**Threat Intelligence Analysis**

**Cover Page**

**Project Title:** Threat Intelligence Analysis

**Organization:** OKZ University of Lagos

**Analyst:** Israel Okezie Ozomagbo

**Role:** Threat Intelligence Analyst

**Submission Date**:27th May,2025.

Table of Contents

1. Executive Summary
2. OSINT Findings- Summary of Discovered Footprints
3. Malware Analysis-Observations, IOCs and Threat Indicators
4. Threat Actors Profile- Group attribution, known motives, and operations
5. TTP Mapping-MITRE heatmap and explanation of tactics

6. Recommendations

8. References

1. **Executive Summary: Threat Intelligence Assessment for OKZ University of Lagos.**

**Objectives**

This project is aimed at identifying and assessing the type of cyber threats faced by OKZ University of Lagos. It is a proactive approach to find the threat before the breach and promoting a culture of vigilance, awareness and formulation of a long term cybersecurity strategies that adapts to evolving threats and technologies.

**Overview**

***Disclaimer: The name of the university stated here is a dummy name as the original organization cannot be named. Also, all information are passively gathered.***

This executive summary highlights the findings of an open-source intelligence (OSINT) reconnaissance assessment conducted on OKZ University of Lagos using tools like **theHarvester**, hunter.io, waybackmachine, HaveIbeenpwnd,crt.sh etc to gather publicly available information. The goal was to identify potential exposure points, vulnerabilities and threats that could be leveraged by threat actors in planning cyberattacks against the university.

**Key Findings**

1. **Email Exposure**

A total of 24 unique email addresses were discovered from the university's domain. Some addresses associated with students, academic and administrative staff were also discovered. This information can be exploited for phishing campaigns and social engineering attacks.

1. **Subdomain**

About 400 subdomains related to the university’s primary domain was found. These subdomains might contain sensitive information or services that could be vulnerable to attack. Some of the subdomains were actually not adequately secured as they are discovered to have invalid SSL and TLS certificates and badly configured DNS records. This could be a potential entry points for attackers.

1. **IP Addresses**

A lot of IP addresses associated with critical infrastructure such as web servers, email servers, and login portals were found and this that may be vulnerable to brute force or known exploits if not properly secured.

1. **Interesting urls**

A number of interesting urls were found and this could be used to identify potential vulnerabilities like outdated software or misconfigured services. Also, attackers can create a potential network usernames by twisting the information before the ‘@’ symbol and can attempt to brute-force their way into services like SSH,VPNs or FTP.

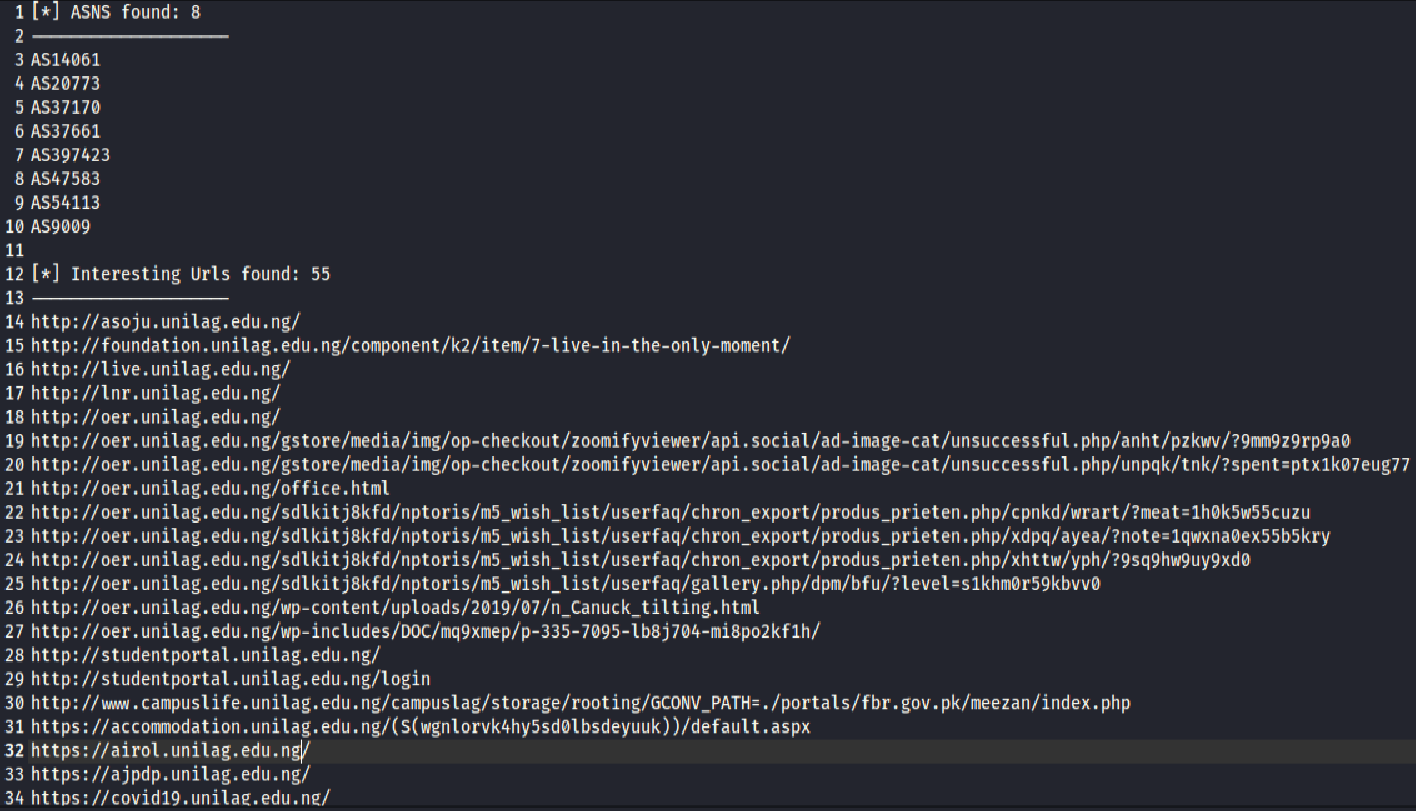
**Risks and Implications**

* **Phishing Risk**: The availability of personal and institutional email addresses greatly increases the risk of email-based attacks.
* **Credential Harvesting**: Publicly exposed login portals and known subdomains might be exploited for unauthorized access attempts.
* **Reputation and Data Integrity**: Academic institutions are frequent targets of intellectual property theft and ransomware campaigns. Publicly available information can serve as the first step in such intrusions.

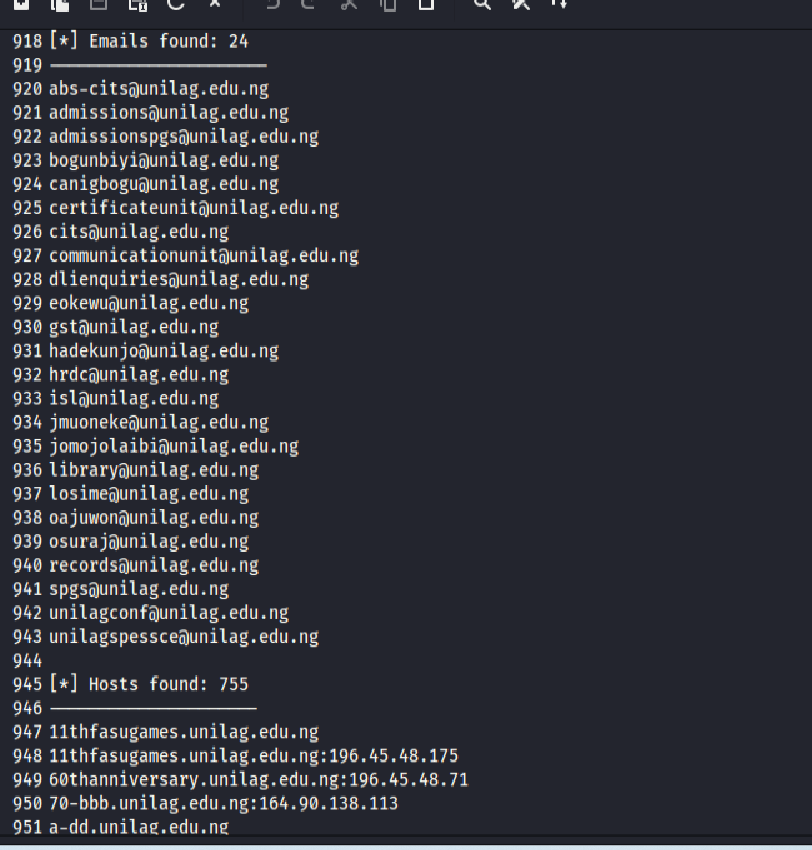
**Part 2: Basic Threat Intel or OSINT(Information Gathering)**

**Threat Intelligent tools used**: theHarvester,Crt.sh,hunter.io,waybackmachine,HaveIbeenpwned,Domaindumpster

***Screenshots of information gathered with OSINT Tools.***



***Screenshot of information gathered with OSINT Tools***.



c) To learn more and to exchange Threat Intelligence news, we suggest that OKZ University should join the below professional organizations

* **NCSC**:The NCSC provides regular updates and advice on emerging threats, vulnerabilities, and best practices.
* **CISA**: CISA's Threat Intelligence Platform (TIP) provides a centralized hub for threat intelligence data, allowing organizations to access and share information with other agencies and partners.
* **LevelBlue**:Offers free IT security tools and dashboard to help detect and investigate threats .
* **Google Threat Analysis Group**: Explore the latest news, real-world incidents, expert analysis, and trends about cyber security
* **Recorded Future**: They pinpoints threats that matter most, empowering you to prioritize and act swiftly before attacks take a shape and impact your environment.

Part 3: Security Risk Assessment

Below is a breakdown of the types of information found on OKZ University of Lagos.

* 1. Threats, vulnerabilities ,potential risks and controls were also mentioned in a tabular form.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Information**  **Found** | **Sources** | **Vulnerabilities** | **Applicable**  **Threats** | **Potential**  **Risks** | **Controls** |
| ***Emails*** | **Employee**  **emails such**  **as firstname@okz**  **.edu.ng** | **Twitter,**  **Social Media,**  **Press Releases,**  **Publications** | **Employee emails and email formats**  **were exposed** | **Email**  **Phishing**  **Spear**  **Phishing** | **Unauthorized**  **Access** | **OKZ University**  **must train**  **employees in**  **Phishing and online security from time to time.** |
| **DDOS,**  **Social**  **Engineering** | **Data**  **Breaches** |
| ***Certificates*** | **Secure Sockets**  **Layer and Transport**  **Layer Security**  **(SSL/TLS)**  **Certificates for**  **their web services(demo.**  **Okz.edu.ng, connect.**  **Donate.okz.edu.ng,**  **Connect.api.okz.edu.**  **Ng, testonline.ok.edu.**  **Ng)** | **SSL/TLS**  **Checkers**  **(crt.sh was used to validate certificate installation** | **Exposure of weak and expired certificates** | **Revoked,**  **Expired or**  **Compromised**  **Certificates** | **Man-in-the-Middle attacks if**  **Certificates expire or are not configured properly.**  **Loss of clients’ trust** | **OKZ University should conduct regular audits on its certificates.**  **They should activate automatic renewal of expired certificates** |
| ***Social Media*** | **Posts made about**  **School projects,**  **services,**  **Key staff members, and stake-holders** | **LinkedIn, Twitter,**  **Publications** | **Employees, Lecturers, Senior admin members,**  **Over-sharing information.** | **Key staff targeted**  **Phishing, Account**  **Hijacking, Classified**  **Information leakage,**  **Identity theft.** | **Reputational**  **Damage,**  **Login credential**  **Compromise, Accounts**  **compromise,**  **Spear phishing.** | **Social Awareness**  **Trainings, Policies about sharing on social media,**  **Regular monitoring of**  **Social media handles.** |
| ***Subdomains*** | **About 300 Subdomains were**  **Found. This includes**  **Testonline.okz.edu.ng,**  **Tetfund.okz.edu.ng,**  **Foundation.okz.edu.**  **Ng etc** | **OSINT Tools such as Crt.sh** | **Shadow IT,**  **Unmonitored**  **Subdomains, Badly**  **Configured DNS and**  **CNAME Records, Subdomain enumeration for reconnaissance.** | **Attackers can use**  **DNS Poisoning, Redirecting users to**  **Malicious sites. Also knowing which subdomains that exist allows attackers to prioritize targets.** | **Subdomains created unofficially by the employees or the teams may not be properly tracked.**  **Badly configured DNS records can allow attackers to hijack subdomains and redirect traffic to fraudulent sites, and perform distributed denial of service attacks(DDoS).** | **Implement robust monitoring and security measures.**  **Remove unused or abandoned subdomains.**  **Conduct regular subdomain inventory**  **Use EASM tools: Employ External Attack Surface Management to continuously monitor your domain and identify vulnerabilities like misconfigured or abandoned subdomains.** |

**b) OKZ University Online presence and It’s implications**

We have been able to gather some valuable information of OKZ University that are available online using the Open Source Intelligence Tools(OSINT)We also took screenshots to show the results .

Our findings includes about 8 ASNS numbers, 55 interesting urls,129 ips,24 emails,755 hosts etc.

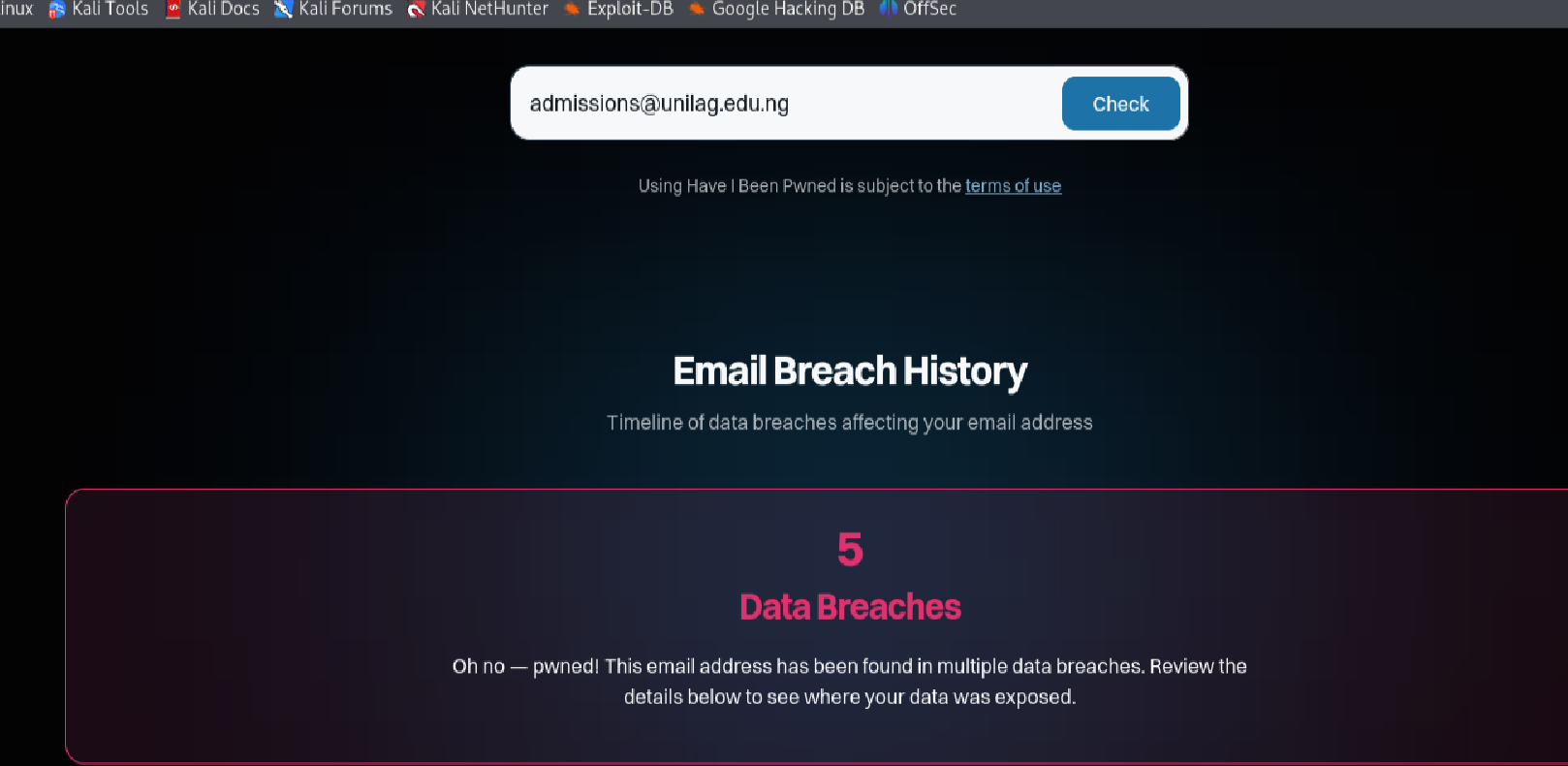
Having validated our findings with tools like crt.sh, HaveIbeenpwnd, waybackmachine, We have discovered some threats to the organisation as discussed further below.

**i)Emails**: [Email security](https://perception-point.io/guides/email-security/email-security-threats-solutions-8-critical-best-practices/) breaches occur when unauthorized individuals gain access to an organization’s email accounts or intercept email communications. These breaches can lead to the loss of sensitive information, financial damage, and harm to an organization’s reputation. They exploit vulnerabilities in email systems or human error, leading to unauthorized access and data theft.

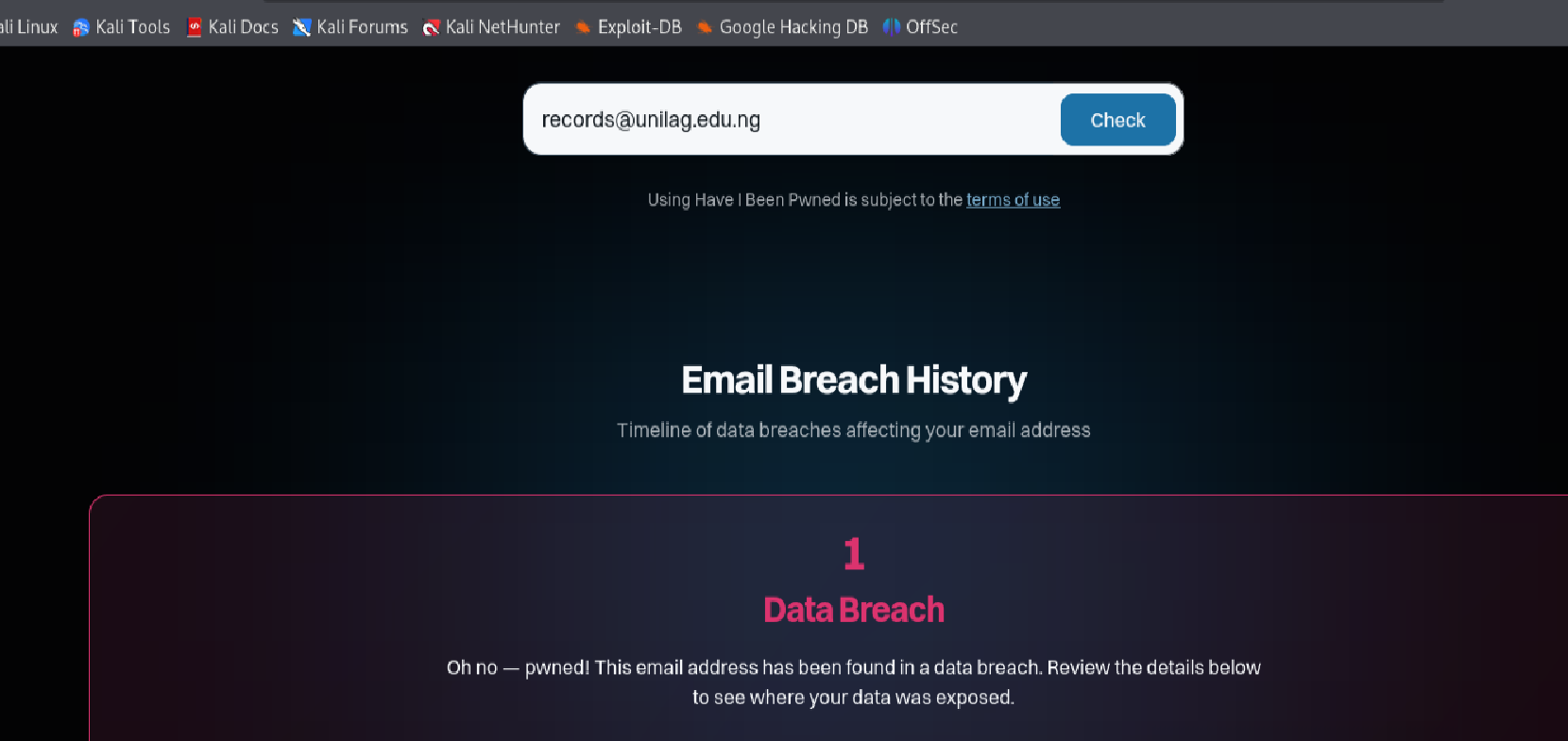
From our findings, some high profile emails like [admissions@okz.edu.ng](mailto:admissions@okz.edu.ng), and [admissions@okz.edu.ng](mailto:admissions@okz.edu.ng) have been breached few times as shown in the screenshot.

**Tool used to confirm email breaches : HaveIbeenpwned**

***Screenshot showing email breaches***



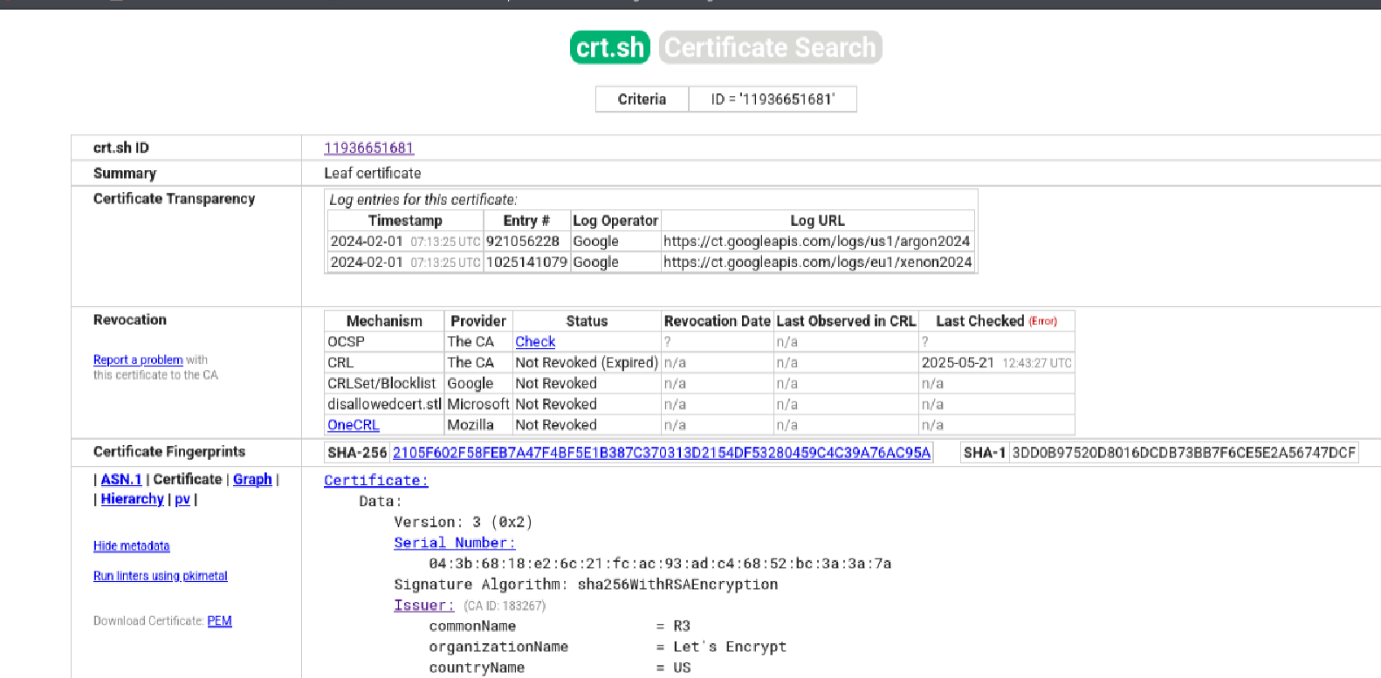
***Screenshot showing email breaches***



**ii) Subdomains**: We have also discovered that there are many subdomains with expired or invalid SSL certificates. SSL certificates protect sensitive information, such as passwords, credit card details, and other personal data, from being intercepted by unauthorized parties. The screenshot below shows some of the expired certificates discovered.

**Tool used to validate the SSL certificate : crt.sh**

*Screenshot showing invalid subdomains*



*Screenshots showing invalid subdomains*



Based on the vulnerabilities from the findings such as expired ssl certificates of,

unmonitored subdomains, email breaches already noticed, oversharing of information by the employees, IT Shadowing, OKZ university lagos is susceptible to the following threat actors which are well-known to attack Educational Institutions.

Part 4: **Threat Actors Profile**

Threat actors that are actively attacking Educational Institutions such as OKZ University are listed below:

1. **Vice Society (Ransomware Group)**

* **IOCs**:
  + **File hashes** of known ransomware variants (e.g., .docx, .xlsx, .pdf files that are weaponized).
  + **Domain names** used for command-and-control (C2) servers: e.g., [vicelog.xyz](http://vicelog.xyz).
  + **IP addresses** used by C2 servers: Specific to **Russian and Eastern European** locations.
* **TTPs**:
  + **Initial Access**: Phishing emails with malicious attachments or links.
  + **Execution**: Ransomware payload executed via scripts or macro files.
  + **Persistence**: Use of **web shells** or **remote access tools** (RATs) to maintain access.
  + **Exfiltration**: Data exfiltration is followed by **double extortion** — threatening to release sensitive data unless ransom is paid.
  + **Impact**: Disruption of services and significant data breaches.
* **Motives**:
* **Financial gain** through ransom demands.
* **Secondary objective**: Stealing data for later leaks or resale.
* **Targeting Patterns**:
* **Primary targets**: **Educational institutions**, particularly in the US, UK, and Europe.
* **Tactics**: Vice Society tends to attack entities with large, centralized

networks with outdated security measures.

* **Geography/History**:
  + **Russia**, Eastern Europe, **US**, **UK**, **Australia**.

<https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/>

<https://www.bbc.co.uk/news/uk-england-gloucestershire-63637883>

**APT40 or BRONZE MOHAWK (Chinese State-Sponsored)**

**IOCs**:

**IP addresses** associated with Chinese government infrastructure.

**File hashes** related to backdoors such as **Mimikatz** or **Web Shells**.

Domains like **research.ppt.cn** (used for espionage-themed social engineering).

**TTPs**:

**Initial Access**: Phishing emails, exploitation of **zero-day vulnerabilities** in software like **Adobe Flash** or **Microsoft Office**.

**Execution**: Use of **Living-off-the-Land** (LoL) techniques (e.g., PowerShell scripts for lateral movement).

**Exfiltration**: Use of **encrypted communications** (e.g., **SSL VPN** tunnelling or DNS exfiltration).

**Impact**: Data theft targeting intellectual property, university research, and sensitive data.

**Motives**:

* **Espionage**: Collecting **sensitive research data** for Chinese government or corporate

advantage.

**Targeting Patterns**:

* Targets **universities** with significant research in technology, defence, and scientific fields.
* Active across **global universities**, especially those with prominent **academic partnerships with Western governments**.

**Geography/History**:

Primarily **China**-linked, targeting universities in **the United States**, **Canada**, **Europe**, and **Australia**.

<https://www.avertium.com/resources/threat-reports/bronze-mohawk-and-cyber-espionage>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-200a>

1. **Mustang Panda (Chinese APT)**

**IOCs**:

**C2 domain names** used in spear-phishing campaigns: e.g., **gov.cn**, **edu.cn**.

**IP ranges** linked to Chinese universities or government entities.

**TTPs**:

**Initial Access**: Exploit public-facing services (e.g., **web servers**, **email systems**), often leveraging **zero-day vulnerabilities**.

**Execution**: **Web shells** to maintain access and move laterally.

**Exfiltration**: Targeted exfiltration of **intellectual property** (focus on advanced technology sectors).

**Motives**:

**Cyber espionage** to acquire **critical academic and technological research** for Chinese national interests.

**Targeting Patterns**:

**Universities and research centers** with strong ties to **AI**, **biotechnology**, and **semiconductor research**.

Often targets **high-profile professors** or **researchers** working on sensitive technologies.

**Geography/History**:

Primarily targeting the **US**, **Europe**, and **Japan** for technological or industrial espionage.

<https://cyble.com/blog/vietnamese-entities-targeted-by-china-linked-mustang-panda-in-cyber-espionage/>

**APT35 or Charming Kitten (Iranian State-Sponsored)**

**IOCs**:

**IP addresses** related to Iranian infrastructure and **Tor** nodes for anonymized C2.

**File hashes** of **Win32-based backdoors** such as **Poison Ivy** and **Sonic**.

**SSL certificates** associated with Iranian domains and infrastructure.

**TTPs**:

**Initial Access**: Spear-phishing emails disguised as academic research papers or critical alerts (e.g., Iran-based universities impersonated).

**Exploitation**: **Credential stuffing** and **password spraying** to access university portals.

**Exfiltration**: Focus on stealing **sensitive government, military, and academic data**.

**Motives**:

**Espionage** aimed at obtaining **nuclear, military, and political research**.

**Geopolitical motives**: Disrupt or steal academic data related to international policies or military research.

**Targeting Patterns**:

**Targeted academia**, particularly **scholars** or **students** working on politically sensitive subjects like nuclear technology or defense.

**Geopolitical intelligence** (related to the Middle East, US-Iran relations).

**Geography/History**:

Targets institutions primarily in **North America**, **Europe**, and **the Middle East**, specifically universities tied to **US** and **Israeli** research.

<https://en.wikipedia.org/wiki/Charming_Kitten>

<https://threatpost.com/charming-kitten-uses-fake-interview-requests-to-target-public-figures/152628/>

**5. Clop OR TA505 (Ransomware Group)**

* **IOCs**:
  + File hashes for **Clop ransomware variants** (e.g., **Clop2.exe**).
  + Known **C2 domains** (e.g., **clop.ransom.com**).
  + **VPN and RDP login attempts** tied to specific user credentials (Linked to breaches).
* **TTPs**:
  + **Initial Access**: RDP brute force or exploiting **unpatched VPN systems** (e.g., Pulse Secure).
  + **Execution**: Use of ransomware loaders like **Cobalt Strike** and **PowerShell-based payloads**.
  + **Exfiltration**: **Double extortion** method; data is stolen before encryption.
  + **Impact**: High disruption and financial cost due to critical system encryption and potential leak of academic research data.
* **Motives**:
  + **Financial gain** via ransom.
  + Secondary objective: **Data extortion** or selling stolen data.
* **Targeting Patterns**:
  + Historically targets **higher education institutions**, with some attacks focusing on **large research organizations**.
  + **Ransom demand tactics**: Targets both large universities and specific **research departments** like medical and AI-related fields.
* **Geography/History**:
  + Targets across **North America**, **Europe**, and **Asia** (notably **the United States**, **Germany**, and **the UK**).

<https://www.cyfirma.com/research/cl0p-ransomware-latest-attacks/>

PART5 :**TTP Mapping with - MITRE ATT&CK for APT40**

Having identified about five threat actors such as **Vice Society,APT40,Mustang Panda,APT35 and Clop**, We think that **APT40** poses the greatest threat **to OKZ University Lagos.**

The following reasons supports our claim:

1. **Valuable Research Data**: Universities often perform cutting-edge research and such intellectual property (IP) can be worth millions of dollars. While university researchers might think of the prestige of developing techniques and making discoveries, failing to think about cybersecurity to protect this research can make it vulnerable to [data leaks and data breaches](https://www.upguard.com/blog/data-breach-vs-data-leak).

Cybercriminals such as **APT40** are well-known for intellectual property theft.

**Lack of Cyber Security**: The Educational Sector has been very slow in adopt

ng the use of modern cyber security solutions due to funding reasons. Public Institutions are mostly poorly funded by government and in turn, cybersecurity is often deprioritized in Favor of staff salaries, school resources, and infrastructure upgrades.

cybercriminals often target the schools with the least funding since they typically have poor cyber defences.

1. **Personal Data:** Educational organizations keep data on the learners enrolled with them. This data may include personally identifiable information, such as:

Full names

Street addresses

Email addresses

Phone numbers

Grades and aptitude information

Credit card details

Social security numbers

Student loan information

The bigger the organization, the more records it is likely to store. Unfortunately, from a cybersecurity standpoint, a larger organization is likely to have organizational and security challenges and large amounts of student data.

This means that threat actors know where they might find large amounts of personal data and where that data is likely to be easy to access and for this reason **APT40** find educational sector an easy target and where they can operate easily for long time without detection.

**APT40 THREAT PROFILE**

Threat Profile: APT40 (BRONZE MOHAWK)

APT40, also known by its alias BRONZE MOHAWK, is a Chinese state-sponsored cyber espionage group. It is primarily linked to the Hainan State Security Department (HSSD), an agency within China's intelligence community. APT40 has been active since at least 2013, and its operations primarily focus on intellectual property theft, industrial espionage, and geopolitical intelligence gathering. This group is known to target high-value research, particularly in sectors like biotechnology, maritime research, and defence technologies.

**Key Characteristics and Targeting Patterns**

APT40 typically targets global academic institutions, defence contractors, and energy companies. Their focus has been on sectors with technological research, military applications, and maritime industry advancements. The group has a notable history of exploiting zero-day vulnerabilities, utilizing spear-phishing, and web shell installations for long-term persistence.

**Notable Campaigns and Attacks**:

1. Operation Cloud Hopper (2017-2019)
   * APT40 was identified as a key player in the Cloud Hopper campaign, which targeted Managed Service Providers (MSPs) that provided services to universities, defence contractors, and government entities. Through these third parties, APT40 compromised the supply chains of several organizations globally.
   * Tactics: Spear-phishing, exploitation of vulnerabilities in remote desktop services, and use of web shells to maintain access.
2. Targeting U.S. Universities (2018)
   * APT40 is known for targeting universities conducting research in maritime technologies, advanced materials, and biotech. By compromising the networks of these institutions, APT40 harvested sensitive academic research related to underwater technology and oceanographic systems.
   * These attacks often include phishing emails disguised as research collaborations or official communications, exploiting credential stuffing and RDP brute-force techniques.
3. Maritime Industry Attacks (2020)
   * In 2020, APT40 targeted the maritime industry by exploiting vulnerabilities in VPN and RDP systems, allowing them to gain access to sensitive logistics and operational data. This allowed them to monitor and steal trade secrets related to shipping technologies and marine engineering.
4. **MITRE ATT&CK Mapping for APT40**

APT40’s behaviour and tactics align closely with several MITRE ATT&CK techniques. Below is a detailed mapping of APT40’s tactics, techniques, and procedures (TTPs) as observed in their campaigns:

**Tactic 1: Initial Access**

1. Phishing (T1566)
   * APT40 frequently uses spear-phishing emails as an initial attack vector, often sending emails with attachments or links to compromised documents that exploit zero-day vulnerabilities in Microsoft Office or Adobe Flash.
   * Example: Targeted emails disguised as official communications or academic collaboration invitations.
2. Exploitation for Initial Access (T1203)
   * APT40 has been known to exploit unpatched vulnerabilities in VPN systems (e.g., Pulse Secure, FortiGate) and remote desktop protocols (RDP) to gain initial access into academic and defence industry networks.
   * Example: Exploiting RDP to gain initial access into vulnerable academic systems with weak password policies.

**Tactic 2: Execution**

1. Command and Scripting Interpreter (T1059)
   * Once access is gained, APT40 uses PowerShell, VBScript, and other scripting languages to execute commands and move laterally within the network. These tools help to maintain persistence and execute further attacks or exfiltration of data.
   * Example: Using PowerShell scripts to download additional payloads or enable lateral movement.
2. Exploitation of Remote Services (T1210)
   * APT40 is known to use RDP and VPN vulnerabilities to remotely execute scripts and commands once they have gained access to an organization’s internal network.
   * Example: Exploiting unpatched RDP vulnerabilities to execute payloads within compromised systems.

**Tactic 3: Persistence**

1. Web Shells (T1100)
   * APT40 installs web shells on compromised web servers as a means of maintaining persistence and controlling the target’s environment. Web shells are often used in environments with poorly configured public-facing web applications.
   * Example: Deploying a PHP-based web shell to maintain access to a university’s public-facing web portal.
2. Scheduled Task/Job (T1053)
   * APT40 uses scheduled tasks to create persistent access. This tactic helps ensure the adversary can maintain access to systems by running commands at specific intervals.
   * Example: Creating scheduled tasks that execute malicious scripts at regular intervals, ensuring long-term access to the network.

**Tactic 4: Privilege Escalation**

Exploitation for Privilege Escalation (T1068)

* + APT40 leverages local privilege escalation vulnerabilities within Windows operating systems to escalate privileges within compromised systems. This allows them to gain administrator or root access to critical systems.
  + Example: Using EternalBlue or CVE-2020-0796 vulnerabilities to escalate privileges and gain full control of compromised systems.

Bypass User Account Control (T1088)

* + APT40 bypasses User Account Control (UAC) mechanisms on Windows to execute higher-privilege actions without triggering security alerts or notifications.
  + Example: Using UAC bypass techniques to escalate privileges on compromised systems without detection.

Tactic 5: Defence Evasion

Obfuscated Files or Information (T1027)

* + APT40 regularly employs obfuscation techniques to evade detection by security products. This includes encoding and compressing files or using fileless malware that doesn’t touch the disk.
  + Example: Using Base64 encoding to hide malicious scripts or payloads in phishing emails.

Disabling Security Tools (T1089)

* + APT40 attempts to disable security software (e.g., antivirus, endpoint detection) by terminating processes or modifying configuration settings, thereby avoiding detection during later stages of the attack.
  + Example: Disabling Windows Defender or other endpoint security tools using PowerShell commands.

**Tactic 6: Credential Access**

1. Credential Dumping (T1003)
   * APT40 often uses credential dumping tools like Mimikatz to extract cleartext passwords and other credential information from memory. These credentials are then used to gain additional access to other network resources.
   * Example: Using Mimikatz to dump credentials from a compromised academic system and move laterally to other systems within the university.
2. Brute Force (T1110)
   * Password spraying and RDP brute-force attacks are common in APT40 campaigns. They often target accounts with weak or reused passwords to gain access to internal systems.
   * Example: Attempting to guess weak passwords on VPN or RDP services exposed to the internet.

**Tactic 7: Exfiltration**

Exfiltration Over Command and Control Channel (T1041)

* + After gathering the targeted data, APT40 uses encrypted C2 channels (e.g., HTTPS, DNS tunnelling) to exfiltrate stolen research or intellectual property from compromised university or defence networks.
  + Example: Using HTTPS or DNS tunnelling to send exfiltrated research data to external servers under their control.

Exfiltration to Cloud Storage (T1537)

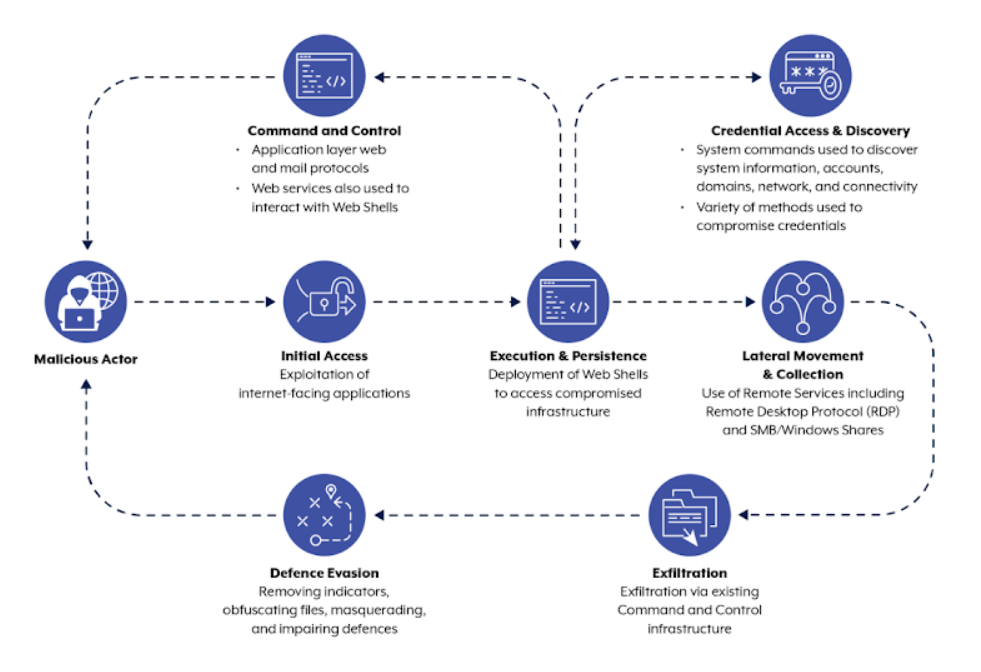
* + In some cases, APT40 utilizes cloud-based file storage platforms (e.g., Dropbox, Google Drive) for exfiltration, leveraging obfuscated uploads to evade detection by security tools.
  + Example: Exfiltrating sensitive research data via cloud storage platforms.

**Tactic 8: Impact**

Data Encrypted for Impact (T1486)

* + Although primarily focused on espionage, APT40 has also used data encryption in specific campaigns to disrupt organizations’ access to critical data. However, data encryption is typically not their main focus (unlike ransomware groups).
  + Example: Encrypting sensitive files before exfiltrating them as a secondary tactic of disruption.

***Diagram showing APT40 TTP***



**Conclusion**

APT40 is a ferocious , persistent, and strategic threat actor with a clear focus on cyber espionage and intellectual property theft. Their tactics shows the group’s capabilities and objectives. They gain initial access through phishing and exploitation, maintaining long-term persistence with web shells and credential dumping, and stealing valuable research from targeted institutions, particularly universities and defence-related entities. The group's targeting is highly sophisticated, and their use of the MITRE ATT&CK framework demonstrates a well-coordinated attack chain designed to infiltrate and exfiltrate sensitive data while evading detection for extended periods.

**APT40 MAPPING WITH MITRE ATT&CK FRAME WORK**

We mapped their TTPs to the MITRE ATT&CK matrix, organizations can better prepare their defences, particularly by focusing on phishing defences, vulnerability patching, and monitoring for anomalous activities such as the use of web shells or unauthorized RDP connections.

**Part 5: TACTICS,TECHNIQUE AND PROCEDURES (TTP) MAPPING**

|  |  |  |
| --- | --- | --- |
| **TACTIC** | **TECHNIQUE** | **PROCEDURE** |
| ***Reconnaissance*** | **T1598.001 Gather Victim Identity Information** | **Adversaries may send spear phishing messages via third-party services to elicit sensitive information that can be used during targeting. Spear phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spear phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex:** [**Establish Accounts**](https://attack.mitre.org/techniques/T1585) **or** [**Compromise Accounts**](https://attack.mitre.org/techniques/T1586)**) and/or sending multiple, seemingly urgent messages.** |
| ***Resource Development*** | [**T1584**](https://attack.mitre.org/techniques/T1584)  **Compromise**  **Infrastructure** | **Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, network devices, and third-party web and DNS services. Instead of buying, leasing, or renting infrastructure an adversary may compromise infrastructure and use it during other phases of the adversary lifecycle. Additionally, adversaries may compromise numerous machines to form a botnet they can leverage** |
|  |  |  |
| ***Initial Access*** | [**T1190**](https://attack.mitre.org/techniques/T1190) **Exploit public facing application** | **Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.** |
| ***Execution*** | **T1059.001** [**PowerShell**](https://attack.mitre.org/techniques/T1059/001) | **Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system. Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the Start-Process cmdlet which can be used to run an executable and the Invoke-Command cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).** |
| ***Persistence*** | **T1078.004**  **Cloud Account** | **Valid accounts in cloud environments may allow adversaries to perform actions to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. Cloud Accounts can exist solely in the cloud; alternatively, they may be hybrid-joined between on-premises systems and the cloud through syncing or federation with other identity sources such as Windows Active Directory.** |
| ***Privileged Escalation*** | **T1068 Exploitation for Privilege Escalassions** | **Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions.** |
| ***Defence Evasion*** | **T1140**  **De-obfuscate/Decode Files or Information** | **Adversaries may use** [**Obfuscated Files or Information**](https://attack.mitre.org/techniques/T1027) **to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.** |
| ***Credential Access*** | **T1110 Brute Force** | **Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.** |
| ***Discovery*** | **T1082**  **System Information**  **Discovery** | **An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from** [**System Information Discovery**](https://attack.mitre.org/techniques/T1082) **during automated discovery to shape follow-on behaviours, including whether or not the adversary fully infects the target and/or attempts specific actions.** |
| ***Lateral Movement*** | **T1563 Remote Service Session Hijacking** | **Adversaries may take control of preexisting sessions with remote services to move laterally in an environment. Users may use valid credentials to log into a service specifically designed to accept remote connections, such as telnet, SSH, and RDP. When a user logs into a service, a session will be established that will allow them to maintain a continuous interaction with that service.** |
| ***Collection*** | **T1557 Adversary-in-the- middle** | **Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviours such as** [**Network Sniffing**](https://attack.mitre.org/techniques/T1040)**,** [**Transmitted Data Manipulation**](https://attack.mitre.org/techniques/T1565/002)**, or replay attacks (**[**Exploitation for Credential Access**](https://attack.mitre.org/techniques/T1212)**). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.** |
| ***Command and Control*** | **T1071 Application Layer Protocol** | **Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.** |
| ***Exfiltration*** | **T1041 Exfiltration over C2 Channel** | **Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.** |
| ***Impact*** | **T1486 Data Encrypted for Impact** | **Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.** |
|  |  |  |

**PART6.** **Recommendations**

1. **Implement Email Security Measures**:

* Implement a multi-factor authentication(MFA) across all OKZ University of Lagos accounts to reduce the risks posed by stolen email credentials.
* Conduct security awareness training periodically, focusing on identifying phishing attempts and safeguarding of personal information.

1. **Subdomain Management**:

* Regularly audit subdomains and decommission or secure unused services to close potential vulnerabilities.
* Establish a process for regularly auditing DNS records to ensure that any unnecessary exposed services are disabled or properly secured.

1. **Security Awareness Training**:

Ensure that staff are well educated about phishing threats and safe practices for publishing personal information online.

1. **Threat Surface Reduction**:

Use network security tools periodically to scan and minimize exposed services or misconfigurations.

**Conclusion**

This assessment of OKZ University of Lagos highlighted critical areas of potential exposure that could be exploited by adversaries.

By deploying a proactive management of digital footprints and tighter access control, the school can significantly reduce the university’s risk of cyber-attacks.

**REFERENCES**

Understanding APT40: Insights from CISA’s Latest Joint Security Advisory

By Jade Brown.

[**https://www.bitdefender.com/en-gb/blog/businessinsights/understanding-apt40-insights-from-cisas-latest-joint-security-advisory**](https://www.bitdefender.com/en-gb/blog/businessinsights/understanding-apt40-insights-from-cisas-latest-joint-security-advisory)

**Vice Society: Profiling a Persistent Threat to the Education Sector by JR Gumarin**

[**https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/**](https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/)

**Defending Education: Top Cyber Security Challenges in Higher Education by David Dixon**

[**https://cyberlab.co.uk/2024/10/23/defending-education-cyber-challenges/**](https://cyberlab.co.uk/2024/10/23/defending-education-cyber-challenges/)

[**https://attack.mitre.org/techniques/T1068/**](https://attack.mitre.org/techniques/T1068/)