Subject: Re: Request for Additional Information Regarding Cybersecurity Breach Incident 234

Dear Kathleen,

I hope this email finds you well. Thank you for reaching out to me regarding the cybersecurity breach incident reported in ticket NO. 234. I understand the urgency of this matter and am ready to provide the necessary information to assist with your investigation.

Please find the requested details below:

We first noticed the suspicious activities on 2024/07/17 at approximately 10:45 AM when our monitoring system flagged an unusual number of HTTP 404 and 500 errors originating from the IP address in question. Apart from the high volume of 404 and 500 errors, we observed intermittent system slowdowns and occasional timeout errors on our web services. No other specific error messages were noted.

We have detected several failed login attempts from the same IP address, indicating possible brute force attempts. However, there is no confirmed evidence of compromised credentials at this time. The only recent software update was a scheduled Apache server update performed on 2024/07/15. No new software installations have been conducted in the past month.

We noticed that the suspicious IP address has been associated with previous low-level scanning activities over the past month, though those did not trigger significant alerts at the time. The traceroute for the suspicious IP address shows multiple hops through various international servers, which complicates pinpointing the exact server origin. The detailed traceroute is sent to you on the secure email that follows this email.

Please let me know if you need any further details or additional logs to aid your investigation. I am committed to working closely with your team to identify and mitigate the root cause of this breach.

Thank you for your cooperation and support in addressing this incident. If you have any further questions or need clarification on any of the provided information, please do not hesitate to contact me.

Best regards,

Pavan Kumar K

IT Operations Director

Turn a New Leaf

pavan.k@tnf.com (Ph) +1 888 888 8888