Incident Report – Malware attack on EL systems, NALC and Timberr customers

Date: 2025-04-20

Handlers: Aryan Puttur, Grant J Hewitt, John H Lee, Prakash Kanchan, Suraj Khadka

Executive Summary

On April 1st 2025, at 11:00 PM ET, the EL SOC received a complaint from a NALC customer about their systems being infected by NALC's website. The Incident Response (IR) team found that an EL employee was spear-phished with a reverse-shell malware, causing an administrative credential breach of the NALC and Timberr WordPress servers. The attacker then uploaded the malware onto the NALC and Timberr websites using the compromised credentials, resulting in 7 unique IPs downloading the malware. The malware posts have since been deleted, the malicious IPs have been blocked, and the details on how to identify and mitigate the malware have been communicated with all NALC and Timberr customers. EL, NALC, and Timberr WordPress servers are reverted to a clean state and the websites are now operating normally with increased security measures in place. However, the remediation costs along with the reputational damage of this attack creates an estimated total financial loss of around $1 million to EL.

Background

NALC (North American Lumber Coalition) reorganized from Electric Lumber (EL) after a security breach in 2017. EL now handles IT for regional lumber companies such as NALC and Timberr, including websites and HR systems. Bob, the former NALC system administrator (and current EL CIO) maintains administrative access to several systems including the EL, NALC and Timberr WordPress sites.

EL, Timberr and NALC's WordPress sites expose their administrative web interfaces to the internet and use simple username/password authentication – rendering them susceptible to brute force attempts and unauthorized access after credential breaches. Additionally, all three WordPress sites have not implemented any malware or virus scanning on uploaded attachments – making them susceptible to malware dissemination.

Similarly, EL has not implemented AV or phishing-detection software on their mail infrastructure, leaving EL employees exposed to phishing attacks. Additionally, while EL's internal systems have endpoint protection, EL does not enforce this on employees who "bring

their own devices (BYOD)" or use cloud virtual machines (VMs). This means that there's no mitigation for malware that gets downloaded or executed on these unmonitored devices.

EL also does not have adequate backups for their systems – which means during an incident, there are no system or data backups available, leading to longer recovery times and a heightened risk of ransomware or wiper attacks.

Timeline

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

- **October 28, 2024**
  - 02:32 - EL CIO Bob reads email with suspicious subject '`Account Validated at the Squirrel Board!`'
- **October 30, 2024**
  - 16:37 – Bob receives "`Cool lumber calculator`" email
  - 16:38 – Bob receives "`sorry about the attachment`" email
- **November 12, 2024**
  - 16:48 – Bob reads and deletes both the "`Cool lumber calculator`" and "`sorry about the attachment`" emails
  - 18:15 – Bob receives another email with subject '`lumber calculator`', this one likely with the attachment included.
  - 18:41 – Bob appears to reply to the email with subject '`lumber calculator`', indicating he likely downloaded the suspicious attachment and potentially compromised credentials or his home device (IP `54.163.246.12`) by running `lumber.exe` locally (a Windows reverse-shell payload)
  - 19:28 – Suspected attacker (`99.59.250.79`) starts browsing NALC WordPress Server (`10.111.10.102`), successfully logging in with admin credentials or sessions likely stolen from Bob.
  - 19:34 – Attacker uploads `estimator.zip` to NALC WordPress server
  - 19:36 – Attacker creates post titled '`Blog Home`' on NALC WordPress and links malware uploaded to a "`Try our estimator`" button
  - 19:38 – Attacker repeats the process on Timberr WordPress server with Bob's administrator identity, and uploads `estimator.zip`
  - 19:44 – Attacker creates post titled '`Blog Home`' on Timberr WordPress and links malware uploaded to a "`Try our estimator`" button
  - 19:39 – IP `64.66.99.129` downloads the estimator.zip malicious file from NALC WordPress
  - 19:40 – IP `143.215.16.136` downloads the estimator.zip malicious file from NALC WordPress
  - 19:41 – IP `98.192.93.204` downloads the estimator.zip malicious file from NALC WordPress
  - 19:45 – IP `107.127.28.2` downloads the estimator.zip malicious file from Timberr WordPress

- **November 13, 2024**
  - 02:36 – IP `205.169.39.16` downloads the estimator.zip malicious file from NALC WordPress
  - 02:36 - IP `205.169.39.31` downloads the estimator.zip malicious file from NALC WordPress
- **December 18, 2024**
  - 04:00 – IP `111.7.100.26` downloads the estimator.zip malicious file from Timberr WordPress
- **April 1, 2025**
  - 23:00 – EL SOC team receives an alert that a NALC customer complained about their computer being infected by the NALC website
  - 23:30 - SOC assigns incident response team consisting of Grant, John, Prakash, Aryan, and Suraj to investigate. Initially, they are provided with a Splunk index including a mix of logs captured from several systems on EL's network[1]. Incident ticket **INC08212** was created at Severity 2.
  - 23:50 – Team begins looking through the available logs in Splunk
- **April 2, 2025**
  - 01:00 - Team starts looking at WordPress traffic across EL servers for suspicious behavior
  - 01:10 – Team identifies numerous brute-force attacks against all three WordPress Servers in November and December of 2024, but none appear successful.
  - 02:00 – Broad investigation across EL internal infrastructure (AD, GitLab, MySQL, file servers) shows no immediate signs of compromise
  - 04:00 – Investigators identify multiple downloads of a suspicious file '`estimator.zip`' from both NALC and Timberr WordPress servers
  - 05:00 – SQL and Web logs confirm that '`estimator.zip`' was uploaded to NALC and Timberr WordPress servers at 19:34 and 19:36, respectively, on November 12, 2024. Both uploads came from attacker IP `99.59.250.79`, after successful administrator logins to the respective WordPress servers.
  - 06:00 – IR team instructs Perimeter team to blacklist `99.59.250.79` and temporarily take NALC and Timberr WordPress servers offline while triage is ongoing.
- **April 8th, 2025**
  - 08:00 – IR team receives email logs from EL IT team
  - 09:00 – Team identifies emails sent to Bob's account in October, 2024 with suspicious subjects such as '`Cool lumber calculator`', '`Sorry about the attachment`', and '`Account validated at The Squirrel Board`'. The team also identifies Bob receiving another email with the subject '`lumber calculator`' on November 12, 2024 at 6:15 PM. **The IR team believes that this is the email with actual malware attached, and the prior two emails were part of a social engineering/spear-phishing effort by the attacker.**

[1] Assumption: Based on what we had for week 1

- 09:30 – Team confirms that EL CIO Bob (`s-1-5-21-961585791-869121210-3005720737-1601`) appears to interact with the '`lumber calculator`' phishing email by replying to it at 18:41 on November 12, 2024 from his personal device or cloud VM (with IP `54.163.246.12`).
- 10:00 – IR team assesses that Bob likely compromised his machine by executing the '`lumber.exe`' reverse-shell malware, which in turn led to the subsequent compromise of the NALC and Timberr WordPress servers
- 10:15 – Team correlates Bob's response to the '`lumber calculator`' email at 18:41 with the subsequent suspicious traffic from `99.59.250.79` starting at around 19:34 which uploaded '`estimator.zip`' malware to NALC and Timberr WordPress servers on November 12, 2024 under Bob's administrative accounts.
- 10:30 – Investigators determine that these uploads were paired with WordPress posts (made under Bob's administrative accounts), encouraging users to "`Try our estimator`" with links to the malicious "`estimator.zip`" files on both the NALC and Timberr WordPress servers
- 10:45 – IR team instructs SOC team
  - to blacklist `54.163.246.12`
  - for Bob's offline devices be taken in for analysis
  - to reset credentials on all WordPress servers
  - to reset all of Bob's corporate credentials
  - to delete all of Bob's SSH keys from EL infrastructure.
- 10:50 - IR team instructs the SOC team immediately conduct antivirus/malware scans and quarantine any matched hashes for '`estimator.zip`' on all EL, NALC, and Timberr devices
- 11:00 – IR team requests for more information and logs from EL IT teams for further analysis

- **April 14, 2025**
  - 08:00 – IR team receives export of Bob's Documents and Desktop folders, SQL databases backing all three WordPress servers (NALC, Timberr, and EL), and archives of the EL, NALC and Timberr WordPress sites themselves
  - 09:00 – Using the provided files, investigators determine the following:
    - '`estimator.zip`' contains '`lumber.exe`', a Metasploit reverse-shell malware according to VirusTotal.com
    - The reverse shell exploit is hardcoded to call back to IP `54.158.34.216`
    - Bob's Documents folder contains an SSH key to the EL server and his Desktop contains another SSH key to an unidentified server.
    - Bob's machine data also shows risky behaviors that haven't yet been explicitly banned on the EL Information Security Policy (ISP) – such as
      - Use of GitHub, whereas EL uses GitLab. This may be Bob's personal GitHub account storing sensitive EL intellectual property.

        - SSH keys to multiple enterprise servers that are locally stored
        - Installation of open-source software like OpenOffice
- 09:15 - IR team instructs Perimeter team to blacklist `54.158.34.216`
- 09:20 - IR team instructs the SOC team immediately conduct AV scans and quarantine any matched hashes for '`lumber.exe`' on all EL, NALC, and Timberr devices
- 09:30 - IR team instructs IT to restore offline NALC and Timberr WordPress servers to clean backups (prior to November 1, 2024) and apply latest patches on WordPress. No posts with this malicious file are found on EL WordPress, but the IR team recommends it be taken offline with the same remediations applied since Bob had an SSH key to this server on his compromised device.
- 09:40 – IR team confirms that no lateral movement of malware occurred within the broader infrastructure (e.g., AD, GitLab, MySQL) from Bob's machine
- 10:00 – IR team identifies multiple IPs which downloaded 'estimator.zip' from the WordPress servers: `111.7.100.26`, `205.169.39.31`, `205.169.39.16`, `107.127.28.2`, `98.192.93.204`, `64.66.99.129`, `143.215.16.136`
- 10:05 – Team members send this list of IPs with corresponding reverse lookup information to EL IT and NALC/Timberr Customer Executives to identify whether these correspond to any NALC/Timberr customers.
- 11:00 - 22:00 – IR team convenes a "war room" with EL IT, EL SOC, EL executive leadership, and representatives from NALC/Timberr to implement the following remediation plan:
    - Ensure EL, NALC and Timberr WordPress servers are reset to clean backups with new administrator credentials (including new salts, keys and database credentials in `wp-config.php`) before being reconnected to the network
    - Reset SSH public keys on all EL infrastructure – this ensures the private keys compromised from Bob's computer cannot be reused for access.
    - Implement external firewall devices in the DMZs of EL, NALC, and Timberr that proxy all traffic to/from the three networks. Firewalls should implement whitelisting on trusted IP blocks for access to external resources (such as the WordPress servers) and only allow inbound access via the VPN to other internal resources as needed. Further, the firewalls should include Web-Application Firewall functionality that automatically filters out brute-forcing and other common web exploitation techniques.
    - Implement Multi-Factor Authentication and SSO for Webmail and restrict external access to EL VPN IP space.
    - Install Anti-Virus and Anti-Phishing scanners on the EL Web-Mail infrastructure
    - Temporarily block any "Bring Your Own Device" (BYOD) access at EL, NALC, and Timberr until a BYOD endpoint management tool can be purchased and a clear BYOD policy added to the Information Security Policy (ISP) at EL.

        - Ensure Bob's device was re-imaged, and any EL intellectual property is purged from GitHub. Additionally, delegate access from Bob (for personally administering WordPress and EL Infrastructure) and shift responsibility to the WordPress administrator and IT teams. This will prevent spear-phishing campaigns from targeting individual executives with elevated access.
        - Work with Bob and NALC/Timberr Executive Departments to compile breach communications for any customers that downloaded the malware file. The communications will also include specific instructions to help NALC/Timberr customers identify and eliminate the malware and block malware traffic.
- **April 15, 2025**
    - 06:00 – IR team confirmed with Executive Leadership that breach communications have been sent
    - 08:35 – Incident Handlers conclude forensic investigation; **INC08212** is marked remediated
    - 08:45 – Incident Handlers begin preparing Incident Report
- **April 19, 2025**
    - 08:35 – Incident report is complete, along with long term recommendations
    - 08:40 – Incident **INC08212** marked as Resolved.

Findings

Between October 28, 2024 at 2:32 AM and October 30, 2024 at 4:38 PM, Electric Lumber CIO Bob received a series of suspected spear-phishing emails with subject lines like "`Cool lumber calculator`", and "`Sorry about the attachment`".

On November 12, 2024 at 4:48 PM Bob deleted these suspicious emails but then received another email with subject "`lumber calculator`" at 6:15 PM that we assess contained the malicious ZIP file named "`estimator.zip`", which in turn contained a reverse-shell malware file named "`lumber.exe`". The IR team believes that the October emails referring with subject lines like "`Cool lumber calculator`", and "`Sorry about the attachment`" were social engineering efforts, to make Bob more likely to trust the November 12th follow-up with attached malware.

On November 12, 2024 at 6:41 PM, Bob replied to the "`lumber calculator`" email. We assess that Bob extracted and executed "`lumber.exe`" which opened a reverse shell to attacker's IP `54.158.34.216`. This exploit gave the attacker remote access to Bob's machine. We believe the attacker then leveraged stored credentials or session cookies on Bob's machine to login to both the Timberr and NALC WordPress sites. Copies of Bob's Desktop and Documents folders revealed he stored shortcuts to multiple internal EL servers locally in addition to at least two SSH private keys to different servers. One of these links was to the EL-MySQL server (`10.111.1.220`), which contained sensitive customer information for 6384 customers. There is no evidence of the

attacker targeting other parts of the EL infrastructure or any lateral movement from Bob's machine.

November 12, 2024 at 7:34 PM and 7:38 PM, we observed the malicious actor login with Bob's admin credentials to the NALC and Timberr WordPress Servers respectively (from `99.59.250.79`), and upload the malware "`estimator.zip`." The attacker then exposed these uploaded files via WordPress posts created under the same administrative identity, encouraging users to "Try our estimator."

Between November 12, 2024 and December 18, 2024, we see this malicious file being downloaded by several IPs likely belonging to NALC/Timberr clients: `111.7.100.26`, `205.169.39.31`, `205.169.39.16`, `107.127.28.2`, `98.192.93.204`, `64.66.99.129`, `143.215.16.136`. No incoming malicious traffic was observed from any of these IPs following their downloading of the malware.

Besides this particular malware attack, there are also several instances of reconnaissance scans and failed brute-force login attempts between October 1, 2024 and January 2, 2025 on the EL, NALC and WordPress servers. In at least one case, we see the apparent successful upload and attempted execution of a Windows file named '`spread.exe`' via a `ThinkPHP` exploit against the EL WordPress server. All three WordPress servers are Linux devices so this file was not executed successfully. Nonetheless, these attempts point to the need for additional security hardening of all three WordPress servers to prevent another breach.

Actions Taken

On April 1st, 2025 at 11 PM - Immediately upon notification of a customer complaint that NALC's website infected their systems, the SOC initiated an incident, **INC08212**, and assigned an Incident Response team to investigate. The IR team conducted the following actions in order to detect, contain, eradicate and recover from the attack -

1. **Detect and Investigate**
    - The EL SOC created an incident record and dispatched an IR team to begin immediate log review and threat scoping.
    - Due to inadequate IR preparedness at EL, the IR team was only able to gain a limited set of data points for forensics –
        - a "catch all" log index on Splunk
        - email logs
        - snapshots of suspected machines, databases and WordPress servers.
    - The IR team used these limited data points to piece together a timeline of the attack
        - IR team determined that a spear-phishing email titled "`lumber calculator`" sent to Bob (EL's CIO) on November 12, 2024 at 6:41 PM, was the likely initial vector for malware.

- IR team believes the email included a file attachment (`estimator.zip`) containing the malware "`lumber.exe`." Double-clicking this file triggered a reverse shell exploit - granting the attacker access to traffic and files from Bob's machine starting November 12, 2024 at 6:41 PM
- IR team believes this reverse shell exploit leaked administrator credentials for NALC and Timberr WordPress servers to the attacker
- On November 12, 2024 at 7:34PM and 7.38PM the attacker logged in successfully as administrator to both NALC and Timberr WordPress servers, from IP `99.59.250.79` and uploaded `estimator.zip`
- On November 12, 2024 at 7:36PM and 7.44PM the attacker made posts linking to the malicious `estimator.zip`, using Bob's administrator identity.

2. Contain and Eradicate

- Malware and Server Cleanup
  - Revert NALC, Timberr, and EL WordPress servers to clean backups pre-November 1, 2024
  - Run AV scans and quarantine any matched hashes for `estimator.zip`, `lumber.exe`, or other flagged malware on all EL-managed infrastructure
  - Apply latest patches to all WordPress servers, update/eliminate vulnerable plugins like `ThinkPHP`
- Network Containment and Monitoring
  - Block all traffic from and to/from IPs `54.158.34.216` and `99.59.250.79`
  - Monitor traffic from impacted systems to confirm no additional malware beacons or data exfiltration attempts.
  - Install Anti-Virus and Anti-Phishing software on the EL Email Server and enable SSO and MFA for all Email accounts
  - Temporarily block any "bring your own device" ability at EL
  - Implement external firewall devices in the DMZs of EL, NALC, and Timberr that proxy all traffic to/from the three networks.
  - Configure WAFs on all Network Firewalls to filter web-exploitation attempts
  - Limit external access to internal resources to VPN-only with MFA-enabled
- Credential and Access Control Measures
  - Reset all EL, NALC and Timberr WordPress administrator credentials; enable administrative logins only via SSO and MFA
  - Remove SSH public keys tied to Bob's identity from all EL infrastructure
  - Update database credentials, salts, and keys in `wp-config.php` files on EL, NALC and Timberr WordPress Servers
  - Remove all external access to administrative functions on EL, NALC, Timberr WordPress sites
  - Restrict access to Webmail to only internal EL IPs and EL VPN IPs.
  - Re-image Bob's computer

3. **Recovery, Verification and Closure**
    - Create and implement a patching schedule for all EL-managed servers and devices
    - Conduct a post-incident forensic review of Bob's files, WordPress archives, and mail logs to confirm no ongoing threats.
    - Verify that no lateral movement occurred within the broader infrastructure (e.g., AD, GitLab, MySQL) from Bob's machine or other IPs that downloaded the malware
    - Ensure WordPress functionality was restored, and all systems operate with stricter access measures in place.
    - Begin ISP update/draft on BYOD policy, clean desk policy, and application whitelisting
    - Compile and send breach communications with IoC's and details on identification and eradication of malware – to all NALC, Timberr customers.
    - Create Incident Report with implemented short-term measures, and long-term recommendations
    - Mark the incident **INC08212** as resolved after validating that there are no more active threats, service is recovered and stable, and all stakeholders are notified of the breach.

Financial Impact

Item	Cost
Customer Remediation & Third-Party Liability[1]	$170,000
Lost Contracts (NALC & Timberr)[2]	$375,000
Projected Future Business Loss (Reputation Damage)[3]	$250,000
Labor and Internal Response Costs[4]	$64,350
Security Tooling & Infrastructure Hardening[5]	$150,000
Total	**$1,009,350**

Detailed Cost

1. Customer Remediation & Third-Party Liability
    a. 7 affected downstream customers (~10,000 per client)
    b. 10 estimated customers lost during incident downtime (~10,000 per client)
2. Lost Contracts
    a. If either NALC or Timberr scales down their engagement or withdraws, EL could lose up to $125,000 per client annually
3. Future Business Loss
    a. Reputation damage leads to suppressed client growth and customer hesitation
        i. Est. $75,000/yr growth loss

4. Labor and Internal Response Costs
    a. Incident Response Team (2) - 40 hrs, $100/hr, $8,000
    b. SOC Analysts (2) - 40 hrs, $85/hr, $6,800
    c. Email/Admin Engineers (1) - 30 hrs, $75/hr, $2,250
    d. CISO - 10 hrs, $250/hr, $2,500
    e. Legal Counsel - 10 hrs, $400/hr, $4,000
    f. Customer Support Reps (2) - 40 hrs, $60/hr, $2,400
    g. DevOps & Backup Review – 60 hrs, $100/hr, $4,000
    h. Dedicated support to clients (tech + comms) 1,000 hrs, $30hr, $30,000
5. Security Tooling & Infrastructure Hardening
    a. Email Anti-Virus and Anti-Phishing licenses
    b. WordPress security updates and hardening
    c. Firewall infrastructure and WAF software configuration
    d. Backup system deployment and testing
    e. Training of employees

Lessons Learned

Successes

- The use of Splunk for log aggregation and querying enabled the IR team to effectively trace the attacker's path, including suspicious admin logins, malware uploads, and file downloads across affected servers.
- Seamless collaboration among the response team members enabled a structured response process, including log analysis, file tracing, and credential resets.
- Clear communication protocols between EL, NALC, Timberr and third-party customers ensured that malware eradication steps were shared promptly with affected customers and operations on all WordPress sites resumed without extended downtime.

Opportunities for Improvement

Issue: Lack of Anti-Virus and Anti-Phishing services for Corporate Email
Recommendation: Purchase and deploy Anti-Virus and Anti-Phishing solution to all EL-managed Mail infrastructure. This would scan attachments and mail content for malware and suspicious activity prior to user interaction. Additionally, enforce MFA for all Email accounts to add a layer of defense if credentials are compromised.
Action Item Owner: SOC and IT teams

Issue: Lack of endpoint security policies and tools for BYOD devices and cloud-hosted VMs
Recommendation: Create a consistent policy for BYOD and cloud VM use, and their connectivity to EL infrastructure via VPN. Enforce endpoint protection policies across all corporate devices, including BYOD and virtual environments, using endpoint detection and response (EDR) solutions.

Action Item Owner: SOC and IT teams

Issue: WordPress servers exposed to the open Internet with weak authentication
Recommendation: Enforce MFA and SSO logins to all WordPress servers. Proxy all traffic to/from WordPress servers via DMZ Firewalls with WAFs capable of detecting and blocking brute-force attempts and known malicious traffic.
Action Item Owner: IT team

Issue: Insecure storage of credentials and keys to critical infrastructure on employee desktops
Recommendation: Create a clear policy of "clear desk" and credential management. Implement SSO wherever possible. Provide encrypted credential vaults and restrict local storage of administrative credentials for services that do not support SSO. Regularly audit user machines for unauthorized key files.
Action Item Owner: SOC and Identity & Access Management teams

Issue: Lack of WordPress malware detection
Recommendation: Integrate server-side AV or File Integrity Monitoring (FIM) tools into WordPress environments to scan all uploaded content in real-time.
Action Item Owner: SOC and IT teams

Issue: No automated alerting suspicious uploads/downloads or administrator account anomalies
Recommendation: Configure alert rules in Splunk SIEM for repeated file downloads, unknown IP logins, and abnormal user behavior such as off-hours access or credential usage across multiple systems.
Action Item Owner: SOC team

Issue: Poor backup strategy and lack of restore points
Recommendation: Establish regular automated backups for all mission-critical systems and validate restore procedures to reduce future downtime and data loss risk.
Action Item Owner: Infrastructure & Business Continuity teams

Issue: Centralized access and privileges for the CIO (Bob) creates a single point of failure with cascading effects in the event of a compromise
Recommendation: Require the CIO to delegate access to dedicated administrators for each specific system. Implement policies to prevent the aggregation of privileges to any one user.
Action Item Owner: Executive and Technical Leadership teams

ASSUMPTIONS MADE FOR THIS ASSIGMENT

- Only a limited set of logs and files are available to the IR team, as per assignment scope
- Details of the actual NALC customer complaint or their IP range/details are unavailable.
- EL email/webmail is missing phishing protection and malware attachment scanners
- Bob was using a personal device or cloud VM/VDI to administer the WordPress servers and to access Webmail. One such device is the IP 54.163.246.12
- The callback IP on the malware reverse shell exploit (54.158.34.216) is registered by the same entity that registered 54.163.246.12. We assume this is an artefact of sanitizing the project's malware by the GA Tech team, and that for the purposes of this assignment we treat these two as unrelated IPs.
- Bob's habit of storing SSH keys locally likely means he also had other credentials or sessions cached locally - which an attacker could have accessed via the reverse-shell exploit on 'lumber.exe'
- INC08212 is the incident ticket number
- EL has a VPN in place but many systems are accessible without it
- EL has a single sign on identity provider.