmail.com with an affiliate link was assessed.



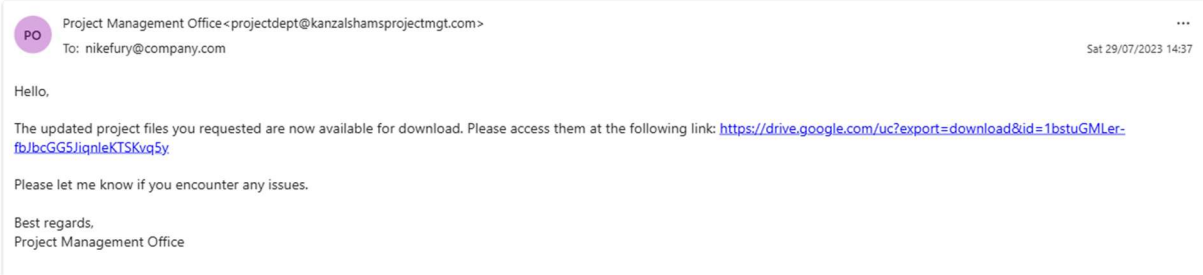
VirusTotal showed no threats, suggesting it's likely graymail. Source and URL patterns are logged for monitoring. No signs of credential theft or redirection, and no further reports of suspicious activity or account compromise from the recipient.

Indicators of Compromise (IOCs)

Type	Value	Notes
Domain	authorityhacker.com	Legitimate but monitored for affiliate campaigns
Code	aef49w31123	External referral tracking code:
Email Sender	jasonconrad099@gmail.com	Suspicious sender

Download Updated Project Files

The reported email is shown below.



Preliminary analysis shows the link points to a binary file hosted on Google Drive.

Out of 96 vendors, 3 flagged the URL as malicious, including BitDefender, ESET, and Fortinet, all identifying it as malware. The file type is application/binary, and the last analysis was a month ago.

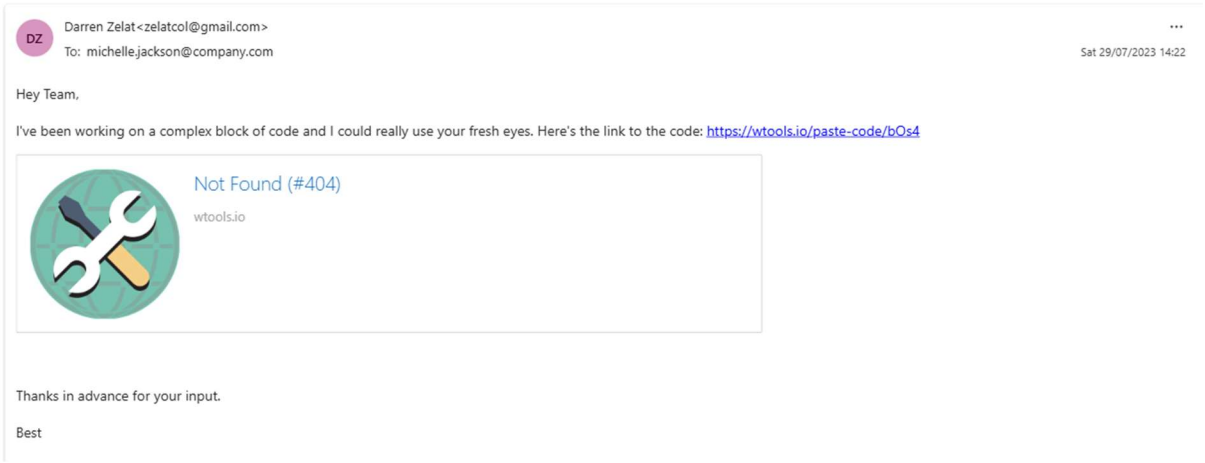
Indicators of Compromise (IOCs)

Type	Value	Notes

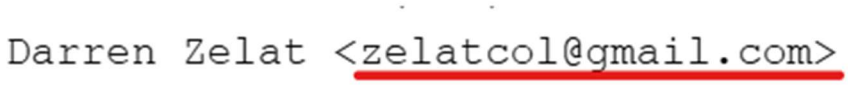
URL	https://drive.google.com/uc?export=download&id=1bstuGMLer-fbJbcGG5JiqnleKTSKvq5y	Host of malicious content
Associated Malware	LOKIBOT	A known credential stealer and infostealer Trojan
File Type	application/binary	Likely created to bypass filters

Code Review Request

The reported email is shown below.

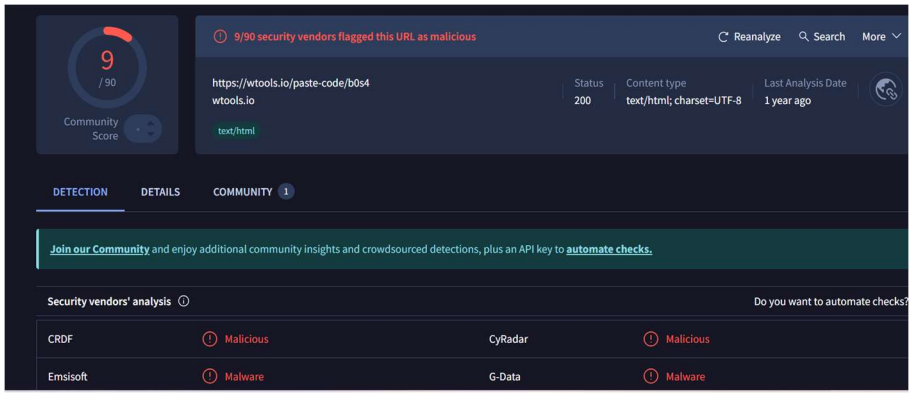


The email came from a `@gmail.com` address. This means it was sent from a personal email, not a company email. This is not consistent with internal communication practices within organizations, especially for professional matters like code reviews. If the sender really worked at the company, they should have used the company's official email address like the one the receiver (Michelle) used.



The sender is "Darren Zelat," but they didn't include any job title, phone number, or way to confirm who they are. This lack of transparency raises suspicion and makes it hard to trust the email. There is no proof that this person works at the company, making identity spoofing or impersonation highly plausible.

The email contains a link to https://wtools.io/paste-code/bOs4, a pastebin-like site often used to host malicious content. VirusTotal flagged the URL as suspicious, with 9 security vendors confirming the risk.



Indicators of Compromise (IOCs)

Indicator	Type	Risk Level
Use of Personal Gmail address	Identity & Authenticity	High
Generic greeting and no context	Social engineering tactic	High
Public code-sharing site Link	Potential payload delivery	High
URL flagged by 9 vendors on VirusTotal	Confirmed malicious signal	High
No name, role or contact info	Unprofessional/ Impersonation	Medium
Sent on a weekend	Anomalous behaviour	Low
No thread or history	Cold contact pattern	Medium

Response Actions

As mentioned, the response actions include, but are not limited to:

- Initial assessments focused on classifying emails as spam or phishing based on the sender, subject line urgency, and suspicious links.
- Links were examined for discrepancies between the display text and actual URLs.
- Domain and header analysis revealed signs of spoofing, impersonation, and unfamiliar routing paths, with all domains flagged for poor reputation by VirusTotal and AbuseIPDB.

Communication

Initial Identification and Assessment:

IT/Cybersecurity Team: Staff member must notify the internal IT and cybersecurity team immediately via email or messaging platforms about the identified phishing email

User Reporting and Confirmation:

Staff Reporting the Threat: Acknowledge user reports, thank staff for their vigilance, and follow up via email or messaging. A sample email is shown below.

Dear Shina,

Thank you for your quick action in reporting the suspicious email. Your vigilance plays a crucial role in protecting our company's security.

After a thorough review, we've confirmed the email was a phishing attempt. Our IT and cybersecurity teams have taken immediate action to address the threat.

We appreciate your commitment to maintaining a secure digital environment. Please continue to report any suspicious activity you encounter.

If you have any concerns, feel free to reach out to the IT/Cybersecurity team.

Best regards,
IT | Cybersecurity

Investigation and Analysis:

- **Cross-Functional Communication**: Set up channels for collaboration between IT, cybersecurity, management, and legal teams.
- **Regular Updates:** Share progress updates with stakeholders through email, meetings, or internal platforms

Response and Mitigation:

- **IT/Cybersecurity Team:** Alert the team to mitigate the threat, including isolating affected systems and disabling compromised accounts.
- **Affected Staff:** Inform staff about the situation, actions being taken, and necessary steps.
- **Incident Response Team:** If needed, involve the incident response team and set up real-time communication channels.

Lessons Learned and Future Improvements:

Post-Incident Review: Share outcomes with IT, cybersecurity, management, and relevant stakeholders, discussing lessons learned and improvement recommendations.

Ongoing User Education:

- **All Staff**: We'll regularly educate staff on phishing threats through training sessions, workshops, and informative emails.

Suspicious Sign-ins

Confidential Security Report

Subject: Suspicious Login Investigation – User: Erwin Smith

Prepared by: Cybersecurity Incident Response Team

Date: April 9, 2025

This report summarizes the results of an investigation into suspicious sign-in activity associated with the user Erwin Smith. The sign-in records revealed unauthorized access attempts from foreign IP addresses. The user is known to be UK-based, and login patterns from countries such as China and Thailand raised red flags. Post-analysis confirmed indicators of compromise. Immediate response actions were taken to contain the threat and prevent recurrence.

Investigation Steps

1. **Log Analysis**:
    - We reviewed the signin_logs_erwin.csv and activity_logs_erwin.csv files.
    - We extracted and analyzed all unique IP addresses and correlated them with respective activity logs.
    - We flagged any logins that were not followed by user activity.
2. **IP Address and Location Correlation**:
    - We mapped the IP addresses to their respective geographic locations.
    - We focused on anomalies that deviated from the user's known location and working pattern.
3. **Threat Behavior Identification**:
    - We analyzed the timing and frequency of the login attempts.
    - We flagged logins from outside the UK.
    - We reviewed if these logins were followed by any account activity.

Key Findings & Evidence

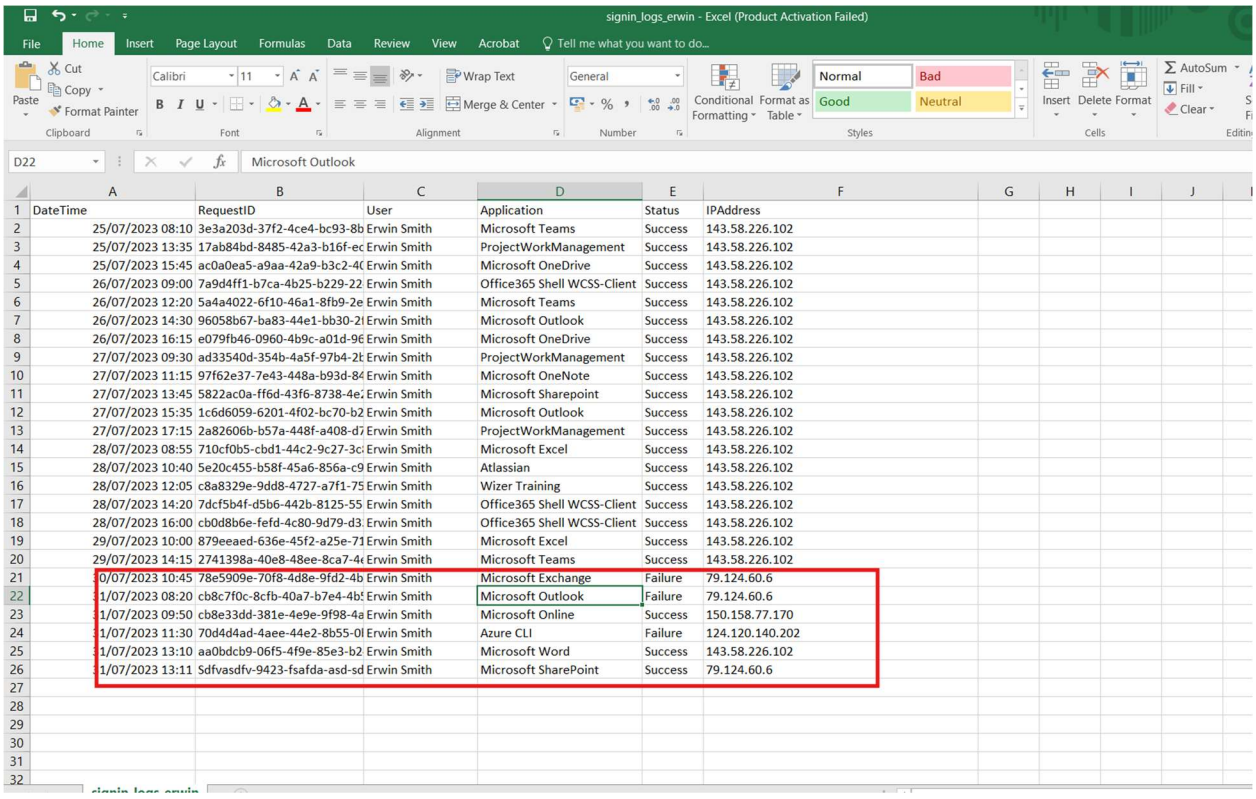
Through our analysis, we were able to distinguish between legitimate and malicious sign-in activity based on origin, behaviour, and usage pattern. Our investigation revealed the following:

Malicious Sign-in Attempts

- The attacker attempted logins across various Microsoft services (Exchange, Online, Azure CLI, Outlook, and SharePoint).
- The first two login attempts failed; the next sign-in to Microsoft Online succeeded.
- A failed Azure CLI login followed, and then a successful sign-in to Microsoft SharePoint.
- This behavior indicates the use of brute-force techniques to guess credentials.

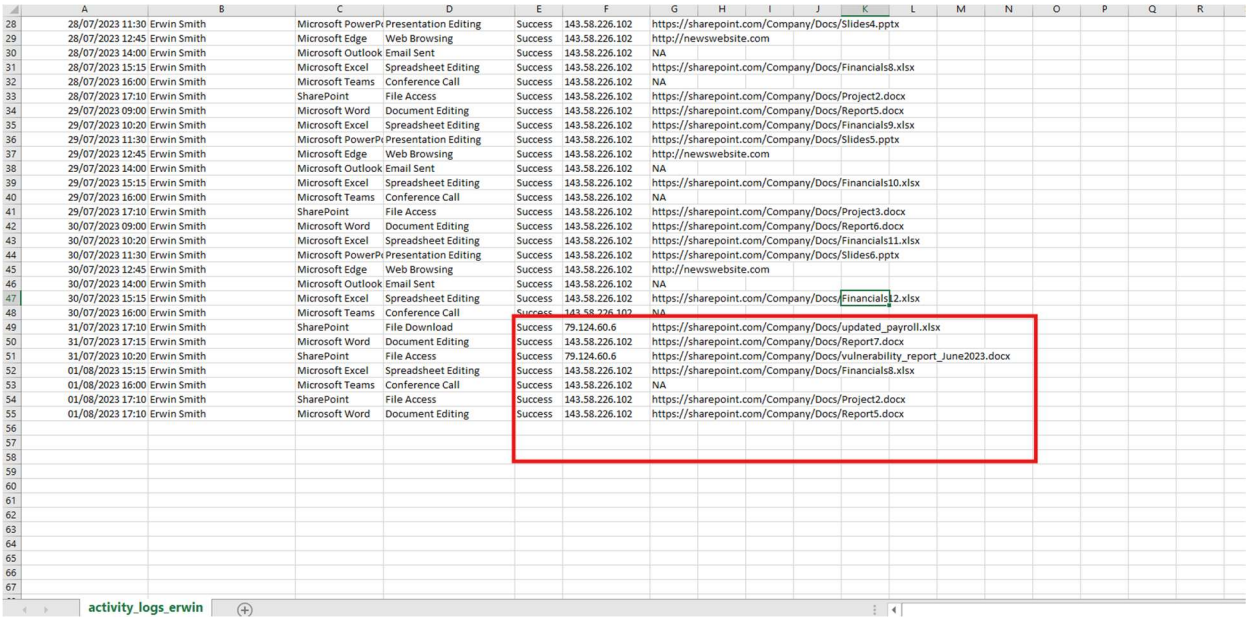
Evidence of Brute-Force Behaviour

- Multiple login attempts within a short time frame.
- Successful access following failed attempts.
- Use of different services to test credentials.



	A	B	C	D	E	F
1	DateTime	RequestID	User	Application	Status	IPAddress
2	25/07/2023 08:10	3e3a203d-37f2-4ce4-bc93-8b	Erwin Smith	Microsoft Teams	Success	143.58.226.102
3	25/07/2023 13:35	17ab84bd-8485-42a3-b16f-ec	Erwin Smith	ProjectWorkManagement	Success	143.58.226.102
4	25/07/2023 15:45	ac0a0ea5-a9aa-42a9-b3c2-4(	Erwin Smith	Microsoft OneDrive	Success	143.58.226.102
5	26/07/2023 09:00	7a9d4ff1-b7ca-4b25-b229-22	Erwin Smith	Office365 Shell WCSS-Client	Success	143.58.226.102
6	26/07/2023 12:20	5a4a4022-6f10-46a1-8fb9-2e	Erwin Smith	Microsoft Teams	Success	143.58.226.102
7	26/07/2023 14:30	96058b67-ba83-44e1-bb30-2(	Erwin Smith	Microsoft Outlook	Success	143.58.226.102
8	26/07/2023 16:15	e079fb46-0960-4b9c-a01d-9(	Erwin Smith	Microsoft OneDrive	Success	143.58.226.102
9	27/07/2023 09:30	ad33540d-354b-4a5f-97b4-2(	Erwin Smith	ProjectWorkManagement	Success	143.58.226.102
10	27/07/2023 11:15	97f62e37-7e43-448a-b93d-84	Erwin Smith	Microsoft OneNote	Success	143.58.226.102
11	27/07/2023 13:45	5822ac0a-ff6d-43f6-8738-4e	Erwin Smith	Microsoft Sharepoint	Success	143.58.226.102
12	27/07/2023 15:35	1c6d6059-6201-4f02-bc70-b2	Erwin Smith	Microsoft Outlook	Success	143.58.226.102
13	27/07/2023 17:15	2a82606b-b57a-448f-a408-d7	Erwin Smith	ProjectWorkManagement	Success	143.58.226.102
14	28/07/2023 08:55	710cf0b5-cbd1-44c2-9c27-3c	Erwin Smith	Microsoft Excel	Success	143.58.226.102
15	28/07/2023 10:40	5e20c455-b58f-45a6-856a-c9	Erwin Smith	Atlassian	Success	143.58.226.102
16	28/07/2023 12:05	c8a8329e-9dd8-4727-a7f1-75	Erwin Smith	Wizer Training	Success	143.58.226.102
17	28/07/2023 14:20	7dcf5b4f-d5b6-442b-8125-55	Erwin Smith	Office365 Shell WCSS-Client	Success	143.58.226.102
18	28/07/2023 16:00	cb0d8b6e-fefd-4c80-9d79-d3	Erwin Smith	Office365 Shell WCSS-Client	Success	143.58.226.102
19	29/07/2023 10:00	879eeaed-636e-45f2-a25e-71	Erwin Smith	Microsoft Excel	Success	143.58.226.102
20	29/07/2023 14:15	2741398a-40e8-48ee-8ca7-4(	Erwin Smith	Microsoft Teams	Success	143.58.226.102
21	30/07/2023 10:45	78e5909e-70f8-4d8e-9fd2-4b	Erwin Smith	Microsoft Exchange	Failure	79.124.60.6
22	31/07/2023 08:20	cb8c7f0c-8cfb-40a7-b7e4-4b	Erwin Smith	Microsoft Outlook	Failure	79.124.60.6
23	31/07/2023 09:50	cb8e33dd-381e-4e9e-9f98-4a	Erwin Smith	Microsoft Online	Success	150.158.77.170
24	31/07/2023 11:30	70d4d4ad-4aee-44e2-8b55-0l	Erwin Smith	Azure CLI	Failure	124.120.140.202
25	31/07/2023 13:10	aa0bdcb9-06f5-4f9e-85e3-b2	Erwin Smith	Microsoft Word	Success	143.58.226.102
26	31/07/2023 13:11	Sdfvasdfv-9423-fsafda-asd-sd	Erwin Smith	Microsoft SharePoint	Success	79.124.60.6

Figure 2: Evidence of Brute-Force behaviour



	A	B	C	D	E	F	G
28	28/07/2023 11:30	Erwin Smith	Microsoft PowerP	Presentation Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Slides4.pptx
29	28/07/2023 12:45	Erwin Smith	Microsoft Edge	Web Browsing	Success	143.58.226.102	http://newswebsite.com
30	28/07/2023 14:00	Erwin Smith	Microsoft Outlook	Email Sent	Success	143.58.226.102	NA
31	28/07/2023 15:15	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials8.xlsx
32	28/07/2023 16:00	Erwin Smith	Microsoft Teams	Conference Call	Success	143.58.226.102	NA
33	28/07/2023 17:10	Erwin Smith	SharePoint	File Access	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Project2.docx
34	29/07/2023 09:00	Erwin Smith	Microsoft Word	Document Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Report5.docx
35	29/07/2023 10:20	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials9.xlsx
36	29/07/2023 11:30	Erwin Smith	Microsoft PowerP	Presentation Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Slides5.pptx
37	29/07/2023 12:45	Erwin Smith	Microsoft Edge	Web Browsing	Success	143.58.226.102	http://newswebsite.com
38	29/07/2023 14:00	Erwin Smith	Microsoft Outlook	Email Sent	Success	143.58.226.102	NA
39	29/07/2023 15:15	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials10.xlsx
40	29/07/2023 16:00	Erwin Smith	Microsoft Teams	Conference Call	Success	143.58.226.102	NA
41	29/07/2023 17:10	Erwin Smith	SharePoint	File Access	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Project3.docx
42	30/07/2023 09:00	Erwin Smith	Microsoft Word	Document Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Report6.docx
43	30/07/2023 10:20	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials11.xlsx
44	30/07/2023 11:30	Erwin Smith	Microsoft PowerP	Presentation Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Slides6.pptx
45	30/07/2023 12:45	Erwin Smith	Microsoft Edge	Web Browsing	Success	143.58.226.102	http://newswebsite.com
46	30/07/2023 14:00	Erwin Smith	Microsoft Outlook	Email Sent	Success	143.58.226.102	NA
47	30/07/2023 15:15	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials12.xlsx
48	30/07/2023 16:00	Erwin Smith	Microsoft Teams	Conference Call	Success	143.58.226.102	NA
49	31/07/2023 17:10	Erwin Smith	SharePoint	File Download	Success	79.124.60.6	https://sharepoint.com/Company/Docs/updated_payroll.xlsx
50	31/07/2023 17:15	Erwin Smith	Microsoft Word	Document Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Report7.docx
51	31/07/2023 10:20	Erwin Smith	SharePoint	File Access	Success	79.124.60.6	https://sharepoint.com/Company/Docs/vulnerability_report_June2023.docx
52	01/08/2023 15:15	Erwin Smith	Microsoft Excel	Spreadsheet Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Financials8.xlsx
53	01/08/2023 16:00	Erwin Smith	Microsoft Teams	Conference Call	Success	143.58.226.102	NA
54	01/08/2023 17:10	Erwin Smith	SharePoint	File Access	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Project2.docx
55	01/08/2023 17:10	Erwin Smith	Microsoft Word	Document Editing	Success	143.58.226.102	https://sharepoint.com/Company/Docs/Report5.docx

activity_logs_erwin

Figure 3: Activity Logs

File Access & Downloads

- From the activity log, we saw that the attacker (IP: 79.124.60.6) downloaded the file updated_payroll.xlsx possibly to tamper with salary disbursement.
- The same IP also accessed the vulnerability_report.xlsx potentially to identify exploitable weaknesses in our infrastructure.

Sign-in IPs and Associated Data

IP Address	Sign-in Count	Activity Count	Geographic Origin	Assessment
143.58.226.102	20	52	United Kingdom	Legitimate
79.124.60.6	3	2	Bulgaria	Suspicious (possible VPN)
150.158.77.170	1	0	China	Malicious
124.120.140.202	1	0	Thailand	Malicious

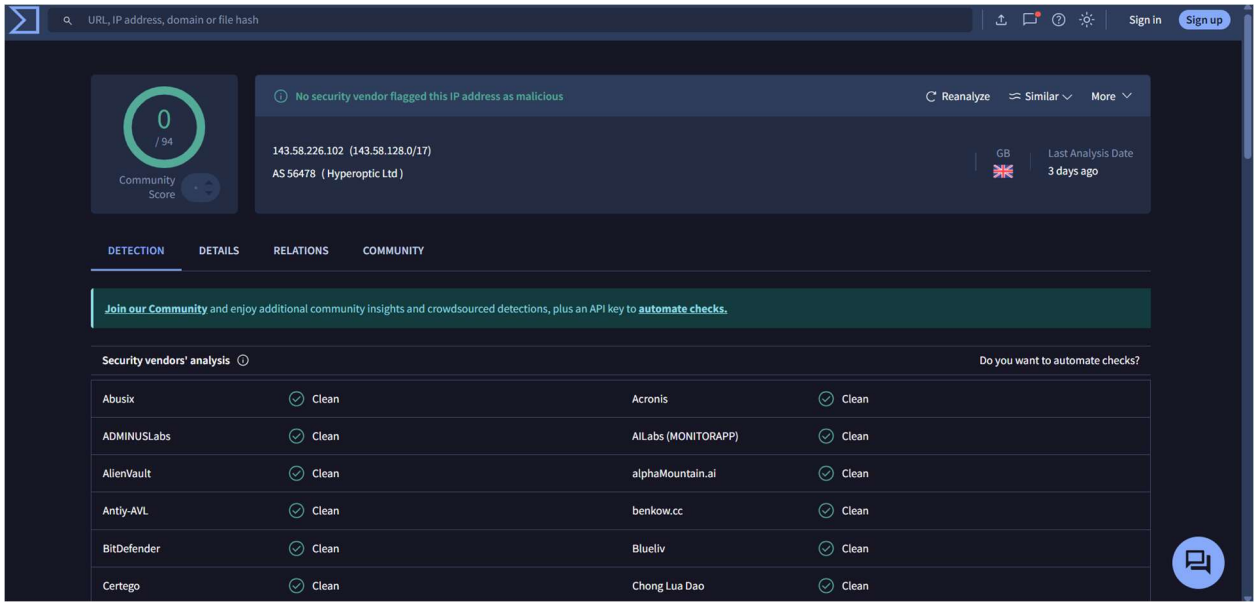


Figure 4: Shows the IP is clean and is resident in the UK

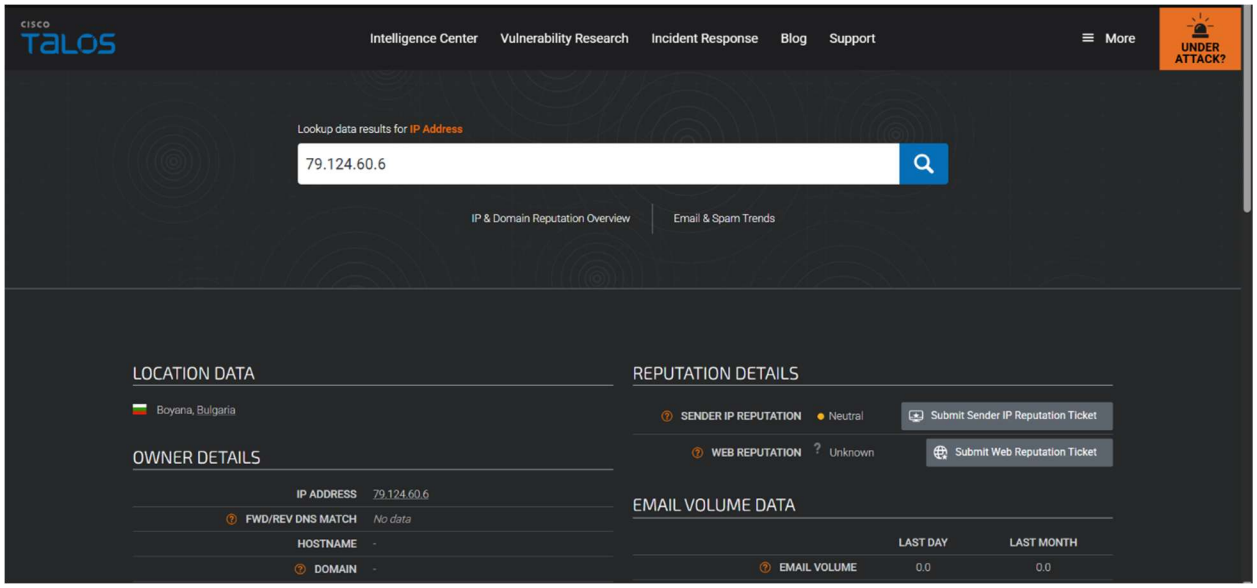


Figure 5: Shows the IP as not resident in the UK

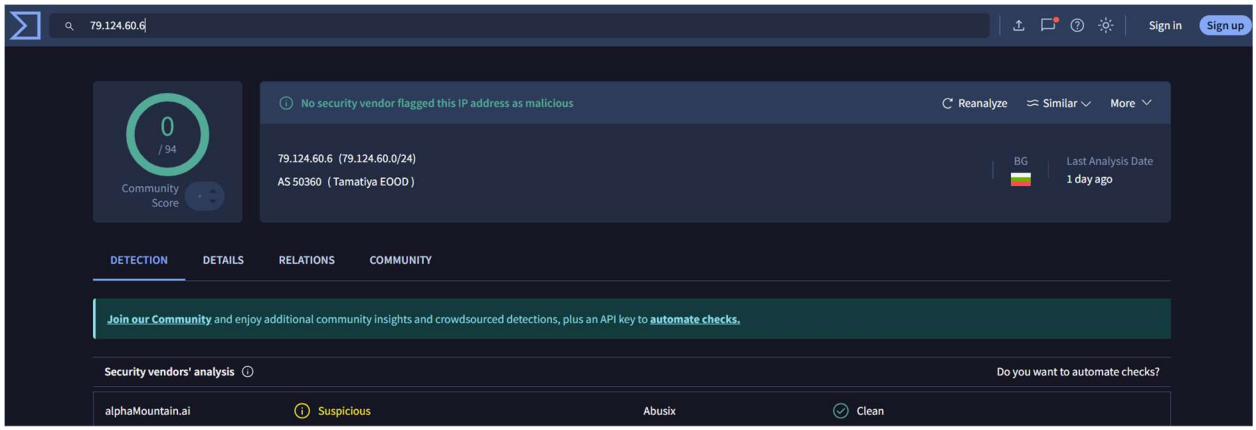


Figure 6: Shows that the ip has been flagged as suspicious

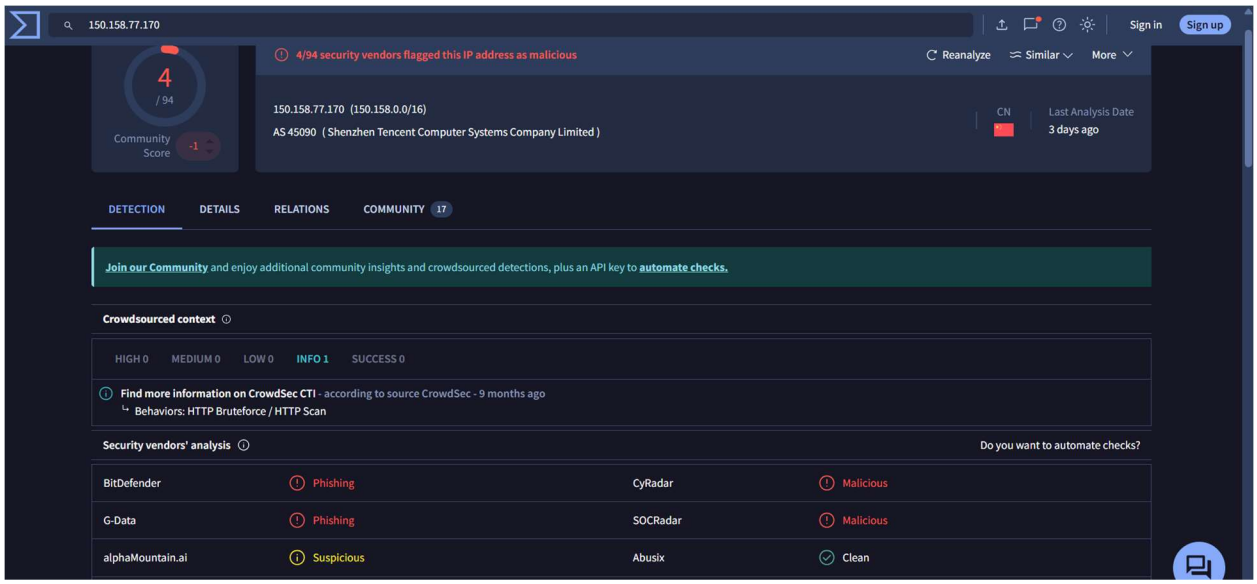


Figure 7: Shows the ip 150.158.77.170 is malicious and resident in China

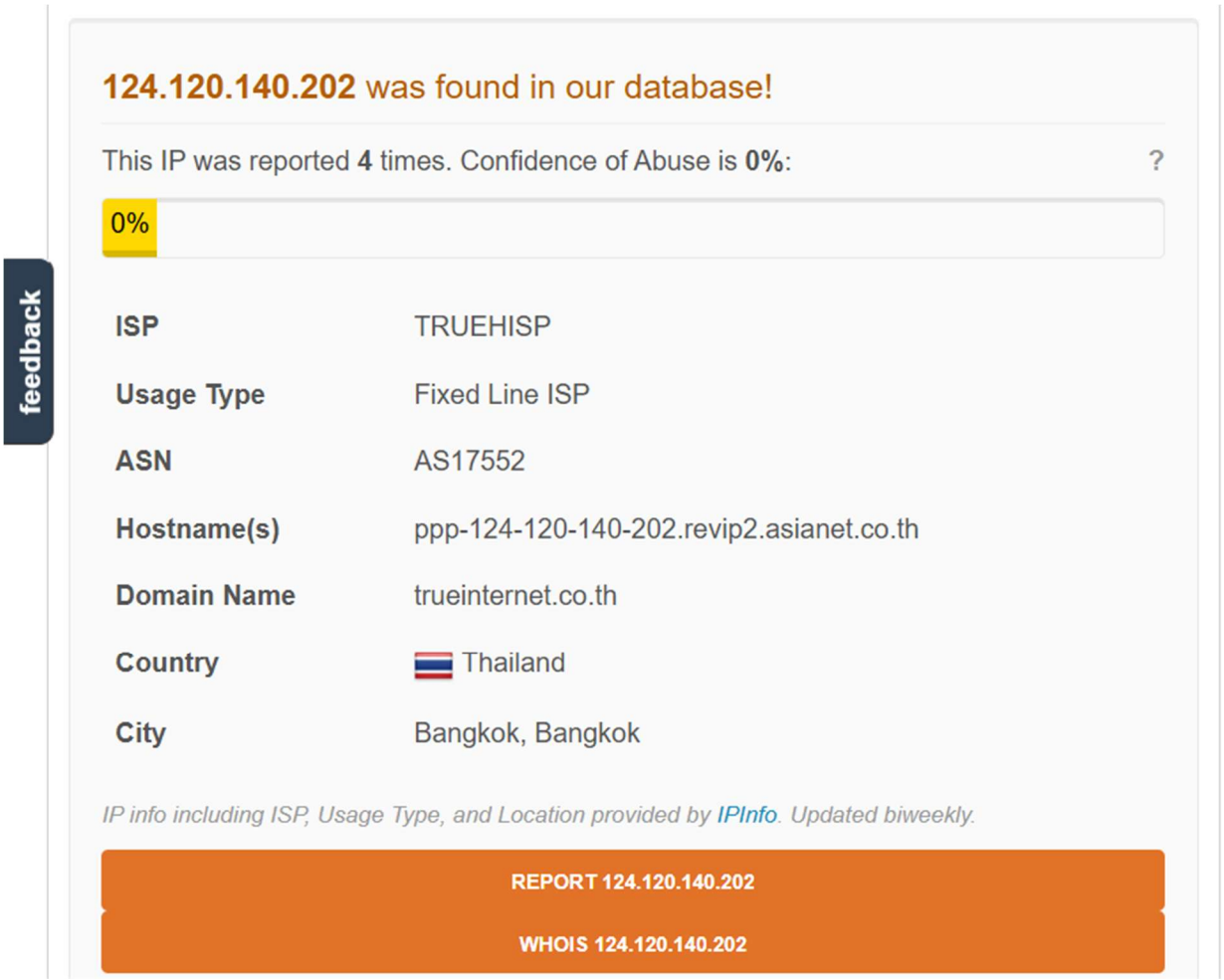


Figure 8: Shows that the IP has been reported as malicious

Indicators of Compromise (IoCs)

We identified the following IoCs:

- **IP: 150.158.77.170** (China)
- **IP: 124.120.140.202** (Thailand)
- **IP: 79.124.60.6** (Bulgaria)

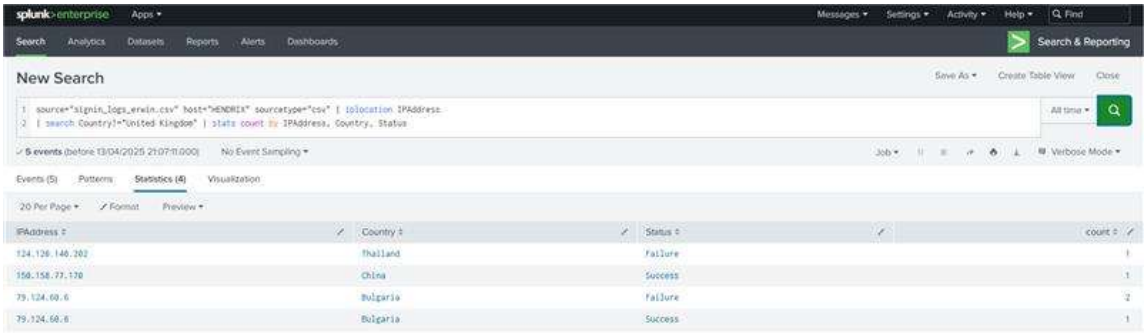


Figure 9: Indicators of Compromise (IoCs)

Files downloaded during the breach:

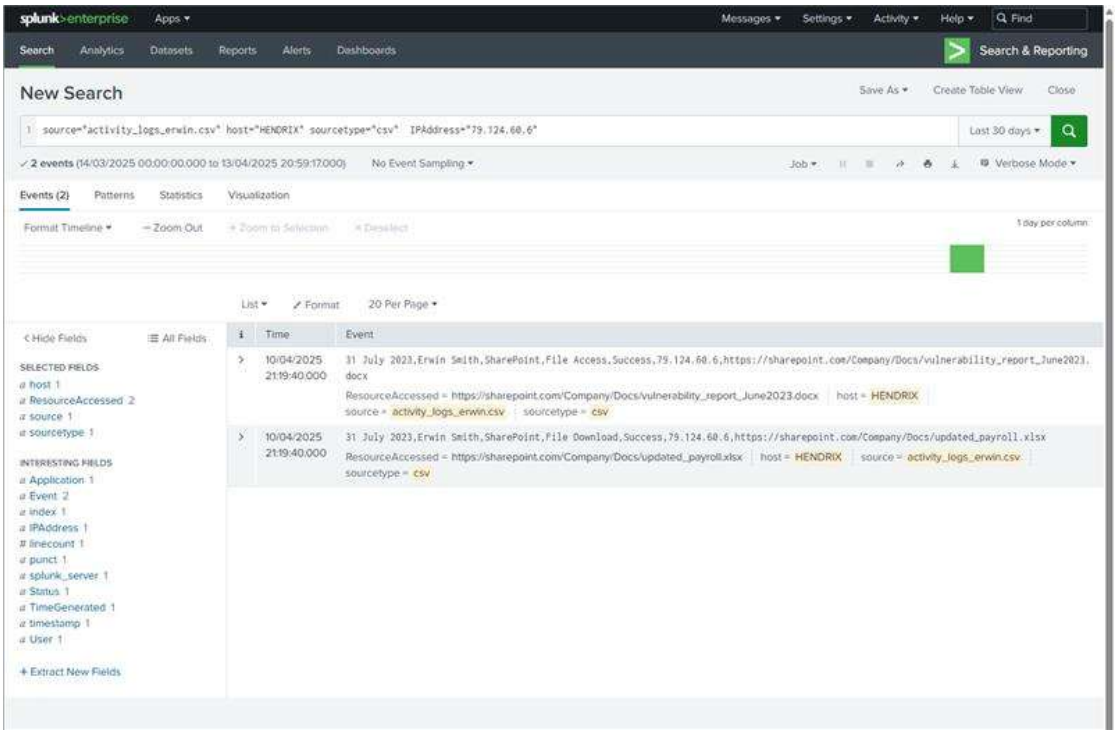


Figure 10: Downloaded files

- updated_payroll.xlsx
- vulnerability_report.xlsx

These IoCs suggest that the attacker's intent included modifying financial records and identifying vulnerabilities within our systems.

Recommended Response Actions

Action	Description
Session Revocation	Immediately terminate all active sessions linked to flagged IPs.
Credential Reset	Enforce a password change for Erwin Smith.
Conditional Access	Restrict future access to known UK-based IPs.
Multi-Factor Authentication (MFA)	Enable MFA for additional security on the account.
Threat Intel Update	Log IoCs into SIEM for future alerting.
Forensic Audit	Investigate historical activity for data exfiltration.
Payroll System Review	Audit salary disbursement entries for tampering.
Patch Validation	Cross-reference accessed vulnerabilities with patch records.

Communication

- Immediately notify key stakeholders, including management, IT, HR, and legal teams, about the incident.
- Activate the crisis communication plan to provide clear and consistent information to employees.
- Provide regular updates to stakeholders about the incident, investigation progress, and steps being taken to address the situation.

Investigate and Analyse Malware

File Analysis

On March 11, 2024, a CrowdStrike alert was triggered within Cyberbulwork's infrastructure due to a VIP user visiting a malicious domain and downloading a suspicious file. This report details the investigation findings and outlines the remediation steps taken.

```
alert_all_security_Crowdstrike_csp_IAAT_A2 . Source = Crowdstrike.CSP. Category = IAAIT. Subcategory = IAAIT_A2.

Time = 11-03-2024 09:14:54
Index = messaging_cisco_esa
Host = remacdmzma01

Dest IP = 117.50.0.178
Dest Domain = accessbank.com
Dest Hostname = ucmail288.sendcloud.org
Source IP = 117.50.0.178
Source Domain = https://duchessgarden.sn/
Source Hostname = 117.50.0.178
Email Attachment = Catalogue.rar
File signature = ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
Email Recipient = sandra.odwyer@accessbank.com, VIP
Email Sender = c6d90d50-df87-11ee-a2fc-525400450766@azxmarket.com
File name = diskpart.exe
User = sandra.odwyer@accessbank.com
Source User = c6d90d50-df87-11ee-a2fc-525400450766@azxmarket.com

Internal_Message_Id = 182466097
Message_Id = 1710148473773_104856_99823_6034.sc-10_9_1_75-inbound0@azxmarket.com
Signature = accepted

Additional Info: Event_Count=1; Subject==?utf-8?q?Professional_Stainless_Steel_Manufacturer?\=; NRD=gracefulinox.com; ESASDRDomainAge=30 days (or greater); ESAAVVerdict=NEGATIVE;
ESAHeloDomain=ucmail288.sendcloud.org; cs6Label=SDRRepScore; cs6=Neutral
================================================================================
Hostname .......:remacdmzma01
AlertGroup......:Crowdstrike_AlertGroup
Service.........:Crowdstrike.CSP
NodeAlias.......:ecpvm005270:8081
Component.......:IEEIT_A2
SubOrigin.......:
SubSource.......:
EventId.........:azxmarket.com-Catalogue.rar
EventDate.......:11/03/2024 09:16:10
Assignment......:SECOAN Security Operations Centre
KSD Attached....:N/A
Ticket Ref......:MBP_FulDev
================================================================================
```

Key Details from the Alert

Alert Metadata

- **Alert Source:** CrowdStrike.CSP
- **Category:** IAAIT
- **Subcategory:** IAAIT_A2
- **Time:** 11-03-2024 09:14:54
- **Host:** remacmdzmao1
- **Assignment:** SECOAN Security Operations Centre

File and Email Details

- **Email Attachment:** Catalogue.rar
- **Extracted File Name:** diskpart.exe

- **File Signature (SHA-256):** ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- **Email Sender Address:** c6d90d5d-df87-11ee-a2fc-525400450766@azxmarket.com
- **Email Recipient:** sandra.odwyer@accessbank.com (VIP user)
- **Email Subject:** "Professional Stainless Steel Manufacturer?"

Network and Domain Information

- **Source Domain:** https://duchessgarden.sn/
- **Destination Domain:** accessbank.com
- **Source IP:** 117.50.0.178
- **Destination Hostname:** ucmail288.sendcloud.org
- **Associated Domain:** gracefulinox.com (NRD)
- **Domain Age:** 30 days or greater (ESASDRDomainAge)

Investigation Findings

File Analysis

The downloaded file, diskpart.exe, was extracted from the Catalogue.rar archive. The SHA-256 signature (ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa) uniquely identifies this malicious file. The file appears to be disguised as the legitimate Windows utility "diskpart" but contains malicious code.

Threat Intelligence

1. The file was delivered through a social engineering email with a professional-sounding subject line to entice the recipient to open the attachment.
2. The sender domain (azxmarket.com) appears to be used for phishing purposes, with a structured UUID in the email address suggesting automated campaign generation.
3. The source domain (duchessgarden.sn) is likely a compromised or malicious site being used to host and distribute malware.

4. Domain age of 30+ days suggests the threat actor established infrastructure in advance of launching the attack.

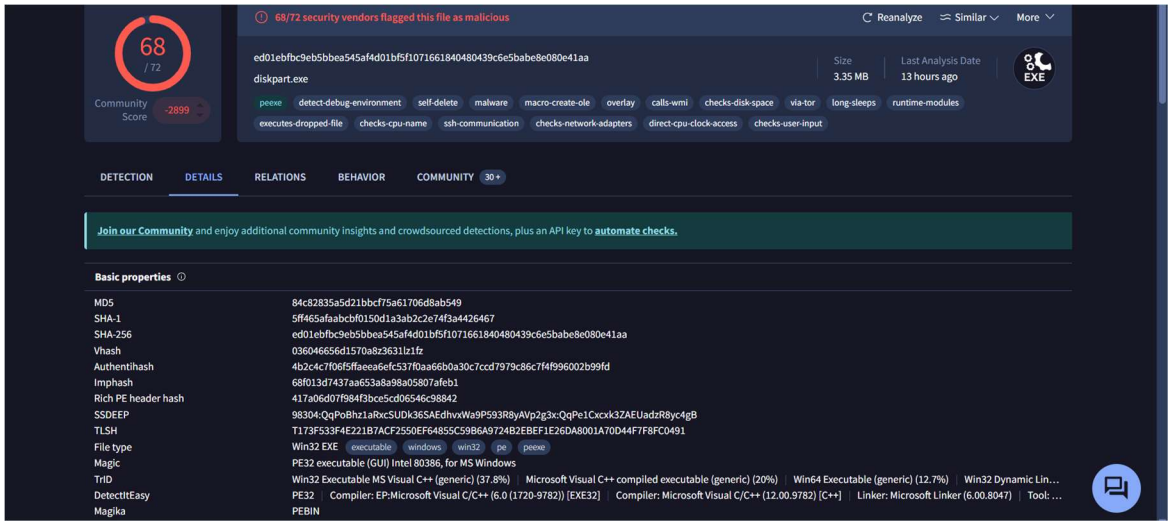
Potential Ransomware Association

While the specific ransomware family is not identified in the alert, the delivery method and targeting of a VIP user align with common ransomware deployment tactics. The executable disguised as a legitimate Windows utility suggests preparation for unauthorized system modification or data encryption.

Hash Signatures

The primary signature detected in the alert is:

- SHA-256: ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa



This SHA-256 hash uniquely identifies the malicious file and should be used for threat hunting across our organisation's environment.

Incident Response Steps

1. Containment

- Isolated the affected host (remacmdzmao1) from the Cyberbulwork network to prevent lateral movement.

- Suspended the VIP user account (sandra.odwyer@accessbank.com) temporarily.
- Blocked all communications to and from the malicious domains:
    - https://duchessgarden.sn/
    - azxmarket.com
    - gracefulinox.com
- Added IP address (117.50.0.178) to firewall block lists.
- Implemented email filtering rules to quarantine similar messages.

2. Investigation

- Performed sandbox analysis of diskpart.exe to observe its behavior in an isolated environment.
- Reviewed CrowdStrike logs for evidence of execution, persistence mechanisms, or data exfiltration.
- Examined email flow logs to identify any other recipients within Cyberbulwork.
- Analyzed message headers to determine if other phishing emails from the same campaign reached the organization.
- Conducted memory analysis on the affected system to identify any in-memory threats.

3. Eradication

- Removed all instances of Catalogue.rar and diskpart.exe from affected systems.
- Eliminated all persistence mechanisms created by the malware (registry keys, scheduled tasks, startup items).
- Performed full-system scans using updated signature definitions.
- Checked for any secondary payloads that may have been downloaded after initial infection.
- Verified system integrity using file integrity monitoring tools.

4. Recovery

- Restored affected systems from clean backups.
- Reset credentials for the affected user and any potentially compromised accounts.

- Implemented additional monitoring for the VIP user's account and workstation.
- Performed verification testing to ensure systems are functioning properly and securely.
- Re-enabled network access only after confirming the absence of malicious activity.

5. Post-Incident Activities

- Conducted targeted security awareness training for all Cyberbulwork VIP users.
- Enhanced email security configurations to improve detection of similar threats.
- Updated the security incident playbook based on lessons learned.
- Shared indicators of compromise with industry partners and threat intelligence platforms.
- Implemented additional technical controls to prevent similar incidents.

Recommendations

Based on this incident, the following improvements are recommended for Cyberbulwork's security posture:

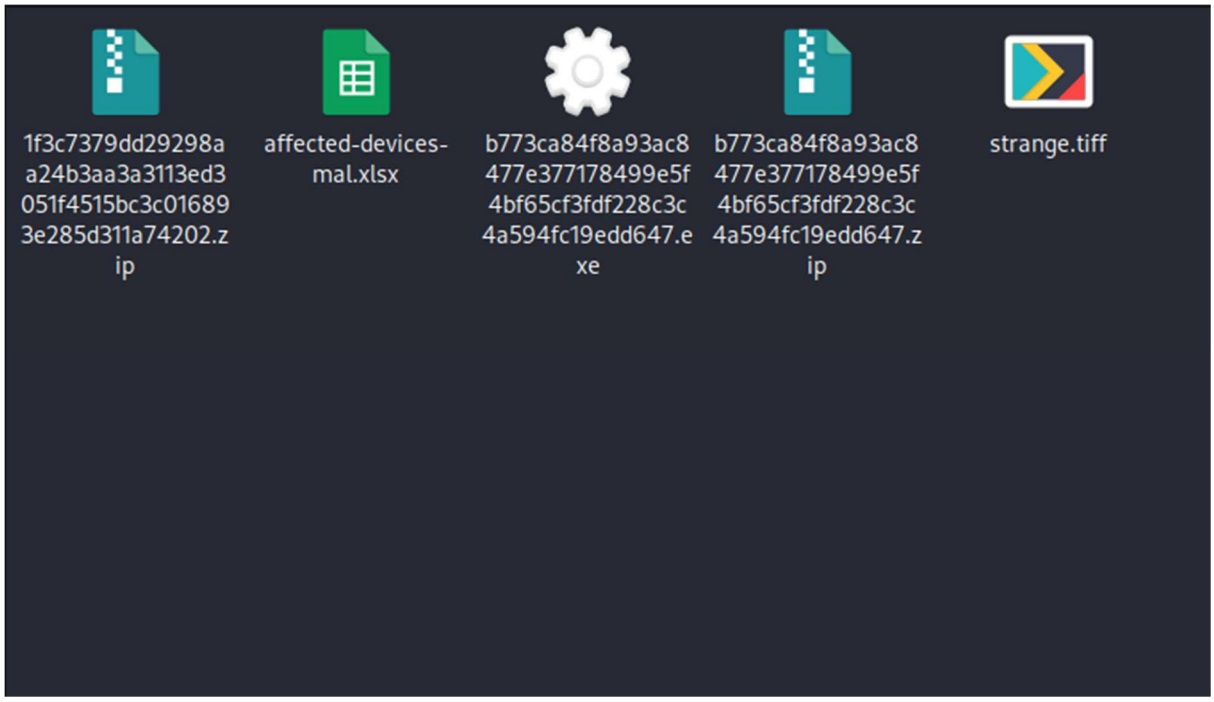
1. Implement stricter email attachment policies, particularly for executable content in archives.
2. Deploy additional security controls for VIP users, including enhanced email scanning and application whitelisting.
3. Consider implementing hardware-based security keys for high-privilege users.
4. Review and strengthen the organization's ransomware response plan.
5. Enhance monitoring of newly registered domains in email communications.
6. Implement regular phishing simulation exercises tailored for executive users.

This incident at Cyberbulwork demonstrates the sophisticated social engineering tactics used by threat actors to target high-value individuals within organizations. The timely detection by CrowdStrike and swift response by the security team prevented potential data encryption or exfiltration, protecting Cyberbulwork's assets and operational continuity.

Malware Analysis and Investigation

A suspicious file flagged by an IT Infrastructure Engineer on one of our high-volume servers was analyzed for potential malware. The file was detonated using the ANY.RUN sandbox to observe its behavior in a

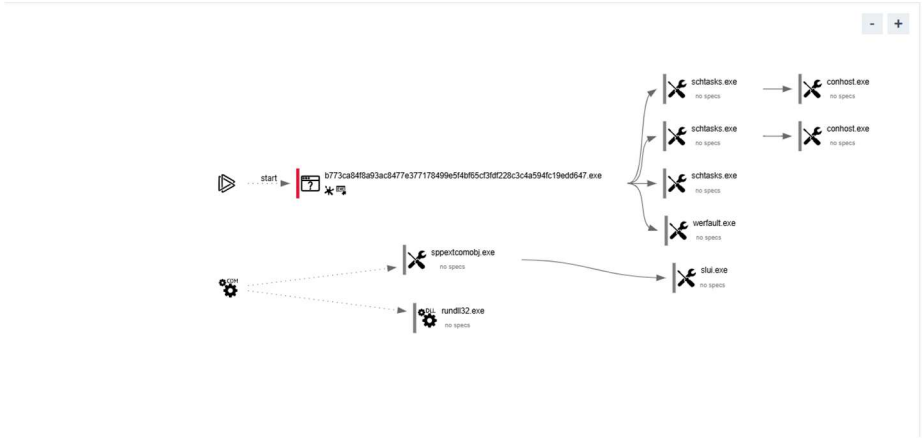
controlled environment. This report outlines the findings, Indicators of Compromise (IoCs), and a detailed action plan to mitigate any harm caused by the malware.



Contaminated files.

Detonation Analysis for the (b773ca84...exe)

The following process tree was generated during the detonation of the suspicious file (b773ca84...exe) in the ANY.RUN sandbox:



Process Tree

Initial Process (b773ca84...exe):

This is the primary executable responsible for initiating malicious activity.

Child Processes

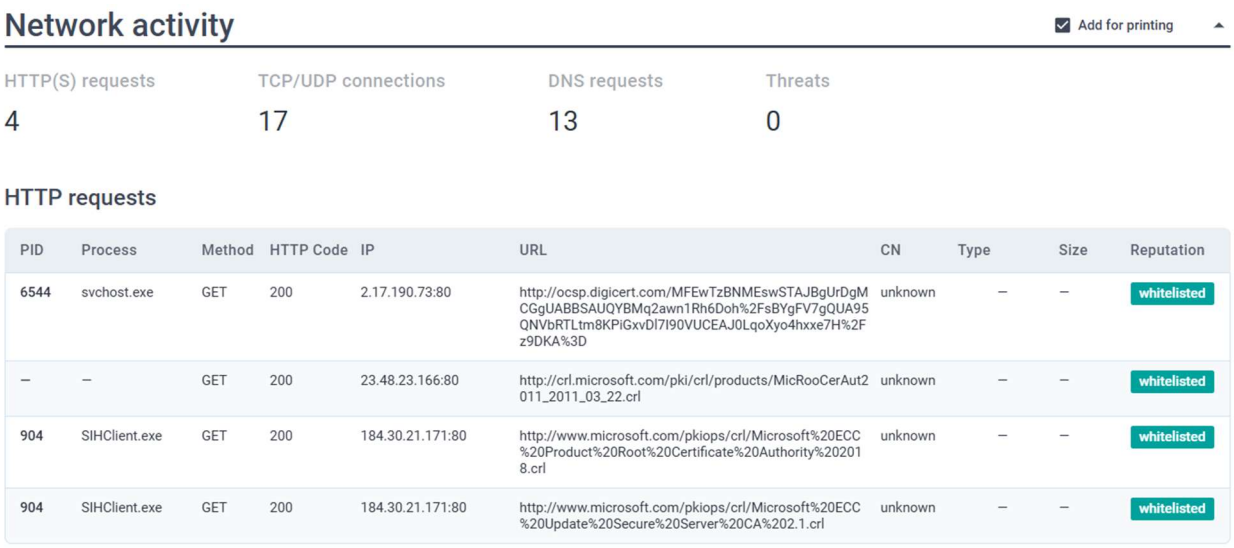
The malware spawns multiple child processes, including:

1. schtasks.exe: Used to create scheduled tasks for persistence.
2. werfault.exe: Likely abused to generate fake crash dumps or interact with Windows Error Reporting (WER).
3. slui.exe: A legitimate Windows process, possibly exploited for privilege escalation or persistence.
4. sppextcomobj.exe and rundll32.exe: Commonly abused processes for executing DLLs or performing system-level operations.

Key Observations

1) The malware uses schtasks.exe to list and modify scheduled tasks, ensuring persistence through "Windows Update BETA."
2) werfault.exe is executed from an unusual location, generating crash dumps and metadata files in system directories.
3) Legitimate Windows processes such as sppextcomobj.exe and rundll32.exe are exploited for stealthy execution.

Network Behavior Analysis



Network activity

Add for printing

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
4	17	13	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6544	svchost.exe	GET	200	2.17.190.73:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	unknown	–	–	whitelisted
–	–	GET	200	23.48.23.166:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
904	SIHClient.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
904	SIHClient.exe	GET	200	184.30.21.171:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted

This image shows network activity captured during the sandbox analysis, including HTTP requests and TCP/UDP connections.

HTTP Requests:

- Connections were made to legitimate domains such as:
    - ocsp.digicert.com (IP: 2.17.190.73) for certificate validation.
    - crl.microsoft.com (IP: 23.48.23.166) for certificate revocation checks.
    - Microsoft-related URLs (settings-win.data.microsoft.com, client.wns.windows.com) for system updates.

TCP/UDP Connections:

- Connections were established with:
    - settings-win.data.microsoft.com (IP: 51.104.136.2) via HTTPS.
    - login.live.com (IP: 20.190.159.130) for authentication services.
    - No malicious domains or IPs were detected during this stage.

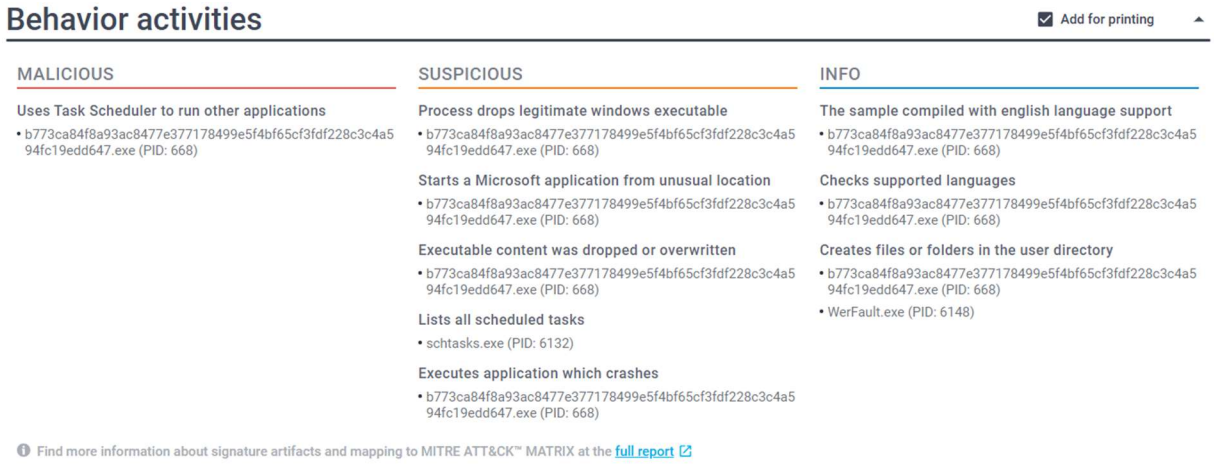
DNS Requests:

- DNS queries included:

- Legitimate domains like settings-win.data.microsoft.com, crl.microsoft.com, and login.live.com.
- All DNS requests were marked as "whitelisted."

All observed connections were marked as "whitelisted" during analysis, suggesting the dropper primarily connects to legitimate Microsoft services. This indicates the sample may be establishing a foothold before subsequent malicious activity or command-and-control communication occurs.

Persistence Mechanisms



The malware establishes persistence through:

1. **Task Scheduler Abuse**:
    - Creates scheduled tasks to ensure execution after system restart
    - Likely creates a task named "Windows Update BETA" based on behavior classification
    - Uses schtasks.exe with elevated rights (/rl highest parameter)
2. **Strategic File Placement**:
    - Places MuiUnattend.exe in %AppData%\Microsoft\Windows\MuiUnattend\
    - Uses legitimate-sounding file names to avoid detection

Indicators of Compromise (IoCs)

Type	Indicator
File Hashes	SHA256: B773CA84F8A93AC8477E377178499E5F4BF65CF3FDF228C3C4A594FC19EDD647
	MD5: CD466F12DDBE80DC64F34868F9AE4126
Files	%AppData%\Microsoft\Windows\MuiUnattend\MuiUnattend.exe
	%ProgramData%\Microsoft\Windows\WER\Temp*.tmp.dmp
	%ProgramData%\Microsoft\Windows\WER\Temp*.tmp.xml
Processes	Multiple instances of schtasks.exe with unusual parameters
	werfault.exe triggered by malicious activity
Scheduled Tasks	Look for tasks with names similar to "Windows Update BETA"

Action Plan for Mitigation

Immediate Containment

1. **Remove Malicious Files**:
    - Identify and delete dropped files, such as MuiUnattend.exe, located in %AppData%\Microsoft\Windows\MuiUnattend.
    - Remove crash dump and metadata files created in %ProgramData%\Microsoft\Windows\WER and %AppData%\Local\CrashDumps.
2. **Disable Persistence Mechanisms**:
    - Review and delete suspicious scheduled tasks created by the malware, such as "Windows Update BETA."
    - Monitor and remove registry entries related to scheduled tasks or application history modifications.
3. **Quarantine Affected Hosts**:
    - Isolate infected systems from the network to prevent further propagation or communication with external servers.

Forensic Investigation

1. **Analyze Dropped Files**:
    - Examine MuiUnattend.exe for embedded payloads or malicious configurations.
    - Review crash dumps for potential follow-on malware or injected code.
2. **Monitor System Activity**:
    - Investigate processes like schtasks.exe, werfault.exe, and rundll32.exe for unusual behavior or command-line arguments.
3. **Network Traffic Analysis**:
    - Verify all outbound connections to ensure no malicious domains or IP addresses are contacted beyond legitimate Microsoft services.

System Hardening

1. **Patch Vulnerabilities**:
    - Ensure all systems are updated with the latest security patches to prevent exploitation of known vulnerabilities.
2. **Restrict Task Scheduler Abuse**:
    - Implement policies to restrict unauthorized creation of scheduled tasks with elevated privileges (/rl highest).
3. **Deploy Detection Rules**:
    - Use endpoint protection tools to monitor suspicious file drops, task creation, and registry changes.
    - Deploy YARA rules targeting file names like MuiUnattend.exe and processes such as schtasks.exe.

User Awareness & Training

1. Educate users on recognizing phishing emails and suspicious attachments that may deliver malware.
2. Enforce stricter policies on downloading and executing files from untrusted sources.

Follow-Up Actions

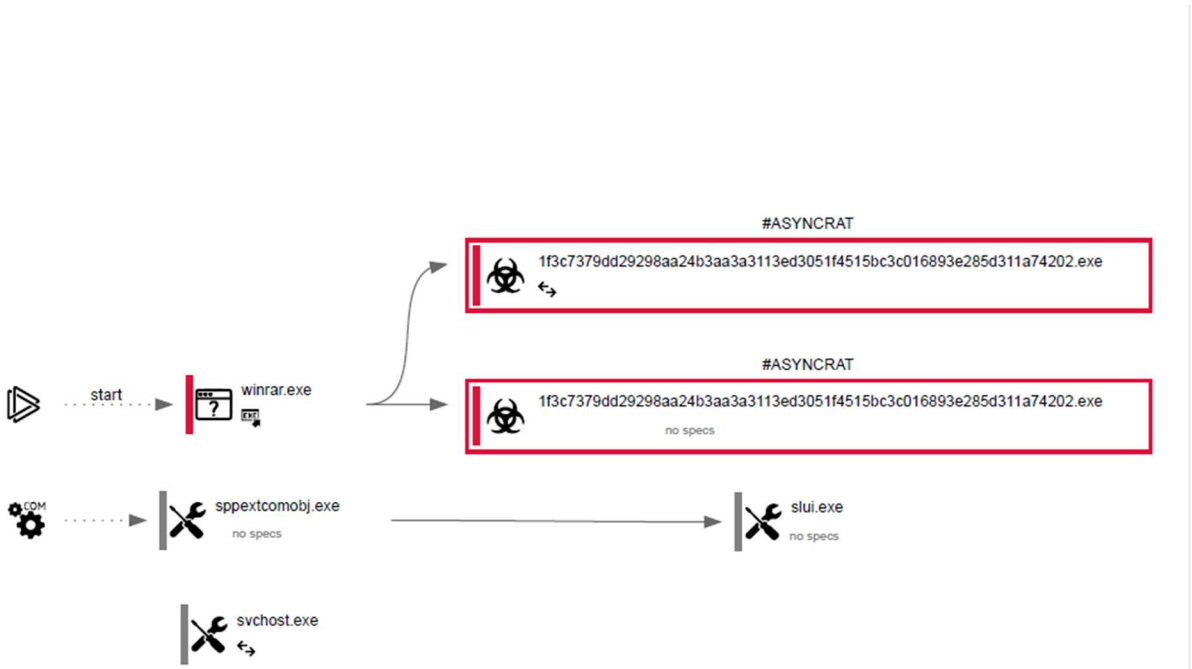
1. Conduct a full system scan using antivirus/EDR tools to ensure complete removal of malware artifacts.
2. Share Indicators of Compromise (IoCs) with relevant stakeholders and threat intelligence platforms to improve detection across the organization.

By implementing these steps, the potential harm caused by the malware can be mitigated effectively while strengthening defenses against similar attacks in the future.

Analysis of the 1f3c7379...zip

We analyzed the file 1f3c7379dd29298aa24b3aa3a3113ed3051f4515bc3c016893e285d311a74202.zip, identified as AsyncRAT v0.5.7B, a Remote Access Trojan (RAT). This malware enables attackers to remotely control infected systems, exfiltrate data, and establish persistence. It was detonated in the ANY.RUN sandbox, where we observed its behavior, including network activity, persistence mechanisms, and Indicators of Compromise (IoCs). Below are our findings and recommendations for mitigation.

Detonation Analysis



Process Tree Visualization

Behavior Observed

During detonation in the sandbox environment, the following activities were documented:

Process Activity

- The malware dropped an executable (1f3c7379...exe) into temporary directories and spawned multiple processes:
    - WinRAR.exe: Used to extract the malicious executable from the ZIP archive.
    - AsyncRAT executable (1f3c7379...exe): Initiated Command-and-Control (C2) communication and persistence mechanisms.
    - svchost.exe: Abused for network communication with legitimate services.

File System Changes

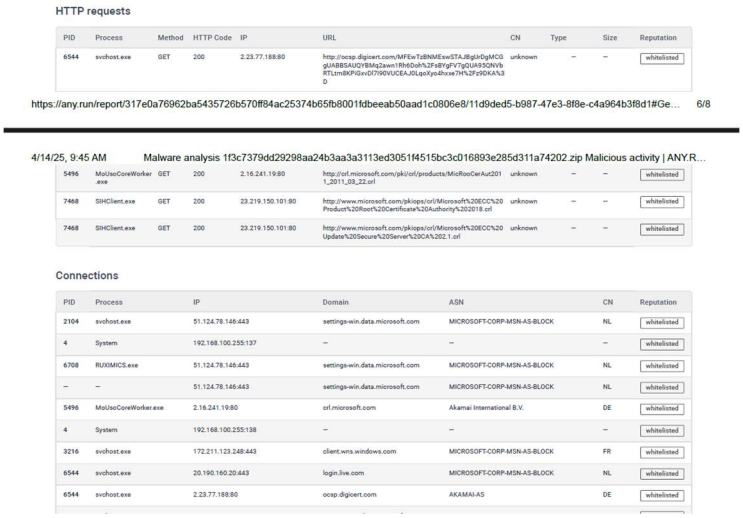
- Dropped files include:

- 1f3c7379dd29298aa24b3aa3a3113ed3051f4515bc3c016893e285d311a74202.exe in %AppData%\Local\Temp\.
- Encrypted configuration file (cred.dat) in %AppData%\WinRAR.

Registry Modifications

- Altered HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory to store extracted file paths for tracking purposes.

Network Behavior Analysis


HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
6544	svchost.exe	GET	200	2.23.77.188:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2Fs8YgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%30	unknown	–	–	whitelisted

https://any.run/report/317e0a76962ba5435726b570ff84ac25374b65fb8001fdbeeab50aad1c0806e8/11d9ded5-b987-47e3-8f8e-c4a964b3f8d1#Ge… 6/8

4/14/25, 9:45 AM Malware analysis 1f3c7379dd29298aa24b3aa3a3113ed3051f4515bc3c016893e285d311a74202.zip Malicious activity | ANY.R…

5496	MoUsoCoreWorker.exe	GET	200	2.16.241.19:80	http://crl.microsoft.com/pki/crl/products/MicRooCerAut2011_2011_03_22.crl	unknown	–	–	whitelisted
7468	SIHClient.exe	GET	200	23.219.150.101:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Product%20Root%20Certificate%20Authority%202018.crl	unknown	–	–	whitelisted
7468	SIHClient.exe	GET	200	23.219.150.101:80	http://www.microsoft.com/pkiops/crl/Microsoft%20ECC%20Update%20Secure%20Server%20CA%202.1.crl	unknown	–	–	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2104	svchost.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
4	System	192.168.100.255:137	–	–	–	whitelisted
6708	RUXIMICS.exe	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
–	–	51.124.78.146:443	settings-win.data.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
5496	MoUsoCoreWorker.exe	2.16.241.19:80	crl.microsoft.com	Akamai International B.V.	DE	whitelisted
4	System	192.168.100.255:138	–	–	–	whitelisted
3216	svchost.exe	172.211.123.248:443	client.wns.windows.com	MICROSOFT-CORP-MSN-AS-BLOCK	FR	whitelisted
6544	svchost.exe	20.190.160.20:443	login.live.com	MICROSOFT-CORP-MSN-AS-BLOCK	NL	whitelisted
6544	svchost.exe	2.23.77.188:80	ocsp.digicert.com	AKAMAI-AS	DE	whitelisted

Network Activity Table

Observed Network Activity

The following network patterns were captured during sandbox execution:

C2 Communication

- Connected to malicious domain donzola.duckdns.org (IP: 192.169.69.26) on port 2000, leveraging dynamic DNS services for resiliency.

Legitimate Connections

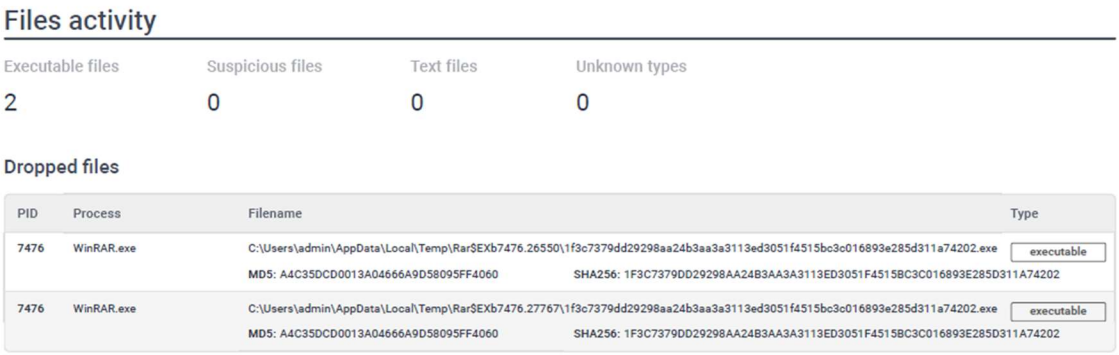
- Established connections to whitelisted domains such as:
    - settings-win.data.microsoft.com (Microsoft telemetry services).

- crl.microsoft.com (Certificate Revocation List checks).

Exfiltration Attempts

- Sent system GUID, computer name, and keystrokes to its C2 server.

Persistence Mechanisms



File System Changes

Identified Techniques

The malware employs several persistence mechanisms:

1. Registry Modification:
    - Alters registry keys (HKEY_CURRENT_USER\SOFTWARE\WinRAR\ArcHistory) to track extracted files.
2. Dropped Files:
    - Places encrypted configuration files (cred.dat) in %AppData%\WinRAR.
3. Dynamic DNS Usage:
    - Maintains communication with C2 infrastructure via dynamic DNS domains.

Indicators of Compromise (IoCs)

Type	Indicator

SHA256 Hash	1F3C7379DD29298AA24B3AA3A3113ED3051F4515BC3C016893E285D311A74202
MD5 Hash	A4C35DCD0013A04666A9D58095FF4060
Domains	donzola.duckdns.org
IP Addresses	192.169.69.26
Ports	2000
Files	%AppData%\WinRAR\cred.dat, %AppData%\Local\Temp\1f3c7379...exe

Action Plan

Containment Measures

1. Block all outbound traffic to the domain donzola.duckdns.org and IP address 192.169.69.26.
2. Remove dropped files such as cred.dat and the AsyncRAT executable from affected directories.
3. Review and delete any suspicious registry modifications under HKEY_CURRENT_USER\SOFTWARE\WinRAR.

Forensic Investigation

1. Analyze memory dumps for additional payloads or encryption keys used by AsyncRAT.
2. Investigate logs for evidence of data exfiltration or lateral movement.

System Hardening

1. Patch systems to address vulnerabilities that may have been exploited by the malware.
2. Restrict the use of dynamic DNS services within your network.
3. Deploy endpoint detection rules targeting AsyncRAT behaviors, such as mutex creation (AsyncMutex_iuykt5yr5ur58n8tnur8herjncr8tk) or unusual registry modifications.

The analysis of the two malware samples, PE32 Dropper (b773ca84...exe) and AsyncRAT Payload (1f3c7379...zip), highlights the sophisticated techniques attackers use to establish persistence, evade detection, and exfiltrate sensitive data.

The PE32 Dropper serves as the initial stage, leveraging legitimate Windows processes and Task Scheduler abuse to maintain persistence while appearing benign. It sets the groundwork for further malicious activity by dropping files and creating scheduled tasks.

The AsyncRAT Payload, on the other hand, is a fully functional Remote Access Trojan that enables attackers to remotely control infected systems, steal sensitive information such as keystrokes and system identifiers, and communicate with Command-and-Control (C2) servers using dynamic DNS services. Its use of encrypted communication and anti-analysis techniques like mutex creation demonstrates its advanced capabilities. By addressing these findings and implementing the recommended actions, we can mitigate the risks posed by these malware samples while strengthening defenses against similar threats in the future.

Microsoft July 2023 Patch Tuesday Vulnerability Management Report

The July 2023 Microsoft Patch Tuesday contained 132 vulnerabilities, including 37 Remote Code Execution (RCE) vulnerabilities. Six RCE vulnerabilities are actively exploited, posing an imminent risk to our organization. This report details our investigation, immediate action strategy, and recommended strategies for improving our security posture.

Part 1: Understanding the Risk

Summary of Patch Tuesday – July 2023

- Total vulnerabilities addressed: 132
- Remote Code Execution (RCE) vulnerabilities: 37
- Exploited in the wild: 6 RCE vulnerabilities

High-Risk Vulnerabilities

CVE-2023-36884 – Office and Windows HTML RCE Vulnerability

CVE-2023-35311 – Microsoft Outlook Spoofing Vulnerability

CVE-2023-32049 – Windows SmartScreen Security Feature Bypass

CVE-2023-36874 – Windows Error Reporting Privilege Escalation

CVE-2023-32046 – Windows MSHTML Platform RCE

CVE-2023-35332 – Windows Routing and Remote Access RCE

Implications

Business Operations Impact

- **Critical system downtime**
    - Exploited vulnerabilities may result in system disruptions that disrupt critical company activities.
    - Customer-facing applications may encounter disruptions, reducing revenue cultivation.
- **Productivity Loss**
    - Staff could momentarily be unable to access important Microsoft apps
    - Disruption of usual workflow during vulnerability remediation efforts.

Data Security Implications

- **Intellectual Property Risk:**
    - CVE-2023-36884 vulnerability in Microsoft Office apps may disclose proprietary documents.
    - Exploiting systems may jeopardize research and development data.
- **Customer Data Exposure:**
    - Personally identifiable information (PII) kept in enterprise systems might be compromised.
    - Customer financial data may be targeted by attackers using these vulnerabilities.

Financial Impact Analysis

- **Direct costs**
    - Labor expenses for emergency response and remediation are anticipated to be between 120 and 160 person-hours.
    - Potential system restoration expenses if systems are affected. Possible need for external security specialists to resolve complicated attacks.
- **Indirect costs**
    - Brand reputation impact caused by prospective security problems.
    - Loss of customer trust after a security breach.
    - Increased insurance rates due to security incidents

Part 2: Immediate Action Plan

Prioritization Matrix

Vulnerability ID	Severity	Exploited	Affected Systems	Priority
CVE-2023-36884	Critical	Yes	Office/Windows	High
CVE-2023-35311	High	Yes	Outlook	High
CVE-2023-32049	High	Yes	Windows Defender	High
Remaining RCEs	Varies	No	Mixed	Medium

Action Plan

1) Phase One: Preparation and Risk Assessment

a) Asset Inventory Review.

Objective: Identify all computers that run Microsoft software.

Actions:

- Retrieve the current asset list from a CMDB or asset management platform.
- Categorize systems as critical (e.g., finance, executive devices), high-usage, or legacy.
- Identify systems that are connected to the internet or handle sensitive information.
- Generate a comprehensive inventory of affected systems.

b) Vulnerability Exposure Mapping:

- Cross-reference asset list with CVEs from Microsoft's July Patch Tuesday.
- Identify which systems are affected by:
    - Actively exploited vulnerabilities (e.g., CVE-2023-36884, CVE-2023-35311).
    - High-risk vulnerabilities having the possibility for lateral movement or privilege escalation.

c) Change Management Preparations

- Send a change request for patch deployment to the Change Advisory Board (CAB), which will include:
    - Impact evaluation.
    - Rollback strategy.
    - Test schedule.
    - Communication timeline.

2) Phase 2: Testing & Staging

a) Patch Test Environment

- Use a virtualized test environment to simulate production.
- Include a variety of Windows operating system versions, MS Office setups, and domain-joined and independent computers.
- Download all essential patches from the Microsoft Update Catalog.
- Use checksums to verify the integrity of the patch file.
- Test for:
    - The system stability
    - Compatible with business-critical applications.
    - Endpoint behavior after patching.

b) Pre-deployment snapshots.

- Take virtual machine (VM) snapshots or system images of sample endpoints and servers.
- Confirm that rollback is functional in the event of a patch failure.

3) Phase 3: Deployment Strategy

a) Deployment Tools

- **Tools used**: Microsoft Endpoint Configuration Manager (SCCM), Windows Server Update Services (WSUS), Intune (for cloud endpoints).
    - **Action:**
        - Schedule a staggered rollout.
        - Use maintenance windows to reduce business disturbance.
        - Check deployment logs for errors or anomalies.

4) Phase 4: Post-Deployment Monitoring

a) Validation.

- Use SCCM compliance reports or PowerShell scripts to confirm:
- Patches were installed successfully.
- No key services were interrupted.
- Reboots of the system were performed when needed.

b) Rollback Handling

- Maintain the ability to roll back patches from test snapshots or remove updates via CLI.
- Keep track of helpdesk tickets for issues reported by users.

5) Communication Plan

a) Stakeholder notification (pre-deployment)

- The target audience includes all employees, department leaders, IT, compliance, and executives.
- Method: Email plus internal portal announcement.
    - Content:
        - Summary of upcoming security updates.
        - Why the updates are crucial.
        - Expected consequences (for example, restarts and temporary slowdowns).

- Timeline for deployment.

b) Technical Team Briefing.

- Conduct a briefing with the IT support and infrastructure staff.
- Share:
  - Complete patch notes.
  - Asset Targeting List.
  - Escalation procedure for patch-related failures.

c) Post-Deployment Communications

- Send a confirmation email after the patching is completed.
- Email should include:
  - Summary of fixes that have been applied.
  - Systems were successfully upgraded.
  - Any important occurrences or resolutions.
  - Reminder to notify IT of any new concerns.

Mitigation Plan for Unpatched Serious Vulnerabilities

1) **Threat detection and monitoring.**

   a. Enable advanced threat protection.

- To identify exploitation activities, use technologies such as Microsoft Defender for Endpoints, Sysmon, and EDR solutions.
- Monitor logs for IOCs (Indicators of Compromise) associated with CVEs that have not been patched.

b) Real-time alerting

- Set up using a SIEM (Microsoft Sentinel):

- Custom alert rules for unusual activities.
- Watchlists for files, registry changes, and processes linked to known vulnerabilities.

2) Vulnerability Isolation:

a. Network Segmentation

- Isolate susceptible systems from the larger network.
- Transfer them to dedicated VLANs or firewall zones.
- Limit access via Access Control Lists (ACLs).

b. Limit external exposure.

- Block inbound internet traffic to vulnerable endpoints/services.
- Use application firewalls to filter out certain protocols or requests
- Implement network behavior analysis tools.
- Conduct frequent traffic analysis evaluations.

3) Endpoint Protection Measures

a) Application Control Enforcement

- Enable application whitelisting on vulnerable systems.
- Prevent execution from temporary folders and user profiles.
- Limit script execution (PowerShell, VBScript, etc.)
- Deploy Microsoft's attack surface reduction rules.

b) System Hardening

- Disable susceptible features and components wherever feasible.
- Remove any unwanted software and services.
- Implement the least privilege access constraints.
- Apply secure configuration baselines.

c) Memory Protection

- Enable the Exploit Protection features in Windows Defender.
- Configure data execution prevention (DEP) for all programs.
- Implement third-party exploit mitigation tools.

Part 3: Long-term Vulnerability Management Strategy

1) Improvements to the Vulnerability Management Program

a) Program Structure and Governance.

- Establish a formal vulnerability management program.
    - Establish a specialized vulnerability management team with clear roles and responsibilities.
    - Create and record formal vulnerability management policies and processes.
    - Set up a governance framework with executive sponsorship.
    - Establish key performance indicators (KPIs) to assess program efficiency.
- Cross-functional Vulnerability Management Committee
    - Create a committee with representation from IT, security, risk management, and business units.
    - Organize monthly meetings to analyze vulnerability metrics and handle issues.
    - Facilitate communication among security teams and business stakeholders.
    - Ensure that security goals are aligned with business objectives.
- Policy Development and Implementation
    - Create a thorough vulnerability management policy that specifies:
        - Scan frequency requirements
        - Timeframes for remediation depend on the degree of the vulnerability
        - Exception Management Processes

        - Roles and duties
    - Create standard operating procedures for all aspects of vulnerability management.
    - Implement a structured exception procedure, including risk acceptance documentation.

b) Risk-Based Approach to Vulnerability Management

- Asset Classification Framework
- Set up a formal asset classification system based on:
    - Business Criticality
    - Data sensitivity
    - Exposed to external risks
    - Regulatory requirements
- Use categorization to drive vulnerability prioritization.
- Review and update asset classifications quarterly.

c) Patch Management Process Improvements

- Standardized Patch Cycle Implementation
- Establish a consistent monthly patching plan that aligns with vendor release cycles.
- Develop a standardized protocol for patch testing, approval, and deployment.
- Define the emergency patch methods for major vulnerabilities.
- Document the rollback processes for each system type.

d) Automation Implementation

- Implement an enterprise patch management solution with centralized control.
- Implement automatic patch compliance reporting.
- Configure automated deployment of low-risk systems and fixes.

- Create scripted deployment techniques for complicated systems.

e) Test and Validation Procedures

- Create a specialized testing environment that reflects production.
- Create standardized testing methodologies for various system kinds.
- Create application-specific tests for essential business systems.
- Establish sign-off requirements prior to production deployment.

Android Device Security Assessment and MDM Implementation Strategy

Overview

Our organization has 250 outdated Android smartphones (50% of our fleet) and no Mobile Device Management solution in place, posing serious security issues. This study offers a thorough evaluation and strategic roadmap for addressing these risks. The deliberate execution of these recommendations will considerably minimize our present security vulnerability while developing long-term strategies for managing mobile device security.

Part 1: Understanding the Risk

Specific Vulnerabilities Identified:

CVE-2023-26083

- Severity: High. (CVSS 8.8)
- Impact: Remote code execution vulnerability in the Android System component.
- Affected versions include Android 10, 11, 12, 12L, and 13.
- Risk: Attackers might remotely execute arbitrary code with elevated privileges without user intervention, potentially resulting in full device compromise.

CVE-2021-29256

- Severity: Critical (CVSS: 9.8).
- Impact: A vulnerability in Qualcomm components used in many Android smartphones allows for remote code execution.

- Affected Versions: Multiple Android versions utilizing specific Qualcomm chipsets.
- Risk: Allows attackers to execute malware via specially crafted network packets.

CVE-2023-2136

- Severity: High. (CVSS 7.8)
- Impact: Privilege escalation vulnerability in the Android Framework.
- Affected versions include Android 11, 12, 12L, and 13.
- Risk: Allows local attackers to get elevated system rights without authorization.

Risk Assessment for Outdated Devices

Devices 1+ Year Out of Date (40% = 200 devices):

- Missing vital security updates for known vulnerabilities.
- Increased vulnerability exposure.
- Unpatched system programs may be exploitable
- Risks associated with data leaks and illegal access

Devices 2+ Years Out of Date (10% = 50 devices):

- Significantly greater risk profile, with many serious vulnerabilities left unpatched.
- Possibly insufficient protection against common attack vectors.
- Manufacturers may stop providing security upgrades.
- Possible entry points for lateral movement into the organization's network.

Part 2: Short-term Action Plan

Immediate Actions

Device Inventory and Prioritization

- Conduct an inventory of all 500 Android devices.
- Identify particular OS versions, patch levels, and hardware requirements.
- Prioritize updates for devices with significant vulnerabilities.

User Communication Strategy

- Send an organization-wide security alert explaining the urgency (without causing panic)
- Create a tiered communication plan:
    - Immediate attention (2+ years outdated)
    - Urgent attention (1+ year outdated)
    - Standard update reminder (all others)

Update Deployment

- Establish temporary update stations in common areas
- Schedule department-specific update windows
- Provide clear step-by-step update instructions:
    - Connect to corporate WiFi (not cellular data)
    - Navigate to Settings > System > System Update
    - Download and install all available updates
    - Restart the device when prompted

Troubleshooting Support

- Create a dedicated email address for update assistance
- Schedule "update clinics" for hands-on support
- Develop FAQ document addressing common update problems

Implementation Timeline

Week 1

- Complete inventory and risk assessment
- Deploy communications
- Set up support infrastructure

Week 2

- Begin updates for the highest-risk devices (2+ years outdated)
- Run first update clinics
- Track progress and adjust strategy as needed

Weeks 3-4

- Complete updates for all devices
- Document any devices that cannot be updated
- Prepare replacement recommendations for incompatible devices

Part 3: Long-term Strategy

MDM Solution Evaluation

Solution	Key Features	Pros / Cons
Microsoft Intune	Device enrollment, app management, conditional access	Pros: Strong integration with Microsoft ecosystem, policy-based management Cons: Higher cost, complex initial setup
VMware Workspace ONE	UEM capabilities, advanced security	Pros: Comprehensive features, excellent for BYOD Cons: Complex administration, higher learning curve
MobileIron	Zero trust security, threat defense	Pros: Strong security focus, good for regulated industries Cons: Can be resource-intensive
ManageEngine MDM	Basic MDM functionality, cost-effective	Pros: Simple interface, good value option Cons: Fewer advanced features

IBM MaaS360	AI security analytics, containerization	Pros: Strong security features, detailed reporting Cons: Higher cost for full feature set

Comprehensive Update Policy Recommendations

Regular Update Schedule

- Mandatory security updates within 30 days after release.
- OS version changes are assessed within 90 days after the stable release.
- Monthly compliance report to department heads.

Device Lifecycle Management

- Maximum device age: 3 years
- Maximum OS version lag: 1 major version
- Automatic flagging of non-compliant devices

User Education Program

- Quarterly security awareness training
- Update procedure documentation in employee handbook
- Security bulletin board with current threat information

Recommended Solution

Given the organization's size (500 devices) and present absence of MDM infrastructure, I propose adopting Microsoft Intune or ManageEngine MDM, depending on your existing infrastructure and financial constraints:

- In a Microsoft-centric environment, Intune offers seamless interaction with current Microsoft products as well as excellent security measures, despite its greater cost.
- If you're on a tight budget, ManageEngine provides a decent blend of critical functionality at a cheaper cost.

Implementation Roadmap

Immediate (1-3 months)

- Select and procure MDM solution
- Establish a pilot group of 50 devices
- Develop policies and configurations

Short-term (3-6 months)

- Full deployment across all devices
- User training and support
- Integration with existing security systems

Long-term (6-12 months)

- Regular security posture reviews
- Policy refinement based on metrics
- Consider enhanced threat protection add-ons

Future Device Strategy Recommendations

Consider a Managed Device Program

- Consider migrating to organization-owned devices with uniform setups.
- Implement periodic device refresh cycles (every 2-3 years).
- Create minimal security requirements for new device purchases.

BYOD Policy Enhancement

- If BYOD continues, develop more rigid enrollment criteria.
- Consider containerization of company data.
- Establish specific security criteria for personal devices.

Zero Trust Implementation

- Move toward the continuous verification model.

- Implement conditional access policies.
- Enforce encryption and provide safe authentication.

Appendix: Incidence Playbooks

CyberBulwork Malware Incident playbook

According to CyberBulwork's incident response policy, the Cyber Security Incident Response Team (CSIRT) is activated whenever a cybersecurity incident is detected, leveraging the appropriate incident response playbook to guide actions. The CSIRT comprises the core IT and cybersecurity teams, with extended support from legal, compliance, public relations, and executive leadership. This collaborative approach ensures that technical containment and resolution efforts are complemented by adherence to regulatory requirements and effective communication with internal and external stakeholders.

The CSIRT's primary responsibilities include identifying and analyzing threats, containing the impact, eradicating malicious elements, recovering affected systems, and conducting post-incident reviews to strengthen organizational resilience. Legal representatives ensure compliance with applicable laws and regulations, public relations specialists manage external communications to preserve CyberBulwork's reputation, and executive leadership provides oversight and allocates resources to support the team's efforts. By maintaining this multidisciplinary structure, CyberBulwork ensures a swift and comprehensive response to cybersecurity incidents while minimizing operational disruptions.

Preparation Phase

Category	Action	Details
Asset Inventory Management	- Maintain an up-to-date inventory of all hardware, software, and systems.	Use tools like CMDB or asset management platforms to track assets critical to operations.
	- Identify critical systems and high-value targets (e.g., VIP users, finance systems).	Classify assets based on sensitivity, business impact, and exposure to external threats.
	- Regularly update the inventory to reflect changes in the environment.	Conduct quarterly reviews of asset classifications.
Vulnerability Assessment	- Conduct regular vulnerability scans using tools like Nessus or Qualys.	Focus on identifying known vulnerabilities in critical systems and applications.
	- Map vulnerabilities to affected systems using CVE databases.	Prioritize vulnerabilities actively exploited in the wild (e.g., CVE-2023-36884).

Patch Management	- Establish a standardized patching schedule aligned with vendor release cycles.	Implement monthly patch cycles and emergency patching for critical vulnerabilities.
	- Test patches in a controlled environment before deployment.	Use virtualized test environments to simulate production systems for compatibility testing.
	- Maintain rollback plans for failed patches.	Take system snapshots or VM backups before deploying patches.
Threat Intelligence	- Subscribe to threat intelligence feeds (e.g., VirusTotal, AbuseIPDB).	Monitor for Indicators of Compromise (IoCs) relevant to your organization's environment.
	- Share IoCs with industry partners and threat intelligence platforms.	Enhance collective defense by contributing findings from incidents.
Incident Response Planning	- Develop and maintain incident response playbooks for common attack scenarios (e.g., phishing, malware).	Include detailed steps for detection, containment, eradication, recovery, and communication.
	- Conduct tabletop exercises to simulate incident scenarios and test response plans.	Involve cross-functional teams (IT, legal, HR) in exercises for comprehensive preparedness.
Security Awareness Training	- Conduct regular training sessions on phishing recognition and reporting procedures.	Tailor training for high-risk groups like executives or finance teams.
	- Implement phishing simulation exercises to test employee awareness and response.	Provide feedback and additional training based on results of simulations.
Access Control Policies	- Enforce Multi-Factor Authentication (MFA) for all users, especially privileged accounts.	Ensure MFA is mandatory for remote access and sensitive applications.
	- Restrict access based on the principle of least privilege.	Regularly review access permissions to ensure they align with job roles and responsibilities.
Network Segmentation	- Segment networks to isolate critical systems from less secure environments.	Use VLANs or firewall rules to limit lateral movement during an attack.
	- Restrict external access to sensitive systems using IP whitelisting or VPNs.	Ensure only authorized users can access critical resources remotely.
Endpoint Protection	- Deploy Endpoint Detection and Response (EDR) solutions across all endpoints.	Monitor endpoints for suspicious activity in real-time using tools like CrowdStrike or SentinelOne.

	- Enable application whitelisting to prevent unauthorized software execution.	Block execution from temporary folders or user profiles where malware often resides.

Detection Phase

Section	Activity	Details/Examples
Automated Detection Systems	Email Gateway Filters	- Flag suspicious/mimicked internal sender domains - URL reputation scanning - Attachment scanning (executables focus)
	SIEM Correlation Rules	- Correlate email-based IOCs - Alert on patterns from past incidents - Rule for brute-force (failed + successful login attempts)
	Endpoint Detection	- Detect browser redirects from email links - Alert on file downloads from email links - Monitor connections to IPs like 150.158.77.170, 124.120.140.202, etc.
User-Based Detection	Reporting Mechanism	- Central mailbox: suspicious@cyberbulwork.com - One-click report button in email client
	Behavioral Indicators	- Generic greetings (e.g., “Hey Team”) - Unclear links/download prompts - Use of personal emails (e.g., @gmail.com)

		- Poor branding or inconsistent formatting
	Contextual Awareness	- Unexpected code review requests - Suspicious download prompts - Unusual software update messages - Team-building links with odd URLs
Proactive Detection Processes	Header Analysis	- Check for spoofing - Identify suspicious routing paths - Mismatch in From/Reply-To - Originating IPs from risky regions
	Threat Hunting	- Look for "team-building activity" phrasing - Detect keywords like "update," "security," or "download" - Watch for known/new phishing domains - Detect lateral movement
	Domain Reputation Checks	- Use VirusTotal, AbuseIPDB, internal DBs for checking domain/IP reputation
Detection Response Workflow	Initial Alert Triage	- Identify alert source (user or system) - Classify severity by type/volume - Log alert in IR system
	Preliminary Analysis	- Extract sender, links, attachments

		- Check sender reputation & headers - Document pattern anomalies - Search for similar past alerts
	Threat Confirmation	- Analyze in sandbox - Compare with known IOCs - Use threat intelligence feeds - Determine targeted vs. broad campaign
	Detection Escalation	- Escalate confirmed threats to containment - Hand over full analysis to IR team - Update detection systems - Notify stakeholders per plan

Containment Phase

Objective: Isolate threats to prevent lateral movement, data exfiltration, or further damage.

Immediate Containment Actions

Action	Details	Example from Incidents
Isolate Affected Systems	Disconnect compromised devices from the network. Use VLAN segmentation or firewall rules.	VIP host remacdmzma01 was isolated after downloading Catalogue.rar.
Block Malicious IoCs	Update firewalls, EDR, and email filters to block domains, IPs, and file hashes.	Blocked theannoyingsite.com and IP 209.85.215.1701.
Terminate Malicious Processes	Use EDR tools to kill processes like schtasks.exe or werfault.exe spawned by malware.	Terminated diskpart.exe (SHA-256: ed01ebf...).

Disable Compromised Accounts	Suspend accounts linked to suspicious logins (e.g., Erwin Smith).	Revoked sessions for IPs 150.158.77.170 (China) and 124.120.140.202 (Thailand).
Preserve Evidence	Capture memory dumps, logs, and malware samples for forensic analysis.	Preserved AsyncRAT executable (1f3c7379...exe) and crash dumps.

Threat-Specific Containment

Threat Type	**Steps**
Phishing	Quarantine emails, disable embedded links, and notify recipients.
Malware	Remove persistence mechanisms (e.g., scheduled tasks like Windows Update BETA).
Unauthorized Access	Restrict access to critical systems using conditional policies (e.g., allow only UK IPs).
Ransomware	Disable SMBv1, suspend backups to prevent encryption, and halt suspicious services.

Recovery Phase

Objective: Restore systems to a secure, operational state while mitigating recurrence risks**.**

System Restoration

Action	**Details**	**Example**
Restore from Backups	Use verified clean backups. Validate file integrity pre-deployment.	Restored VIP workstation after Catalogue.rar incident.
Rebuild Compromised Systems	Reimage endpoints if backups are unavailable or corrupted.	Rebuilt systems infected by AsyncRAT.
Patch Vulnerabilities	Deploy patches for exploited CVEs (e.g., CVE-2023-36884).	

Credential Management

Step	Execution
Password Resets	Enforce resets for compromised accounts and privileged users.
Enable MFA	Implement MFA globally, especially for VIPs and admin accounts.

Post-Recovery Validation

Task	Tools/Methods
Verify System Integrity	Use checksums, file integrity monitoring (FIM), and antivirus scans.
Test Critical Functions	Confirm business apps (e.g., payroll systems) operate normally.
Monitor for Resurgence	Deploy EDR alerts for known IoCs (e.g., donzola.duckdns.org).

Communication and Reporting

Stakeholder	Actions
Internal Teams	Notify IT, legal, and management of containment status.
External Partners	Share IoCs with threat intel platforms (e.g., VirusTotal, ISACs).
Regulators	Disclose breaches per GDPR/CCPA if sensitive data was exposed.

Post-Incident Phase

This phase focuses on analyzing the incident, improving defenses, and ensuring organizational resilience. Below is a structured approach to post-incident activities, aligned with industry best practices and frameworks like NIST SP 800-61.

Post-Incident Review and Documentation

Objective: Systematically evaluate the incident response process and identify improvements.

Step	Actions	Details
Incident Debrief	Conduct a blameless post-mortem meeting with all stakeholders (IT, legal, PR, leadership).	Discuss timelines, response effectiveness, and gaps using tools like chronological event logs.
Root Cause Analysis (RCA)	Identify root causes using methods like the **5 Whys** or **Fishbone Diagram**.	Example: If phishing caused a breach, determine why filters failed or why users clicked malicious links.
Document Findings	Compile a detailed report covering: - Incident timeline - Impact assessment - Lessons learned - Actionable recommendations.	Share findings with leadership and update the Incident Response Plan (IRP)

Continuous Improvement

Objective: Implement changes to prevent recurrence and strengthen security posture.

Step	Actions	Details
Update IRP and Playbooks	Revise procedures based on lessons learned (e.g., enhancing phishing detection rules).	Incorporate new IoCs, response steps, or tools identified during the incident.
Enforce Security Controls	Address vulnerabilities exposed by the incident: - Patch systems - Strengthen access controls - Deploy advanced monitoring.	Example: Enable MFA globally after credential theft
Conduct Training	Provide targeted security awareness sessions for staff and technical workshops for IT teams.	Simulate phishing attacks or tabletop exercises to test updated protocols.

Stakeholder Communication and Compliance

Objective: Ensure transparency and meet regulatory obligations.

Step	Actions	Details
Internal Reporting	Share a summarized incident report with executives, legal, and affected departments.	Highlight business impact, remediation steps, and future risk mitigation
External Disclosure	Notify regulators, customers, or partners if sensitive data was compromised.	Follow GDPR, CCPA, or other applicable laws
Threat Intelligence Sharing	Submit IoCs (e.g., malicious IPs, hashes) to platforms like VirusTotal or ISACs.	Enhance collective defense and reputation

Metrics and KPIs for Evaluation

Track post-incident performance using:

Metric	Purpose
Mean Time to Detect (MTTD)	Measure how quickly incidents are identified.
Mean Time to Respond (MTTR)	Assess efficiency of containment and eradication.
Recurrence Rate	Track repeat incidents to validate control effectiveness

By following this playbook, CyberBulwork can transform incident lessons into actionable improvements, reducing future risks and enhancing cyber resilience.

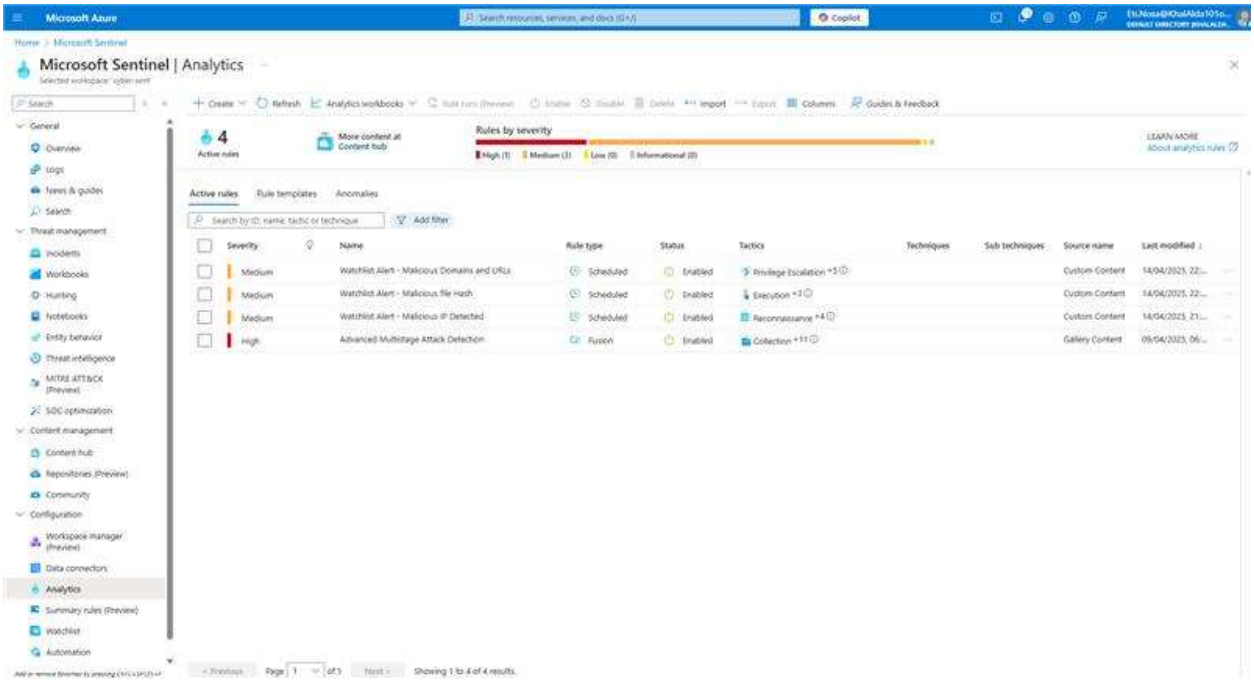
Appendix: Creating Custom Alerts

Creating Custom Alerts

At Cyberbulwork, we have implemented a robust threat detection framework in Microsoft Sentinel, leveraging custom analytics rules and watchlists to proactively identify and respond to emerging threats. This report details our current configuration, the integration of critical Indicators of Compromise (IoCs), and our ongoing commitment to security excellence.

Custom Analytics Rules Overview

We have established four active custom analytics rules in Microsoft Sentinel, each tailored to detect specific threat vectors relevant to our environment. These rules are categorized by severity and mapped to MITRE ATT&CK tactics and techniques for comprehensive coverage.



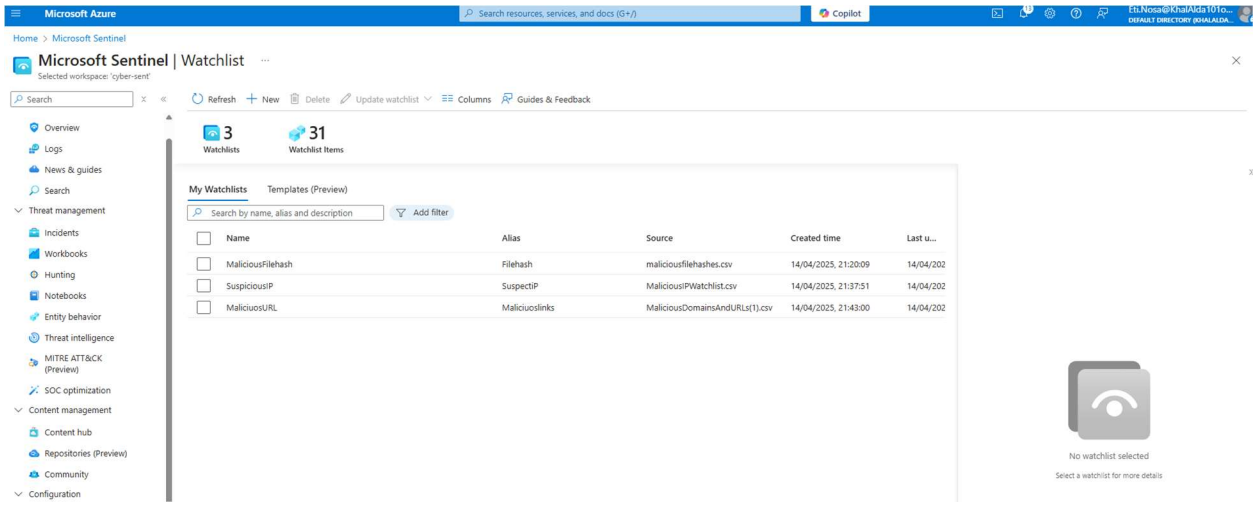
Scheduled Query Rule

This screenshot provides a summary of our active analytics rules, their severity, type, and mapping to MITRE ATT&CK tactics and techniques.

Severity	Rule Name	Rule Type	Status	Tactics	Techniques	Last Modified
Medium	Watchlist Alert - Malicious Domains and URLs	Scheduled	Enabled	Privilege Escalation	Collection	14/04/2025
Medium	Watchlist Alert - Malicious file hash	Scheduled	Enabled	Execution	Execution	14/04/2025
Medium	Watchlist Alert - Malicious IP Detected	Scheduled	Enabled	Reconnaissance	Reconnaissance	14/04/2025

Watchlist Integration

To enhance our detection capabilities, we have created and actively maintain three dedicated watchlists. These watchlists are automatically referenced by our custom rules to ensure rapid identification of known malicious entities.



Watchlist

This screenshot shows our three active watchlists, the number of items in each, and their sources.

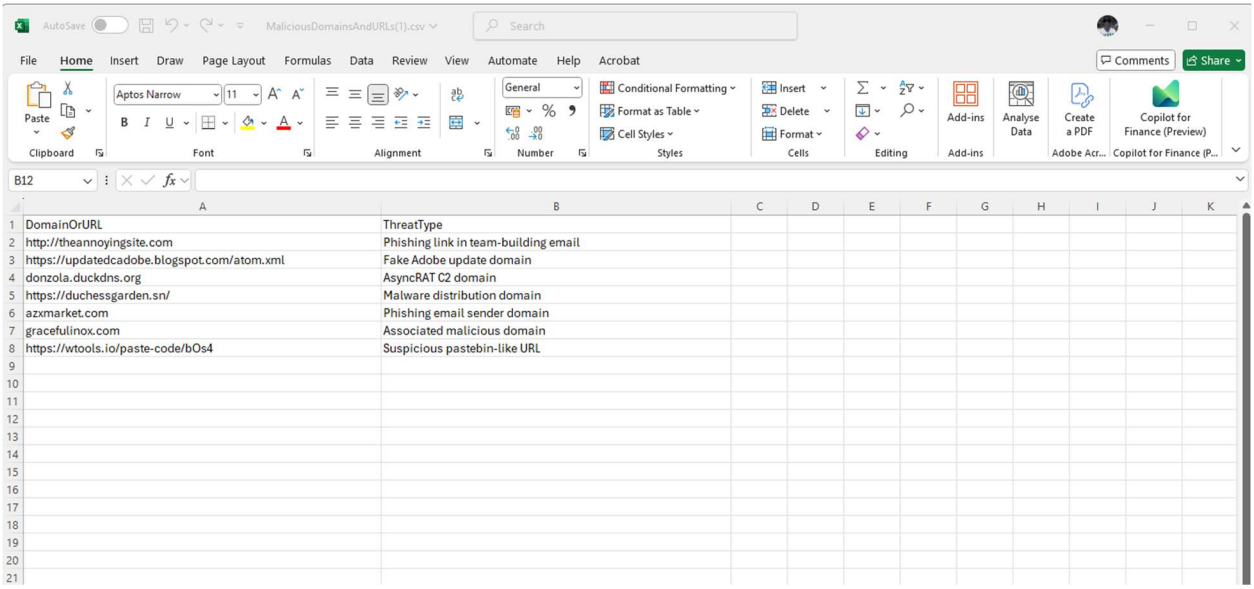
Name	Alias	Source File	Created Time
MaliciousFilehash	Filehash	maliciousfilehashes.csv	14/04/2025, 21:20:09

SuspiciousIP	SuspectIP	MaliciousIPWatchlist.csv	14/04/2025, 21:37:51
MaliciousURL	Maliciouslinks	MaliciousDomainsAndURLs(1).csv	14/04/2025, 21:43:00

Currently, our watchlists contain a total of 31 unique threat indicators, ensuring broad coverage of the latest IoCs relevant to our sector.

Malicious Domains and URLs

Our MaliciousURL watchlist is populated with high-risk domains and URLs directly linked to recent threat activity targeting Cyberbulwork. Each entry is classified by threat type for context-aware alerting.



	A	B
1	DomainOrURL	ThreatType
2	http://theannoyingsite.com	Phishing link in team-building email
3	https://updatedcadobe.blogspot.com/atom.xml	Fake Adobe update domain
4	donzola.duckdns.org	AsyncRAT C2 domain
5	https://duchessgarden.sn/	Malware distribution domain
6	azxmarket.com	Phishing email sender domain
7	gracefulinox.com	Associated malicious domain
8	https://wtools.io/paste-code/bOs4	Suspicious pastebin-like URL

Malicious IP and Domains & URL Watchlist

This screenshot displays the contents of our MaliciousDomainsAndURLs(1).csv watchlist, showing the domains/URLs and their associated threat types.

Domain/URL	**Threat Type**
http://theannoyingsite.com	Phishing link in team-building email
https://updatedcadobe.blogspot.com/atom.xml	Fake Adobe update domain
donzola.duckdns.org	AsyncRAT C2 domain
https://duchessgarden.sn/	Malware distribution domain
azxmarket.com	Phishing email sender domain

gracefulinox.com	Associated malicious domain
https://wtools.io/paste-code/bOs4	Suspicious pastebin-like URL

Security Posture and Next Steps

Our approach ensures:

- Real-time detection of malicious domains, IPs, and file hashes
- Automated correlation of multistage attacks
- Alignment with industry-standard frameworks (MITRE ATT&CK)
- Rapid response to emerging threats through dynamic watchlist updates

Next Steps:

- We will continue to refine rule severity based on threat intelligence and incident outcomes.
- Our team will expand behavioral analytics to detect advanced persistence and lateral movement techniques.
- Regular reviews of watchlist content will ensure our detection capabilities remain current and effective.

Through the strategic deployment of custom analytics rules and comprehensive watchlists in Microsoft Sentinel, we at Cyberbulwork have significantly enhanced our organization's ability to detect, analyze, and respond to a wide range of cyber threats. The integration of relevant Indicators of Compromise (IoCs) into our detection framework ensures that our security operations remain proactive and aligned with industry best practices.

Our current setup not only provides real-time visibility into malicious activities targeting our environment but also enables us to automate and streamline our incident response processes. By continuously updating our watchlists and refining our detection rules, we are committed to maintaining a resilient security posture that can adapt to the evolving threat landscape.

As we move forward, Cyberbulwork will continue to invest in advanced threat detection capabilities, regular review of our security controls, and ongoing staff training. These efforts will ensure that we remain vigilant, responsive, and prepared to defend our organization against both current and emerging cyber risks.

Appendix: Meeting Minutes

CyberBulwork

SECURITY OPERATIONS SPRINT: 6TH APRIL 2025, 8:00 PM - 8:40 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Oluwaseyi Adebayo
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda

AGENDA

- Overview of the security operation task

NOTES/KEY DISCUSSIONS

Sprint 5 Leadership:

- Etinosa Imafidon, Daniel Owoeye-Wise, and Alli-Balogun Luqman Damilare were assigned leadership to lead the security operation sprint, the last internship sprint.

Team Research Assignment

- All members are expected to go through the task before the next meeting.
- Findings from the research and Azure setup will be discussed in the next meeting, scheduled for Monday, 7th April, 2025.

Task Delegation:

- Technical Report Writing: Ololade Elizabeth Adesagba and Shado Peculiar Unini volunteered to carry out this task.
- PowerPoint Slides Preparation: Dike Promise Chimamanda and Motunrayo Sanusi volunteered to work on the slides.

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Monday, 7th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 8:39 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Oluwaseyi Adebayo
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi

CyberBulwork

SECURITY OPERATIONS SPRINT: 7TH APRIL 2025, 8:00 PM - 8:40 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda

AGENDA

- Overview of the security operation task

NOTES/KEY DISCUSSIONS

Sprint 5 Leadership:

- Etinosa Imafidon, Daniel Owoeye-Wise, and Alli-Balogun Luqman Damilare were assigned leadership to lead the security operation sprint, the last internship sprint.

Team Email/Response Analysis Assignment - Link

One of the tasks in this sprint is to Investigate Active Email Threats sent to staffs of our organization. Each team member was assigned a threat to work on.

- Affiliate marketing best practices: **Etinosa Imafidon**
- Code review request: **Motunrayo Sanusi** & **Dike Promise Chimamanda**
- Download updated project: **Muizz Babatunde Majeed** & **Daniel Owoeye-Wise**
- Important Adobe update: **Alli-Balogun Luqman Damilare** & **Shado Peculiar Unini**
- Team building activity: **Ololade Elizabeth Adesagba** & **Oluwaseyi Adebayo**

Task Delegation:

- Technical Report Writing: Ololade Elizabeth Adesagba and Shado Peculiar Unini volunteered to carry out this task.
- PowerPoint Slides Preparation: Dike Promise Chimamanda and Motunrayo Sanusi volunteered to work on the slides.

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Tuesday, 8th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10:00p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi

CyberBulwork

SECURITY OPERATIONS SPRINT: 8TH APRIL 2025, 8:00 PM – 09:40 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi

- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- Initial phishing campaign investigation
- Investigate Active Email Threats

NOTES/KEY DISCUSSIONS

- Discussed the suspicious “team-building activity” email.
- Shina reported the phishing email and its link to http://theannoyingsite.com
- AnyRun analysis confirmed browser manipulation tactics. Decisions:
- Quarantine all similar emails.
- Increase user awareness messaging on social engineering.

Additional Notes:

- The team will meet again on Wednesday, 9th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 9:40 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare

- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 9TH APRIL 2025, 8:00 PM - 10PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- File detonation results & threat intelligence updates

NOTES/KEY DISCUSSIONS

- Reviewed sandbox analysis of Catalogue.rar containing diskpart.exe.
- Confirmed SHA-256 match with known malware signature.
- Identified persistence via scheduled task “Windows Update BETA, Decisions:
- Create SIEM alert rules for dropped file hashes.

- Notify VIP users about email attachment risks.

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Thursday, 10th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 10TH APRIL 2025, 8:00 PM - 10:40 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise

- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- Vulnerability Management: Microsoft Patch Tuesday

NOTES/KEY DISCUSSIONS

- **Overview of the July 2023 Patch Tuesday:**

The team reviewed Microsoft's release of **132 vulnerabilities**, highlighting **37 Remote Code Execution (RCE)** flaws and **6 actively exploited vulnerabilities**. Critical CVEs impacting **Office**, **Windows HTML components**, **Outlook spoofing**, **SmartScreen**, and **privilege escalation paths** were prioritized for immediate attention.

- **Vulnerability Scoping and Asset Identification:**

Using internal asset inventory tools, the team mapped vulnerabilities to specific business-critical systems. High-risk systems were identified based on exposure level, user role, and data sensitivity, forming the basis for a **risk-based patching sequence**.

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Friday, 11th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10:40 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 11TH APRIL 2025, 8:00 PM - 10:30 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- Vulnerability Management: Microsoft Patch Tuesday (Continued)

NOTES/KEY DISCUSSIONS

- **Patch Testing and Controlled Rollout:**

Patches were deployed first in a **controlled staging environment** to detect possible stability or compatibility issues. Key metrics like system uptime, application behavior, and CPU/memory performance were monitored during testing.

- **Patch Deployment Tools and Strategy:**

The deployment was executed using **SCCM**, **WSUS**, and **Microsoft Intune**. A **phased rollout** approach was taken, starting with non-critical departments before full-scale enterprise deployment. Rollbacks were pre-planned in case of deployment failures.

- **Post-Deployment Validation and Monitoring:**

Patch success was validated through compliance dashboards and system logs. The team set up alerts for failed installations, service degradation, and unexpected reboots. No major issues were reported post-deployment.

Improvement Recommendations and Next Steps:

- Establishment of a **formal vulnerability management lifecycle** aligned with CIS benchmarks.
- Introduction of **automated patching workflows** and **compliance reports**.
- Enhancement of asset tagging and classification to support more **granular risk-based prioritization**.
- Stakeholder debriefs were conducted with technical summaries and patch impact analysis

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Saturday, 12th April 2025, at 2 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10:30 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 12TH APRIL 2025, 2:00 PM - 4:30 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- Mobile Device security.

NOTES/KEY DISCUSSIONS

- The team identified that 50% (250) of Android devices within the organization's mobile fleet were outdated and not enrolled in any Mobile Device Management (MDM) solution. These devices were found to be running vulnerable firmware versions, exposing them to CVE-2023-26083 (GPU memory flaw) and CVE-2021-29256 (privilege escalation bug).
- We conducted an urgent device inventory, and devices were prioritized based on risk exposure and business use. Affected users received clear update instructions and technical support to bring devices into compliance. Where feasible, non-compliant devices were isolated from corporate resources.
- A broadcast email and follow-up notifications were sent to users with outdated devices. The message emphasized the security risks and outlined steps to update their devices. Support teams were on standby to assist with the update process and troubleshoot issues.
- A mobile security policy was drafted to include **mandatory OS updates**, **device enrollment in MDM**, **app restrictions**, and **device lifecycle guidelines**. Training materials and FAQs will be created to help users understand and comply with the new policies.

Additional Notes:

- The team will meet again on Sunday, 13th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed

- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 13TH APRIL 2025, 8:00 PM - 10:40 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

AGENDA

- Incident Playbook

NOTES/KEY DISCUSSIONS

To enable effective response to similar scenarios experienced, create incident playbooks for each incident in previous tasks. This should include all important steps that should be taken.

Additional Notes:

- As the sprint lead, Alli-Balogun Luqman Damilare volunteered to open a Microsoft Azure account for the team's use.
- The team will meet again on Monday, 14th April 2025, at 8 pm GMT+1.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise
- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda
- Motunrayo Sanusi
- Oluwaseyi Adebayo

CyberBulwork

SECURITY OPERATIONS SPRINT: 14TH APRIL 2025, 8:00 PM - 10:30 PM GMT+1 / Microsoft Teams

---

ATTENDEES AT THE START OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise

- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Motunrayo Sanusi
- Dike Promise Chimamanda
- Oluwaseyi Adebayo

Agenda

- Creating Custom Alerts on Microsoft Sentinel

Key Discussions & Notes

- The focus of the sprint was on **creating custom alerts in Microsoft Sentinel** to improve threat detection.
- **Etinosa Imafidon** successfully created the alerts using **Indicators of Compromise (IOCs)** gathered from the incident report.
- Alerts were tailored to detect threat patterns relevant to previously analyzed incidents.
- The team discussed the continued use of **Kusto Query Language (KQL)** to fine-tune analytic rules and improve detection accuracy.

Additional Notes

- Ololade Elizabeth Adesagba, the team lead, assured the team that the incident report would be ready before the end of the day.

Closing:

- Ololade Elizabeth Adesagba thanked everyone for joining the meeting, and the meeting was adjourned at 10:30 p.m.

ATTENDEES AT THE END OF THE MEETING

- Ololade Elizabeth Adesagba
- Daniel Owoeye-Wise

- Muizz Babatunde Majeed
- Shado Peculiar Unini
- Etinosa Imafidon
- Alli-Balogun Luqman Damilare
- Dike Promise Chimamanda