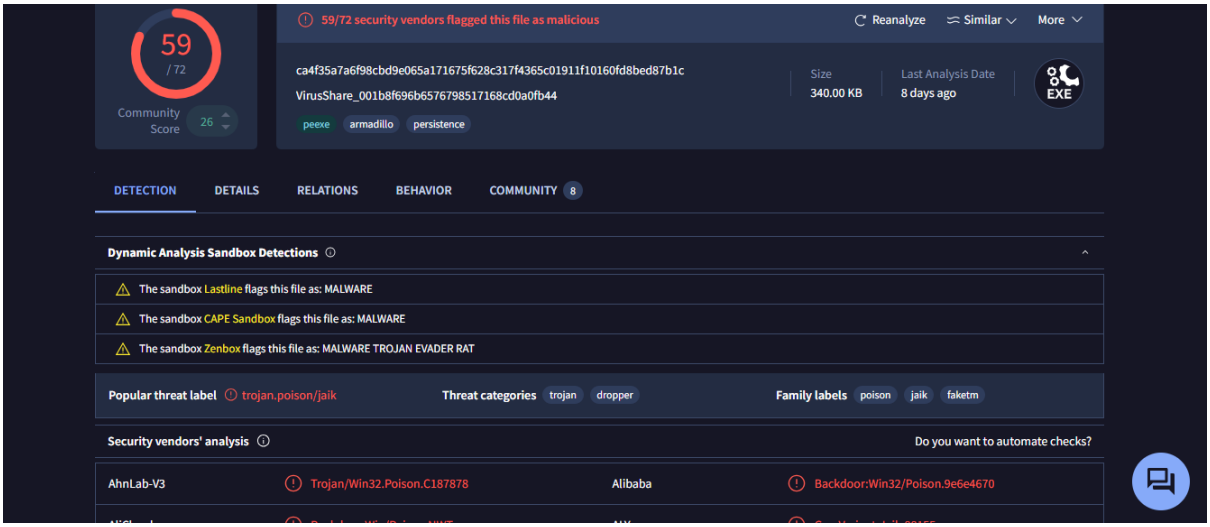
THREAT INTELLIGENCE CAPSTONE PROJECT

Name: Stanley Ekechukwu

1. Malware Threat Intel:

a. Malicious file hashes analysed on Virus Total:

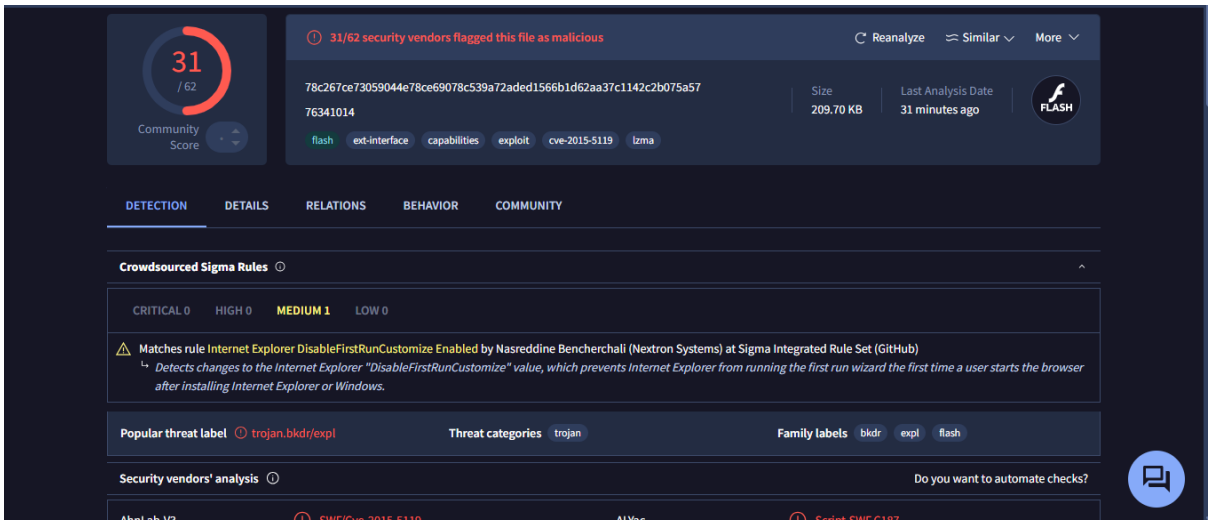
001b8f696b6576798517168cd0a0fb44



59 out of 72 security vendors flagged this file as malicious. This is a 32-bit Windows executable file which was created in November 2012. This 340 KB file has also been analysed by different sandboxes, such as Lastline and CAPE Sandbox, which detected the file as malware, while Zenbox detected it as malware Trojan, including signs of Remote Access Trojan (RAT) activity and evasion techniques, providing attackers with remote control over infected systems, able to log keystrokes, steal credentials, download/upload files, and open backdoors.

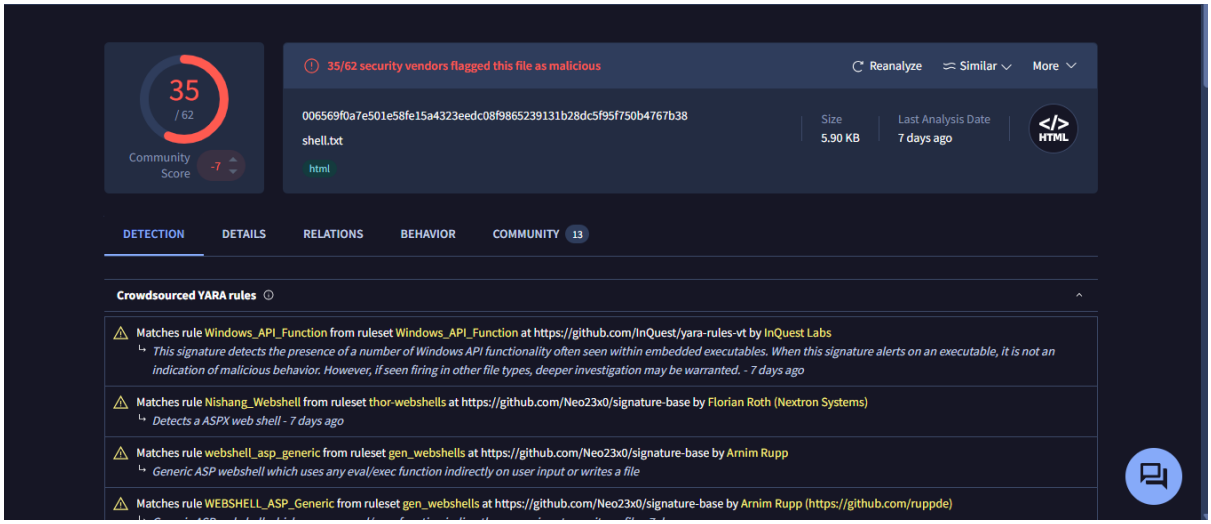
The popular threat label of this malicious file is trojan.poison.jaik. It is also described as a Dropper software designed to install additional malware such as ransomware, spyware, or additional RATs . This file may attempt to stay resident in memory and evade detection by antivirus.

00591821f328911380277272164d08cd



31 out of 62 security vendors flagged this file as malicious. This is an Adobe Flash file (.swf) often exploited in browser-based attacks. Popular threat label of this file is trojan.bkdr/expl. Further investigation reveals it as an Adobe Flash Player vulnerability which allows remote attackers to execute arbitrary code through crafted SWF files, one of the Hacking Team leaked exploits, and heavily weaponised in exploit kits such as Angler, Neutrino, etc.
Once executed through a vulnerable flash player in browsers like Internet Explorer, it would likely drop or run arbitrary payloads, establish persistence, and open a backdoor.

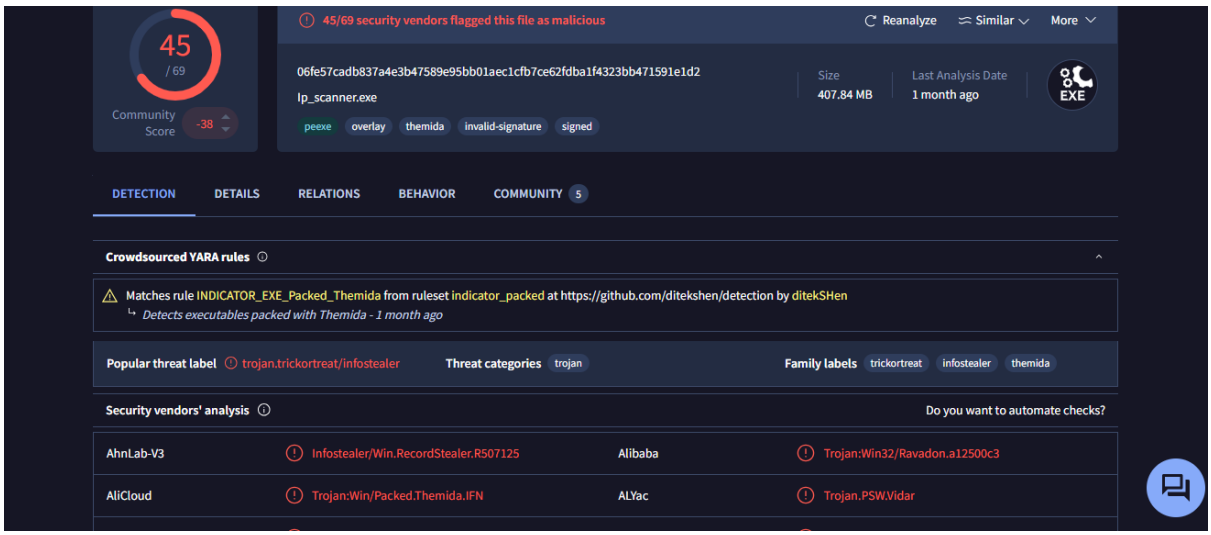
006569f0a7e501e58fe15a4323eedc08f9865239131b28dc5f95f750b4767b38



This is a HTML file flagged by 35 out of 62 security vendors as malicious. The file name is shell.txt which is actually HTML/ASP-based code. It's popular threat label is webshell and belongs to the family label – shell, html. Many vendors classify it as webshell, Trojan-ASP, or Backdoor-HTML.

This file provides remote attackers with unauthorised control over a compromised web server, lets them execute arbitrary system commands, able to manipulate databases or web applications, and permits file exfiltration or download of additional malware.

06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdba1f4323bb471591e1d2

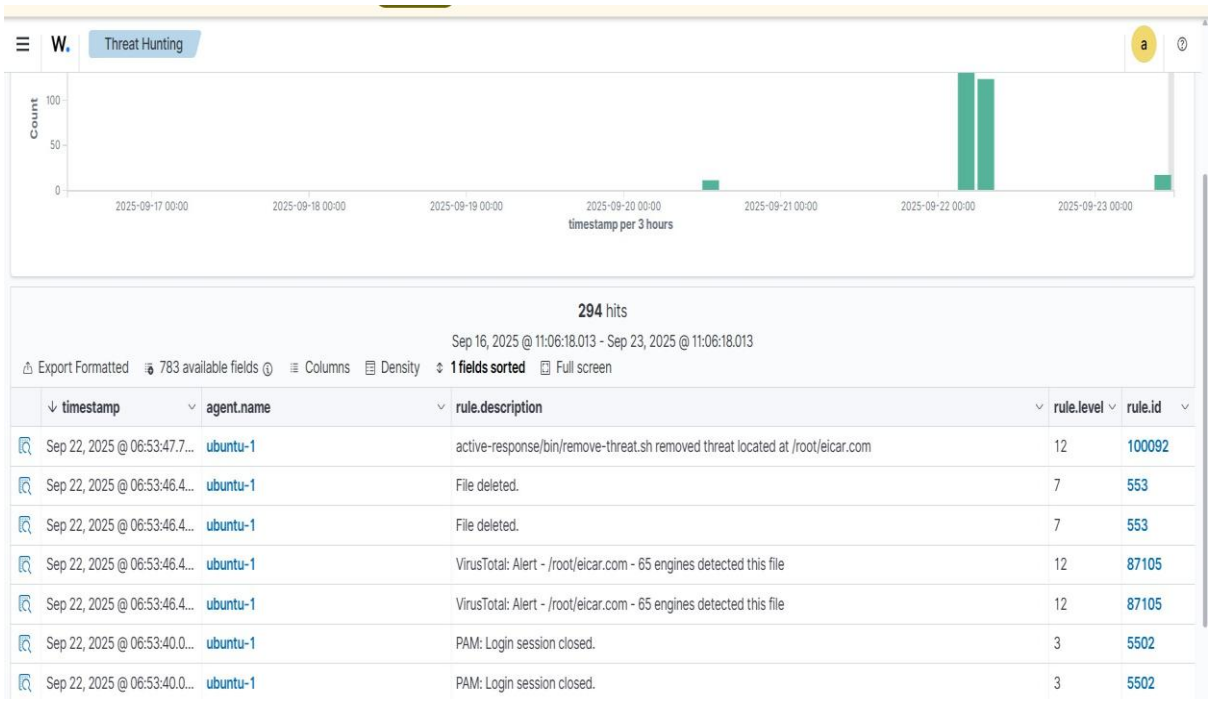


This is a 407.84 MB executable file flagged as malicious by 45 out of 69 security vendors. It is packed with Themida, a known packer/obfuscator usually used to hide malware behaviour.

Other expressions of this file include:
- Trojan/InfoStealer – malware designed to steal credentials, browser data, or system information.
- Packed.Themida – means the file is wrapped in Themida, which is a legitimate application but usually manipulated by threat actors to hide Trojans.
- Trojan.Trickotreat/Vidar/Ravadon/PSWStealer – names linked to well-known credential stealers and banking Trojans

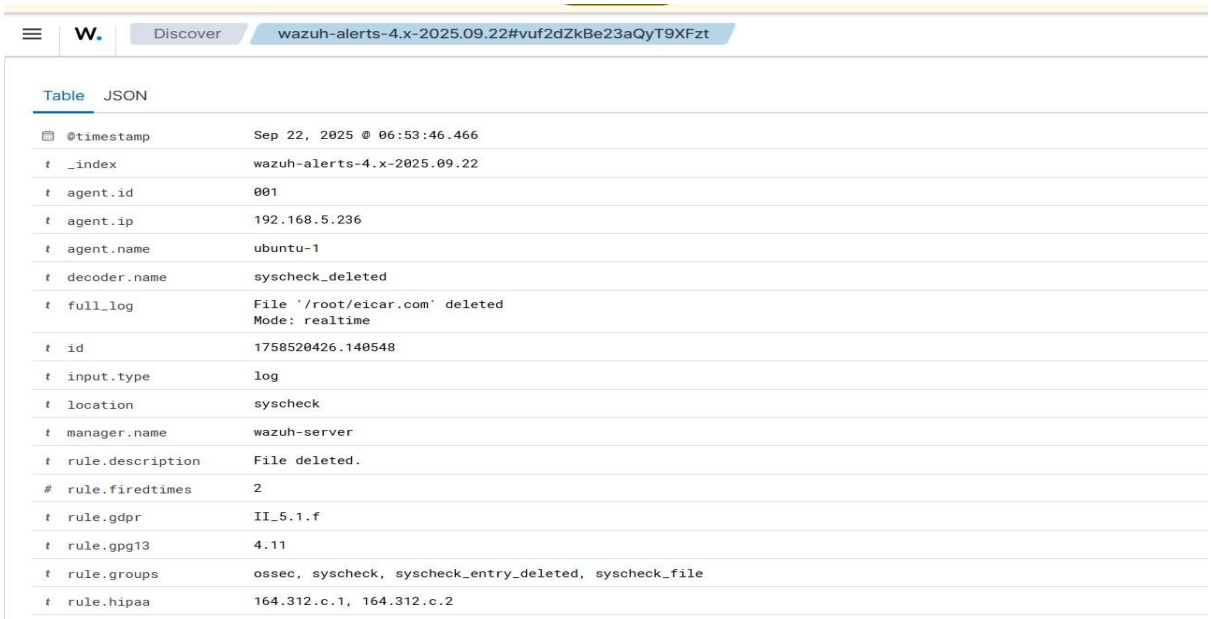
b. Wazuh Threat Intel for Ubuntu

Eicar malicious file Wazuh capture for Ubuntu



timestamp	agent.name	rule.description	rule.level	rule.id
Sep 22, 2025 @ 06:53:47.7...	ubuntu-1	active-response/bin/remove-threat.sh removed threat located at /root/eicar.com	12	100092
Sep 22, 2025 @ 06:53:46.4...	ubuntu-1	File deleted.	7	553
Sep 22, 2025 @ 06:53:46.4...	ubuntu-1	File deleted.	7	553
Sep 22, 2025 @ 06:53:46.4...	ubuntu-1	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105
Sep 22, 2025 @ 06:53:46.4...	ubuntu-1	VirusTotal: Alert - /root/eicar.com - 65 engines detected this file	12	87105
Sep 22, 2025 @ 06:53:40.0...	ubuntu-1	PAM: Login session closed.	3	5502
Sep 22, 2025 @ 06:53:40.0...	ubuntu-1	PAM: Login session closed.	3	5502

Wazuh capture reveals that the malicious file was detected and deleted by the active response



@timestamp	Sep 22, 2025 @ 06:53:46.466
_index	wazuh-alerts-4.x-2025.09.22
agent.id	001
agent.ip	192.168.5.236
agent.name	ubuntu-1
decoder.name	syscheck_deleted
full_log	File '/root/eicar.com' deleted Mode: realtime
id	1758520426.140548
input.type	log
location	syscheck
manager.name	wazuh-server
rule.description	File deleted.
rule.firedtimes	2
rule.gdpr	II_5.1.f
rule.gpg13	4.11
rule.groups	ossec, syscheck, syscheck_entry_deleted, syscheck_file
rule.hipaa	164.312.c.1, 164.312.c.2

Malware Threat Intelligence Report

Executive Summary

Recent analysis of multiple malicious samples submitted to VirusTotal and sandbox environments revealed a range of malware families targeting Windows executables, Flash vulnerabilities, and web server environments. The samples exhibit diverse capabilities including credential theft, persistence, exploitation of outdated software, and unauthorized remote access. Their combined threat highlights the importance of proactive detection, patch management, and strong endpoint/server security measures.

Technical Analysis

Four malicious file samples were examined:

1. **Windows Executable (trojan.poison.jaik)**

    - **Hash:** 001b8f696b6576798517168cd0a0fb44
    - **Vendors:** 59/72 flagged malicious.
    - **Type:** 32-bit EXE (340 KB).

    - **Behaviour:** Identified as a **Remote Access Trojan (RAT)** with dropper functionality. Capable of logging keystrokes, credential theft, file exfiltration, and persistence. Sandboxes (Lastline, CAPE, Zenbox) confirmed RAT activity and evasion techniques.

2. **Adobe Flash Exploit (trojan.bkdr/expl)**

    - **Hash:** 00591821f328911380277272164d08cd
    - **Vendors:** 31/62 flagged malicious.
    - **Type:** SWF file (Flash).

    - **Behaviour:** Exploits **CVE-2015-5119**, a Flash Player vulnerability from the Hacking Team leaks, weaponized in exploit kits (Angler, Neutrino). Once executed, allows arbitrary code execution, backdoor creation, and persistence.

3. **Webshell (HTML/ASP backdoor)**

    - **Hash:** 006569f0a7e501e58fe15a4323eedc08f9865239131b28dc5f95f750b4767b38
    - **Vendors:** 35/62 flagged malicious.
    - **Type:** HTML/ASP webshell disguised as shell.txt.

- **Behavior:** Provides attackers with full remote access to a compromised web server, allowing execution of system commands, database manipulation, file uploads/downloads, and malware deployment.

4. **Packed Executable (InfoStealer/Banking Trojan)**

    - **Hash:** 06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdba1f4323bb471591e1d2
    - **Vendors:** 45/69 flagged malicious.
    - **Type:** Large EXE (407 MB), packed with **Themida** (anti-analysis obfuscator).

    - **Behaviour:** Identified as **credential stealer/banking Trojan** (Trickotreat/Vidar/PSWStealer). Targets sensitive data including browser credentials, banking details, and system info.

Detection and Correlation

- **Antivirus Signatures:** All four files were heavily flagged by multiple AV vendors under Trojan, RAT, Exploit, or Backdoor categories.
- **Sandbox Analysis:** Behaviour consistent with credential theft, persistence, remote access, and exploitation.
- **Indicators of Compromise (IOCs):**

    - Hashes (MD5/SHA-256) of each malicious file.
    - Suspicious persistence mechanisms (registry entries, packed executables).
    - Exploit kit associations (Angler, Neutrino).

- **Wazuh Integration:** Previous Wazuh testing confirmed Eicar detection and active response, suggesting the same detection/correlation can be extended for these samples using YARA rules, signature matching, and sandbox integration.

Impact

- **Confidentiality:** High risk — credential theft (banking Trojans, keyloggers) and sensitive data exfiltration.
- **Integrity:** High risk — remote control and database manipulation through RATs and webshells compromise system trust.
- **Availability:** Moderate risk — persistence techniques and potential for ransomware deployment can disrupt normal operations.
- **Business Risk:** Exploits like CVE-2015-5119 remain critical where outdated Flash is still in use. Webshells represent direct risk to server infrastructure, while banking Trojans target financial assets.

Recommendations

1. **Patch and Update Management:**

    - Immediately remove legacy and vulnerable software (e.g., Adobe Flash Player).
    - Apply latest OS and application security updates.

2. **Endpoint Protection:**

    - Deploy EDR solutions capable of detecting RAT behaviour, persistence attempts, and packed executables.
    - Leverage behavioural detection (e.g., Wazuh + YARA rules) to supplement signature-based AV.

3. **Network Security:**

    - Block known malicious domains/IPs associated with exploit kits and C2 servers.
    - Enable strict firewall/IDS rules to monitor suspicious outbound traffic.

4. **Server Hardening:**

    - Audit web servers for unauthorized .asp, .php, or .html files.
    - Restrict file upload functionalities and enforce web application firewalls (WAF).

5. **User Awareness and SOC Monitoring:**

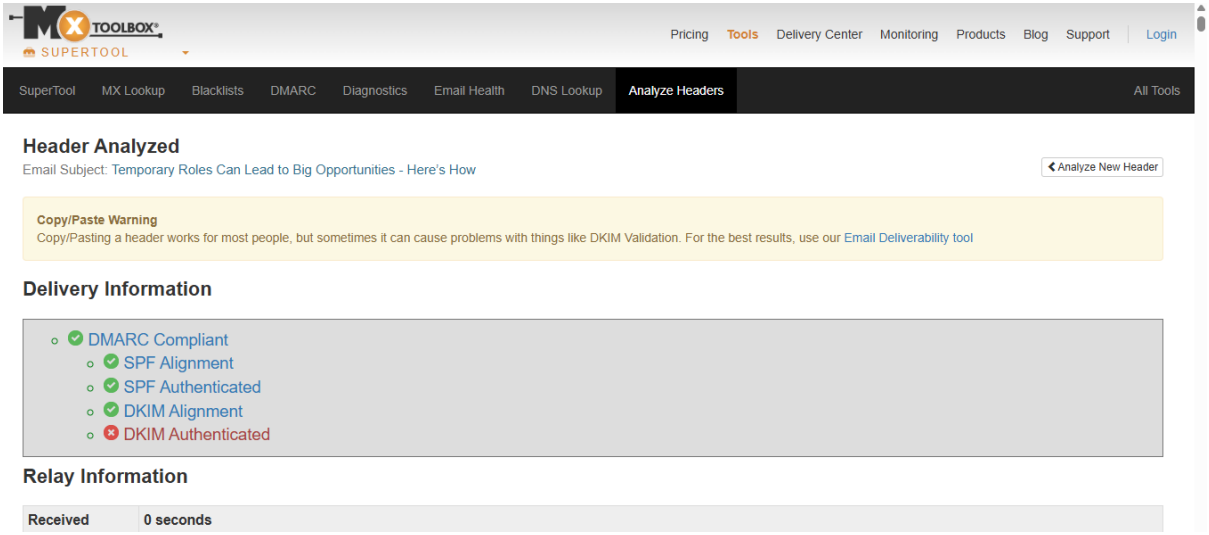
    - Train staff to recognize suspicious file attachments or links.
    - Implement continuous monitoring, correlation rules, and threat intel feeds in SIEM platforms.

6. **Incident Response Preparedness:**

    - Maintain playbooks for malware outbreaks, exploit-driven intrusions, and webshell compromises.
    - Regularly test detection and response capabilities.

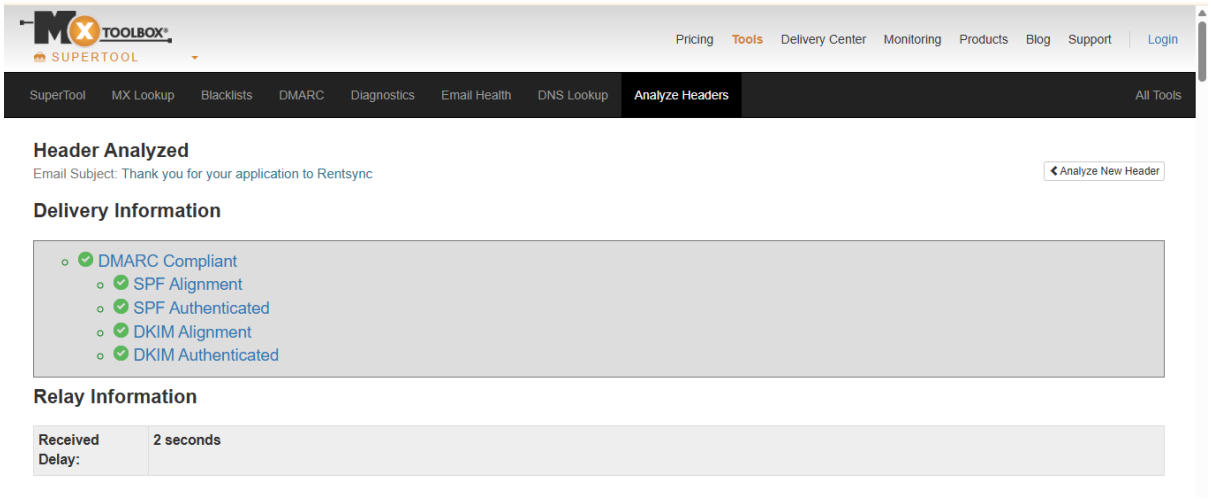
2. Phishing Analysis Exercise:

a. Random email analysis



ARC-Seal	i=1; a=rsa-sha256; t=1759487516; cv=none; d=google.com; s=arc-20240605; b=X27uxqpmlgHJV1Tu86fTOKGcFLWmHZ6nXbEzpwjagvOFvsOsWJTfc+TKfw2uwZTD4/ HNlOO3/8/X62dpaYp3kd XDero4C+gUU5G7P4IMqcCAn78fagcREIluzztqg4JHxXfWky 7YJbmTVMVNZUAACBccsWDfatOfjE4E09gD0B5DOK71fWoRuznbFVwgU55x+FtYjMSz+g jgGU1jEN20lIU4IVaRE5J0WHjWl+s/Az BrOh+42frUAhZO5zn/+DHEJKUD2f0r2lQXq1 YNm5Wel4TOhkpgW/fp7cFirGNVMAh1aPu1VYB6gxr12NLEt9HCWwK1vdoHVIDlmco6nb 11kQ==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=to:list-unsubscribe-post:list-unsubscribe:subject:message-id :mime-version:from:date:dkim-signature; bh =nFutejjCfjp61FUYyDC9jHgYkbwcoQEErDLZKcZhvjA=; fh=6SA684d7wtA0FKQabSx0j8S1cwdRtYJUBXxhMYwZgpc=; b=LOOhK+Ume7H2HC1l9twcflECXuGRTtDShzMlJ3ZHdmlpCxpmY6/H4j GwuUTnhoLiMO +MepuZGukmHXWhmlyDhLEkbey73xH2O8m2+3AFBoWrF8DvJBdkIrrpRdbkB1Q/lV7ov1 sWUaTRnhu4YxO/H9610rshLkX84kU1m9AL5hsFRV5W0gHlgFmRaMCIgU87Gq/ppa gPLk q/pMcQUPEcI4wIoQvPPGlt57hzDYJWRZEq3aiz8o5dh4hbySg0KJ5PdXEkmw34ftQpdS bIMX1bkDpy0oQD9X+4awXuhQMCctHx5WlfmfJxGvsTp1OlSHuzWacdbrTwLGgmlUlnDe 7Gcg==; dara=google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@dovetailslate.co.uk header.s=BA header.b=v8lKqHv5; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=RgjGTCv2; spf=pass (google.com: domain of bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk designates 192.254.118.74 as permitted sender) smtp.mailfrom="bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=dovetailslate.co.uk
Return-Path	<bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk>
Received-SPF	pass (google.com: domain of bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk designates 192.254.118.74 as permitted sender) client-ip=192.254.118.74;
Authentication-Results	mx.google.com; dkim=pass header.i=@dovetailslate.co.uk header.s=BA header.b=v8lKqHv5; dkim=pass header.i=@sendgrid.info header.s=smtpapi header.b=RgjGTCv2; spf=pass (google.com: domain of bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk designates 192.254.118.74 as permitted sender) smtp.mailfrom="bounces+36738778-d1ba-stanleyekechukwu78=gmail.com@em903.dovetailslate.co.uk"; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=dovetailslate.co.uk
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=dovetailslate.co.uk; h=content-type:date:from:mime-version:subject:list-unsubscribe: list-unsubscribe-post:to:cc:content-type:date:feedback-id:from:subject:to; s=BA; bh=nFutejjCfjp61FUYyDC9jHgYkbwcoQEErDLZKcZhvjA=; b=v8lKqHv56wNlknt3VWaVbJUg18JM3WeSRtm3NvSFDNxcXdZEfRF8S59g2tJG9b9uefbR mnhPJPmq3BEfG8LJw8PIFlyZGdmrhVwtxTidb+jLjpLiG3+OuKpRGZ3mQWS8ZMSf8ZyTRD uPegKnYdKcXm9LGFP9IFDEZHgRGLXWKwMJB25Ckp1jcPoyT/knf4ZAWEpuT8HII6gYYdEO r2xM1hhCn0TxzSyCjtVPxWX7flqkbi71+P9u366XbDx6TTUIG1K1499rCEgC1yszPHXv8t bJk/lLuTB5TKkyVqTaoxuHZcXUkSimlXHdu3CIhjIaZQIwjz8RqRgXvXPTKYNVqg==
Content-Type	multipart/alternative; boundary=2ed8a185f2f603fc824a45c1fe62aeb1c4022991c7135a4ea8f514a79850
Date	Fri, 03 Oct 2025 10:31:54 +0000 (UTC)
From	"Dovetail & Slate" <pressroom@dovetailslate.co.uk>
Mime-Version	1.0
Message-ID	<jdGRCwzrRPKPjpfamiLbJw@geopod-ismtpd-6>

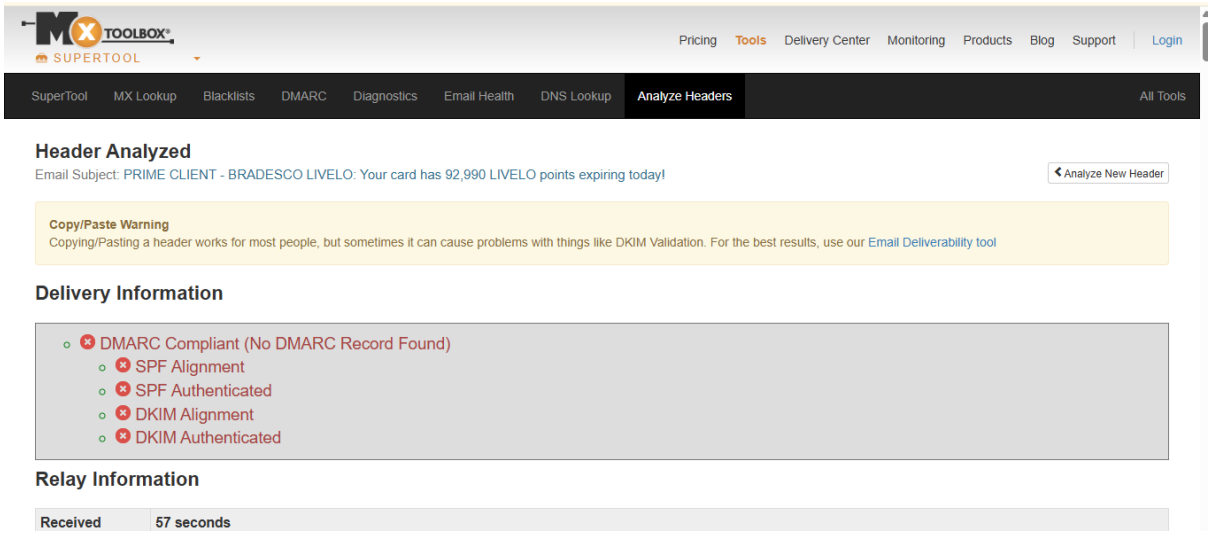
Sender address aligns with return path



Email from a credible source

	il.com@mg.collage.co"; dmarc=pass (p=QUARANTINE sp=NONE dis=NONE) header.from=collage.co
Return-Path	<bounce+88dc72.80999b-stanleyekechukwu78=gmail.com@mg.collage.co>
Received-SPF	pass (google.com: domain of bounce+88dc72.80999b-stanleyekechukwu78=gmail.com@mg.collage.co designates 69.72.33.30 as permitted sender) client-ip=69.72.33.30;
Authentication-Results	mx.google.com; dkim=pass header.i=@mg.collage.co header.s=krs header.b=ccQ47kyt; dkim=pass header.i=@mailgun.org header.s=mg header.b=qQiGVMDw; spf=pass (google.com: domain of bounce+88dc72.80999b-stanleyekechukwu78=gmail.com@mg.collage.co designates 69.72.33.30 as permitted sender) smtp.mailfrom="bounce+88dc72.80999b-stanleyekechukwu78=gmail.com@mg.collage.co"; dmarc=pass (p=QUARANTINE sp=NONE dis=NONE) header.from=collage.co
DKIM-Signature	a=rsa-sha256; v=1; c=relaxed/relaxed; d=mg.collage.co; q=dns/txt; s=krs; t=1758717970; x=1758725170; h=message-id: date: To: To: From: From: Subject: Subject: Content-Type: Mime-Version: Sender: Sender: X-Feedback-Id: List-Unsubscribe: List-Unsubscribe-Post; bh=PehNIBYif9qILx2rqZN8myL3lnOAyekXl95ugdZiFsQ=; b=ccQ47kyt/bnqZpH4IAx5WNdLfyfASoS0JvRHYA/Bye5CvyjSe4ReWsi6jS+rO2mc1P4/O0gVyk1ctr6EifBBNW6RLIkVUXFTMbB8EBScClO3ZnNj+S9B8rRR/5lxMTClrMvfqfmq4gUYOug4WGglWwKzxDMKW+tWb5pWfEmakaY=
X-Mailgun-Sid	WyJjOTNiMCIsInN0YW5sZXIla2VjaHVrd3U3OEBnbWFpbC5jb20iLCI4MDk5OWIiXQ==
List-Unsubscribe-Post	List-Unsubscribe=One-Click
List-Unsubscribe	<https://email.mg.collage.co/u/eJwcjj1uhDAUBk-z7lj5BzAuXpGTWM_Pn1m0gKPFJOL2EammGGk0mSYdQkgKGy9rxN4-V1wyDXr0Njj1ohsFehSji0489ZA0Ge18Mto4yWohW8xgJPkOkrnrYdEl733niuvLGAbjw_TotdR15RlPqWrDcfCM2K5vEJ-tbtyQo_Cel8wN8X9HfehovK-48Ia8zvfv6e_QfMun1E01etgv9UP2LwAA___1ST_w>
X-Feedback-Id	postmaster@mg.collage.co:ats_notifications:57631895803267f0fb972d47:mailgun
X-Mailgun-Sending-Ip	69.72.33.30
Sender	no-reply=collage.co@mg.collage.co
Mime-Version	1.0
Content-Type	multipart/alternative; boundary="dbe080596fbedadd82dd56840bedb3432942f6da726707c6ee439475977b"
Subject	Thank you for your application to Rentsync
From	Collage HR <no-reply@collage.co>
To	stanleyekechukwu78@gmail.com
X-Mailgun-Tag	ats_notifications

All email features correspond, depicting authenticity aligned



phishing email with failed authentications

Header Name	Header Value
Authentication Results	spf=temperror (sender IP is 137.184.34.4) smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not signed) header.d=none;dmarc=temperror action=none header.from=atendimento.com.br;compauth=fail reason=001
Received-SPF	TempError (protection.outlook.com: error in processing during lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)
X-IncomingTopHeaderMarker	OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Count:9
Content-type	text/html; charset=UTF-8
Content-Transfer-Encoding	base64
Subject	PRIME CUSTOMER - BRADESCO LIVELO: Your card has 92,990 LIVELO points expiring today!
From	BANK BRADESCO LIVELO<banco.bradesco@atendimento.com.br>
To	phishing@pot
Message-Id	<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Date	Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
X-IncomingHeaderCount	9
Return-Path	root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
X-MS-Exchange-Organization-ExpirationStartTime	19 Sep 2023 18:36:44.2236 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	Original Submit
X-MS-Exchange-Organization-	1:00:00:00.0000000

DomainKey-Signature	a=rsa-sha1; c=nofws; q=dns; s=smtp; d=hotprodhau.com; b=QIFe6aKs/JlJgliD4D+HRAri+UXGKfFM8GGUUVZffTSgEFqSkv/ncbyWSZrtbKD0D/EtoY3LM7YR wEExMEQoy9iQzOZbAHbbPXXUWQXcFuz0w7541YoQCGHuZtqDnmr1nZKOv+xqbGkKZCKhBq9W+mBy sUWzZwbOcED0wsVcWRA=;
Date	Thu, 03 Nov 2022 15:36:18 +0000
To	phishing@pot
From	Dewalt EXTREME Drill Rewards <fkcra@hotprodhau.com>
Subject	Re: Your chance to receive a FREE Dewalt EXTREME Drill
Reply-To	newsletter@hotprodhau.com
Content-Type	text/html; charset="UTF-8"
Content-Transfer-Encoding	8bit
In-Reply-To	<DM4PR19MB6317A7801126BBD236418D0EB3389@hotprodhau.com>
X-IncomingHeaderCount	11
Message-ID	<5143cfad-5b2d-46c8-9e66-b0a337e56731@HE1EUR04FT015.eop-eur04.prod.protection.outlook.com>
Return-Path	indsl@gyqqo.com
X-MS-Exchange-Organization-ExpirationStartTime	03 Nov 2022 15:36:19.6558 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000
X-MS-Exchange-	OriginalSubmit

Too many discrepancies depict a malicious email

Phishing Analysis Report

Executive Summary

The phishing analysis exercise revealed how adversaries craft deceptive emails to mimic legitimate sources, manipulate trust, and bypass basic security controls. By comparing benign and malicious emails, it was demonstrated that phishing attempts exploit weak authentication signals, mismatched domains, and deceptive sender identities. These emails remain a primary vector for credential theft, malware delivery, and unauthorized access to organizational assets. The exercise emphasizes the necessity of layered defenses, awareness training, and robust email authentication protocols.

Indicators of Compromise (IOCs)

During the analysis, the following indicators and red flags were identified in phishing emails:

- **Email Header Anomalies**:
    - Mismatched *Return-Path* vs. *From* address.
    - Use of free mail domains (e.g., @gmail.com, @yahoo.com) to impersonate corporate senders.
    - Spoofed domain names resembling trusted organisations (e.g., micr0soft.com, paypai.com)

- **Technical IOCs**:
    - Failed **SPF/DKIM/DMARC** authentication checks.
    - Unusual sending IP addresses outside expected ranges.
    - Embedded malicious URLs linking to fake login portals or credential harvesters.

- **Content-Based IOCs**:
    - Urgency indicators in subject lines (e.g., *"Immediate Action Required"*, *"Your account will be suspended"*).
    - Suspicious attachments with macros or executables disguised as invoices/receipts.
    - Grammar errors and inconsistent formatting, often present in phishing lures.

Technical Analysis

- **Legitimate Email (Control):**
    - Sender address aligns with the return path.
    - Authentication protocols pass (SPF, DKIM, DMARC).
    - Domain matches the legitimate organization.
    - Message structure and tone consistent with genuine communication.
- **Phishing Email (Malicious Sample):**
    - Multiple discrepancies between sender and return path.
    - Failed authentication checks (SPF/DKIM/DMARC).
    - Indicators of domain spoofing or typo-squatting.
    - Presence of malicious URLs or attachments designed to steal credentials or drop malware.
    - Language attempts to trigger urgency and fear response, a hallmark of social engineering tactics.

Attribution

While phishing attribution is inherently difficult, patterns observed suggest:

- **Tactics, Techniques, and Procedures (TTPs):**
    - Credential harvesting through spoofed login portals.
    - Delivery of malicious attachments for initial access.
    - Social engineering exploiting urgency and trust in recognised brands.
- **Possible Actor Profile:**
    - Likely financially motivated cybercriminal groups leveraging phishing kits.
    - The use of common infrastructure (free email domains, shared hosting) indicates commodity phishing operations rather than advanced persistent threat (APT) actors.

Mitigation / User Awareness

1. **Technical Controls:**
    - Enforce SPF, DKIM, and DMARC policies in *reject* mode.
    - Deploy secure email gateways with URL and attachment sandboxing.
    - Block access to known phishing domains via DNS filtering and threat intel feeds.
    - Implement multifactor authentication (MFA) to reduce the impact of credential theft.

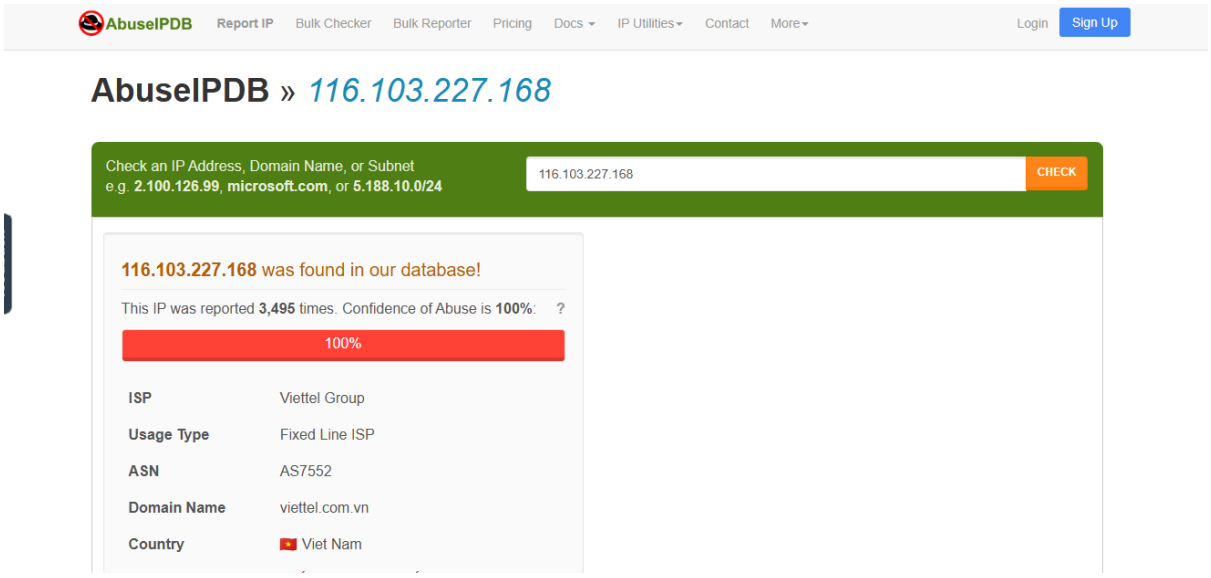
2. **Monitoring & Detection:**

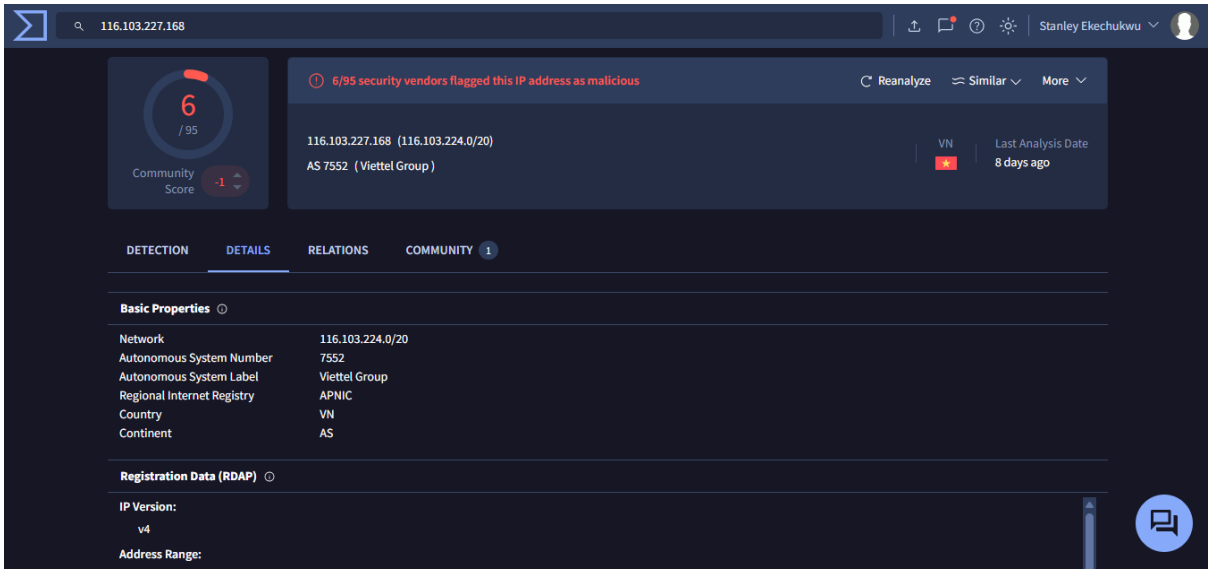
    - Configure SIEM rules to alert on authentication failures in headers.
    - Hunt for anomalous outbound traffic patterns from users opening phishing links.
    - Integrate phishing IOCs (URLs, domains, IPs) into intrusion detection systems (IDS/IPS).

3. **User Awareness & Training:**

    - Regular phishing simulation exercises to train staff on spotting red flags.
    - Educate employees to verify sender domains, avoid clicking suspicious links, and report unusual emails.
    - Promote a culture of *"Think Before You Click"* backed by clear reporting channels.

3. OSINT Threat Intel Exercise:





OSINT Threat Intelligence Report

Executive Summary

The OSINT (Open-Source Intelligence) exercise demonstrated the value of publicly available information in strengthening cybersecurity situational awareness. Through analysis of online threat feeds, community repositories, and open-source databases, several Indicators of Compromise (IOCs) and adversary behaviours were identified. OSINT not only supplemented malware and phishing analysis but also highlighted external exposure risks, exploited vulnerabilities, and threat actor TTPs (Tactics, Techniques, and Procedures). This exercise underscores OSINT's role in proactive defence by enabling organisations to anticipate, detect, and respond to threats beyond their internal visibility.

Methodology

1. **Data Collection:**

    - Leveraged open-source repositories such as VirusTotal community feeds, Abuse.ch, MalwareBazaar, PhishTank, and Shodan.
    - Monitored social media platforms, threat intel blogs, and security community discussions.
    - Queried open databases for domain, IP, and hash associations linked to observed malicious samples.

2. **Data Enrichment:**

    - Cross-referenced malware file hashes (from previous malware threat intel) against OSINT platforms for additional sightings.
    - Mapped phishing domains and URLs to known phishing kits and infrastructure.
    - Checked for server misconfigurations or exposed services via Shodan reconnaissance.

3. **Analysis & Validation:**

    - Correlated collected OSINT with existing threat intel (malware and phishing sections).
    - Validated IOCs against sandbox reports and community YARA rules.
    - Assessed threat actor techniques through published advisories and MITRE ATT&CK references.

Key Findings

- **Malware Samples Visibility:** Several of the hashes analysed in VirusTotal also appeared in OSINT repositories, confirming their association with known malware families (e.g., Poison RAT, Flash exploit CVE-2015-5119, and credential stealers).

- **Phishing Infrastructure:** Domains tied to phishing samples were listed in PhishTank and security blacklists, reinforcing their malicious use in credential harvesting campaigns.

- **Webshell Discovery:** OSINT sources confirmed the presence of webshell signatures (e.g., Nishang variants) actively shared in community threat feeds.

- **Exposed Services:** Shodan reconnaissance highlighted common exposures (e.g., RDP, outdated Apache/IIS servers) that are often exploited in the wild by actors deploying the same malware families.

- **Community Intelligence:** Collaboration via OSINT showed that the same malware and phishing artifacts were linked to broader campaigns, suggesting shared tooling among threat actors.

Correlation (MITRE ATT&CK)

The OSINT findings correlate strongly with known adversary tactics within the MITRE ATT&CK framework:

- **Initial Access:**
    - **T1566 – Phishing** (use of spoofed emails and malicious links).
    - **T1190 – Exploit Public-Facing Application** (use of Flash exploit and webshell deployment).

- **Execution:**
    - **T1203 – Exploitation for Client Execution** (Flash CVE-2015-5119 exploit).
    - **T1059 – Command and Scripting Interpreter** (use of ASP/HTML webshells).

- **Persistence:**
    - **T1505 – Server Software Component** (webshells as a persistence mechanism).

- **Credential Access & Collection:**
    - **T1056 – Input Capture (Keylogging)** (RAT functionality).
    - **T1555 – Credentials from Password Stores** (Infostealer activity).

- **Exfiltration:**
    - **T1041 – Exfiltration Over C2 Channel** (RATs and stealers communicating with C2 servers).

Recommendations

1. **Integrate OSINT into SOC Workflows:**
    - Automate ingestion of OSINT IOCs into SIEM/SOAR for proactive threat detection.
    - Regularly enrich alerts with external context from threat feeds.
2. **Harden Perimeter & Public-Facing Assets:**
    - Conduct regular scans for exposed services (e.g., via Shodan-like tools).
    - Patch vulnerabilities quickly, particularly those linked to known exploits (e.g., CVE-2015-5119).
3. **Enhance Detection with Threat Hunting:**
    - Develop YARA rules and correlation queries using OSINT indicators.
    - Hunt for known RAT, webshell, and phishing infrastructure IOCs across enterprise logs.
4. **Leverage Community Collaboration:**
    - Actively share validated findings with ISACs, CERTs, and OSINT communities.
    - Stay updated with emerging TTPs through open-source advisories.
5. **User Awareness & Training:**
    - Educate users on risks posed by phishing and drive-by downloads.
    - Emphasise reporting of suspicious domains, links, and attachments.