NIGHTMARE ON CYBER STREET

DIGITAL FORENSICS

PART I

On the witching night of October 31st, ACM has become the target of a malevolent spirit, rumored to haunt the network and drain it of its sensitive data.

Whispers among employees speak of ghostly apparitions appearing on screens, flickering lights, and eerie noises emanating from the server room.

As Halloween approaches, strange activities escalate, and a crucial report containing trade secrets vanishes into the void. The cybersecurity team has been summoned to investigate the spectral breach before it’s too late.

OBJECTIVE

Identify the treacherous insider responsible for collaborating with the spirit.

Determine the dark method of data exfiltration used to steal the sensitive information.

WINDOWS EVENT LOGS

Date	Event ID	User	Action	Source IP
2024-10-31	4624	ghostly.jane	Successful Login	10.0.0.13
2024-10-31	4625	zombie.bob	Failed Login Attempt	192.168.1.13
2024-10-31	4624	admin.witch	RDP Session Start	172.16.0.6
2024-10-31	4672	admin.witch	Privileged Login	172.16.0.6
2024-10-31	4634	admin.witch	Session Terminated	172.16.0.6

EMAIL

From: it_spooks@acm-haunt.com
To: ghostly.jane@acm.com
Subject: Urgent! Ghostly Password Reset Required!
Date: Fri, 31 Oct 2024 03:30:00 GMT
X-Mailer: PHP/7.4
Received: from phantom-ip.com (212.48.75.22)
Message-ID: ghostly-123@acm-haunt.com

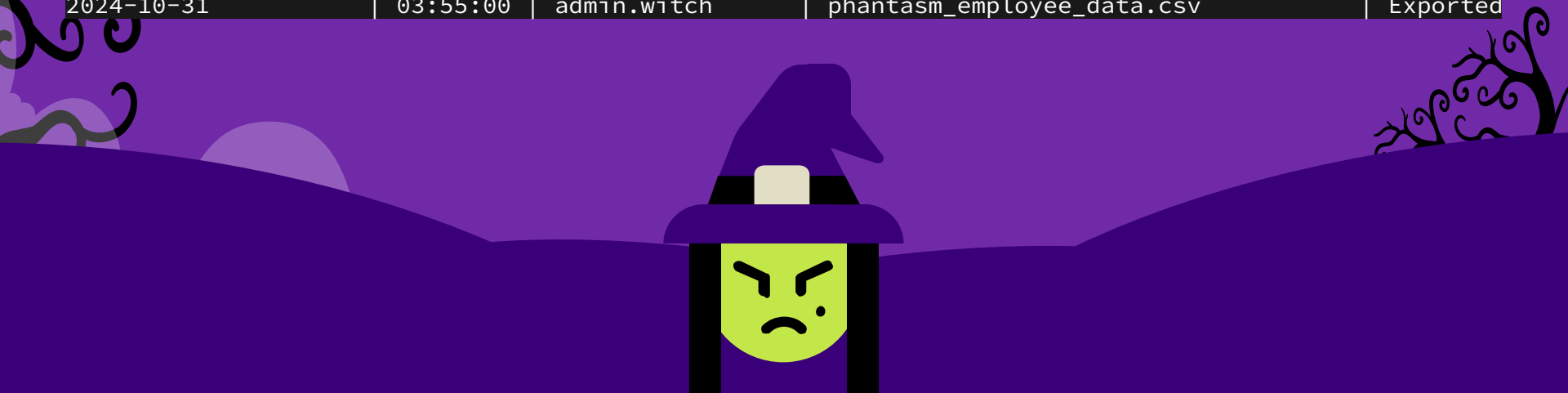
Hi Jane,
This is an urgent notice to reset your password immediately to prevent any access issues. Please complete this within the next 30 minutes to avoid any disruptions.
Failure to change your password in the specified time frame could result in termination. If you need assistance, contact the IT department.
Best Regards,
President Karina

FIREWALL LOGS

Date	Time	Source IP	Destination IP	Protocol	Action	Data Size
2024-10-31	03:15:10	10.0.0.13	104.21.3.51	HTTPS	Allowed	150MB
2024-10-31	03:30:12	192.168.1.13	88.208.3.98	FTP	Allowed	250MB
2024-10-31	03:45:55	172.16.0.6	88.208.3.98	FTP	Allowed	1GB

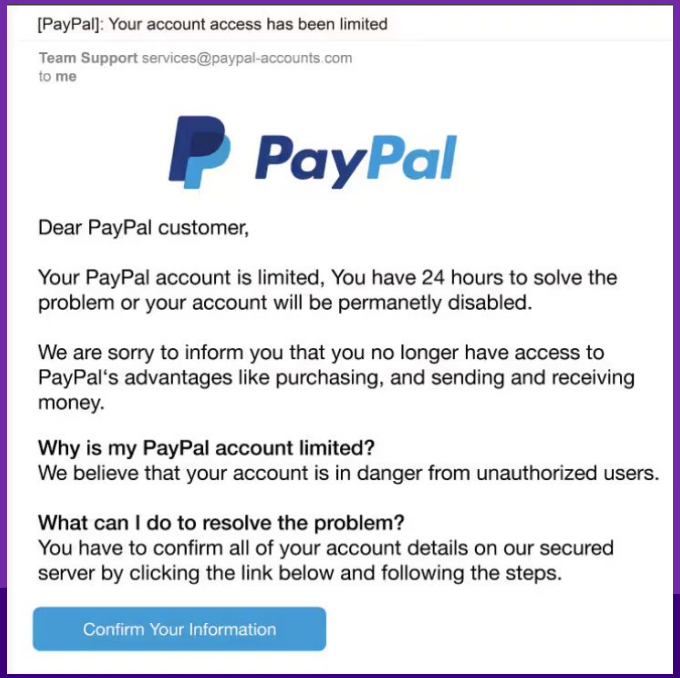
FILE ACCESS LOGS

Date	Time	User	File Accessed	Action
2024-10-31	03:30:00	ghostly.jane	haunted_financials.xlsx	Opened
2024-10-31	03:50:15	admin.witch	cursed_confidential.zip	Copied
2024-10-31	03:55:00	admin.witch	phantasm_employee_data.csv	Exported



PHISHING
PART II

PAYPAL DECEPTION??


[PayPal]: Your account access has been limited

Team Support services@paypal-accounts.com
to **me**

PayPal

Dear PayPal customer,

Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled.

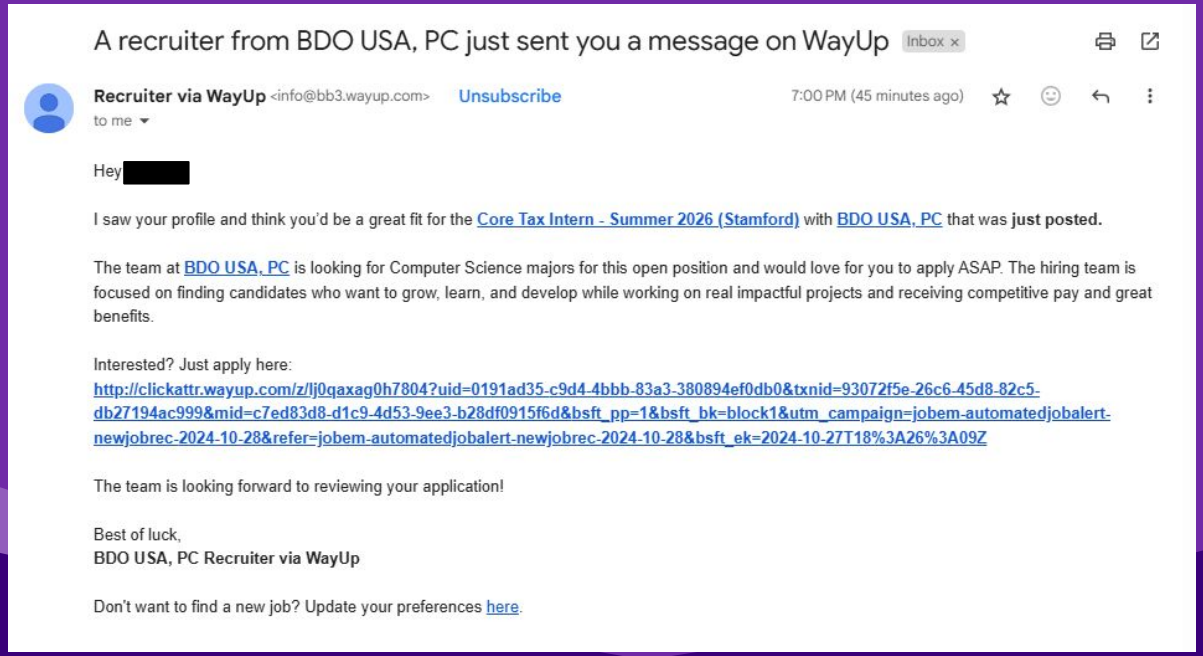
We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money.

Why is my PayPal account limited?
We believe that your account is in danger from unauthorized users.

What can I do to resolve the problem?
You have to confirm all of your account details on our secured server by clicking the link below and following the steps.

Confirm Your Information

WAYUP OR WAYDOWN



A recruiter from BDO USA, PC just sent you a message on WayUp Inbox ×

Recruiter via WayUp <info@bb3.wayup.com> Unsubscribe 7:00 PM (45 minutes ago)

to me

Hey [redacted]

I saw your profile and think you'd be a great fit for the Core Tax Intern - Summer 2026 (Stamford) with BDO USA, PC that was **just posted.**

The team at BDO USA, PC is looking for Computer Science majors for this open position and would love for you to apply ASAP. The hiring team is focused on finding candidates who want to grow, learn, and develop while working on real impactful projects and receiving competitive pay and great benefits.

Interested? Just apply here:
http://clickattr.wayup.com/z/lj0qaxag0h7804?uid=0191ad35-c9d4-4bbb-83a3-380894ef0db0&txnid=93072f5e-26c6-45d8-82c5-db27194ac999&mid=c7ed83d8-d1c9-4d53-9ee3-b28df0915f6d&bsft_pp=1&bsft_bk=block1&utm_campaign=jobem-automatedjobalert-newjobrec-2024-10-28&refer=jobem-automatedjobalert-newjobrec-2024-10-28&bsft_ek=2024-10-27T18%3A26%3A09Z

The team is looking forward to reviewing your application!

Best of luck,
BDO USA, PC Recruiter via WayUp

Don't want to find a new job? Update your preferences here.

GEEK SQUAD LEGENDS

PR **Poul Rosing** 10/17/24
To: [redacted]

Your Purchase Is Verified and Confirmed 714443056266

Geek SQUAD

Billing details:

Order date : october17th, 2024
Subscriber : apollo101416@gmail.com
Order Confirmed Id: 189583015476

We respect the Geek Squad you selected. We attest to the appropriate processing of your membership request with pleasure. In the coming day or two, you will be able to view the $375.99 membership cost that was charged to the credit card linked to your email account.

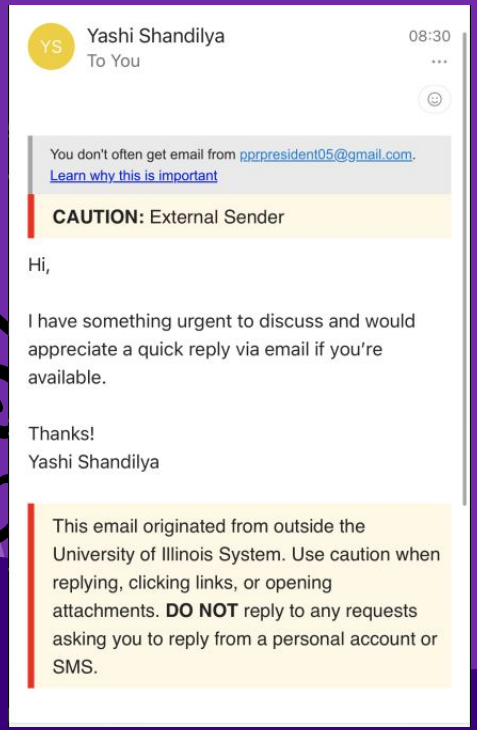
Purchase Recap

Order Details: Geek Squad
Support: 2 Device
Period : 1 Year
Amount: $375.99

Within a day, USD 375.99 will be taken out of your account. To cancel or request a refund, please contact our customer service department as soon as possible.

Customer Support: + 1 866 837 3331

PHISHED FOR REAL



Yashi Shandilya 08:30
To You

You don't often get email from pprpresident05@gmail.com.
Learn why this is important

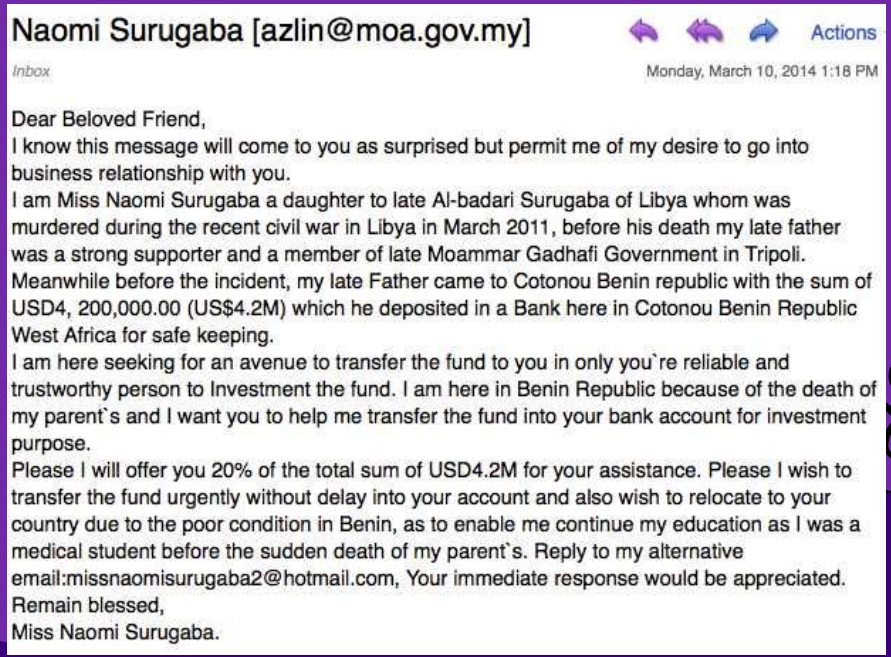
CAUTION: External Sender

Hi,

I have something urgent to discuss and would appreciate a quick reply via email if you're available.

Thanks!
Yashi Shandilya

This email originated from outside the University of Illinois System. Use caution when replying, clicking links, or opening attachments. **DO NOT** reply to any requests asking you to reply from a personal account or SMS.



Naomi Surugaba [azlin@moa.gov.my] Actions

Inbox Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

CRYPTOGRAPHY

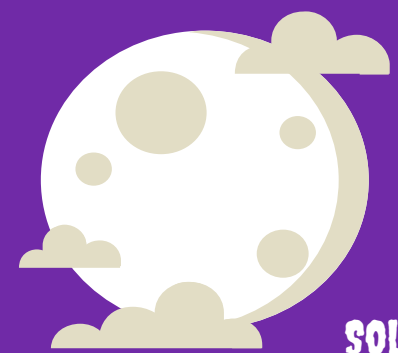
PART III

CAESAR CYPHER

SOLVE THE FOLLOWING CYPHERS TO GET YOUR LAST PIECE OF THE PUZZLE

RFPNCR GUR PLORE PELCG

NBY JBUHNIG IZ NBY MNUWE IPYLZFIQ



SPOOKY RIDDLE

PART IV