Docs

- Threat Actor Email
- Equipment Email
- Attack Symptoms
- Company Info

Threat Actor Email

From: John Carter (IT Supervisor)

To: Sarah Barnes (System Administrator), Lisa Reynolds (Network Administrator)

CC: IT Security Team

Hi Sarah, Lisa,

Thank you both for all the hard work in getting to the bottom of this incident. Given the indicators we've found—spear-phishing emails, PowerShell-based backdoors, and the subsequent lateral movement—it's becoming crucial to determine which threat actors are capable of deploying such a sophisticated attack on Nexora Dynamics.

Based on what we know, I'd like to hear your thoughts on which APT groups could be responsible for this breach. Specifically, we should consider threat actors who have the means, motivation, and methods aligned with what we're seeing.

Some potential groups that come to mind include:

- **APT 33**: Their history of targeting organizations in the aerospace, energy, and manufacturing sectors, along with their known use of spear-phishing, PowerShell scripting, and credential theft, makes them a prime suspect. Given their preference for leveraging wiper malware and disruptive attacks, it seems possible they could be involved.
- **APT 28 (Fancy Bear)**: Known for cyber-espionage and deploying highly targeted attacks, especially on government and corporate entities. They have a history of leveraging spear-phishing campaigns and sophisticated backdoors.
- **APT 34 (OilRig)**: Another group often linked to targeting industries similar to ours. They have been known to use PowerShell extensively and conduct credential-harvesting attacks similar to what we're seeing. Their focus on Middle Eastern and global energy sectors might make them a candidate.
- **APT 29 (Cozy Bear)**: Their tactics often involve quiet, persistent access with the aim of gathering intelligence over time. They're adept at moving laterally within a network and using stealthy methods to exfiltrate data.

Given that we haven’t seen an outright ransomware attack or clear financial motivation, it’s likely we’re dealing with either a nation-state actor or an APT with a strategic interest in our sector. Let me know your thoughts on these possibilities or if you believe another threat actor could be involved.

Understanding the likely threat actor is critical in determining how to respond effectively and prevent further attacks. Any additional insights on their TTPs or motivations would be invaluable as we put together a defense and recovery strategy.

Thanks,
John

From: Sarah Barnes (System Administrator)
To: John Carter (IT Supervisor), Lisa Reynolds (Network Administrator)
CC: IT Security Team

Hi John, Lisa,

Based on what we’ve seen so far, I’d agree that **APT 33** is a strong candidate given their known focus on sectors similar to ours and their use of PowerShell-based backdoors. Their track record of using spear-phishing to gain initial access and then deploying malware to spread within the network aligns closely with what we're experiencing.

That said, I wouldn’t rule out **APT 34 (OilRig)** either. They have been quite active and have a known preference for targeting the same industries. Their techniques often involve credential harvesting and lateral movement using legitimate admin tools, similar to what we’re observing here.

While **APT 28 (Fancy Bear)** and **APT 29 (Cozy Bear)** are always worth considering given their sophisticated capabilities, their recent activity seems to focus on government and diplomatic entities, which makes them slightly less likely than the others mentioned. However, it’s possible that they could have motives aligning with our industry, especially if they are pursuing intelligence-gathering objectives.

If I were to prioritize, I’d say APT 33 and APT 34 are the most likely suspects based on their TTPs and the nature of our organization. I’ll start gathering more intel on their recent activity to see if anything matches up directly with what we’ve been seeing.

Let me know if there’s anything specific you'd like me to focus on.

Best,
Sarah

From: Lisa Reynolds (Network Administrator)
To: John Carter (IT Supervisor), Sarah Barnes (System Administrator)
CC: IT Security Team

Hi John, Sarah,

I agree with both of you on **APT 33** being a likely candidate. The tactics of using spear-phishing to gain entry, followed by fileless malware like a PowerShell backdoor, are in line with what we know of their playbook. Their interest in critical infrastructure and energy-related sectors also makes sense given our organization's profile.

I’d add that **APT 34 (OilRig)**’s known use of **custom backdoors and VPN exploits** could fit our incident as well. Their history of targeting supply chains and service providers in industries like ours makes them a good fit for further investigation. They’re known for deploying a mix of custom and commodity malware, which could explain the combination of tools we’ve found so far.

I’ll dig deeper into any network signatures or known IoCs specific to APT 33 and APT 34 to see if we can make a more definitive match. We might also want to consider any geopolitical tensions or motives that would make our organization a higher priority for these actors.

I’ll keep gathering more details and share anything relevant as it comes up.

Thanks,
Lisa

Equipment Email

All,

Just wanted to report on the list of IT equipment impacted by the recent network issues, including make, model, and serial numbers for each. Please review the details below and let me know if any additional information is required for troubleshooting.

1. **Web Server**
   - **Make**: Dell PowerEdge R740
   - **Model**: PER740XA2
   - **Serial Number**: DCH45T9P8Q0
2. **Database Server**
   - **Make**: HPE ProLiant DL380 Gen10
   - **Model**: DL380-G10-XL
   - **Serial Number**: USE689PR4C1
3. **Load Balancer**
   - **Make**: F5 Networks BIG-IP 2000 Series
   - **Model**: BIG-IP i2600
   - **Serial Number**: F512AX97R3
4. **Firewall**
   - **Make**: Cisco Firepower 2100 Series
   - **Model**: FPR-2110
   - **Serial Number**: CFP212345C
5. **Router**
   - **Make**: Cisco ASR 1000 Series Aggregation Services Router
   - **Model**: ASR1001-HX
   - **Serial Number**: CASR10X689A
6. **Switch**
   - **Make**: Cisco Catalyst 9300 Series
   - **Model**: C9300-24P-E
   - **Serial Number**: CAT9356YPQ2
7. **Content Delivery Network (CDN)**

- **Make**: Akamai Adaptive Media Delivery (Cloud-based)
- **Model**: N/A (Cloud Service)

8. **DNS Server**
   - **Make**: Infoblox DDI Appliance
   - **Model**: Trinzic 1410
   - **Serial Number**: TZN76423X98
9. **Email Server**
   - **Make**: Microsoft Exchange Server 2019 (Running on VMware)
   - **Model**: N/A (Virtualized)
10. **VPN Gateway**
    - **Make**: Palo Alto Networks GlobalProtect
    - **Model**: PA-5220
    - **Serial Number**: PANGP52321K

Let me know if you need any further details for logging or inventory purposes.

Best regards,

John Carter

IT Engineer, Nexora Dynamics

Attack Symptoms

Email 1: From Lisa Reynolds (Network Administrator) to John Carter

Subject: Urgent: Network Slowdown and Unusual Traffic

Hi John,

We’re seeing major slowdowns across multiple systems. I’ve received reports from both users and monitoring tools. It looks like the web server and the database server are getting hit the hardest right now. I checked the traffic logs, and there are a lot of suspicious incoming connections from the following IP ranges:

- 192.168.45.0/24
- 203.123.155.200
- 45.76.19.132

It looks like the load balancer is struggling too, and a couple of servers crashed earlier today and rebooted. Can you take a look at the firewall and router traffic on your end? This might be more than a typical traffic spike.

Thanks,
Lisa Reynolds
Network Administrator

Email 2: From John Carter (Mid-Level IT Engineer) to Lisa Reynolds, Alex Torres (Security Analyst), and Sarah Barnes (System Administrator)

Subject: RE: Urgent: Network Slowdown and Unusual Traffic

Hi Team,

Thanks for the heads-up, Lisa. I just pulled some data from the firewall and router logs. The firewall is getting hammered with requests from the IP addresses you mentioned, and I’m seeing a bunch of others as well:

- 198.51.100.45
- 64.233.187.99
- 103.45.89.223

These IPs are making thousands of connection attempts every minute. Our bandwidth is completely maxed out, and I think it’s spilling over to affect the VPN gateway too—remote users are reporting connection drops. We may need to start blocking some of these IPs at the firewall level immediately.

Alex, can you cross-reference these IPs with any known malicious actors? Sarah, can you check on the DNS and email servers? There are likely other systems being affected that we haven't caught yet.

Let’s regroup after you’ve had a chance to review the data.

Best,
John Carter
Mid-Level IT Engineer

Email 3: From Alex Torres (Security Analyst) to John Carter, Lisa Reynolds, and Sarah Barnes

Subject: RE: Urgent: Network Slowdown and Unusual Traffic

Hey team,

I just checked the IPs that John and Lisa listed, and several of them are flagged in our threat intelligence database as being part of known botnet activity. Here’s the breakdown:

- **203.123.155.200**: Identified as part of the Mirai botnet.
- **45.76.19.132**: Previously associated with DDoS activity targeting financial institutions.
- **103.45.89.223**: Blacklisted due to frequent brute-force attack attempts.

This is definitely coordinated, and it looks like they’re targeting multiple layers of our infrastructure. I recommend we move forward with blocking these IPs and maybe even implement rate-limiting on the load balancer. Let me know if I should proceed.

Alex Torres
Security Analyst

Email 4: From Sarah Barnes (System Administrator) to John Carter, Lisa Reynolds, and Alex Torres

Subject: RE: Urgent: Network Slowdown and Unusual Traffic

Hi All,

I've checked the DNS and email servers, and both are showing significant strain. The DNS server has been getting bombarded with requests for random subdomains, which is likely contributing to the slowdowns. The email server is also showing unusual traffic, and there are some delays in delivery.

I'm working on clearing the queue for the email server, but we might need to offload some of this traffic before it gets worse. Should we also look into adjusting DNS settings to filter out some of the bad traffic? Let me know if there's anything else I can assist with.

Sarah Barnes
System Administrator

Email 5: From John Carter to Lisa Reynolds, Alex Torres, and Sarah Barnes

Subject: RE: Urgent: Network Slowdown and Unusual Traffic

Thanks for the quick responses, everyone. Let's go ahead and start with blocking those malicious IP addresses on the firewall, and Alex, go ahead with the rate-limiting setup on the load balancer. Sarah, adjusting the DNS settings to filter out the bogus requests sounds like a good move. Once we've got these measures in place, we should monitor for further spikes and reconvene if the situation escalates.

I'll update management with our progress. Let's stay on this and continue collaborating. Thanks again for jumping on it so quickly.

Best,
John Carter
Mid-Level IT Engineer

Company Info

Company Name: Nexora Dynamics

Industry: Engineering Services

Company Size: Medium-sized enterprise (250-500 employees)

Headquarters: Baltimore, MD

Established: 2008

Company Overview:

Nexora Dynamics is a leading provider of cutting-edge engineering services, specializing in advanced technology solutions for industries such as aerospace, defense, energy, and infrastructure. With a focus on innovation, Nexora Dynamics offers a range of services, including systems design, testing, and operational support, tailored to meet the needs of both private sector clients and government agencies.

As a medium-sized firm, Nexora Dynamics maintains agility and a customer-first approach while delivering robust solutions that rival those of much larger competitors. The company’s mission is to empower clients with high-quality engineering solutions that drive efficiency, sustainability, and technological advancement.

Core Services:

1. **Systems Engineering**:
   - Design and implementation of complex systems across various industries, ensuring integration, performance, and reliability.
2. **Product Development & Testing**:
   - Full product lifecycle support, from initial concept to prototyping, testing, and production readiness.
3. **SCADA Systems & Automation**:

- Expertise in SCADA (Supervisory Control and Data Acquisition) systems, with a focus on automation and control systems for critical infrastructure.

4. **Cybersecurity & Risk Management**:
   - Comprehensive OT (Operational Technology) security assessments, vulnerability testing, and implementation of robust security measures for critical systems.
5. **Consulting & Technical Support**:
   - Advisory and on-site technical support services for optimizing operations, improving safety standards, and reducing downtime.

Key Clients:

- Aerospace and defense contractors
- Energy sector companies (nuclear, oil & gas, renewable)
- Government agencies (Department of Defense, Homeland Security)
- Infrastructure and transportation companies

Company Vision:

To be the trusted partner for organizations seeking innovative engineering solutions that solve complex challenges and propel them into the future. Nexora Dynamics is committed to fostering a collaborative environment that drives forward-thinking solutions and enables clients to thrive in an increasingly technological world.

Values:

- **Innovation**: Continuously pushing the boundaries of technology to provide groundbreaking solutions.
- **Integrity**: Maintaining the highest ethical standards and ensuring transparency in every project.
- **Excellence**: Delivering superior results by investing in top talent and cutting-edge tools.
- **Customer Focus**: Building lasting relationships by consistently exceeding client expectations.

Leadership Team:

- **CEO**: **Emily Lawson**
  Emily brings over 20 years of leadership experience in the engineering and technology

sectors. She is responsible for overseeing the company's strategic direction and growth.

- **COO**: **David Chen**
  David manages day-to-day operations, ensuring that Nexora Dynamics consistently delivers on its promises to clients, from project execution to customer satisfaction.
- **CTO**: **Sophia Martinez**
  Sophia leads Nexora's technology strategy, focusing on innovation, research and development, and the integration of emerging technologies in engineering services.
- **Head of Engineering**: **Mark Thompson**
  Mark oversees all engineering projects, ensuring technical excellence and adherence to industry standards. He works closely with clients to understand their needs and deliver solutions that exceed expectations.
- **CIO (Chief Information Officer)**: **Jordan Steele**
  Rachel is responsible for managing Nexora's cybersecurity strategies, protecting both internal systems and client infrastructure from evolving cyber threats.

Office Location:

Nexora Dynamics
3200 Innovation Parkway
Suite 500
Baltimore, MD 21201
United States