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

Revision #1

Created 2025-11-25 17:50:23 UTC by David Rizzo

Updated 2025-11-25 17:50:32 UTC by David Rizzo