Nexora Dynamics Investigation – Final Report

Case Details

Case Number: ND-2025-02-03-001 **Investigator Name:** David Rizzo **Date:** March 2, 2025

1. Executive Summary

Nexora Dynamics, a medium-sized engineering services firm, experienced a significant security breach. The attack began with a successful spear-phishing campaign targeting a contractor, ultimately leading to widespread lateral movement, data exfiltration, and potential disruption of critical systems. An analysis of the timeline, attack vectors, and vulnerabilities has prompted an urgent review of Nexora Dynamics' security posture and the implementation of several key mitigation strategies.

2. Incident Overview

- **Incident Date:** Week 4
- **Reported By:** Network Administrator
- **Location:** Service Slowdown
- **Affected Systems:** - Web Server: Dell PowerEdge R740 - Load Balancer: F5 Networks BIG-IP 2000 Series - Content Delivery Network (CDN): Akamai Adaptive Media Delivery (Cloud-based) - DNS Server: Infoblox DDI Appliance - Email Server: Microsoft Exchange Server 2019 (Running on VMware) - VPN Gateway: Palo Alto Networks Global Protect

3. Investigation Process

Initial Detection

The network anomaly at Nexora Dynamics was first detected by Lisa Reynolds, the Network Administrator. Lisa observed major slowdowns across multiple systems and received reports from both users and monitoring tools [1]. She noted that the web server and the database server were getting hit the hardest. Upon checking traffic logs, Lisa identified a high volume of suspicious incoming connections from the following IP ranges:

- 192.168.45.0/24
- 203.123.155.200
- 45.76.19.132

Lisa also noted that the load balancer was struggling and that a couple of servers had crashed and rebooted earlier that day.

Tools Used for Investigation

- **Firewall and Router Logs:** John Carter pulled data from these logs to identify the volume of requests and suspicious IP addresses.
- **Threat Intelligence Database:** Alex Torres cross-referenced IP addresses with a threat intelligence database to identify known malicious actors.
- **Network Monitoring Tools:** Lisa Reynolds initially detected the slowdowns using network monitoring tools.
- **Endpoint Detection and Response (EDR) Solution:** Alex Torres reviewed endpoint protection logs to investigate the tools used by the attackers. An upgrade to a better EDR solution was recommended.

Interviews

Sarah (Employee)

- The network is experiencing slowness, impacting productivity and causing disruptions to various tasks and services.
- Specifically, sending emails and accessing files are taking longer than usual, and the web server has become inaccessible.

- These issues are causing significant disruption to daily operations, including inconsistent access to essential services like Workday and benefits platforms.

John Carter (Junior Network Engineer)

- Started a week ago
- The network is experiencing a noticeable slowdown, with webpages taking longer to load than usual.
- Users reporting difficulty accessing services, including occasional "service unavailable" errors.
- This slowdown coincides with a sudden spike in traffic from IP addresses that don't normally interact with the network.
- Unusually high bandwidth usage despite no increase in legitimate user activity.
- This suspicious activity suggests the possibility of further downtime and performance issues.

Jordan Steele (Chief Information Officer)

- The network is suffering from slowdowns, causing webpages to load slowly and hindering access to services, sometimes resulting in complete downtime.
- Servers are randomly crashing and rebooting without a clear cause.
- Spike in network traffic and bandwidth usage, straining the infrastructure.
- These issues are leading to revenue loss and the potential for client distrust and loss.

4. Technical Findings

Symptoms Observed

- **Network Slowdowns:** Major slowdowns were observed across multiple systems. The web server and database server experienced the most impact.
- **Unusual Network Traffic:** Suspicious incoming connections were noted from specific IP ranges. Thousands of connection attempts per minute from unusual IP addresses maxed out bandwidth.
- **Load Balancer Issues:** The load balancer struggled, and some servers crashed and rebooted.

- **Compromised VPN Gateway:** Remote users reported connection drops, indicating the VPN gateway was affected.
- **DNS Server Strain:** The DNS server was bombarded with requests for random subdomains.
- **Email Server Issues:** The email server showed unusual traffic and delivery delays.

Affected Equipment

- **Web Server:** Dell PowerEdge R740
- **Database Server:** HPE ProLiant DL380 Gen10
- **Load Balancer:** F5 Networks BIG-IP 2000 Series
- **Firewall:** Cisco Firepower 2100 Series
- **Router:** Cisco ASR 1000 Series Aggregation Services Router
- **Switch:** Cisco Catalyst 9300 Series
- **Content Delivery Network (CDN):** Akamai Adaptive Media Delivery (Cloud-based)
- **DNS Server:** Infoblox DDI Appliance
- **Email Server:** Microsoft Exchange Server 2019 (Running on VMware)
- **VPN Gateway:** Palo Alto Networks Global Protect

Cyber Actors

- **APT 33:** Considered a strong candidate due to their focus on sectors like Nexora Dynamics (aerospace, energy, manufacturing) and use of PowerShell-based backdoors and spear-phishing. "*Given their preference for leveraging wiper malware and disruptive attacks, it seems possible they could be involved.*"
- **APT 34 (OilRig):** Another likely suspect due to their targeting of similar industries, credential harvesting techniques, and lateral movement using legitimate admin tools. "*Their techniques often involve credential harvesting and lateral movement using legitimate admin tools, similar to what we're observing here.*"
- **APT 28 (Fancy Bear) and APT 29 (Cozy Bear):** Considered less likely, though not entirely ruled out, due to their typical focus on government and diplomatic entities.

Attack Vectors

- **Initial Breach:** Began with a spear-phishing email to a contractor ("*Week 1, 10:15 AM* : Initial access to the network was established through a phishing email sent to a contractor."). The email contained a malicious macro-enabled document that opened a reverse shell via PowerShell.
- **Credential Theft:** "*Week 1, 3:30 PM*: The attackers escalated privileges on the compromised contractor's laptop using Mimikatz to dump credentials."
- **Lateral Movement:** "*Week 2, 1:00 AM*: Attackers began lateral movement across the internal network, using RDP and SMB to access other systems."
- **Persistence:** "*Week 3, 4:45 AM*: A series of scheduled tasks were created on various servers to maintain persistence."
- **Reconnaissance:** "*Week 4, 9:15 PM*: Attackers started scanning the network to identify additional targets and map out the entire environment. They conducted internal recon using tools like Nmap to find other systems and services they could exploit."
- **Privilege Escalation:** "*Week 5, 2:30 AM*: After mapping out their targets, the attackers used pass-the-hash attacks to access systems without having to break password hashes."
- **Command & Control:** "*Week 7, 12:15 PM*: Noticed a spike in encrypted outbound traffic to a known Cobalt Strike C2 server."
- **Disabling Security Tools:** "*Week 9, 5:45 AM*: Multiple machines showed disabled security tools and services. The attackers seemed to systematically turn off antivirus programs and firewalls on key servers to avoid detection and leave backdoors open."
- **Data Exfiltration:** "*Week 12, 1:30 PM*: Data exfiltration started on a larger scale."
- **Log Wiping:** "*Week 13, 11:00 PM*: The final phase involved wiping logs and clearing traces on most of the compromised machines."

5. Root Cause Analysis (vulnerabilities)

- **Phishing Vulnerability:** Lack of effective email filtering and user awareness training allowed the initial phishing attack to succeed.
- **Cached Credentials:** "*Storing admin credentials insecurely on end-user devices is an oversight*." The presence of cached admin credentials on the contractor's laptop allowed for immediate privilege escalation.
- **Weak Endpoint Security:** Existing endpoint detection and response (EDR) solution failed to detect malicious activity and the installation of persistent backdoors.

- **Inadequate Monitoring and Alerting:** The existing monitoring and alerting system failed to correlate events and detect unusual patterns in a timely manner.
- **Patch Management:** Vulnerable services unpatched allowed the attacker to move through the network.

6. Recommendations (mitigations)

- **Advanced Email Filtering and User Training:** Improve email filtering and provide regular security awareness training, especially for contractors.
- **Multi-Factor Authentication (MFA):** Enforce MFA, especially for remote contractors, to prevent credential theft.
- **Disable Cached Credentials:** Disable cached admin credentials on contractor and remote devices.
- **Network Segmentation:** Implement internal firewalls or VLANs to isolate different systems and departments.
- **Role-Based Access Control (RBAC) and Privileged Access Management (PAM):** Implement RBAC and PAM to control admin privileges more tightly and monitor for privilege escalation.
- **Endpoint Detection and Response (EDR):** Upgrade to an EDR solution that can detect suspicious activities.
- **Application Whitelisting:** Prevent unauthorized tools from running.
- **Automated Patch Management:** Automate patching for critical systems.
- **Regular Vulnerability Assessments:** Conduct regular vulnerability assessments to identify potential weak spots.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Implement IDS/IPS to catch lateral movement and unusual network activity.
- **Security Information and Event Management (SIEM):** Implement a SIEM solution for correlating logs across systems.
- **Penetration Testing:** Conduct periodic penetration testing to simulate real-world attacks and validate the effectiveness of defenses.
- **Incident Response Training:** Conduct incident response training and update the incident response plan.

7. Conclusion

Nexora Dynamics faced a sophisticated and persistent cyberattack that exploited multiple vulnerabilities in its security infrastructure. The quick identification of these vulnerabilities and the subsequent development of comprehensive mitigation strategies are crucial steps toward improving the company's overall security posture and preventing future incidents.

Revision #3
Created 2025-11-25 17:42:19 UTC by David Rizzo
Updated 2025-11-25 17:44:19 UTC by David Rizzo