

Incident Response Report

Incident ID: IR-20210430-001

Date: February 24, 2026

Analyst: Ruslan

Incident Type: Suspicious Network Activity, Internal Reconnaissance, and Potential Data Exfiltration

Status: Action Required

1. Executive Summary

On April 30, 2021, network traffic monitoring captured suspicious activity originating from an internal workstation (IP: 192.168.1.26). The user of this system interacted with an internal FTP server and multiple external web services in a manner suggesting possible unauthorized data gathering and exfiltration.

The initial compromise or insider activity involved successful authentication to the internal FTP server (192.168.1.20) using the credentials kali / AfricaCTF2021. The user transferred a media file (a JPEG image taken by an LG smartphone camera). Following the internal data transfer, the host queried the domain for archiving software (www.7-zip.org), sent anomalous UDP traffic to an external IP, and established encrypted TLS 1.3 communications with protonmail.com.

Forensic analysis of the FTP server revealed a non-standard folder created days prior, indicating potential staging. The combination of archiving tool queries, internal file access, and connections to external encrypted email services strongly points towards a data exfiltration attempt.

2. Timeline

Timestamp (UTC)	Event Category	Event Description	MITRE ATT&CK ID
01:01:26	Authentication	Valid Accounts: Successful FTP login to 192.168.1.20 using user kali and password AfricaCTF2021.	T1078 (Valid Accounts)
01:01:56	File Transfer	Data Transfer: Media file 20210429_152157.jpg was transferred via the unencrypted FTP session.	T1048 (Exfiltration Over Alternative Protocol)
01:02:57	Tool Acquisition	DNS Query: Host queried IPv6 DNS for www.7-zip.org (Packet 15174), likely to download compression tools.	T1071.004 (Application Layer Protocol: DNS)
01:02:59 – 01:03:18	Network Activity	Outbound Traffic: 10 UDP packets (Len=52) sent to external IP 24.39.217.246 on port 54150.	T1071 (Application Layer Protocol)
01:04:29	External Connection	Encrypted Channel: TLS 1.3 handshake initiated with protonmail.com (IP: 185.70.41.35).	T1071.001 (Web Protocols)
01:06:39	Web Browsing	HTTP Traffic: Unencrypted GET request to external site http://dfir.science/ (IP: 104.21.89.171).	T1071.001 (Web Protocols)

3. Technical Details

3.1. Investigated Asset (Client Workstation)

- **Internal IP:** 192.168.1.26
- **MAC address:** c8:09:a8:57:47:93 (Network card: IntelCor)
- **IPv6 DNS Server:** fe80::c80b:adff:feaa:1db7

3.2. Compromised Asset (FTP Server)

- **Internal IP:** 192.168.1.20
- **MAC address:** 08:00:27:a6:1f:86
- **Hardware Manufacturer Country:** United States (PCS Systemtechnik GmbH)
- **Staging Discovery:** A non-standard directory named ftp was discovered on the server. Directory metadata shows it was created prior to the main incident window, specifically on **April 20 at 17:53**, indicating persistent unauthorized access or staging activity.

3.3. Network Activity & Data Exfiltration Analysis

The activity utilized both plain-text internal protocols and encrypted external channels:

1. **Internal Authentication & Transfer:** The attacker/insider logged into the internal FTP server using the password AfricaCTF2021. The file 20210429_152157.jpg was interacted with. File metadata indicates the picture was taken using an LG camera, model **LM-Q725K**.
2. **Tooling:** Shortly after accessing internal files, a DNS lookup for www.7-zip.org was captured, indicating the user's intent to acquire an archiving tool to compress the gathered files.
3. **Encrypted External Comms (ProtonMail):** To bypass network inspection, the user established a secure TLS 1.3 session with ProtonMail.
 - *First TLS 1.3 Client Random:*
24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70
4. **Advanced Cryptography:** Deep packet inspection of TLS traffic (Session ID: da4a00...) revealed the ephemeral public key provided by the server during the handshake:
 - *Key:*
04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f6
2ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da9293
21f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

4. IoCs

Type	Value	Description	Recommended Action
Credentials	kali : AfricaCTF2021	Compromised FTP account credentials.	Reset / Disable
IPv4	24.39.217.246	Target of suspicious outbound UDP traffic (10 packets).	Block / Investigate
Domain	www.7-zip.org	Archiving tool domain (used for	Monitor

URL	http://dfir.science/	Unencrypted HTTP site visited by the user.	Monitor
Filename	20210429_152157.jpg	Media file involved in internal data transfer.	Analyze Content
Folder Path	/ftp (created Apr 20, 17:53)	Suspicious directory created on the FTP server.	Investigate

5. Containment & Remediation

To prevent further data loss and secure the internal infrastructure, the following steps must be taken:

Immediate Actions (Containment):

1. Physically or logically disconnect workstation 192.168.1.26 from the corporate network to prevent further outbound data exfiltration.
2. Immediately disable the kali account on the FTP server (192.168.1.20) and rotate passwords for all other FTP user accounts.
3. Add the external IP 24.39.217.246 to the firewall Deny List.

Short-term actions (Elimination):

4. Perform host-based forensics on the FTP server to analyze the contents of the /ftp directory created on April 20 at 17:53.
5. Review the contents of the 20210429_152157.jpg (LM-Q725K) image to determine if sensitive physical site information or documents were leaked.
6. Check the endpoints to confirm whether 7-Zip was successfully downloaded and installed, and look for .zip or .7z archive artifacts that may contain staged data.

Long-term actions (Improving security architecture):

7. Deprecate the use of unencrypted FTP (port 21) within the internal network. Migrate to secure alternatives such as SFTP (SSH File Transfer Protocol) or FTPS.
8. Implement strict firewall rules regarding which internal workstations are allowed to connect to external personal webmail services (e.g., ProtonMail), as these are common vectors for data exfiltration.

1. What is the FTP password?
- AfricaCTF2021

No.	Time	Source	Destination	Protocol	Length	Host	Info
486	2021-04-30 01:01:26.86924	192.168.1.20	192.168.1.26	FTP	102		Response: 220 Welcome to Hacker FTP service.
488	2021-04-30 01:01:26.87143	192.168.1.26	192.168.1.20	FTP	76		Request: AUTH TLS
490	2021-04-30 01:01:26.87172	192.168.1.20	192.168.1.26	FTP	104		Response: 530 Please login with USER and PASS.
492	2021-04-30 01:01:26.87196	192.168.1.26	192.168.1.20	FTP	76		Request: AUTH SSL
494	2021-04-30 01:01:26.87207	192.168.1.20	192.168.1.26	FTP	104		Response: 530 Please login with USER and PASS.
496	2021-04-30 01:01:26.88276	192.168.1.26	192.168.1.20	FTP	77		Request: USER kali
498	2021-04-30 01:01:26.88306	192.168.1.20	192.168.1.26	FTP	100		Response: 331 Please specify the password.
500	2021-04-30 01:01:26.88332	192.168.1.26	192.168.1.20	FTP	86		Request: PASS AfricaCTF2021
502	2021-04-30 01:01:26.91337	192.168.1.20	192.168.1.26	FTP	89		Response: 230 Login successful.

2. What is the IPv6 address of the DNS server used by 192.168.1.26?
- fe80::c80b:adff:feaa:1db7

No.	Time	Source	Destination	Protocol	Length	Host	Info
84	2021-04-30 01:00:53.48666	192.168.1.10	192.168.1.10	DNS	84		Standard query 0x22c A fp.msedge.net OPT
140	2021-04-30 01:00:56.49828	192.168.1.26	192.168.1.10	DNS	88		Standard query response 0x22c A fp.msedge.net CNAME 1.perf.msedge.net CNAME a-9019.a-msedge.net CNAME a-9019.a.dns.afd.
141	2021-04-30 01:00:56.56609	192.168.1.10	192.168.1.26	DNS	191		Standard query response 0x3b76 A l-ring.msedge.net CNAME l-ring.l-9999.l-msedge.net CNAME l-9999.l-msedge.net A 13.107.4
171	2021-04-30 01:00:57.08175	192.168.1.26	192.168.1.10	DNS	98		Standard query 0x3b3d A fp-vs-nocache.azureedge.net OPT
172	2021-04-30 01:00:57.16297	192.168.1.10	192.168.1.26	DNS	421		Standard query response 0x3b3d A fp-vs-nocache.azureedge.net CNAME fp-vs-nocache.ec.azureedge.net CNAME cs9.wpc.vcdn.ne
201	2021-04-30 01:00:57.74845	192.168.1.26	192.168.1.10	DNS	97		Standard query 0x2d89 A a-ring-fallback.msedge.net OPT
203	2021-04-30 01:00:57.88245	192.168.1.10	192.168.1.26	DNS	212		Standard query response 0x2d89 A a-ring-fallback.msedge.net CNAME a-9999.dc-msedge.net A 131.253.33.254 NS ns1.dc-msedge
238	2021-04-30 01:00:59.79870	192.168.1.26	192.168.1.10	DNS	111		Standard query response 0x3890 A a-0001.a-fdentry.net.trafficmanager.net OPT
239	2021-04-30 01:00:59.89642	192.168.1.10	192.168.1.26	DNS	273		Standard query response 0x3890 A a-0001.a-fdentry.net.trafficmanager.net CNAME www.bing-com.dual-a-0001.a-msedge.net CN
464	2021-04-30 01:01:11.40551	192.168.1.26	192.168.1.10	DNS	88		Standard query 0x6820 A t-ring.msedge.net OPT
474	2021-04-30 01:01:16.46381	fe80::b011:ed39...	fe80::c80b:adff:fea...	DNS	108		Standard query 0x6820 A t-ring.msedge.net OPT
475	2021-04-30 01:01:16.57807	fe80::c80b:adff:fea...	fe80::b011:ed39:866...	DNS	197		Standard query response 0x6820 A t-ring.msedge.net CNAME t-ring.t-9999.t-msedge.net CNAME t-9999.t-msedge.net A 13.107.2
11844	2021-04-30 01:02:06.36216	fe80::b011:ed39...	fe80::c80b:adff:fea...	DNS	120		Standard query response 0x2a59 A connectivity-check.ubuntu.com OPT
11845	2021-04-30 01:02:06.38503	fe80::c80b:adff:fea...	fe80::b011:ed39:866...	DNS	168		Standard query response 0x2a59 A connectivity-check.ubuntu.com A 34.122.121.32 A 35.224.170.84 A 35.232.111.17 OPT
11859	2021-04-30 01:02:10.06156	fe80::b011:ed39...	fe80::c80b:adff:fea...	DNS	123		Standard query 0x7670 A geo.prod.do.dsp.mp.microsoft.com OPT
11860	2021-04-30 01:02:11.24951	fe80::c80b:adff:fea...	fe80::b011:ed39:866...	DNS	547		Standard query response 0x7670 A geo.prod.do.dsp.mp.microsoft.com CNAME geo-prod.do.dsp.mp.microsoft.com CNAME geo-prod:
11887	2021-04-30 01:02:11.92666	fe80::b011:ed39...	fe80::c80b:adff:fea...	DNS	125		Standard query 0xace A kv501.prod.do.dsp.mp.microsoft.com OPT
11888	2021-04-30 01:02:17.07545	fe80::c80b:adff:fea...	fe80::b011:ed39:866...	DNS	588		Standard query response 0xace A kv501.prod.do.dsp.mp.microsoft.com CNAME kv501.prod.do.dsp.mp.microsoft.com nsatc.net CN

3. What domain is the user looking up in packet 15174?
- www.7-zip.org

No.	Time	Source	Destination	Protocol	Length	Host	Info
15174	2021-04-30 01:02:57.34684	fe80::b011:ed39...	fe80::c80b:adff:fea...	DNS	104		Standard query 0x1ad5 A www.7-zip.org OPT

```

Transaction ID: 0x1ad5
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  Queries
    www.7-zip.org: type A, class IN
      Name: www.7-zip.org
      [Name Length: 13]
      [Label Count: 3]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
  Additional records
    <Root>: type OPT
    [Response In: 15190]

```

4. How many UDP packets were sent from 192.168.1.26 to 24.39.217.246?
- 10

No.	Time	Source	Destination	Protocol	Length	Host	Info
15806	2021-04-30 01:02:59.31268	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
15808	2021-04-30 01:02:59.31515	192.168.1.26	24.39.217.246	UDP	94		51601 → 54150 Len=52
15825	2021-04-30 01:03:01.27064	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
15851	2021-04-30 01:03:03.27323	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
15865	2021-04-30 01:03:06.35654	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
15942	2021-04-30 01:03:08.25509	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
16095	2021-04-30 01:03:10.25517	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
16695	2021-04-30 01:03:14.36347	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
16810	2021-04-30 01:03:16.24950	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52
16955	2021-04-30 01:03:18.25380	192.168.1.26	24.39.217.246	UDP	94		53638 → 54150 Len=52

5. What is the MAC address of the system under investigation in the PCAP file?
- c8:09:a8:57:47:93

```

Frame 15806: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface wlo1, id 0
Ethernet II, Src: IntelCor_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:20:ba)
  Destination: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:20:ba)
  Source: IntelCor_57:47:93 (c8:09:a8:57:47:93)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.26, Dst: 24.39.217.246
User Datagram Protocol, Src Port: 53638, Dst Port: 54150
Data (52 bytes)

```

6. What was the camera model name used to take picture 20210429_152157.jpg?
- LM-Q725K

No.	Time	Source	Destination	S Port	D Port	Protocol	Length	Info
7070	2021-04-30 01:01:56.276106006	192.168.1.26	192.168.1.20	48800		21 FTP		92 Request: STOR 20210429_152157.jpg
11781	2021-04-30 01:01:56.393410863	192.168.1.20	192.168.1.26	41837		57054 FTP-DA...		292 FTP Data: 226 bytes (PASV) (LIST)

Property	Value
Color representation	SRGB
Compressed bits/pixel	
Camera	
Camera maker	LG Electronics
Camera model	LM-Q725K

7. What is the ephemeral public key provided by the server during the TLS handshake in the session with the session ID: da4a0000342e4b73459d7360b4bea971cc303ac18d29b99067e46d16cc07f4ff?

04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f62ca1f0e8f74d727053074a37bceb2cbdc7ce2a8994dcd76dd6834eefc5438c3b6da929321f3a1366bd14c877cc83e5d0731b7f80a6b80916efd4a23a4d

```

Handshake Protocol: Certificate
Handshake Protocol: Certificate Status
Handshake Protocol: Server Key Exchange
  Handshake Type: Server Key Exchange (12)
  Length: 361
  EC Diffie-Hellman Server Params
    Curve Type: named_curve (0x03)
    Named Curve: secp384r1 (0x0018)
    Pubkey Length: 97
    Pubkey: 04edcc123af7b13e90ce101a31c2f996f471a7c8f48a1b81d765085f548059a550f3f4f6...
    Signature Algorithm: rsa_pkcs1_sha256 (0x0401)
    Signature Length: 256
    Signature: 11914710183397b395995313bea183e0abc19619361016080bff249af9c5d88e7f2b8e44...
  Handshake Protocol: Server Hello Done
    Handshake Type: Server Hello Done (14)
    Length: 0

```

8. What is the first TLS 1.3 client random that was used to establish a connection with protonmail.com?

- 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

tls.handshake.type == 1 && tls.handshake.extensions_server_name == "protonmail.com"							
No.	Time	Source	Destination	Protocol	Length	Host	Info
17992	2021-04-30 01:04:29.68221...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello
17997	2021-04-30 01:04:29.68534...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello
18000	2021-04-30 01:04:29.68761...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello
18144	2021-04-30 01:04:32.60026...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello
18145	2021-04-30 01:04:32.60043...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello
18146	2021-04-30 01:04:32.60080...	192.168.1.26	185.70.41.35	TLSv1.3	583		Client Hello

4

▶ Frame 17992: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface wlo1, id 0

▶ Ethernet II, Src: IntelCor_57:47:93 (c8:09:a8:57:47:93), Dst: ca:0b:ad:ad:20:ba (ca:0b:ad:ad:20:ba)

▶ Internet Protocol Version 4, Src: 192.168.1.26, Dst: 185.70.41.35

▶ Transmission Control Protocol, Src Port: 40280, Dst Port: 443, Seq: 1, Ack: 1, Len: 517

▼ Transport Layer Security

- ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 512
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 508
 - Version: TLS 1.2 (0x0303)
 - Random: 24e92513b97a0348f733d16996929a79be21b0b1400cd7e2862a732ce7775b70

9. Which country is the manufacturer of the FTP server’s MAC address registered in?
- United States

▶ Frame 515: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface wlo1, id 0	
▼ Ethernet II, Src: IntelCor_57:47:93 (c8:09:a8:57:47:93), Dst: PcsCompu_a6:1f:86 (08:00:27:a6:1f:86)	
▶ Destination: PcsCompu_a6:1f:86 (08:00:27:a6:1f:86)	
▶ Source: IntelCor_57:47:93 (c8:09:a8:57:47:93)	
▶ Type: IPv4 (0x0800)	
▶ Internet Protocol Version 4, Src: 192.168.1.26, Dst: 192.168.1.20	
▶ Transmission Control Protocol, Src Port: 48794, Dst Port: 21, Seq: 64, Ack: 269, Len: 5	
▶ File Transfer Protocol (FTP)	
[Current working directory:]	

MAC Address Details

Company	PCS Systemtechnik GmbH
Address	600 Suffolk St Lowell MA 01854 US
Range	08:00:27:00:00:00 - 08:00:27:FF:FF:FF
Type/Database	MA-L MAC Address Block Large OUI

10. What time was a non-standard folder created on the FTP server on the 20th of April?
-17:53

519	2021-04-30	01:01:26.92006...	192.168.1.20	192.168.1.26	FTP	97	Response: 200 Switching to Binary mode.
521	2021-04-30	01:01:26.92034...	192.168.1.26	192.168.1.20	FTP	72	Request: PASV
522	2021-04-30	01:01:26.92064...	192.168.1.20	192.168.1.26	FTP	116	Response: 227 Entering Passive Mode (192,168,1,20,37,241).
524	2021-04-30	01:01:26.92591...	192.168.1.26	192.168.1.20	FTP	72	Request: LIST
528	2021-04-30	01:01:26.92657...	192.168.1.20	192.168.1.26	FTP	105	Response: 150 Here comes the directory listing.
535	2021-04-30	01:01:26.92796...	192.168.1.20	192.168.1.26	FTP	90	Response: 226 Directory send OK.
546	2021-04-30	01:01:42.95759...	192.168.1.26	192.168.1.20	FTP	81	Request: CWD Documents
547	2021-04-30	01:01:42.96041...	192.168.1.20	192.168.1.26	FTP	103	Response: 250 Directory successfully changed.
549	2021-04-30	01:01:42.96081...	192.168.1.26	192.168.1.20	FTP	71	Request: PWD

drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Desktop
drwxr-xr-x	2	1000	1000	4096	Apr 29 16:42	Documents
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Downloads
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Music
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Pictures
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Public
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Templates
drwxr-xr-x	2	1000	1000	4096	Feb 23 06:37	Videos
dr-xr-x---	4	65534	65534	4096	Apr 20 17:53	ftp

11. What URL was visited by the user and connected to the IP address 104.21.89.171?
- http://dfir.science/

No.	Time	Source	Destination	Protocol	Length	Host	Info
26257	2021-04-30 01:06:39.57902...	192.168.1.26	104.21.89.171	HTTP	496	dfir.science	GET / HTTP/1.1
26264	2021-04-30 01:06:39.77776...	104.21.89.171	192.168.1.26	HTTP	71		HTTP/1.1 301 Moved Permanently

Type: IPv4 (0x0000)
Internet Protocol Version 4, Src: 192.168.1.26, Dst: 104.21.89.171
Transmission Control Protocol, Src Port: 40302, Dst Port: 80, Seq: 1, Ack: 1, Len: 430
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: dfir.science\r\n