Employee Misconduct Investigation - PCAP Analysis Report

This report outlines the findings of an investigation into alleged employee misconduct, specifically involving the misappropriation of company funds. The investigation aimed to analyze network activity to identify the methods used by the employee in question, determine potential accomplices or external contacts, and collect relevant data to clarify the scope of the unauthorized activities.

Objectives

The primary objectives of this investigation were:

- To determine the techniques and tools employed by the employee to facilitate the suspected misconduct.
- To identify any external parties or accomplices with whom the employee communicated.
- To gather and analyze data that could provide comprehensive insight into the unauthorized activities conducted.

Tools Used: Network Miner, Virustotal.com, Microsoft Outlook

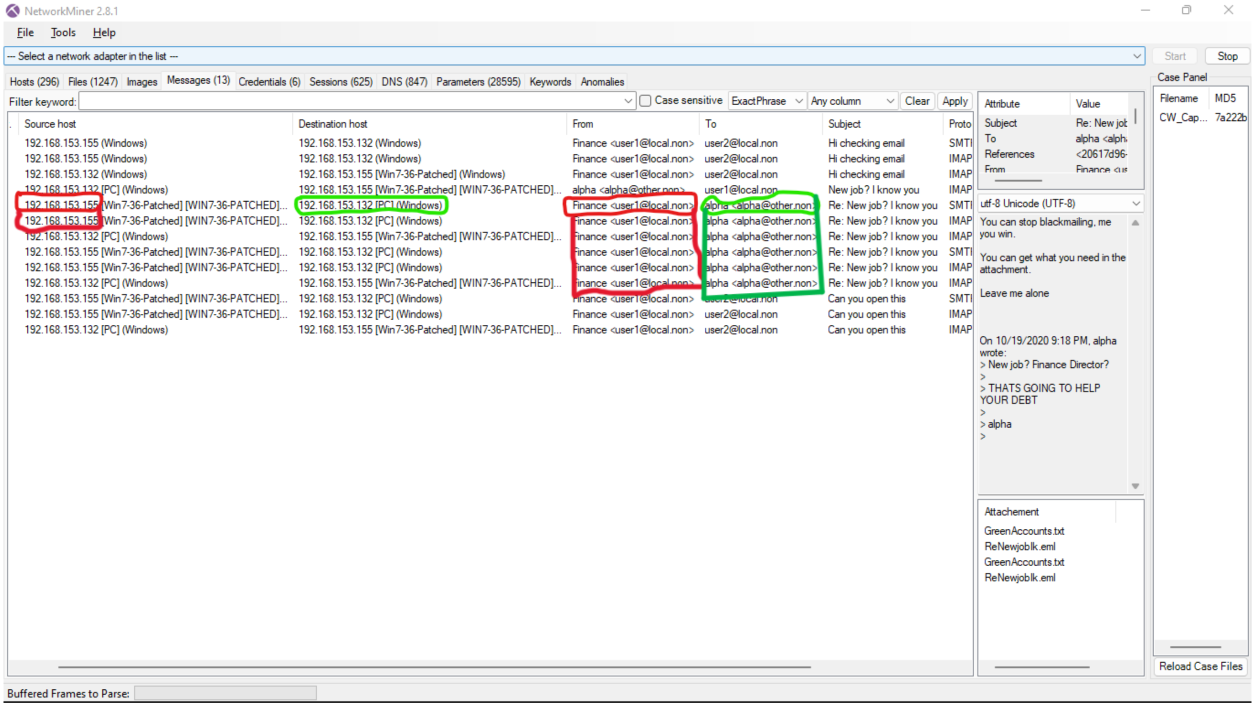
Observations and Findings

1. Suspicious Communication Patterns

Analysis of PCAP data revealed that the user in question, identified as "user1," engaged in frequent communication with an individual labeled "alpha." Notably, "alpha" is not registered within the company's internal network, suggesting they may be an external contact.

While communication between employees and external contacts is not unusual, the high frequency of interactions between user1 and alpha raises concerns, as alpha’s identity remains unverified in the company’s contact records.

Further investigation into the nature and context of these communications may provide insight into whether they were related to unauthorized activities.


NetworkMiner 2.8.1
File Tools Help
--- Select a network adapter in the list ---
Start
Stop
Hosts (296) Files (1247) Images Messages (13) Credentials (6) Sessions (625) DNS (847) Parameters (28595) Keywords Anomalies
Filter keyword:
□ Case sensitive
ExactPhrase
Any column
Clear
Apply
Case Panel
Reload Case Files
Buffered Frames to Parse:

Source host	Destination host	From	To	Subject	Proto
192.168.153.155 (Windows)	192.168.153.132 (Windows)	Finance <user1@local.non>	user2@local.non	Hi checking email	SMTI
192.168.153.155 (Windows)	192.168.153.132 (Windows)	Finance <user1@local.non>	user2@local.non	Hi checking email	IMAP
192.168.153.132 (Windows)	192.168.153.155 [Win7-36-Patched] (Windows)	Finance <user1@local.non>	user2@local.non	Hi checking email	IMAP
192.168.153.132 [PC] (Windows)	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	alpha <alpha@other.non>	user1@local.non	New job? I know you	IMAP
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	SMTI
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	IMAP
192.168.153.132 [PC] (Windows)	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	IMAP
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	SMTI
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	IMAP
192.168.153.132 [PC] (Windows)	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	Finance <user1@local.non>	alpha <alpha@other.non>	Re: New job? I know you	IMAP
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	user2@local.non	Can you open this	SMTI
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	192.168.153.132 [PC] (Windows)	Finance <user1@local.non>	user2@local.non	Can you open this	IMAP
192.168.153.132 [PC] (Windows)	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	Finance <user1@local.non>	user2@local.non	Can you open this	IMAP

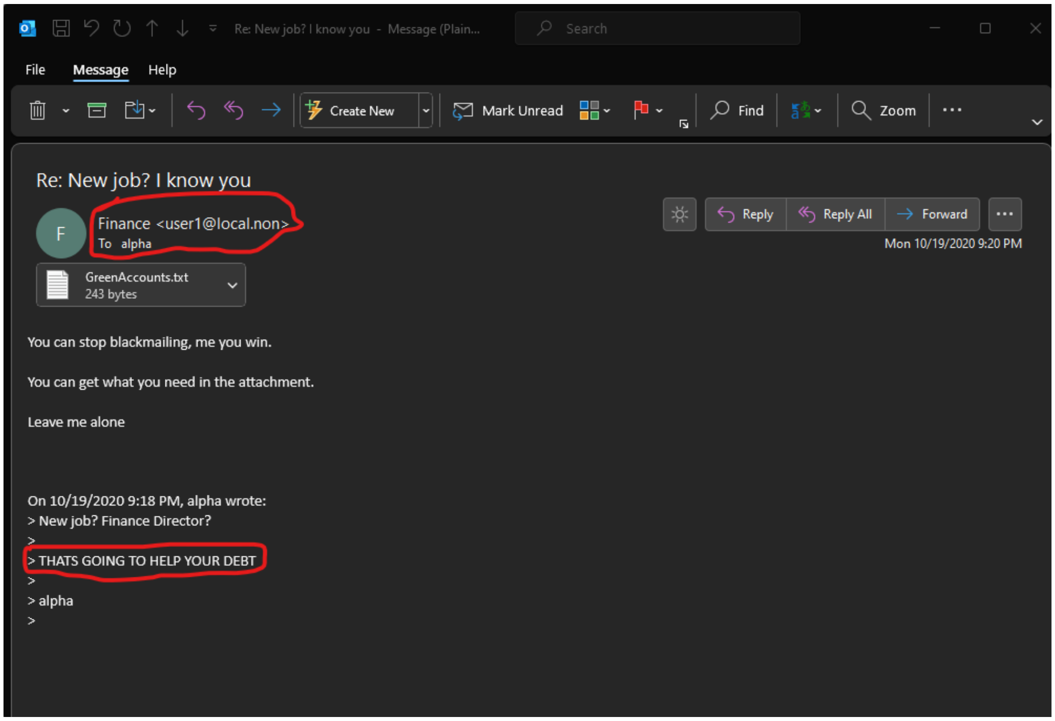
Attribute	Value
Subject	Re: New job
To	alpha <alph
References	<20617d96-
From	Finance <us

utf-8 Unicode (UTF-8)

```
You can stop blackmailing, me
you win.

You can get what you need in the
attachment.

Leave me alone



On 10/19/2020 9:18 PM, alpha
wrote:
> New job? Finance Director?
>
> THATS GOING TO HELP
YOUR DEBT
>
> alpha
>
```

Attachement
GreenAccounts.txt
ReNewjoblk.eml
GreenAccounts.txt
ReNewjoblk.eml

Filename	MD5
CW_Cap...	7a222b



Re: New job? I know you

Finance <user1@local.non>
To alpha

Mon 10/19/2020 9:20 PM

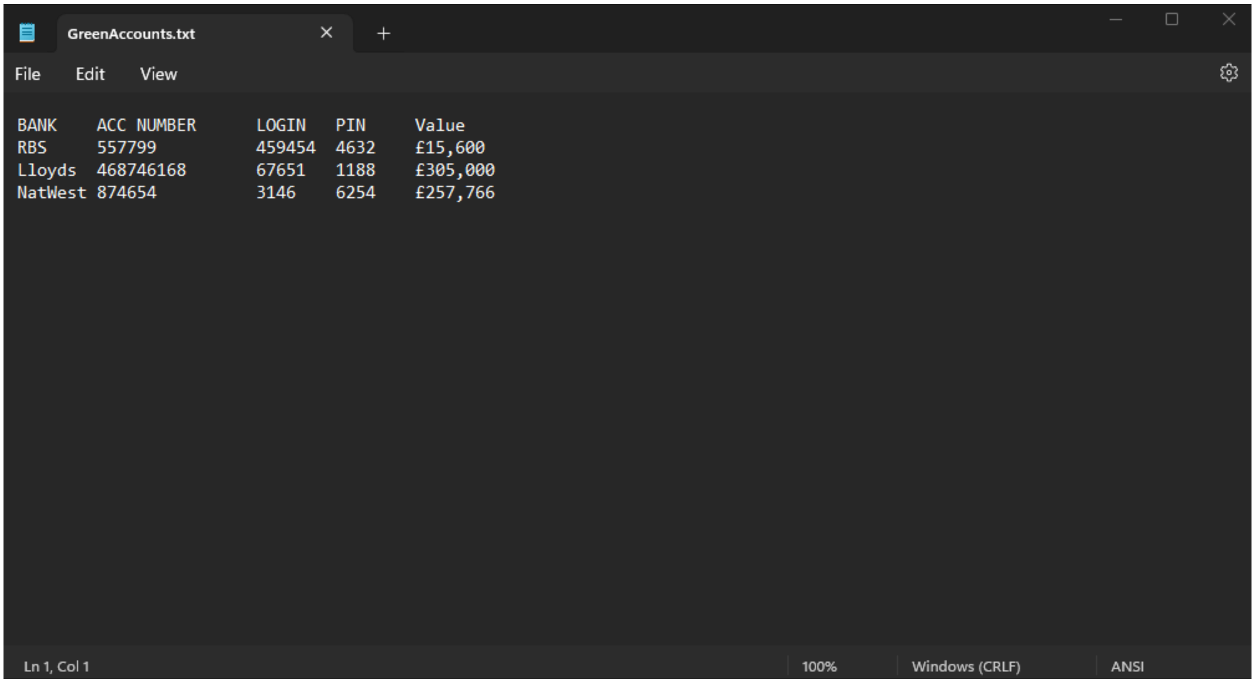
GreenAccounts.txt
243 bytes

You can stop blackmailing, me you win.

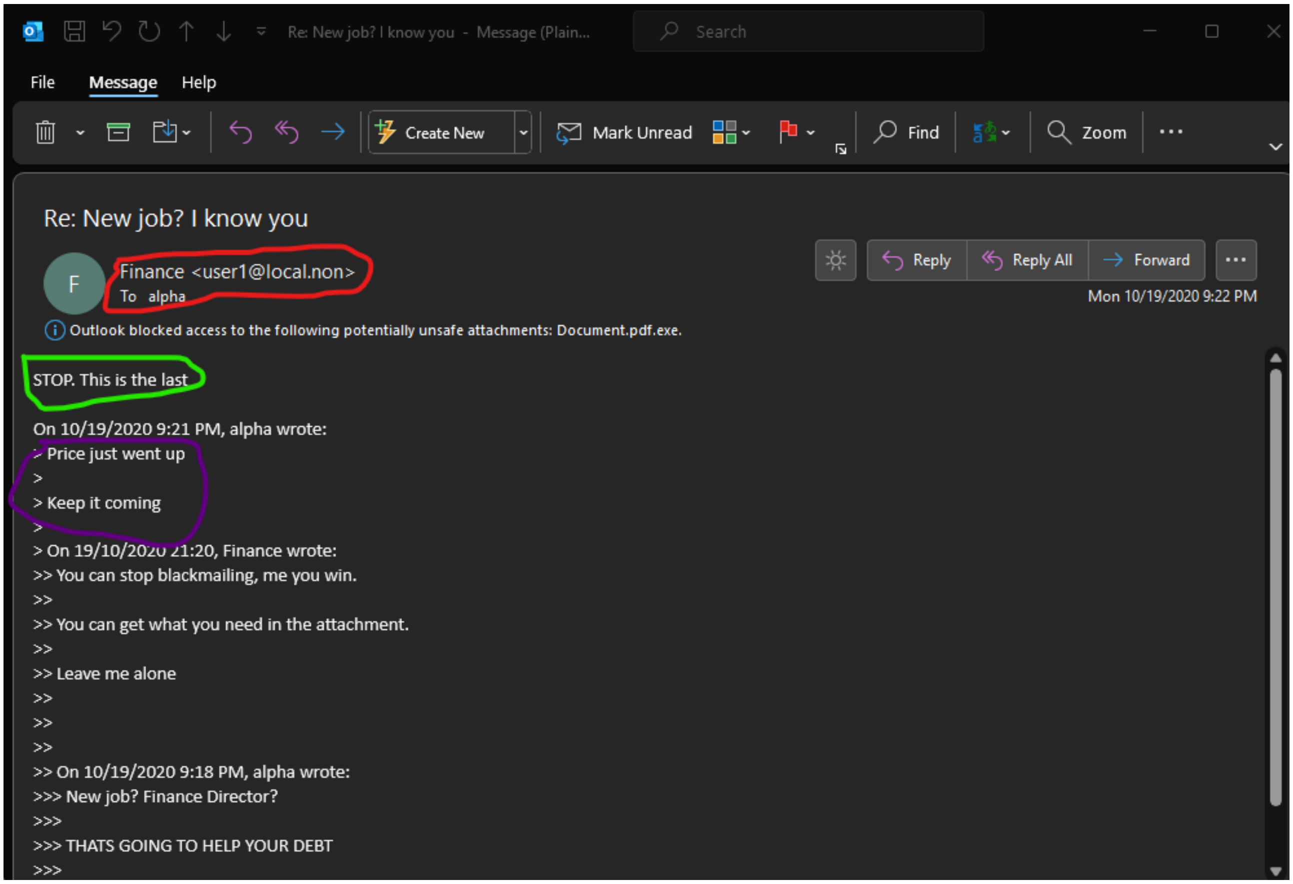
You can get what you need in the attachment.

Leave me alone

On 10/19/2020 9:18 PM, alpha wrote:
> New job? Finance Director?
>
> THATS GOING TO HELP YOUR DEBT
>
> alpha
>



```
BANK     ACC NUMBER       LOGIN   PIN     Value
RBS      557799           459454  4632    £15,600
Lloyds   468746168        67651   1188    £305,000
NatWest  874654           3146    6254    £257,766
```



Re: New job? I know you

Finance <user1@local.non>
To alpha

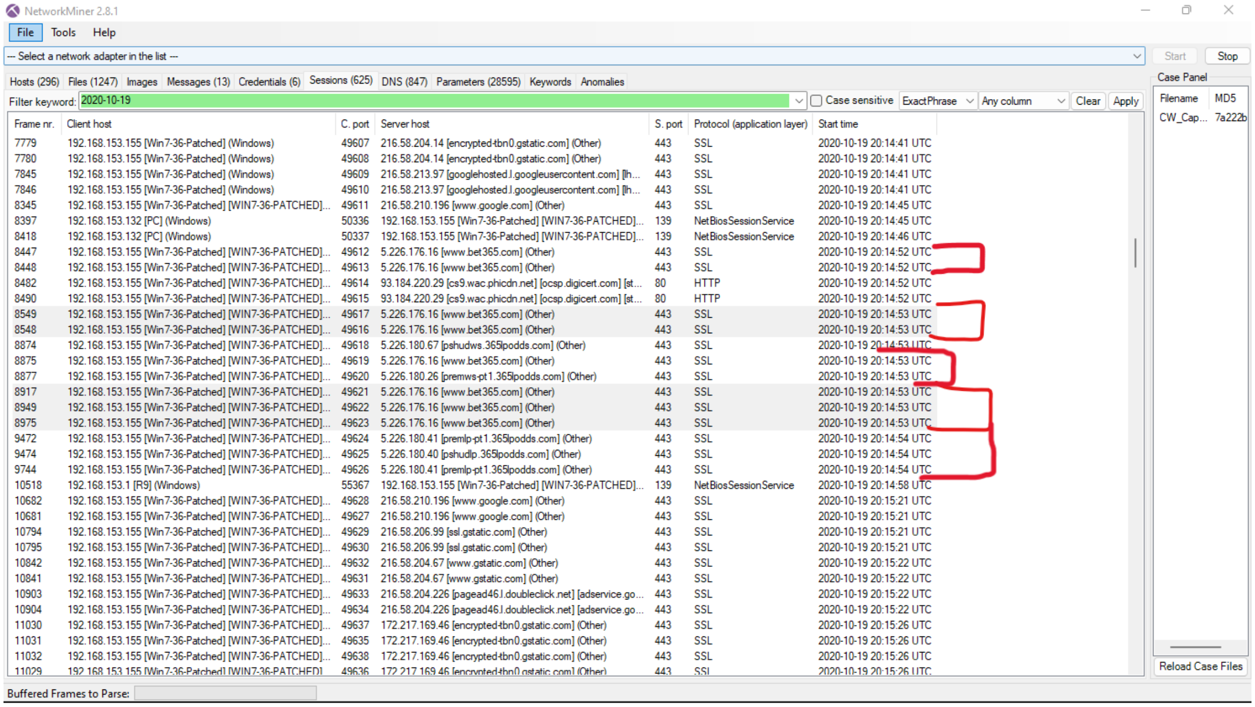
Mon 10/19/2020 9:22 PM

Outlook blocked access to the following potentially unsafe attachments: Document.pdf.exe.

```
STOP. This is the last

On 10/19/2020 9:21 PM, alpha wrote:
> Price just went up
>
> Keep it coming
>
> On 19/10/2020 21:20, Finance wrote:
>> You can stop blackmailing, me you win.
>>
>> You can get what you need in the attachment.
>>
>> Leave me alone
>>
>>
>>
>> On 10/19/2020 9:18 PM, alpha wrote:
>>> New job? Finance Director?
>>>
>>> THATS GOING TO HELP YOUR DEBT
>>>
```

2. Potential Financial Motivation

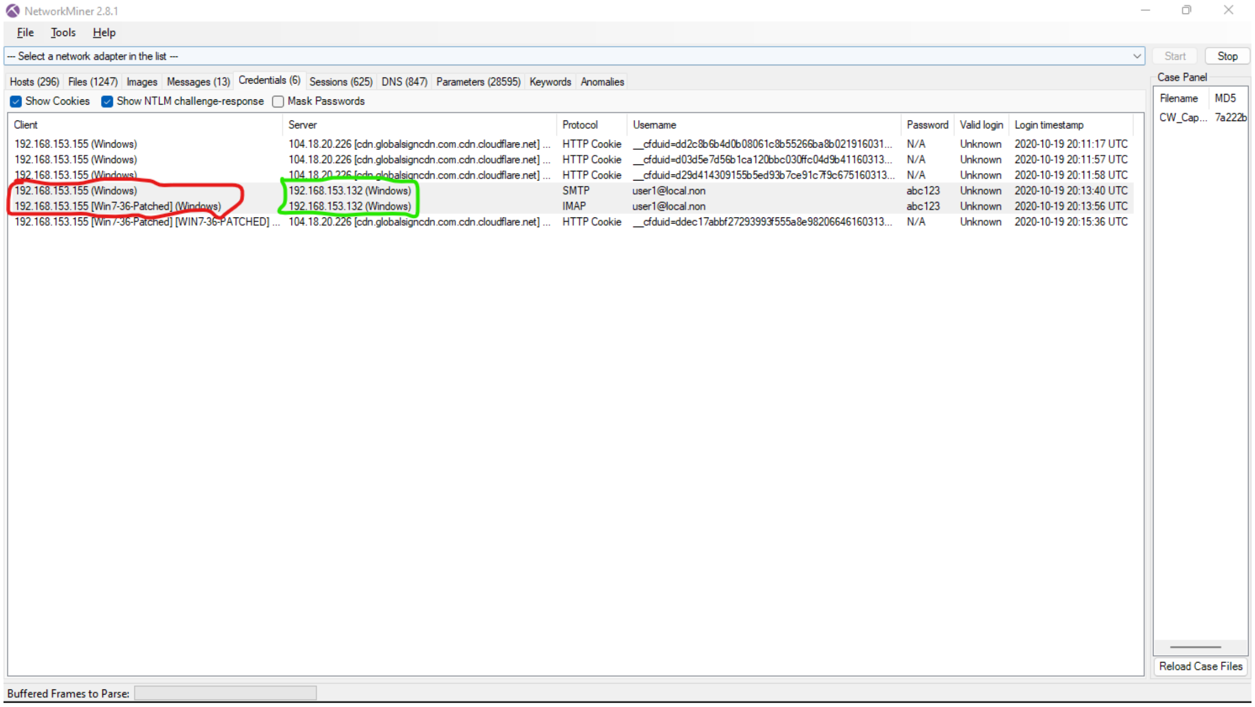
Examination of user1’s browsing activity showed frequent visits to the website "bet365," a known online betting platform. The frequency of visits to this betting site could indicate a potential motive behind the alleged misappropriation of funds. It is plausible that personal financial stress may have led to compromised decision-making, creating a vulnerability that could be exploited by others.



Filter keyword: 2020-10-19

Filename	MD5
CW_Cap...	7a222b

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
7779	192.168.153.155 [Win7-36-Patched] (Windows)	49607	216.58.204.14 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:14:41 UTC
7780	192.168.153.155 [Win7-36-Patched] (Windows)	49608	216.58.204.14 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:14:41 UTC
7845	192.168.153.155 [Win7-36-Patched] (Windows)	49609	216.58.213.97 [googlehosted.l.googleusercontent.com] [lh...	443	SSL	2020-10-19 20:14:41 UTC
7846	192.168.153.155 [Win7-36-Patched] (Windows)	49610	216.58.213.97 [googlehosted.l.googleusercontent.com] [lh...	443	SSL	2020-10-19 20:14:41 UTC
8345	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49611	216.58.210.196 [www.google.com] (Other)	443	SSL	2020-10-19 20:14:45 UTC
8397	192.168.153.132 [PC] (Windows)	50336	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	139	NetBiosSessionService	2020-10-19 20:14:45 UTC
8418	192.168.153.132 [PC] (Windows)	50337	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	139	NetBiosSessionService	2020-10-19 20:14:46 UTC
8447	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49612	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:52 UTC
8448	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49613	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:52 UTC
8482	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49614	93.184.220.29 [cs9.wac.phicdn.net] [ocsp.digicert.com] [st...	80	HTTP	2020-10-19 20:14:52 UTC
8490	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49615	93.184.220.29 [cs9.wac.phicdn.net] [ocsp.digicert.com] [st...	80	HTTP	2020-10-19 20:14:52 UTC
8549	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49617	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8548	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49616	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8874	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49618	5.226.180.67 [pshudws.365lpodds.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8875	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49619	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8877	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49620	5.226.180.26 [premws-pt1.365lpodds.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8917	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49621	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8949	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49622	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
8975	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49623	5.226.176.16 [www.bet365.com] (Other)	443	SSL	2020-10-19 20:14:53 UTC
9472	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49624	5.226.180.41 [premlp-pt1.365lpodds.com] (Other)	443	SSL	2020-10-19 20:14:54 UTC
9474	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49625	5.226.180.40 [pshudlp.365lpodds.com] (Other)	443	SSL	2020-10-19 20:14:54 UTC
9744	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49626	5.226.180.41 [premlp-pt1.365lpodds.com] (Other)	443	SSL	2020-10-19 20:14:54 UTC
10518	192.168.153.1 [R9] (Windows)	55367	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	139	NetBiosSessionService	2020-10-19 20:14:58 UTC
10682	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49628	216.58.210.196 [www.google.com] (Other)	443	SSL	2020-10-19 20:15:21 UTC
10681	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49627	216.58.210.196 [www.google.com] (Other)	443	SSL	2020-10-19 20:15:21 UTC
10794	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49629	216.58.206.99 [ssl.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:21 UTC
10795	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49630	216.58.206.99 [ssl.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:21 UTC
10842	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49632	216.58.204.67 [www.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:22 UTC
10841	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49631	216.58.204.67 [www.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:22 UTC
10903	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49633	216.58.204.226 [pagead46.l.doubleclick.net] [adservice.go...	443	SSL	2020-10-19 20:15:22 UTC
10904	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49634	216.58.204.226 [pagead46.l.doubleclick.net] [adservice.go...	443	SSL	2020-10-19 20:15:22 UTC
11030	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49637	172.217.169.46 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:26 UTC
11031	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49635	172.217.169.46 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:26 UTC
11032	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49638	172.217.169.46 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:26 UTC
11029	192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED]...	49636	172.217.169.46 [encrypted-tbn0.gstatic.com] (Other)	443	SSL	2020-10-19 20:15:26 UTC



☑ Show Cookies ☑ Show NTLM challenge-response □ Mask Passwords

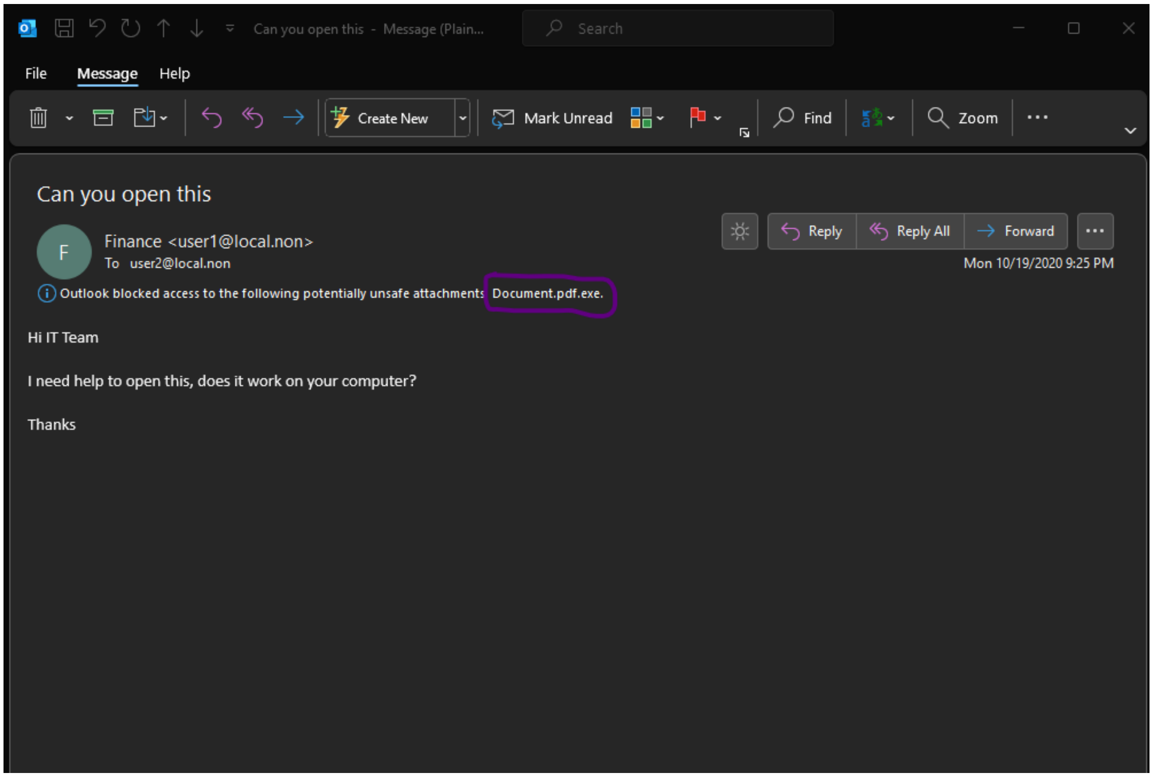
Client	Server	Protocol	Username	Password	Valid login	Login timestamp
192.168.153.155 (Windows)	104.18.20.226 [cdn.globalsigncdn.com.cdn.cloudflare.net] ...	HTTP Cookie	__cfduid=dd2c8b6b4d0b08061c8b55266ba8b021916031...	N/A	Unknown	2020-10-19 20:11:17 UTC
192.168.153.155 (Windows)	104.18.20.226 [cdn.globalsigncdn.com.cdn.cloudflare.net] ...	HTTP Cookie	__cfduid=d03d5e7d56b1ca120bbc030ffc04d9b41160313...	N/A	Unknown	2020-10-19 20:11:57 UTC
192.168.153.155 (Windows)	104.18.20.226 [cdn.globalsigncdn.com.cdn.cloudflare.net] ...	HTTP Cookie	__cfduid=d29d414309155b5ed93b7ce91c7f9c675160313...	N/A	Unknown	2020-10-19 20:11:58 UTC
192.168.153.155 (Windows)	192.168.153.132 (Windows)	SMTP	user1@local.non	abc123	Unknown	2020-10-19 20:13:40 UTC
192.168.153.155 [Win7-36-Patched] (Windows)	192.168.153.132 (Windows)	IMAP	user1@local.non	abc123	Unknown	2020-10-19 20:13:56 UTC
192.168.153.155 [Win7-36-Patched] [WIN7-36-PATCHED] ...	104.18.20.226 [cdn.globalsigncdn.com.cdn.cloudflare.net] ...	HTTP Cookie	__cfduid=ddec17abbf27293993f555a8e98206646160313...	N/A	Unknown	2020-10-19 20:15:36 UTC

Filename	MD5
CW_Cap...	7a222b

3. Suspicious File Transmission

A review of PCAP logs uncovered a notable instance where user1 attempted to send a file with an unusual and potentially dangerous file format to the IT team. The file's metadata suggests it may have contained executable scripts or embedded content capable of altering system settings or compromising data integrity.

This attempt to transmit a suspicious file to IT staff raises additional concerns, particularly if the file was intended to manipulate IT system privileges or obtain unauthorized access.



Can you open this

Finance <user1@local.non>
To user2@local.non

Mon 10/19/2020 9:25 PM

Outlook blocked access to the following potentially unsafe attachment: Document.pdf.exe.

Hi IT Team

I need help to open this, does it work on your computer?

Thanks

The evidence gathered through PCAP analysis suggests the following conclusions:

External Contact and Potential Collusion: The high-frequency communication with an external contact (alpha) who is not within the company's network is unusual and warrants further investigation to confirm or rule out potential collusion.

Motivational Link to Financial Strain: User1's financial stress, coupled with frequent betting activity, may have contributed to a willingness to engage in misconduct. This motivation aligns with the suspected misappropriation of funds.

Security Risks through Suspicious File Transmission: The attempt to send a suspicious file to the IT team indicates a possible effort to manipulate system security settings or privileges.