NALC Phishing Incident Report

Date: 2025-02-25

Handler: Suraj Khadka

Executive Summary

On February 7th, 2025, the North American Lumber Coalition (NALC) Security Operations Center (SOC) detected a phishing attack against internal employees. An employee reported receiving an email, pretending to be from Jason Robinson, an internal sender. The email included a suspicious link, srv-61.kim.johnson.biz/login, which employees unknowingly clicked on. There were 81 phishing emails sent to internal employees of NALC. Our investigation has shown that multiple people interacted with the site, and possibly some users submitted their credentials. The immediate action was taken to block the malicious domain and other artifacts, as well as to reset the user credentials that had been affected. This incident affected the cost of quality work by a total of $23,200. It was necessary to invest in bill for the investigation, containment, and security training.

Background

The North American Lumber Coalition (NALC) and its executives heavily rely on email to communicate with one another and with the people they partner with. Meanwhile, project coordination, vendor management, and confidential data sharing remain the staple method of business-critical information delivery. Since email is a key form of communication, any security bugs in this system may negatively impact business and finances to a great extent.

On February 6, 2025, several NALC employees received a phishing email and Jason Robinson appeared to be the sender of a phishing email. The email came from a legitimate internal user, yet the result of our investigation was that it was neither hacked nor compromised but spoofed using a fake sender address. The email contained a hyperlink to a malicious website (srv-61.kim.johnson.biz/login), which resembled the NALC login portal. Some of the employees who clicked on the link were asked for their login credentials, which in return the threat actors could easily obtain.

NALC's IT Security team was initially warned about the misleading nature of the email by one of the employees. The detailed checking of the network and HTTP logs showed that some employees had accessed the phishing page. It was reported by some employees even they tried to log in, and as a result, they may have failed to secure their credentials. Taking quick action was the first response done to stop further exposure, and then to protect the accounts that were affected.

Timeline

Note: All timestamps are in 24-hour format, Eastern Standard Time

2025-02-06 at 16:15PM ET – First recorded access to srv-61.kim.johnson.biz/login from 10.10.1.7. Employee accessed the phishing website but did submit credentials.
2025-02-06 at 21:06PM ET – Attackers started sending phishing emails to NALC employees, starting from James White email address jwhite@northamericanlumbercoalition.com.
2025-02-06 at 21:11PM ET – Additional employees started accessing the phishing site, indicating ongoing exposure.
2025-02-06 at 21:42PM – 2025-02-07 at 02:47AM ET – Multiple internal users interacted with phishing links were recorded and a few of them had already submitted their login credentials.
2025-02-07 at 03:00AM ET – A total of 41 users accessed the phishing URL were detected and among them seven users submitted their login credentials in the phishing site.
2025-02-08 at 03:30AM ET – An employee of the NALC reported about suspicious links to the NALC security team to verify whether the URL was legitimate or phishing.
2025-02-08 at 04:00AM ET – The Cyber Security team of the NALC creates **INC002567** ticket and initiated the investigation by reviewing HTTP and mail logs and verify that the URL was fake.
2025-02-09 at 10:15AM ET – The Cyber Security team also identified the affected users. Security team compiled all the details and assigned them to the Incident Response (IR) team.
2025-02-09 at 14:40PM ET – The IR team initiated the containment efforts by disabling the compromised accounts and notifying the affected employees of potential credential compromise.
2025-02-09 at 15:55PM ET – The malicious domain srv-61.kim.johnson.biz was blocked at the firewall level by the IR team to prevent further access.
2025-02-10 at 05:00AM ET – The IR team engaged IT personnel to implement password reset policies and conduct phishing awareness training for all employees.
2025-02-10 at 18:00PM ET – Monitoring continued for any further signs of phishing attempts or suspicious login attempts.
2025-02-13 at 05:45PM ET – Under the supervision of the IR team, they ensured everything was normal and operational, and they closed the **INC002567** ticket.

Findings

Summary:

The phishing attack at North American Lumber Coalition (NALC) was carried out using an email spoofing method. The attackers created an email that pretended to be from internal sender Jason Robinson, which tricked employees into clicking on a harmful URL (srv-61.kim.johnson.biz/login). An analysis of HTTP logs proved that several employees visited this phishing site, with at least seven credential submissions. The HTTP metadata logs showed multiple POST requests to the phishing domain, which suggested that login credentials were entered into that phishing site. Further investigation of the mail headers and logs revealed that flawed email security settings allowed the phishing email to get through the filtering systems. Although there was no

immediate detection of lateral movement, the act of compromising employee credentials posed a clear and present serious risk for unauthorized access.

Detailed Analysis

Note: All times in Eastern Standard Time

On February 6th, 2025, around 4:15 PM, the first phishing email was received by NALC internal employees, and it appeared to be from Jason Robinson with the email address "jrobinson@northamericanlumbercoalition.com". Examination of email headers, however, showed the email had been sent via an external SMTP relay instead of the NALC internal mail server. This meant his email was spoofed. In the email, there was a message that they had a new message with instructions to click a provided hyperlink which redirected them to a fake login page(srv-61.kim.johnson.biz/login).

Initial HTTP logs indicated that users were already engaging with the links by 4:30 PM. For the following hours, the fraudulent login page recorded many GET requests from internal IP addresses such as "10.10.1.7", "10.10.0.21", "10.10.3.81", indicating that many employees were accessing the login page.

After 9:11 PM, there was a sudden increase in traffic, which also brought with it other employees interacting with the fake login page. Mail logs confirmed that the phishing email was successfully delivered to many recipients, which increased the probability of further user exposure.

Between 11:51 PM on February 6th and 7:47 AM on February 7th, at least five employees provided their credentials to unauthorized parties, as evidenced by the POST requests in HTTP logs. These POST requests came from different internal IP addresses such as "10.10.2.64", "10.10.1.234" and "10.10.3.175", which means the users credentials were being forwarded to the attacker's server.

Despite employees' interactions with the phishing website continuing, nobody found it suspicious until 03:30 AM on February 8th, when employee reported it to the IT department. However, an employee was the first to flag the email's authenticity. The Security Operations Center (SOC) kicked off an investigation at 4:00 AM on February 8th, and it showed that the unauthorized IP "23.74.164.69" was associated with the phishing site. This was followed by prompt responses to the issue, including notifications to users and network containment actions.

A search in Splunk showed a bunch of HTTP requests to "srv-61.kim.johnson.biz", and the security teams at that point utilized mail logs to immediately confirm the email's sending history. Before 05:00 AM on February 10th, some of the compromised accounts were uncovered, and the management planned to change the passwords of the affected employees as the only way to stop potential misuse.

No evidence of further data exfiltration was found, but the compromised credentials will pose a potential threat for unauthorized access in the future. So, at around 06:00 AM on February 10th,

network administrators made sure to block the phishing domain at the firewall level, making it impossible to access the internal system.

Actions Taken

The SOC, immediately after notification about the phishing email, on the morning of 7th February 2025, started incident INC002567 and managed a team of Incident Response (IR) to evaluate the possible breach. Once the employees and IT teams sent an initial report, the IR team decided to delve deep into email headers, HTTP metadata logs, and user access logs to find out the magnitude of the exposure. With the help of forensic analysis methods, the team identified that multiple employees had clicked on the phishing URL (srv-61.kim.johnson.biz/login) and a few had even put their credentials in. The team immediately took the following actions:

1. Network Containment and Blocking:

- Blocked srv-61.kim.johnson.biz at the firewall and DNS level to completely prevent any further engagement.
- Monitored all outbound network traffic sources for signs of users whose accounts were compromised, that were trying to connect without authorization.

2. Credential Security Measures:

- Set up an immediate password reset for the employees whose accounts were affected by the compromise to prevent the attempt at account hijacking.
- Enforced multi-factor authentication (MFA) on all employees as a mandatory security step.

3. Log Analysis and Threat Hunting:

- Examined the email headers of the phishing page to ascertain whether the source of the email was internal or a method of spoofing.
- Verified all login requests made immediately after the submission of the user's credentials to track down any unauthorized access.
- With the application of Splunk, we were able to trace all events and detect attack pathways.

4. Stakeholder Communication and Awareness:

- Notified affected employees and departments and provided instructions on how to recognize phishing attacks.
- A security advisory was issued to employees company-wide, advising cautious regarding similar phishing attempts.
- Collaboration with the IT security team to recommend and improve email security policies.

5. Remediation Steps:

- Enhanced email filtering and anti-spoofing measures (SPF, DKIM, DMARC) to prevent future phishing attempts.
- Established real-time monitoring and alerting for suspicious login attempts in order to detect future credential misuse.

- Conducted an internal phishing simulation training for technical and non-technical employees to enhance awareness and response to phishing threats.

6. Verification and Incident Closure:

- Post-incident analysis was conducted to ensure no further unauthorized access occurred due to this type of phishing compromise.
- Containment effectiveness was verified and concluded monitoring.
- Marked Incident **INC002567** as resolved after confirming security for all affected accounts and no further signs of compromise have been detected.

Financial Impact

Item	Cost
Investigation Costs[1]	$10,500
Employee Downtime[2]	$700
Security Awareness Training[3]	$2,000
Labor[4]	$10,000
Total	**$23,200**

1. The SOC and other IT team spent 15 hours on log correlation, attack tracking, and response coordination. Each hour of investigative work is estimated at $700. Therefore, investigation costs are 15 investigative hours x $700 per investigative hour = $10,500
2. 7 employees were affected due to account disable and security enforcement measures. Consequently, it cost 7 employees x 2 hours of downtime x $35 per hour = $700.
3. Security Awareness Training cost includes phishing simulation exercises, instructional materials, and training program development.
4. Labor costs cover contributions from the IT, compliance, finance, security, and management teams. Estimated 20 hours of combined work at $500 per hour, which totals $10,000.

Lessons Learned

Successes

- Timely engagement of the Security Operations Center (SOC) after the phishing email was discovered allowed for rapid containment and prevention of further credential misuse.
- A smooth collaboration between the SOC, IT security, and Incident Response (IR) teams facilitated a well-defined incident response that included password resets, domain blocking, and log analysis.
- Work on improving SPF, DKIM, and DMARC policies by Email Security teams. They closed the filtering gaps and informed departments of the changes within a few days to contribute to the prevention of future spoofing scenarios.

- Within hours, all affected employees were notified, and the company-wide phishing awareness training was launched within hours with the main goal being the reinforcement of security best practices.

Opportunities for Improvement

Issue: Delayed in detection of phishing emails.
Recommendation: Implement automated email-based threat detection rules in email security gateways and use web traffic real-time monitoring tools for detecting and blocking links.
Action Item Owner: SOC and Network Monitoring Team

Issue: Employees fell for phishing attempts.
Recommendation: Conduct more frequent awareness training about recognizing phishing and to include also the phishing simulation exercises to prompt employees to report suspicious emails promptly.
Action Item Owner: HR & Security Awareness Team

Issue: Lack of strict email security and authentication policies.
Recommendation: Make available several email authentication protocols, such as configuring SPF to allow only specific senders, DKIM to sign the emails properly, and DMARC to refuse the ones sent without authorization.
Action Item Owner: Email Security Team

Issue: No automated containment for compromised accounts.
Recommendation: Employ policy-based automatic account lockdown that disables accounts for a limited time if someone tries to log in to them several times form unusual locations or after engagement with a known phishing URL.
Action Item Owner: Identity & Access Management Team