Malicious URL Sent via Phishing Email Redirects to Credential Harvesting Site

Analysis by Jonathan

Executive Summary

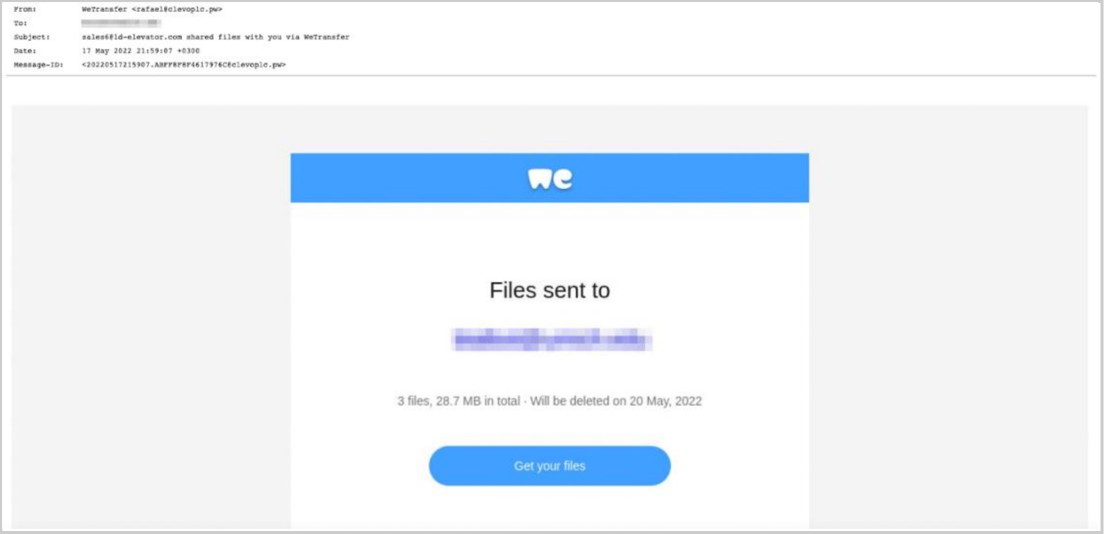
A documented victim was sent a spoofed WeTransfer file transfer email which redirected to a malicious URL:

hxxps://storage api[.]fleek[.]co/b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket/judedavid/weeet/index.html#<redacted recipient email address>

This URL was analyzed for threats by the author with detailed findings in the following section. Specific indicators of compromise are found in the *Indicators and Mitigations* section.

Detailed Findings

The initial email containing the malicious URL was sent as a WeTransfer file transfer email which spoofed the HTML of legitimate WeTransfer emails:

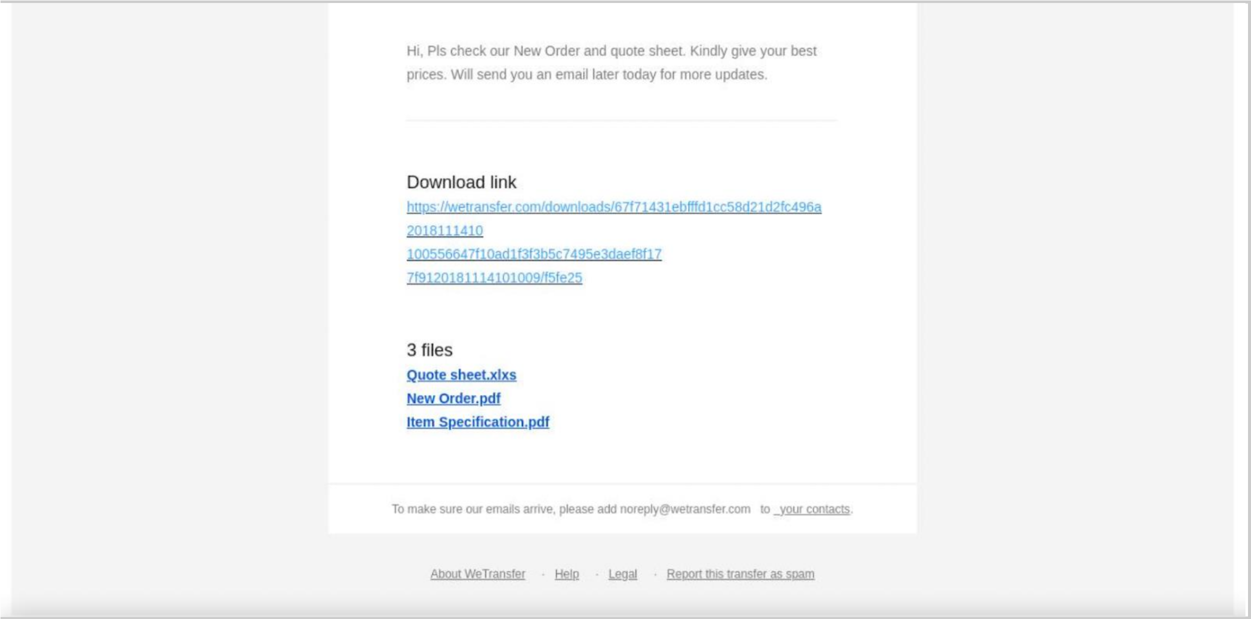


```
From:        WeTransfer <rafael@clevoplc.pw>
To:          [redacted]
Subject:     sales6@ld-elevator.com shared files with you via WeTransfer
Date:        17 May 2022 21:59:07 +0300
Message-ID:  <20220517215907.ABFF8F8F4617976C@clevoplc.pw>
```

Files sent to

[redacted]

3 files, 28.7 MB in total · Will be deleted on 20 May, 2022



Hi, Pls check our New Order and quote sheet. Kindly give your best prices. Will send you an email later today for more updates.

Download link

https://wetransfer.com/downloads/67f71431ebfffd1cc58d21d2fc496a
2018111410
100556647f10ad1f3f3b5c7495e3daef8f17
7f9120181114101009/f5fe25

3 files

Quote sheet.xlxs
New Order.pdf
Item Specification.pdf

To make sure our emails arrive, please add noreply@wetransfer.com to _your contacts.

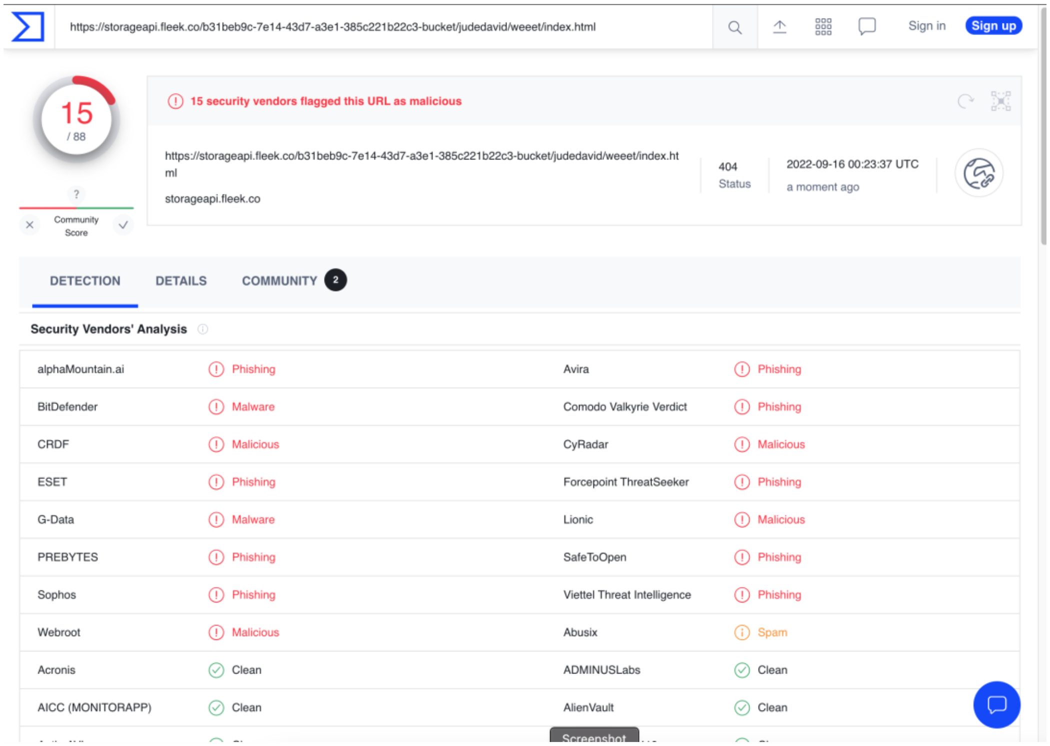
About WeTransfer · Help · Legal · Report this transfer as spam

It should be immediately noted that all three file links and the provided download link redirected to the same malicious URL. Additionally, the message above the download link contains unprofessional and poor English, a common theme among phishing emails.

The email header contained detailed information on the two previous hops; the originating IP address [46.183.220.42] and mail server IP address [104.168.167.223] were searched in DomainTools for active and passive DNS resolutions yielding no significant findings.

The URL and associated domain were both run in VirusTotal and urlscanner.io:

- hxxps://storage api[.]fleek[.]co/b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket/judedavid/weeet/index.html#<redacted recipient email address>
- storage api[.]fleek[.]co



https://storageapi.fleek.co/b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket/judedavid/weeet/index.html

15 / 88

15 security vendors flagged this URL as malicious

https://storageapi.fleek.co/b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket/judedavid/weeet/index.html

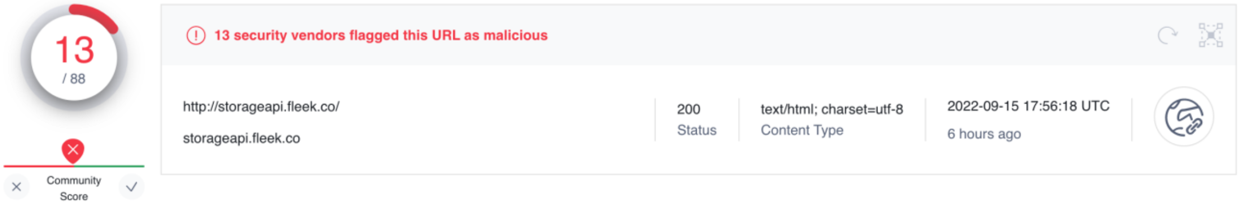
storageapi.fleek.co

404 Status

2022-09-16 00:23:37 UTC
a moment ago

Security Vendors' Analysis

alphaMountain.ai	Phishing	Avira	Phishing
BitDefender	Malware	Comodo Valkyrie Verdict	Phishing
CRDF	Malicious	CyRadar	Malicious
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
G-Data	Malware	Lionic	Malicious
PREBYTES	Phishing	SafeToOpen	Phishing
Sophos	Phishing	Viettel Threat Intelligence	Phishing
Webroot	Malicious	Abusix	Spam
Acronis	✓ Clean	ADMINUSLabs	✓ Clean
AICC (MONITORAPP)	✓ Clean	AlienVault	✓ Clean



13 / 88

13 security vendors flagged this URL as malicious

http://storageapi.fleek.co/

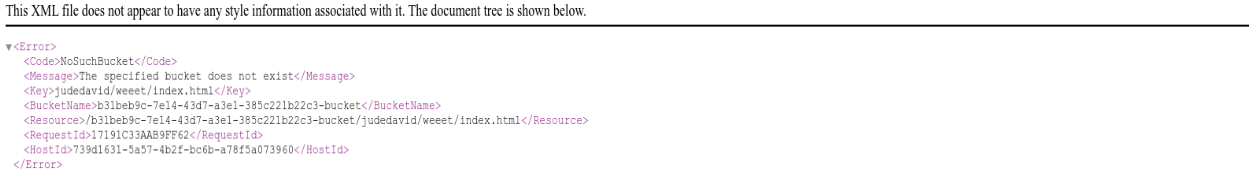
storageapi.fleek.co

200 Status

text/html; charset=utf-8 Content Type

2022-09-15 17:56:18 UTC
6 hours ago

Both the URL and associated domain returned significant indications that the URL is indeed malicious. In addition to searching the URL on VirusTotal, the URL was run using the behavioral analysis sandbox urlscanner.io and Hybrid-Analysis[1].



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Error>
   <Code>NoSuchBucket</Code>
   <Message>The specified bucket does not exist</Message>
   <Key>judedavid/weeet/index.html</Key>
   <BucketName>b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket</BucketName>
   <Resource>/b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket/judedavid/weeet/index.html</Resource>
   <RequestId>17191C33AAB9FF62</RequestId>
   <HostId>739d1631-5a57-4b2f-bc6b-a78f5a073960</HostId>
 </Error>
```

According to the returns from both sandbox tools, the string “b31beb9c-7e14-43d7-a3e1-385c221b22c3-bucket” is a storage bucket ID belonging to the specific bucket of the user judedavid/weeet. Nothing else significant was found in the analysis.

Indicators and Mitigations

[1] https://www.hybrid-analysis.com/

Current Resolution of URL: Current DNS A record: 104.18.7.145 (AS13335 - CLOUDFLARENET, US)

Malicious URL SHA256:

- e417c6110be37151b1ae80518d8e39bddfd74c94eef264bd9c7bf64aed9c00e5

Domain URL SHA256:

- f8e67fcd04c842a4e19ee86d5b3c5a5c6da236aeb5d097a956101b40a18b6124

IP Address 46.183.220.42:

IP Location	Latvia Riga Dataclub S.a.
ASN	AS52048 DATACLUB, BZ (registered Dec 21, 2010)
Resolve Host	p-220-42.dataclub.info
WHOIS	whois.ripe.net

Other IP Addresses:

- 104.168.167.223 – TAGS; domain server
- 104.18.6.145 – TAGS; Cloudflarenet
- 104.18.7.145 – TAGS; Cloudflarenet

Avast AV Detection: mal64.win@25/59@3/109 , TAGS: malicious, phishing

YARA Signatures: NONE

SNORT / SIGMA Signatures: NONE