Incident Log – NALC Phishing Attack

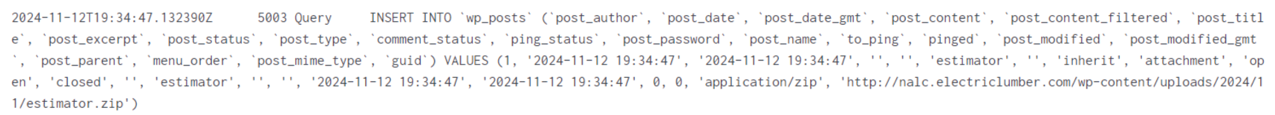
- [2025-04-01]
  - [11:00 pm] Electric Lumber Cyber Security operations (SOC) team receives alert that a NALC customer has complained about their computer being infected by the NALC website. No other detail is provided, and NALC is unable to provide more details on the type of infection, or the client or any other specifics[1]
  - [11:30 pm] SOC assigns incident response team consisting of Grant, John, Prakash, Aryan and Suraj to investigate. Only log available is a "catch all" Splunk log with a mix of events captured from several systems on EL's network[2]
  - [11:50 pm] Team begins searching "final-main" log index on splunk for any IoC's
- [2025-04-02]
  - [1:00 am] Team Started by looking at WordPress traffic that raise suspicious behaviors on all EL WordPress Servers.
  - [1:10 am] The Team (Prakash and Grant) located a brute force login attempt on Timberr wordpress server, on November 19, 2024, from 77.234.44.180.
    - Attacker first enumerated the /author endpoint to get admin user ID
    - Attacker then tried xmlrpc.php to brute force a login using the WordPress xmlrpc exploit.
    - When this failed, the attacker then tried hitting /wp-login.php to brute force login. All 997 attempts failed
  - [2:00 am] The IR Team (Prakash) queried for any suspicious behavior on several machines without any specific IoC's uncovered
    - Splunk server 10.111.1.241 - no suspicious logs (`index="final-main" 10.111.1.241 NOT "TIME-WAIT" NOT "ESTAB" NOT "splunkfwd"`)
    - AD servers
      - AZA – no suspicious logs (`index="final-main" 10.111.1.227 NOT "TIME-WAIT" NOT "ESTAB" NOT "splunkfwd" NOT "The system failed to register host (A or AAAA) resource records (RRs) for network adapter"`)
      - AZB – no suspicious logs (`index="final-main" 10.111.5.217 NOT "TIME-WAIT" NOT "ESTAB" NOT "splunkfwd" NOT "The system failed to register host (A or AAAA) resource records (RRs) for network adapter"`)
    - Gitlab 10.111.1.5 – no suspicious logs (`index="final-main" 10.111.1.5 NOT "aws:softwareInventory"`)
    - EL-MySQL – no suspicious logs (`index="final-main" 10.111.1.220 NOT "ESTAB" NOT "TIME-WAIT" NOT "<n/a>" NOT "splunkfwd" NOT "aws:softwareInventory" NOT "AH00558" NOT "AH00171" NOT "MGSInteractor"`)
    - EL-Files 10.111.1.61 - 0 logs
    - Management server 10.111.1.84, "Terminal" 10.111.3.33 - lots of logs but looks like Bob managing different wordpress servers from this machine. Nothing suspicious outright (`index="final-main" 10.111.1.84 NOT "ESTAB" NOT "TIME-WAIT" NOT "<n/a>" NOT "splunkfwd" NOT "aws:softwareInventory" NOT "The system failed to register`

[1] Assumption: Since we don't have any of this info in the assignment either.

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

```
host (A or AAAA) resource records (RRs) for network
adapter")  and (index="final-main" 10.111.3.33 NOT "ESTAB" NOT
"TIME-WAIT" NOT "<n/a>" NOT "splunkfwd" NOT
"aws:softwareInventory" NOT "The system failed to register
host (A or AAAA) resource records (RRs) for network adapter")
```

- [3:00 am] The team (John) searched for any suspicious traffic going towards the public IP of the NALC Wordpress Server (3.90.31.5) since this was the server that the customer suspected of being compromised. Multiple attempted attacks were identified, including scans for CVE-2022-30023 based on the /boaform endpoint and attempts at Local File Inclusion via /cgi-bin endpoints from IP 185.103.103.58
- [3:30 am] Following up on this IP, (John) they found that it appeared to execute a successful ThinkPHP RCE (https://www.exploit-db.com/exploits/46150) on the EL Wordpress Server to upload and execute 'spread.exe' on December 11, 2024.
- [4:00 am] Investigators (Prakash) then queried the splunk logs for any downloads of files, since the customer likely downloaded something to have a machine infected. This resulted in finding a file **"estimator.zip"** that was downloaded several times from both Timberr and NALC websites `(index="final-main"  "estimator.zip" NOT "404")`
- [4:20 am] Prakash queried the splunk logs further and located INSERT statements into wp_posts that indicates uploads of this attachment into NALC around Nov 12, 2024 at 7:34PM



```
2024-11-12T19:34:47.132390Z      5003 Query     INSERT INTO `wp_posts` (`post_author`, `post_date`, `post_date_gmt`, `post_content`, `post_content_filtered`, `post_titl
e`, `post_excerpt`, `post_status`, `post_type`, `comment_status`, `ping_status`, `post_password`, `post_name`, `to_ping`, `pinged`, `post_modified`, `post_modified_gmt
`, `post_parent`, `menu_order`, `post_mime_type`, `guid`) VALUES (1, '2024-11-12 19:34:47', '2024-11-12 19:34:47', '', '', 'estimator', '', 'inherit', 'attachment', 'op
en', 'closed', '', 'estimator', '', '', '2024-11-12 19:34:47', '2024-11-12 19:34:47', 0, 0, 'application/zip', 'http://nalc.electriclumber.com/wp-content/uploads/2024/1
1/estimator.zip')
```

- [4:25 am] Querying splunk for events around this timestamp indicated revealed the likely attacker IP **99.59.250.79** that uploads a file to NALC (`index="final-main" earliest="11/12/2024:19:34:00" latest="11/12/2024:19:35:00"`)
- [4:35 am] Prakash queried splunk for this IP and found the same IP also uploading something suspicious to Timberr 4 minutes after the upload to NALC
- [5:00 am] Prakash tried broadening the query a bit and found something disturbing – the IP **99.59.250.79** uploaded a suspicious file **"estimator.zip"** to **both NALC and Timberr,** after a **successful administrative login** to both sites.
- [5:30] Prakash queried the logs for "estimator.zip" and additionally found posts made on NALC and Timberr, referring to "Experience the fusion of imagination and expertise with Études Architectural Solutions." and linking a "Try our estimator" button to the malware "estimator.zip". These posts were made on November 12, 2024 at 7:36PM and 7.44PM   respectively.
- [6:00 am] IR team instructs Perimeter team to blacklist 99.59.250.79 and temporarily take NALC and Timberr WordPress servers offline while triage is ongoing.
- [6:30 am] Prakash also queried for other successful administrative logins and found several IPs (76.97.200.112, 54.163.246.12) that logged in successfully. However, at this point it's unclear if these are IPs belonging to legitimate users or attackers
- [7:00 am] Prakash uncovered some other suspicious behavior which needed more analysis
    - 24.216.55.132 - SSH and admin login attempts
    - 67.205.159.181 – running passive scans on the sites, likely reconnaissance
    - 143.110.204.120 – running passive scans on the sites, likely reconnaissance

- [2025-04-07]
  - [8:00 am] Response team receives mail logs
- [2025-04-08] Grant, John, Prakash, Aryan, Suraj
  - [8:00 am] Prakash analyzed the mail log files and found the following potential suspicious activity from user `s-1-5-21-961585791-869121210-3005720737-1110` on `24.216.55.132`. This may be legitimate activity as well, need more information and logs.
    - October 21, 2024, at 12:54 AM - "Test" email created
    - October 21, 2024, at 12:56 AM - someone responded to the "Test" email.
  - [9:00 am] Prakash analyzed the mail log files further, and found the following potential suspicious activity from `s-1-5-21-961585791-869121210-3005720737-1601` at IP `54.163.246.12`
    - October 28, 2024 at 12:56 AM - "VPN Server" email sent, followed by some "Undelivered Mail Returned to Sender" response received
    - October 28, 2024 at 1:03 AM – another "VPN Details" email sent, followed by some "Undelivered Mail Returned to Sender" response received to users- `s-1-5-21-961585791-869121210-3005720737-1603, s-1-5-21-961585791-869121210-3005720737-1605,s-1-5-21-961585791-869121210-3005720737-1606, s-1-5-21-961585791-869121210-3005720737-1602, s-1-5-21-961585791-869121210-3005720737-1604, s-1-5-21-961585791-869121210-3005720737-1607`
    - October 28, 2024 at 2:32 AM - "Account validated at The Squirrel Board!" email received, which looks like a suspicious email
    - October 30, 2024 at 4:37 PM - "Cool lumber calculator" email received
    - October 30, 2024 at 4:38 PM - "sorry about the attachment" received
    - November 12, 2024 at 4:48 PM – Bob deletes both emails after reading them
    - November 12, 2024 at 6:15 PM – Bob receives another email called "lumber calculator", this one likely had the real malicious attachment included
    - November 12, 2024 at 6:41 PM – Bob reads the email and responds to "Cool lumber calculator" email. I believe this "response" is something triggered by clicking on the phishing link or launching the attachment.
    - November 12, 2024 at 7:34PM and 7.38PM - we see the "estimator.zip" being uploaded to NALC and Timberr respectively, from `99.59.250.79`
    - November 12, 2024 at 7:36PM and 7.44PM - we see a "Blog Home" post made with some details referring to "Experience the fusion of imagination and expertise with Études Architectural Solutions." and linking a "Try our estimator" button to the malware "estimator.zip".
  - [9:30 am] Prakash analyzed the logs to find that `s-1-5-21-961585791-869121210-3005720737-1601` corresponds to user "Bob" who has administrator AD accounts. Thus, the conclusion is that this user is Bob- EL's CIO.
  - [10:00 am] Prakash analyzed the logs to find that `54.163.246.12` corresponds to several activities like WordPress administration and Webmail logins over large period of time.
  - [10:15 am] The working hypothesis here is that `54.163.246.12` is Bob's device IP, and Bob interacted with the malicious executable in the phishing email which somehow led to credential leaks and subsequent upload of "estimator.zip" and

the WordPress post linking to “estimator.zip”. More logs are needed for further analysis.
  - [10:50 am] - 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 am] – IR team requests for more information and logs from EL IT teams for further analysis
- [2025-04-14]
  - [8:00 am] Response team receives more details
    - Bob's Documents Folder
    - Bob's Desktop
    - Export of the Electric Lumber database
    - Archives of the three Wordpress sites
- [2025-04-14]
  - [9:00 am] John, Grant, Prakash deep dive into the new set of files available and make the following observations
    - `estimator.zip` was present in both the NALC and Timberr Wordpress servers in the uploads folder. The zip file contains the actual malware (`lumber.exe`) which is a Metasploit reverse shell exploit that would grant an attacker access to traffic from a machine that executes it. The “phone-home” IP in the malware is `54.158.34.216`
    - Bob has an SSH key to the EL Wordpress server in his Documents, so if his computer got compromised by the `lumber.exe` malware, the attacker could have then pivoted to the EL server via this key
    - Additionally, a reverse shell exploit could be used to steal credentials or sessions from Bob’s machine
    - Bob may have also had SSH keys or Credentials to Timberr and NALC wordpress servers on his desktop that were since deleted before SOC snapshotted the desktop
  - [09:20 am] - 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 am] - 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 am] – 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 am] Suraj finds several IPs that downloaded the `estimator.zip` malware (`index="final-main" "*/estimator.zip HTTP/*" 200`)
  - [10:05 am] – 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 am] Team agrees on the following high-level course of events. However, more time and logs are needed to create a detailed timeline of the exploit.
    - 54.163.246.12 seems to be Bob's IPs - several logins to wordpress etc. are logged BEFORE the lumber calc emails

        - Bob receives email from someone about lumber calculator on October 30, 2024 at 4:37 PM
        - Bob likely opened the email on November 12, 2024 at 6:41 PM and executed the attachment, and this gave the attacker reverse http shell access
        - The exact mechanism by which attacker gains NALC and Timberr Wordpress credentials is currently unclear. This may be using session hijacking (if Bob had stored login sessions) or via SSH or stored credentials that got stolen. More logs are needed to determine this step of the kill-chain.
        - Attacker uploads the `estimator.zip` into NALC and Timberr on November 12, 2024 at 7:34PM and 7:38PM respectively, from `99.59.250.79`
        - Attacker creates posts linking to the `estimator.zip` on NALC and Timberr on November 12, 2024 at 7:36PM and 7:44PM respectively – under the administrator identity.
        - Several IPs (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 – likely clients) download this zip file and at least one of them is the NALC customer that had their computer infected
    - [11:00am - 10:00pm] IR team works with EL IT, SOC, Executive leaders, and NALC/Timberr representatives to implement following
        - EL, NALC and Timberr WordPress servers are reset to clean backups with new administrator credentials (including database credentials in wp-config.php) before being reconnected to the network
        - Reset SSH public keys on all EL infrastructure
        - 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.
        - Re-image Bob’s machine, and any EL intellectual property is purged from Bob’s GitHub.
        - Compile breach communications for any customers that downloaded the malware file with EL and NALC/Timberr executives. The communications will also include specific instructions to help NALC/Timberr customers identify and eliminate the malware and block malware traffic.
- [2025-04-15]
    - [6:00 am] Breach communications sent

    - [8:35 am] Incident **INC08212** marked remediated
    - [8:45 am] Incident report compilation begins
- [2025-04-19]
    - [8:35 am] Incident Report complete
    - [8:40 am] Incident **INC08212** marked Resolved