THREAT INTELLIGENCE

Target: A1BC

Lum Rina Ngwan

Role: Threat Intelligence Analyst

Date: 16th June 2025

Table of Content

Executive Summary **2**

Project Scenario
2

Part 1: OSINT Framework – Information Gathering 3

Part 2: Security Risk Assessment 4

Part 3:Threat Actor Profiling

Part 4: Specific Threat actor - MITRE ATT&CK Mapping **9**

Recommendations **9**

Conclusion **9**

Executive Summary

A threat intelligence assessment A1BC of the Banking and Financial sector based on publicly available data collected passively using OSINT tools such as theHarvester, Whois, DNSdumpster, AlienVault OTX, Hunter.io, Shodan and Social media. This report also includes risk assessment, threat actor profiling, and MITRE ATT&CK mapping of the primarily identified threat actor ALPHV (BlackCat). Recommendations for improving the bank's cybersecurity posture are also provided.

Project Scenario

A1BC, in a quest to better understand the possible relevant cyber threats the organisation can face, I (Threat Intelligence Analyst) was assigned by Senior Management to conduct a threat intelligence activity.

In response, I deployed OSINT Framework (Information gathering), implemented a Security Risk Assessment, Threat Actor profiling, assessed the threat landscape, engaged in threat modeling, analyzed findings, proposed recommendations and communicated the results to the stakeholders.

Part 1: OSINT Framework – Information Gathering

A. OSINT Tools

1. **theHarvester:** Collected 125 hostnames, 6 emails, 37 IPs, 14 interesting URLs and 4 ASNS.

2. **Whois:** Disclosed domain registration details and DNS configurations confirming A1BC use of Enom.Inc and privacy preserving..

3. **Shodan:** While analysing A1BC's SSL, found exposed services and IP

addresses from Creolink Communication and infogenie technologies generally running across Apache http, outlook web app, Cisco Pix Sanitized smpd and Open Resty. The most common ports used are 443, 587, 25, 110 and 143 as seen below.

4. **Alienvault OTX:** identified historical malware delivery via fake bank portals, IPs linked to phishing servers, domains tagged in campaigns by TA505, pulses with relevant indicators like SMTP abuse, Brute-force ransomware.

5. **Hunter.io:** 42 publicly listed email addresses with a confidence score above 80% from the various departments of the organisation such as Executive, Finance, Management, Sales, Operations & Logistics, IT/Engineering as well as unknown departments.
   The email format {first}.{last}@

6. **DNSdumpster:** the DNS records revealed infrastructure and possible attack surfaces such as mail servers for phishing, TXT records for spoofing detection. Discovered 30+ subdomains showing each IP address, hostname, ASN and hosting provider and reverse DNS)

7. **Social Media:**
   Linkedin: identified 97 important job (IT, HR and Finance) roles susceptible to phishing or social engineering, job descriptions with tech stacks like Oracle, Unix AIX and INFORMIX).

B. Recommended Advisory Bodies For Threat Intelligence Sharing

In order to stay ahead of cyber threats and collaborate with peers, A1BC should consider joining the following organizations:

1. **FS-ISAC(Financial Service ISAC):** As a financial institution, membership provides access to a wealth of sector-specific threat intelligence and collaboration opportunities.

2. **FIRST (Forum of Incident Response and Security Teams):** A global forum that promotes cooperation and coordination among incident response teams.

3. **ISSA (Information System Security Association):** Offers educational forums, publications, and networking opportunities for information security professionals.

4. **Cyber Threat Alliance (CTA):** Encourages cybersecurity providers to share threat intelligence to improve defense against advanced cyber adversaries.

5. **CISA's Cybersecurity Collaboration Center:** Engages with industry and international partners to strengthen cybersecurity through shared insights and guidance.

Part 2: Security Risk Assessment

With respect to the passively collected information using the OSINT framework, we shall conduct a security risk assessment and analyse it to identify potential threats, vulnerabilities, and risks.

Findings	Risk	Potential Threats	Vulnerabilities	Recommendations
Emails: - Employee emails found via theHarvester and hunter.io - Potential exposure of email addresses on public forums and documents	-Unauthorized access to internal systems - Data breaches via compromised accounts	- Phishing attacks targeting employees - Email spoofing	Public exposure of email addresses	- Implement email filtering and anti-phishing solutions - Conduct regular security awareness training for employees, - Use email obfuscation techniques on public platforms.
Certificates: - SSL/TLS certificates retrieved from shodan - Details include issuer, validity period and associated domains	-Interception of sensitive data - Loss of customer trust due to security warnings	- Man-in-the-middle attack if certificates are misconfigured	- Use of outdated or weak encryption algorithms	- Regularly update and monitor SSL/TLS certificates - Use strong encryption algorithms and protocols - Implement certificate pinning where applicable
Job Postings: -Listing on company website and platforms like linkedin	-Tailored attacks exploiting known vulnerabilities	- Attackers gaining insights into internal technologies and systems	- Disclosure of specific software and tools used internally	- Limit the technical details disclosed in public job posting - Review and sanitize job

- Information about technologies such as Unix AIX and INFORMIX.	in disclosed technologies			descriptions to avoid revealing sensitive information
Ip addresses: - Public Ip ranges associated with the bank identified via Shodan - Services running on these IPs, including open ports and banners	-Denial of Service(Dos) attacks -Unauthorizes access to internal networks	-Direct attacks on exposed services	- Open ports with vulnerable services	- Implement firewalls and intrusion detection/prevention systems - Regularly scan for open ports and services - Restrict access to necessary services only
Subdomains; -Discovered using theHarvester and DNS enumeration tools; [redacted]	- Breach of specific services leading to broader network compromise	- Targeted attacks on less secure subdomains	-Misconfigured or outdated subdomains services	- Regularly audit and monitor subdomains for vulnerabilities - Decommission unused subdomains - Implement security measures like HTTPS and authentication on all subdomains
Social Media; -Employee profiles on Linkedin disclosing roles, projects and tools used. - Potential insights into organizational structure and ongoing initiatives	- Phishing and impersonation attacks targeting specific employees or departments	- Social engineering attacks based on employee information	- Oversharing of roles, projects, tools on public platforms	- Educate employees on the risks of oversharing on social platforms - Develop and enforce a social media policy - Monitor for unauthorized disclosures of company information

By systematically analysing the information gathered through passive reconnaissance, A1BC can identify potential security gaps and implement appropriate controls to mitigate associated risks. Regular assessments and updates to security measures are essential to adapt to evolving threats.

Part 3: Threat Actor Profiling

Profiling threat actors that can target A1BC based on OSINT results consist of taking into consideration;

- Industry: Banking and Financial
- Location: Cameroon, Central Africa
- Attack surface: Emails, public IPs, job postings, exposed services

Threat Actor/ Ransomware group	**Overview**	**Mitre TTPs**	**Relevance**	**links**
OPERA1ER/ Bluebottle	French-speaking cybercrime group targeting Francophone African banks since 2018. Responsible for $11-30 million in theft via spear phishing and Guloader RAT	**T1566** - spear phishing **T1059** - RAT deployment (infostealer.Eamfo via Guloader) **T1048** - Data exfiltration	Directly targets banks in Cameroon and surrounding regions - most relevant	https://therecord.media/cybercrime-group-targeting-banks-in-african-francophone-countries?utm_source=chatgpt.com
Hive	Raas emerging mid-2012, heavily focused on public health and government but also financial institutions (Bank of Zambia attacked in May 2022)	**T1501.003** - Web shells **T1003** - credential dumping **T1486** - File encryption	proven history of targeting African banks, applicable tools (webshell, exchange exploits)	https://en.m.wikipedia.org/wiki/Hive_(ransomware)?utm_source=chatgpt.com https://www.linkedin.com/pulse/exploring-top-cyber-threat-groups-common-tactics-ttps-ross-brewer-mm8ge?utm_source=share&utm_medium=member_ios&utm_campaign=share_via
LockBit	The world's most prolific Raas responsible for approx. 44% of all ransomware globally as of early 2023. known for fast encryption, public data leak	**T1566** - Phishing for initial access **T1078/T1021** - valid credentials and RDP usage **T1486** - data encryption for impact	Highly likely to target African financial institutions given global focus and partnerships with access brokers.	https://en.m.wikipedia.org/wiki/LockBit?utm_source=chatgpt.com

	threat, and significant attacks.			
ALPHV/BlackCat	A highly adaptive Raas, coded in Rust, stemming from DarkSide affiliates. Targets financial services and healthcare; extremely versatile.	**T1566** - phishing **T1003** - credential dumping **T1560/T1486 -** Data exfiltration and encryption	Explicitly targets financial services; known for extortion strategies highly applicable to banks.	https://www.sdosecurity.com/post/top-10-global-ransomware-groups-2025-with-mitre-ttps-and-recommendations?utm_source=chatgpt.com
Play (aka PlayCrypt)	First identified in 2022, targets MSPs to reach downstreams clients. Uses Russian - style encryption (".play" extension.	T1566 - phishing T1059/T1505 - living off the land and web T1486 - Encryption impact	A1BC relies on MSPs, and could be collateral victims due to affiliate targeting.	https://en.m.wikipedia.org/wiki/Play_(hacker_group)?utm_source=chatgpt.com

Historical Ransomware & Cyber Incidents

- DangerousSavanna

A long-running (2020–22) spear-phishing/malware campaign targeting French-speaking African banks:

- Used macro malware, RATs (AsyncRAT, Metasploit)
- Timeline: two years of activity through 2022

- Symantec-reported West African banking attacks (2017–18)

Multiple malware campaigns in Cameroon & Ivory Coast:
Tools: Trojan.NanoCore, Mimikatz, RATs (Gussdoor, Imminent Monitor)

- SWIFT Hacks (2015–16)

APT38 took over SWIFT banking credentials:

- Stole $100 M from the Bangladesh central bank; similar attack in Vietnam
- MITRE TTPs: credential theft, transaction manipulation

Part 4: TTP Mapping with MITRE ATT&CK

Based on data collected, ALPHV(BlackCat) poses the greatest threat to A1BC. The following reasons explain why ALPHV is a primary threat:

- **Financial Sector Focus:** ALPHV is a top-tier ransomware group targeting banks, financial services, and critical infrastructure globally.
- **Advanced Capabilities:** Built in Rust, featuring modular code supporting Windows, Linux, and VMware ESXi; supports double/triple/quadruple extortion tactics.
- **Stealth and Speed:** Uses tools like ExMatter for automated data exfiltration, obfuscation, encrypted strings, and log-clearing to evade detection.
- **Extensive Impact:** Over 1,000 victims and ~$300 M in ransom collected; known to encrypt data, exfiltrate files via APIs, threaten DDoS, and publicize leaks for added pressure.
- **Affiliate Ecosystem:** Supported by seasoned cybercriminals from DarkSide, BlackMatter, and REvil; has affiliates like Scattered Spider using sophisticated tool sets ￼.

Thus, ALPHV is structurally and tactically well-equipped to compromise financial institutions like A1BC.

Detailed Threat Actor Profile: ALPHV (BlackCat)

- **Identity and Origins:**

A Rust-based RaaS (Ransomware-as-a-Service) first identified in Nov 2021. Evolved from BlackMatter/DarkSide lineage, uses an affiliate model with high payouts (up to 90%)￼.

- **Tactics, Techniques, and Procedures:**

Combining phishing, credential theft, remote services, stealth, and multi-stage extortion:

Tactics	Techniques (MITRE IDs)	Description
Initial Access	Spear Phishing (T1566), Valid Accounts via helpdesk (T1598, T1078)	Impersonation of IT staff to steal credentials.
Execution	Command/Script Interpreter (T1059), GPO/Scheduled Tasks	Uses PowerShell, batch scripts, WMI for spread and execution
Persistence	Account Manipulation (T1098), External Remote Services (T1133)	Creates new accounts, deploys AnyDesk/Plink/Ngrok

Privilege Escalation	UAC Bypass (T1548.002), Access Token Manipulation (T1134)	Employs token elevation and abuse of Kerberos
Defense Evasion	Disables security, clears logs (T1562, T1070), Whitelisting (T1562.009)	Uses POORTRY, STONESTOP utilities
Credential Access	MFA bypass via Evilginx2 (T1557), Kerberos ticket forging	Steals session cookies and credentials
Discovery	Network/System Discovery (various: T1018, T1087)	Uses NBSTAT, SMB to identify hosts
Lateral Movement	SMB propagation (T1021), Psexec (T1570), Cobalt Strike	Moves laterally across the network
Collection & Exfiltration	Data staged/exfil via ExMatter, cloud, APIs (T1530, T1048)	ExMatter steals data pre-encryption and leaks to dark/clear web
Impact	Encryption (T1486), DDoS extortion (T1499), Service disruptions (T1490)	Uses quadruple extortion tactics

Recommendations

1. Implement aggressive Multi-Factor Authentication (MFA) and harden helpdesk verification to prevent social-engineering credential theft.
2. Monitor for ExMatter indicators, abnormal cloud uploads, and DDoS-related signals.
3. Harden remote services: VPN, RDP, Exchange; apply patches for CVEs exploited by ALPHV variants.
4. Deploy proactive threat hunting and detection focused on User Account Control (UAC) bypass, log deletion, token forging, scheduled tasks, Server Message Block (SMB) enumeration.
5. Prepare incident response for ransomware: backups, offline storage,

legal/regulatory coordination, and public leak management.

Conclusion

In a nutshell,this threat intelligence project has provided a comprehensive analysis of the cyber risks facing A1BC via passive information gathering, threat actor profiling, and attack surface assessment. Using OSINT tools such as theHarvester, Shodan, Hunter.io, AlienVault OTX, DNSdumpster, Whois and Social Media, we uncovered critical data points including exposed emails, public IP addresses, outdated SSL certificates, and job postings that reveal internal technologies.

We identified and profiled five major threat actors, with ALPHV (BlackCat) emerging as the most significant threat due to its advanced ransomware tactics, financial sector focus, and use of sophisticated attack vectors mapped to the MITRE ATT&CK framework. Historical incidents and ransomware campaigns in the West African banking sector further highlight the relevance of these threats.

This assessment underscores the urgent need for A1BC to strengthen its cybersecurity posture through:

- Improved phishing resistance,
- Remote access security,
- Endpoint protection,
- Threat intelligence sharing, and
- Incident response readiness.

By proactively addressing the identified vulnerabilities and preparing for high-impact threat scenarios, A1BC can significantly reduce its risk exposure and better protect its digital assets, clients, and reputation.