April 11, 2025

Memo: Status Report 2

TO
Electric Lumber CISO, CIO, IT Team

FROM
Cyber Security Operations Team

CC
Grant Hewitt, John Lee, Aryan Puttur, Suraj Khadka, and Prakash Kanchan

RE
Update on Findings of Cyber Incident

UPDATE SINCE LAST WEEK:

Continuing investigations on NALC's potential breach suggests malware uploaded into NALC and Timberr sites via admin credential breaches of the 3 Wordpress servers owned by EL. While a phishing campaign is likely the initial vector, investigations continue on a PHP exploit that may also be involved.

Suspected malware has been downloaded by several IPs (likely belonging to NALC and Timberr customers) - risking compromise of customer systems; and resulting in revenue and reputational losses for EL, NALC and Timberr.

ADDITIONAL FINDINGS SINCE LAST WEEK:

Date	Source IP	Notes
2024-10-23	24.216.55.132	Possible unauthorized webmail access for user: s-1-5-21-961585791-869121210-3005720737-1110
2024-10-23	54.163.246.12	Suspicious email relating to "VPN" info sent to several users from s-1-5-21-961585791-869121210-3005720737-1601, with possible phishing links that trigger a "Account validated at the Squirrel Board" phone-home
2024-10-30	54.163.246.12	Interaction with a "cool lumber calculator" email with attachment
2024-11-12	54.163.246.12, 99.59.250.79	Likely successful opening of phishing/malware in attachment. This is followed by logins to EL, NALC, Timberr wordpress servers and upload of suspected malware "estimator.zip" file into NALC and Timberr sites
2024-10-30	Several	Sensitive Credential Probing from 193.36.224.218, 193.36.224.26, 40.124.169.176
2024-11-12, 2024-11-13, 2024-12-18	Several	Several IPs (possible NALC/Timberr customers) download "estimator.zip" , the suspected malicious attachment - 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

INVESTIGATIVE NEXT STEPS:

- Obtain more details from the NALC customer who reported initial infection
- Obtain a copy of "estimator.zip" for malware analysis
- Obtain a full inventory of EL employees and devices; identify user IDs logged in mail logs; smtp snapshots with email contents/attachments for analysis
- Investigate RCE attack by analyzing file-system snapshot, system & network flow logs from EL WordPress

CONTAINMENT RECOMMENDATIONS:

- Reset credentials on all WordPress servers and delete suspected malware attachment from all posts.
- Reset email credentials of above identified users who received or interacted with likely phishing emails
- Notify all EL, NALC and Timberr customers about potential website compromise
- Advise quarantine of any attachments downloaded since October 2024, and "estimator.zip" in particular
- Temporarily restrict access to administrative interfaces across EL and its customer WordPress sites