

THREAT INTELLIGENCE CAPSTONE PROJECT

Name: Stanley Ekechukwu

1. Malware Threat Intel:

a. Malicious file hashes analysed on Virus Total:

001b8f696b6576798517168cd0a0fb44

The screenshot shows the VirusTotal analysis interface for the file hash 001b8f696b6576798517168cd0a0fb44. The top header indicates a Community Score of 59/72, with a red circle highlighting the number 59. Below the header, the file's metadata is shown: SHA-256 (ca4f35a7a6f98cbd9e065a171675f628c317f4365c01911f10160fd8bed87b1c), VirusShare URL (VirusShare_001b8f696b6576798517168cd0a0fb44), Size (340.00 KB), Last Analysis Date (8 days ago), and Type (EXE). The main content area includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 8 items). Under the DETECTION tab, there's a section for Dynamic Analysis Sandbox Detections, which lists three sandboxes (Lastline, CAPE Sandbox, Zenbox) that flagged the file as MALWARE. Below this, threat labels are listed: trojan.poison.jaik, trojan, dropper, poison, jaik, and faketm. At the bottom, there's a section for Security vendors' analysis, showing results from AhnLab-V3, Alibaba, and Backdoor:Win32/Poison.9e6e4670.

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

The screenshot shows a detailed analysis of a file with the SHA-256 hash 00591821f328911380277272164d08cd. The interface includes a 'Community Score' of 31/62, a list of 31 malicious vendors, and various file metadata like size (209.70 KB) and last analysis date (31 minutes ago). It also displays threat categories (e.g., flash, ext-interface, capabilities, exploit, cve-2015-5119, lzma), a 'Crowdsourced Sigma Rules' section, and a 'Security vendors' analysis' section. A prominent blue button at the bottom right says 'Do you want to automate checks?'. The overall theme is dark with blue highlights.

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

The screenshot shows a malware analysis interface. At the top left is a circular 'Community Score' icon with '35 / 62' and a red minus sign. To its right, a message says '35/62 security vendors flagged this file as malicious'. Below this are file details: '006569f0a7e501e58fe15a4323eedc08f9865239131b28dc5f95f750b4767b38', 'shell.txt', 'html', 'Size 5.90 KB', 'Last Analysis Date 7 days ago', and a 'HTML' download button. Below these are tabs: DETECTION (selected), DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (13). Under 'Crowdsourced YARA rules', there are four entries:

- Matches rule Windows_API_Function from ruleset Windows_API_Function at <https://github.com/InQuest/yara-rules-vt> by InQuest Labs
 - This signature detects the presence of a number of Windows API functionality often seen within embedded executables. When this signature alerts on an executable, it is not an indication of malicious behavior. However, if seen firing in other file types, deeper investigation may be warranted. - 7 days ago
- Matches rule Nishang_Webshell from ruleset thor-webshells at <https://github.com/Neo23x0/signature-base> by Florian Roth (Nextron Systems)
 - Detects a ASPX web shell - 7 days ago
- Matches rule webshell_asp_generic from ruleset gen_webshells at <https://github.com/Neo23x0/signature-base> by Armin Rupp
 - Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file
- Matches rule WEBSHELL_ASP_Generic from ruleset gen_webshells at <https://github.com/Neo23x0/signature-base> by Armin Rupp (<https://github.com/ruppde>)
 - Generic ASP webshell which uses any eval/exec function indirectly on user input or writes a file

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. Its 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.

06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdb1f4323bb471591e1d2

The screenshot shows a detailed analysis of a file. At the top left is a circular 'Community Score' icon with '45 / 69' and a red progress bar. To its right, a message says '45/69 security vendors flagged this file as malicious'. The main header includes the file name '06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdb1f4323bb471591e1d2' and type 'Ip_scanner.exe'. It also shows 'Size 407.84 MB' and 'Last Analysis Date 1 month ago'. A 'REANALYZE' button is at the top right.

Below the header, tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' are visible, with 'COMMUNITY' selected. The 'COMMUNITY' tab shows a count of 5. Under 'Crowdsourced YARA rules', it lists a rule that matches 'INDICATOR_EXE_Packed_Themida' from a GitHub repository. Below this, under 'Popular threat label', it shows 'trojan.trickotreat/infostealer' as the primary label, with 'trojan' as a threat category. 'Family labels' include 'trickotreat', 'infostealer', and 'themida'. The 'Security vendors' analysis' section lists findings from AhnLab-V3, Alibaba, and ALYac, each with a corresponding threat name.

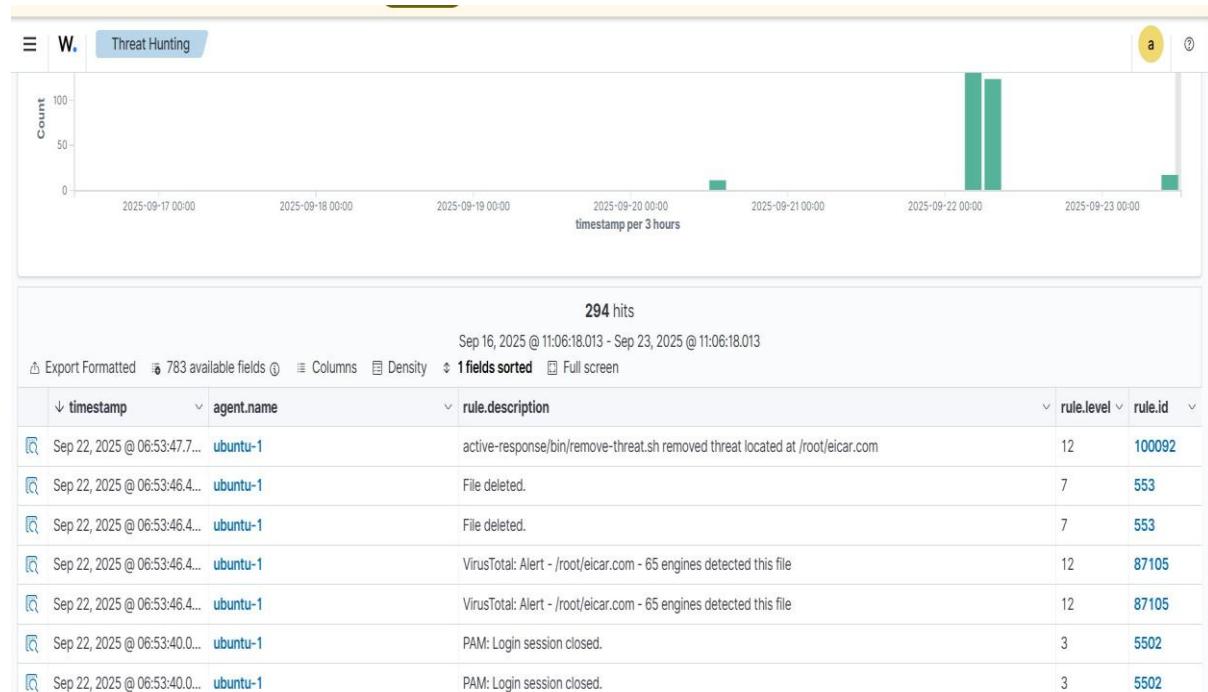
This is a 407.84 MB executable file flagged as malicious by 45 out of 69 security vendors. It is packed with Themida, a known packer/obfuscator usually used to hide malware behaviour.

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



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

The figure shows a Wazuh Discover interface with a table titled 'wazuh-alerts-4.x-2025.09.22#vuf2dZkBe23aQyT9XFzt'. The table displays a single JSON document with various fields and their values.

Table JSON	
@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:** 06fe57cadb837a4e3b47589e95bb01aec1cfb7ce62fdb1f4323bb471591e1d2
- **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

The screenshot shows the MX Toolbox interface for analyzing an email header. The header analyzed is "Email Subject: Temporary Roles Can Lead to Big Opportunities - Here's How".

Delivery Information:

- ✓ DMARC Compliant
- ✓ SPF Alignment
- ✓ SPF Authenticated
- ✓ DKIM Alignment
- ✗ DKIM Authenticated

Relay Information:

Received	0 seconds
ARC-Seal	i=1; a=rsa-sha256; t=1759487516; cv=none; d=google.com; s=arc-20240605; b=X27uxqpmIgHV1Tu86fTOKGcFLWmHZ6nXbEzpWjagvOfVsOsWJFc+TKfw2uwZTD4/HNIO03/x62dpaYp3kdXDero4C+gUU5G7P4lMqcCAn78fagcRElluzztg4JhxXWky7YJbmTMVNzUACBccsWDfatOf E4E09gD0B5DOK71fVoRuZnbFVwgU55x+FtY MSz+g jgGU1jEN20IIU4lVaRE5J0WHjWI+s/AzBrOh+42frUhZ05zn/+DHEJKUD2f02lQXq1YNm5WeI4TOhkpg//fp7cFirGNVMAh1aPuVVB6gxR2NLE9HCWwK1vdohVIdImco6nb 11kQ==
ARC-Message-Signature	i=1; 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 dkim-signature; bh=FutejCj6p1FYyDC9jHg/kbwcoOERdLZKcZhVjA=; fh=6SA684d7wAOFKoabSxj0S1cwbDRYJUBXhMwZgpc=; b=L0Oh+kUm7H2Hc19wvcIECxuGR71DShzMuJ32HdmipCxpmY6fH4jGwuUTrih0LIMO +MepuZGukmHXWhmlyDhLEkbey73xH2O6m2+3AFBoWrF0DvBdklrrpRdbkB1Q/lV7ov1 sWUa1rhnu4Yx0IH9610rshLkX84k1u1m9AL5hsFRV5W0gHlgfMrRaMCigU87Gqjppa gPLk qjPMcQUPEcl4wlQvPGLit57zDYJWRZEq3aizb05dh4bySg0KJ5PdxEkmw34tQpdS blMX1bkDpyo0QD9X+4awXuhQMCCttx5WlmlJxGvsTp10ISHuzVwcdbrTwLggmlUlnDe7Gcg==; dara@google.com
ARC-Authentication-Results	i=1; mx.google.com; dkim=pass header.i=@dovetailslate.co.uk header.s=BA header.b=v8IKqHv5; dkim=pass header.i=@sendgrid.info header.s=smtppapi 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=v8IKqHv5; dkim=pass header.i=@sendgrid.info header.s=smtppapi 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:list-unsubscribe subject:to:cc:content-type:date:feedback-id:from:subjetcto: s=BA; bh=FutejCj6p1FYyDC9jHg/kbwcoOERdLZKcZhVjA=; b=v8IKqHv5wvNlk3VWaVbUg18JM3V/eSRtm3NvSDNxXzdZERf8559g2UJ99b9uefR mnbfJFmp3BEFG8LJw8PfIlyZGdmrhVwbtTdb+jpljG3+OukprGZ3mQWSz2MSf82zYTRD uPegKnfdrkXm9LGFP91fDEZHgRCLXWkwMB25CkpJcPoT/knf4ZAW/EpuT8HlgYYdEO r2xM lhhCn0TxzSyCjVpxWx7flqkb i71+p9u366xbDb6TTUIG1K149r9CeG1yszPHXv8tjkILutB5TkyVqTaxoiHzCUXk5lmXhdz3lhhjaZQlwjz8RqRgRxvPTKYNVqg==
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	<jdGRCWzrRPKPjpfamIbJw@geopod-lsmtpd-6>

Sender address aligns with return path

MX TOOLBOX®
SUPERTOOL

Pricing Tools Delivery Center Monitoring Products Blog Support | Login

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze Headers All Tools

Header Analyzed
Email Subject: Thank you for your application to Rentsync [Analyze New Header](#)

Delivery Information

- **DMARC Compliant**
 - SPF Alignment
 - SPF Authenticated
 - DKIM Alignment
 - DKIM Authenticated

Relay Information

Received	2 seconds
Delay:	

Email from a credible source

	il.com@mg.collage.co", dmarc=pass (p=QUARANTINE sp=NONE dis=NONE) header.from=collage.co
<u>Return-Path</u>	<bounce+88dc72.80999b-stanleyekechukwu78@gmail.com@mg.collage.co>
<u>Received-SPF</u>	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;
<u>Authentication-Results</u>	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=qQjGVMdW; 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
<u>DKIM-Signature</u>	a=rsa-sha256; v=1; c=relaxed/relaxed; d=mg.collage.co; q=dns/txt; s=krs; t=175871970; x=1758725170; h=message-id: date: to: to: from: from: subject: content-type: mime-version: sender: sender: x-feedback-id: list-unsubscribe: list-unsubscribe-post: bh=PehNIBYf9qlLx2rqZN8myL3nOAYekX95ugdZlFs=; b=ccQ47kyt/bnqZpl41Ax5VNdlyfASoS0JvRHya/Bye5CvYjSe4ReVsi6jS+rO2mc1P4/OlgVyk1tr6E1FBNWWGRlikVUXFTMbB8EBScCIO3ZhNj+S9B8eRR/5lxMTCIrmvfqfmq4gUYOug4WGglWwKzxDMKW+tVb5pWfEmakaY=
<u>X-Mailgun-Sid</u>	WyJjOTNiMCIsInN0YYw5sZlIa2VjaHvrd3U3OEbnbWFpbC5jb20lCi4MDk50WIIXQ==
<u>List-Unsubscribe-Post</u>	List-Unsubscribe=One-Click
<u>List-Unsubscribe</u>	<https://email.mg.collage.co/u/eJwcjj1uhDAUBk-z7lj5BzAuXpGTWM_Pn1m0gKPFJOL2EammGGk0mSYdQkgKGy9rxN4-V1wyDXr0Njj1ohsFehSji0489ZA0Ge18Mto4yWohW8xgJPkOkmrYdEl733niuvLGAbjw_Totdr15RIPqWrDcfCM2K5vEJ-tbtyQo_Cel8wN8X9HfehovK-48la8zvfv6e_QfMun1E01etgv9UP2LwAA__1ST_w>
<u>X-Feedback-Id</u>	postmaster@mg.collage.co.ats_notifications:57631895803267fb972d47:mailgun
<u>X-Mailgun-Sending-Ip</u>	69.72.33.30
<u>Sender</u>	no-reply@collage.co@mg.collage.co
<u>Mime-Version</u>	1.0
<u>Content-Type</u>	multipart/alternative; boundary="dbe080596bedadd82dd56840bedb3432942f6da726707c6ee439475977b"
<u>Subject</u>	Thank you for your application to Rentsync
<u>From</u>	Collage HR <no-reply@collage.co>
<u>To</u>	stanleyekechukwu78@gmail.com
<u>X-Mailgun-Tag</u>	ats_notifications

All email features correspond, depicting authenticity aligned

The screenshot shows the MX Toolbox SuperTool interface. At the top, there's a navigation bar with links for Pricing, Tools, Delivery Center, Monitoring, Products, Blog, Support, and Login. Below the navigation is a main menu bar with items like SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, Analyze Headers (which is currently selected), and All Tools.

Header Analyzed

Email Subject: PRIME CUSTOMER - BRADESCO LIVELO: Your card has 92,990 LIVELO points expiring today!

[◀ Analyze New Header](#)

Copy/Paste Warning

Copying/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

Delivery Information

- o **✗ DMARC Compliant (No DMARC Record Found)**
- o **✗ SPF Alignment**
- o **✗ SPF Authenticated**
- o **✗ DKIM Alignment**
- o **✗ DKIM Authenticated**

Relay Information

Received 57 seconds

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=om@atendimento.com.br;comauth=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:62071BC7A7CF5B0844A7B406B0E9EFCDAAC2CB94988E687CF8C56555AD4B52D30;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-ExpirationInterval	1:00:00.00.000000

DomainKey-Signature	a=rsa-sha1; c=nofws; q=dns; s=smtp; d=hotprodhau.com; b=QlFe6aKsJUglID4D+HRAri+UXGKffM8GGUVZftSgEFqSkv/ncbyWSZrtbKD0D/EfoY3LM7YR wEExMEQoy9jQzOZbAHbbPXXUWQXcFuz0w7541YoQCGHuZtqDnmr1nZKOv+xqbGkZCKhBq9W+mBy sUWzZwbOcED0wsVcWRA=;
Date	Thu, 03 Nov 2022 15:36:18 +0000
To	phishing@pot
From	Dewalt EXTREME Drill Rewards <fkra@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	1:00:00.00.000000
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.

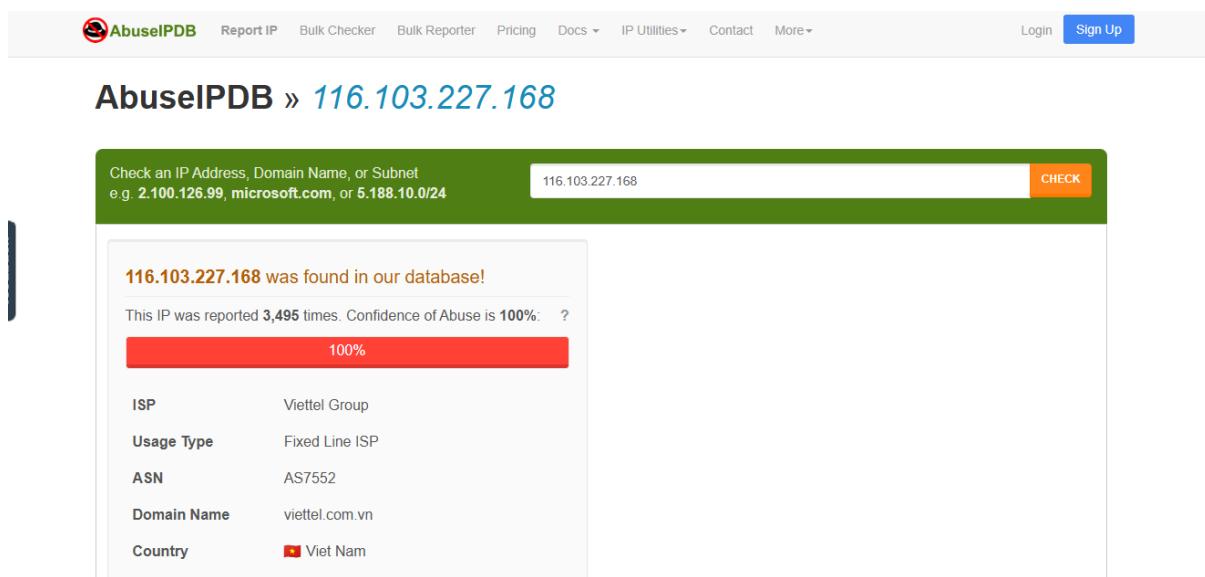
2. Monitoring & Detection:

- 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:

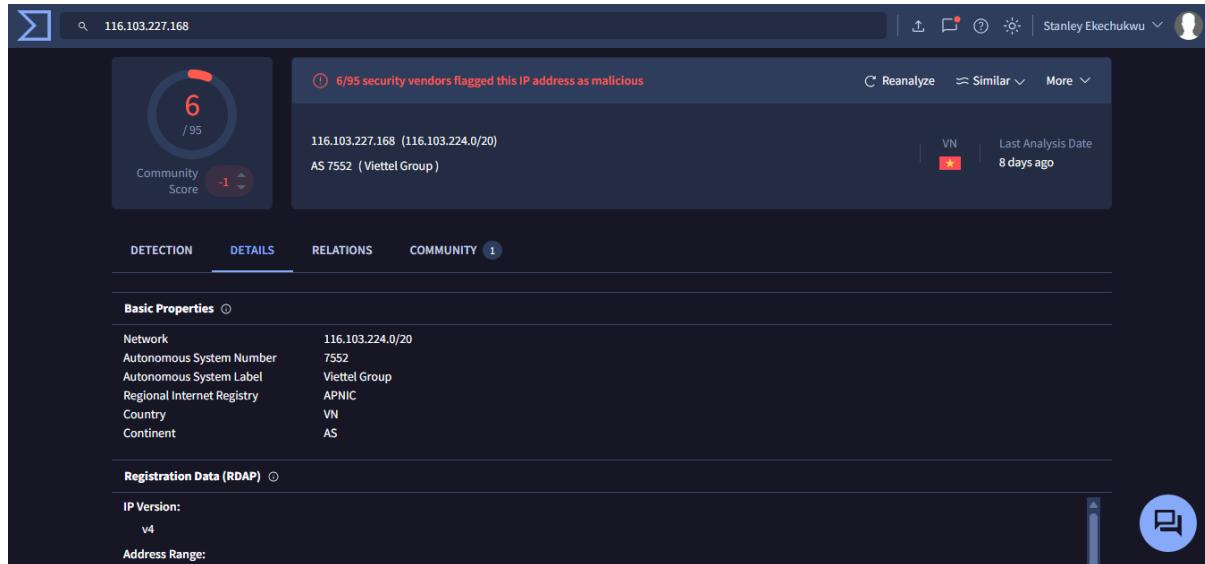
- Regular phishing simulation exercises to train staff on spotting red flags.
- Educate employees to verify sender domains, avoid clicking suspicious links, and report unusual emails.
- Promote a culture of “*Think Before You Click*” backed by clear reporting channels.

3. OSINT Threat Intel Exercise:



The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with links for Report IP, Bulk Checker, Bulk Reporter, Pricing, Docs, IP Utilities, Contact, and More. On the right side of the navigation bar are Login and Sign Up buttons. Below the navigation bar, the URL "AbuseIPDB » 116.103.227.168" is displayed. The main content area has a green header bar with the text "Check an IP Address, Domain Name, or Subnet e.g. 2.100.126.99, microsoft.com, or 5.188.10.0/24" and a search input field containing "116.103.227.168" with a "CHECK" button. The main content area displays the following information about the IP address:

116.103.227.168 was found in our database!	
This IP was reported 3,495 times. Confidence of Abuse is 100%.	
<div style="background-color: red; color: white; padding: 2px 10px; text-align: center;">100%</div>	
ISP	Viettel Group
Usage Type	Fixed Line ISP
ASN	AS7552
Domain Name	viettel.com.vn
Country	 Viet Nam



The screenshot shows the Sigma Threat Intel platform interface. At the top, there is a search bar with the IP address "116.103.227.168". The main content area displays the following information about the IP address:

6 / 95 security vendors flagged this IP address as malicious	
116.103.227.168 (116.103.224.0/20)	
AS 7552 (Viettel Group)	
Community Score	-1
VN	Last Analysis Date 8 days ago

Below this, there are tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY (1). The DETAILS tab is selected, showing the following properties:

Basic Properties	
Network	116.103.224.0/20
Autonomous System Number	7552
Autonomous System Label	Viettel Group
Regional Internet Registry	APNIC
Country	VN
Continent	AS

Below the properties, there are sections for Registration Data (RDAP) and IP Version (v4). There is also a note about the Address Range.

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.