**Investigation and Research Report on the United Nations Data Breach**

**June 11th, 2024**

**Reniel Villahermosa**

**Executive Summary**

This report investigates the ransomware attack on the United Nations Development Programme (UNDP), which resulted in the theft of sensitive data and the subsequent publication of some of that data online. The attack was attributed to the 8Base ransomware gang, a relatively new but experienced group of cybercriminals known for similar data extortion activities.

#### **Incident Overview**

On March 27, 2024, the UNDP received threat intelligence notifications that a data-extortion actor had compromised its local IT infrastructure in UN City, Copenhagen. The attackers stole data including personally identifiable information (PII) of past and current personnel, and procurement information related to suppliers and contractors. Despite the ransom demand, the UNDP maintained its policy of not engaging with threat actors and did not pay the ransom. Consequently, the attackers published some of the stolen data online.

#### **Analysis**

The analysis highlights the sophisticated nature of the phishing emails used to deceive employees and gain access to the network. These emails were crafted to appear as legitimate communications from trusted sources, leveraging urgency and professionalism to bypass scrutiny. Once inside the network, the attackers utilized various tools to steal data and deploy ransomware.

#### **Outcome**

The immediate outcomes of the attack included the theft and online publication of sensitive data, significant disruption to the UNDP's IT operations, and ongoing efforts to assess the full scope of the breach. There has been no evidence of misuse of the stolen data so far.

**Who are the victims of the attacks?**

The victims of the January 2021 United Nations data breach was primarily the staff and departments based in the UN offices in Geneva and Vienna. These offices are pivotal in the functioning of the UN, hosting numerous crucial diplomatic and operational activities. The breach specifically targeted the internal communications and document management systems within these offices.

Affected parties included:

- **Diplomatic Personne**l: Key diplomats and negotiating staff had their communications compromised, potentially exposing sensitive diplomatic strategies and personal information.

- **Operational Departments**: Departments handling operational data, including human resources, legal frameworks, and crisis management teams, experienced breaches of confidential and proprietary information.

- **Support Staff**: Employees responsible for the daily administration and support functions within the UN offices also fell victim to the breach, with their personal and professional data being exposed.

The breach not only risked the personal data of these individuals but also jeopardized the security and privacy of the international operations they manage. The exposed information could potentially be used for coercion, espionage, or other malicious purposes by the attackers, underscoring the severity and broad impact of the breach on the global diplomatic community.

**What Technologies and Tools Were Used in the Attack?**

The United Nations data breach in January 2021 was executed through a sophisticated combination of phishing techniques and exploitation of software vulnerabilities. The primary technologies and tools used in the attack included:

- **Phishing Emails**: The attackers initiated the breach by sending phishing emails to UN staff. These emails were crafted to appear as legitimate communications, possibly from other UN departments or trusted sources, tricking recipients into revealing their credentials or clicking on malicious links.

**Analysis of Phishing Emails Used in the Attack**

The phishing emails used in the attack on the United Nations Development Programme (UNDP) were highly sophisticated, designed to deceive employees and gain unauthorized access to the network. Here is a detailed breakdown of the components and strategies used in these phishing emails:

**Crafting the Email**

**Sender’s Identity**:

- The attackers likely spoofed email addresses to make them appear as if they were sent from trusted sources within the UNDP or associated partners. This tactic is used to exploit the inherent trust within organizational communications.

**Compelling Subject Line**:

- The subject lines were crafted to grab attention and prompt immediate action. Examples might include "Urgent: Account Verification Required" or "Important Update: Security Protocols."

**Professional Tone and Appearance**:

- The emails were designed to mimic legitimate communications, using the same formatting, logos, and language style as authentic UNDP emails. This added to their credibility and reduced suspicion.

**Content of the Email**

**Urgent Call to Action**:

- The emails contained urgent messages requiring the recipient to take immediate action, such as clicking a link to verify account details or download an attachment for important updates. This sense of urgency is a common tactic to bypass rational scrutiny.

**Malicious Links and Attachments**:

- The emails included links to fake login pages that mimicked legitimate UNDP portals. These phishing sites were designed to capture login credentials. Attachments, often disguised as legitimate documents (e.g., PDF reports or Excel spreadsheets), contained malware that, once opened, infected the recipient's device.

**Technical Mechanisms**

**Credential Harvesting**:

- Phishing links redirected recipients to fraudulent websites where they were prompted to enter their login details. These credentials were then harvested by the attackers for further exploitation.

**Malware Deployment**:

- Opening malicious attachments or clicking on embedded links triggered the download of malware onto the recipient’s device. This malware could include keyloggers to capture keystrokes, ransomware to encrypt files, or other forms of malicious software.

**Exploitation of Software Vulnerabilities**:

- The phishing emails might have included scripts that exploited known vulnerabilities in software used by the UNDP, such as Microsoft SharePoint. This allowed attackers to gain higher levels of access and control over the network.

**Behavioral Aspects**

**Psychological Manipulation**:

- The attackers employed social engineering tactics, leveraging authority (e.g., emails purportedly from senior management) and urgency to pressure recipients into acting without careful consideration.

**Spear Phishing:**

- In targeted attacks, emails were personalized using specific details about the recipient, such as their name, role, and recent activities. This level of customization made the phishing attempts more convincing and effective.

- **Exploitation of Microsoft SharePoint Vulnerabilities**: Once the initial access was gained, the attackers exploited known vulnerabilities in Microsoft SharePoint. The vulnerabilities allowed them to escalate their privileges within the network and gain unauthorized access to restricted areas.

- **Malware Deployment**: The attackers deployed malware within the UN’s systems, which was tailored to bypass existing security measures. This malware facilitated the extraction of sensitive data and maintained persistent access to the compromised systems.

- **Data Exfiltration Tools**: Specialized tools were used to collect, compress, and transfer data from the UN’s networks to external servers controlled by the attackers. This allowed them to stealthily extract significant volumes of sensitive information without immediate detection.

- **Command and Control (C2) Infrastructure**: The attackers established a robust command and control infrastructure, enabling them to remotely direct the malware, manage data extraction processes, and adjust their tactics as needed to evade detection.

These technologies and tools enabled the attackers to carry out a highly effective cyber operation, resulting in the exfiltration of sensitive data, but not involving ransomware or direct system destruction. The breach primarily focused on data theft, leaving the systems operational but compromised in terms of data integrity and confidentiality.

**When Did the Attack Happen Within the Network?**

The United Nations data breach that targeted the Geneva and Vienna offices began in late 2019 but was only detected in January 2021. The initial entry point of the attack was through a sophisticated phishing campaign launched in the latter months of 2019. Once the attackers gained initial access, they managed to maintain persistence within the network undetected for over a year.

**Timeline of the Attac**k:

- **Late 2019**: Attacker initiated the breach by sending phishing emails to UN staff, successfully exploiting vulnerabilities in the Microsoft SharePoint system.

- **Early 2020**: Upon gaining access, the attackers established a foothold in the network. They deployed malware and began the process of data exfiltration, targeting sensitive communications and internal documents.

- **Throughout 2020**: The breach continued unnoticed throughout the year, with attackers expanding their control over the compromised systems and extracting data intermittently.

- **January 2021**: Anomalies in data patterns and network traffic were finally noticed by the UN's IT security team, leading to the discovery of unauthorized access and the commencement of a thorough investigation.

This extended period of undetected access allowed the attackers to gather a substantial amount of sensitive information, highlighting the need for improved detection and response capabilities within the UN’s cybersecurity infrastructure.

**What Systems were Targeted?**

**1. Email Servers**

**Function**: Email servers handle all the incoming and outgoing communications within the organization. They are central hubs for both internal and external communications.

**Why Targeted:**

- Email servers contain vast amounts of sensitive information, including personal data, internal communications, and potentially confidential organizational data.

- Once compromised, attackers can use email servers to send phishing emails internally, leveraging the trust between employees to propagate malware or gather more credentials.

**2. Human Resources Systems**

**Function:** These systems manage employee data, payroll, benefits, and recruitment. They are rich in personal identifiable information (PII) of employees.

Why Targeted:

- **Data Theft:** Access to HR systems allows attackers to steal sensitive personal information, which can be used for identity theft, fraud, or further targeted attacks (spear phishing).

- **Ransomware**: Locking HR systems can be particularly crippling for an organization, making them a prime target for ransomware attacks.

**3. Financial Systems**

**Function:** Financial systems manage the organization's budgeting, accounting, procurement, and financial reporting.

**Why Targeted:**

- **Financial Gain:** Direct access to financial systems could allow attackers to redirect payments, manipulate financial data, or steal financial information.

- \*\*High-value Ransom Targets:\*\* Due to their critical nature, these systems are often targeted for ransomware attacks as organizations are more likely to pay to regain access.

**4. Network Infrastructure**

**Function**: This includes servers, routers, and switches that manage network traffic and ensure connectivity within and outside the organization.

**Why Targeted:**

- **Network Control**: Gaining control over the network infrastructure allows attackers to monitor, intercept, or redirect data traffic.

- **Service Disruption**: Disabling or taking control of network infrastructure can lead to significant disruption of organizational operations.

**5. Data Storage Systems**

**Function:** These systems are where the organization’s data is archived, including databases, file servers, and cloud storage solutions.

**Why Targeted:**

- Attackers often target these systems to steal large volumes of data, including intellectual property, strategic information, and backup data.

- Compromising data storage systems can allow attackers to maintain long-term access to sensitive data.

**6. Cloud-Based Services**

**Function**: Many organizations, including the UN, increasingly rely on cloud-based services for various applications and data storage solutions.

**Why Targeted:**

- Cloud services often contain a mixture of sensitive information that spans many facets of an organization.

- Compromising cloud-based systems can provide widespread access to multiple resources.

**Motivations and Groups Involved in the UNDP Data Breach**

The ransomware attack on the United Nations Development Programme (UNDP) was conducted by the 8Base ransomware gang. This group is relatively new but is believed to consist of experienced hackers. Their primary motivation appears to be financial gain through data extortion.

**Motivations of the Attackers**

1. **Financial Gain**: The attackers targeted the UNDP's locally hosted servers in UN City, Copenhagen, and stole data that included human resources and procurement information. The goal was likely to extract a ransom in exchange for not leaking or selling the stolen data.

2. **Data Extortion**: After stealing the data, the 8Base gang published some of it online, suggesting that they intended to pressure the UNDP into paying a ransom. However, the UNDP has stated that they do not engage with threat actors and did not pay any ransom.

**Groups Involved**

1. **8Base Ransomware Gang:** This group claimed responsibility for the attack and was linked to other ransomware operations. Their tactics included stealing sensitive data and threatening to release it if their ransom demands were not met.

2. **Other Potential Actors**: While 8Base was directly involved, the broader landscape of such attacks often includes various state-backed groups or cybercriminal syndicates. However, in this case, the primary attribution was to the 8Base gang.

**Outcome of the Attack**

The outcome of the ransomware attack on the United Nations Development Programme (UNDP) involved several significant consequences:

**Stolen Data**

The attackers, identified as the 8Base ransomware gang, stole sensitive data from the UNDP's locally hosted servers in UN City, Copenhagen. The compromised data included:

- **Personally Identifiable Information (PII)**: This consisted of information related to past and current personnel.

- **Procurement Information**: Details concerning suppliers and other contractors were also stolen.

**Ransom Demand and Data Publication**

-The 8Base gang demanded a ransom from the UNDP, threatening to leak the stolen data if their demands were not met. However, the UNDP has stated that it does not engage with threat actors and did not pay any ransom.

-When the UNDP refused to pay the ransom, the attackers published some of the stolen data online. The published data included invoices, receipts, accounting documents, certificates, confidential agreements, employment contracts, and personal information.

**System Damage**

- **IT Infrastructure Impact:** The attack targeted the local IT infrastructure in UN City, Copenhagen, leading to the compromise of specific servers that contained sensitive information.

**Ongoing Investigation and Mitigation**

- **Containment and Assessment**: The UNDP took immediate actions to identify the source of the breach, contain the affected server, and assess the specifics of the exposed data.

- **Communication with Affected Individuals**: The UNDP has maintained ongoing communication with those affected by the breach, advising them on steps to protect their personal information from misuse.

- **No Evidence of Misuse:** As of the latest updates, there has been no evidence of actual or attempted misuse of the stolen information.

**Recommended Mitigation Techniques for Preventing Future Ransomware Attacks**

To safeguard against future ransomware attacks, especially those similar to the one experienced by the UNDP, implementing a multi-layered cybersecurity strategy is essentiel. The following mitigation techniques are recommended:

**1. Enhance Email Security**

**Implement Advanced Email Filtering:**

- Utilize advanced email filtering solutions that can detect and block phishing emails. These filters should use machine learning algorithms to identify suspicious patterns and content.

**Email Authentication Protocols**:

- Implement email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting & Conformance) to reduce the risk of email spoofing.

**2. Regular Employee Training**

**Phishing Awareness Programs:**

- Conduct regular training sessions to educate employees about phishing attacks, including how to recognize and report suspicious emails. Interactive simulations can help reinforce this knowledge.

**Cyber Hygiene Best Practices**:

- Promote best practices for cyber hygiene, such as using strong, unique passwords, enabling multi-factor authentication (MFA), and avoiding clicking on links or downloading attachments from unknown sources.

**3. Implement Strong Access Controls**

**Principle of Least Privilege**:

- Apply the principle of least privilege (PoLP) to ensure that employees have only the access necessary to perform their job functions. This limits the potential damage if an account is compromised.

**Role-Based Access Control (RBAC):**

- Implement RBAC to manage and enforce user permissions based on their role within the organization. Regularly review and update access controls to reflect changes in employee roles.

**4. Regular Software Updates and Patch Management**

**Timely Patch Deployment**:

- Establish a robust patch management process to ensure that all software, including operating systems and applications, are kept up-to-date with the latest security patches.

**Vulnerability Management:**

- Conduct regular vulnerability assessments and penetration testing to identify and remediate security weaknesses before they can be exploited.

**5. Network Segmentation**

**Isolate Critical Systems**:

- Implement network segmentation to isolate critical systems and sensitive data from the broader network. This limits the ability of ransomware to spread across the organization.

**Use Virtual Local Area Networks (VLANs)**:

- Utilize VLANs to segment the network logically and enforce access control policies between different segments.

**6. Backup and Recovery Solutions**

**Regular Data Backups**:

- Ensure that data is backed up regularly and that backups are stored securely, preferably offline or in an immutable state, to prevent ransomware from encrypting or deleting them.

**Disaster Recovery Planning:**

- Develop and regularly test a comprehensive disaster recovery plan to ensure that the organization can quickly restore operations in the event of a ransomware attack.

**7. Incident Response Planning**

**Develop an Incident Response Plan:**

- Create and maintain an incident response plan that outlines the steps to take in the event of a ransomware attack. Regularly test and update the plan to ensure its effectiveness.

**Establish an Incident Response Team**:

- Form a dedicated incident response team with clearly defined roles and responsibilities to manage and mitigate the impact of ransomware attacks.

**Security Controls to Mitigate Ransomware and Data Breach Risks**

Implementing robust security controls is essential to mitigate the risks associated with ransomware and data breaches. Here are several key security controls that organizations like the UNDP can adopt to enhance their cybersecurity posture:

**1. Access Control**

**Role-Based Access Control (RBAC)**:

- Implement RBAC to ensure that employees have access only to the data and systems necessary for their roles. This minimizes the potential damage in the event of a compromised account.

**Principle of Least Privilege (PoLP)**:

- Enforce PoLP by granting users the minimum level of access required for their job functions. Regularly review and adjust permissions to reflect changes in responsibilities.

**Multi-Factor Authentication (MFA)**:

- Require MFA for accessing critical systems and sensitive data. MFA adds an extra layer of security by requiring additional verification beyond just a password.

2. Data Security

**Regular Data Backups**:

- Perform regular backups of critical data and ensure that backups are stored securely, preferably offline or in immutable storage to prevent ransomware from encrypting or deleting them.

**Data Encryption:**

- Encrypt sensitive data both at rest and in transit to protect it from unauthorized access and ensure data integrity.

**Conclusion**

The ransomware attack on the United Nations Development Programme (UNDP) underscores the growing threat posed by sophisticated cybercriminal groups like the 8Base ransomware gang. This incident highlights several critical aspects of modern cybersecurity challenges, including the exploitation of phishing attacks, the theft of sensitive data, and the complex decisions organizations face regarding ransom demands.

The investigation revealed that the attackers gained access to the UNDP's systems through phishing emails, ultimately stealing personally identifiable information and procurement data. Despite the publication of some of this data online, the UNDP maintained a policy of not engaging with ransom demands, focusing instead on containment and mitigation efforts.

To mitigate such risks in the future, it is imperative for organizations to adopt a multi-layered cybersecurity strategy. Key recommendations include enhancing email security, regular employee training on phishing awareness, implementing strong access controls, maintaining up-to-date software, and establishing robust backup and recovery solutions. Additionally, the implementation of advanced endpoint protection, network segmentation, and comprehensive incident response planning are crucial in defending against ransomware attacks.

The UNDP's experience serves as a cautionary tale for other organizations, emphasizing the importance of proactive cybersecurity measures and the need for continuous improvement in response strategies. By learning from this incident and adopting the recommended security controls, organisations can significantly reduce their vulnerabilities to similar threats and protect their criticl data and operations.

**Citations**

1. Greig, J. (2024, April 17). UN agency says data stolen in ransomware attack. The Record. Retrieved from <https://therecord.media/un-agency-data-stolen-ransomware-attack>
2. Kovacs, E. (2024, April 18). United Nations agency investigating ransomware attack involving data theft. SecurityWeek. Retrieved from <https://www.securityweek.com/united-nations-agency-investigating-ransomware-attack-involving-data-theft>
3. United Nations Development Programme. (2024, April 16). UNDP investigates cyber-security incident. UNDP. Retrieved from <https://www.undp.org/speeches/undp-investigates-cyber-security-incident>
4. Greig, J. (2024, April 17). UN agency says data stolen in ransomware attack. \*The Record\*. Retrieved from <https://therecord.media/un-agency-data-stolen-ransomware-attack>
5. CPO Magazine. (2023, October 11). United Nations data breach: Hackers obtained employee login from dark web, are executing ongoing attacks on UN agencies. \*CPO Magazine\*. Retrieved from <https://www.cpomagazine.com/cyber-security/united-nations-data-breach-hackers-obtained-employee-login-from-dark-web-are-executing-ongoing-attacks-on-un-agencies/>
6. Whittaker, Z. (2024, April 18). United Nations agency investigates ransomware attack claimed by 8Base gang. \*BleepingComputer\*. Retrieved from <https://www.bleepingcomputer.com/news/security/united-nations-agency-investigates-ransomware-attack-claimed-by-8Base-gang/>
7. Whittaker, Z. (2024, April 17). UNDP data stolen in ransomware attack. \*CyberScoop\*. Retrieved from [https://cyberscoop.com/undp-data-stolen-ransomware/\](https://cyberscoop.com/undp-data-stolen-ransomware/%5C)
8. NordLayer. (n.d.). Remote access control. NordLayer. Retrieved from<https://nordlayer.com/learn/access-control/remote-access-control/>