April 3, 2025

Memo: Status Report 1

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
Initial Findings of Cyber Incident

SUMMARY:

NALC customer complaint triggered an incident, and further examination of all servers managed by Electric Lumber (EL). Initial investigation reveals possible administrative credentials breach of EL, NALC and Timberr WordPress servers; along with a potential Remote Code Execution (RCE) breach of EL WordPress server.

OPERATIONAL IMPACT:

Suspected breaches increase the likelihood of further malicious activity - risking compromise of customer systems; and resulting in revenue losses and reputational losses for EL, NALC and Timberr.

FINDINGS - DETAILED:

Several events indicate likely breach and need further investigation

Date	Source IP	WordPress Server(s)	Notes
2024-11-12	99.59.250.79	NALC, Timberr	Credential breach, File upload
2024-10-30	76.97.200.112	EL	Credential breach
2024-10-23	54.163.246.12	EL, NALC and Timberr	Credential breach
2024-12-11	178.124.151.56	EL	ThinkPHP RCE exploit

INVESTIGATIVE NEXT STEPS:

- Obtain details from the NALC customer who reported an infection, including details on type, manifestation, identification, and any available logs/timestamps
- Obtain full inventory of EL employees and devices.
- Obtain full SMTP (email exchange) logs for EL employees
- Investigate RCE attack by analyzing file-system snapshot, system logs, network flow logs from EL WordPress server
- Investigate credential breach by analyzing hashed credentials (for reuse), file-system snapshot, system logs, access logs, network flow logs, and SQL logs for all 3 WordPress servers (EL/NALC/Timberr)

CONTAINMENT RECOMMENDATIONS:

- Take EL Wordpress site down, until further RCE investigations can be completed
- Reset all credentials on all WordPress servers – EL, NALC, Timberr
- Locate and quarantine (for study) any suspicious attachments (e.g. “.zip”, “.exe”) on posts
- Notify all EL, NALC and Timberr customers about potential website compromise – advise quarantine of any attachments downloaded since October 2024.