(APT Group Name) Attack Analysis Report

Prepared by: Mitchelle Anduru

Date: 24/01/2026

Executive summary

A biotechnology firm conducting cancer research experienced a multi-stage intrusion attributed to **APT10 (menuPass)**, with the primary objective of **stealing high-value intellectual property** (experimental datasets and drug formulation information). The attack began with a **targeted spearphishing email** delivering a **macro-enabled Excel attachment** that, once opened and macros enabled, executed **PowerShell** to download and run a remote script that deployed a **remote access tool (RAT)**. The adversary then performed **credential dumping from LSASS**, used stolen administrator credentials to **pivot via RDP** into research servers, **staged data into a ZIP archive**, and **exfiltrated** it over an **encrypted HTTPS C2 channel** using a **non-standard port (8443)** to reduce visibility and blend into normal web traffic. Highest-priority controls include blocking or sandboxing macro-enabled attachments, enforcing **phishing-resistant MFA**, hardening PowerShell with logging and application control, protecting LSASS (Credential Guard/RunAsPPL), restricting RDP through segmentation and jump hosts, and strengthening egress controls and monitoring for suspicious HTTPS destinations and uncommon outbound ports.

Key Findings

- Initial access relied on a **macro-enabled Excel attachment** and **user macro enablement** (T1566.001, T1204.002).
- **PowerShell** was used as a living-off-the-land mechanism to download and execute attacker tooling (T1059.001, T1105).
- The adversary established **interactive remote access (RAT)** to maintain control and coordinate follow-on actions (T1219).
- **Credential exposure via LSASS dumping** enabled escalation and rapid pivot to sensitive research systems (T1003.001 → T1021.001).
- Exfiltration blended into **encrypted HTTPS traffic over port 8443**, reducing inspection visibility and bypassing simplistic egress rules (T1071.001, T1571, T1573.002, T1041).

Detection Opportunities

Technique	Best log source(s)	What to alert on
T1566.001 Spearphishing Attachment	Email gateway logs; attachment sandbox	Macro-enabled attachments (.xlsm) from external senders; failed DMARC/SPF; sandbox detonation verdicts
T1204.002 User Execution (Malicious File)	EDR/Sysmon process creation	Office app spawning child processes; “Enable Content” patterns; Excel launching powershell.exe / cmd.exe
T1059.001 PowerShell	PowerShell Event IDs (4104); EDR telemetry	Encoded commands; web download patterns; PowerShell with unusual parent (Excel); script execution from temp paths
T1105 Ingress Tool Transfer	Proxy/DNS logs; firewall logs	Direct outbound to raw IPs; downloads of .ps1 from non-corporate sources; unusual user-agent strings
T1219 Remote Access Software	EDR; Windows services/tasks; network logs	Unknown remote access binaries; new persistence artifacts; outbound beaconing to rare domain/port
T1003.001 LSASS Memory Dumping	EDR; Sysmon; Windows Security logs	LSASS access attempts; dump file creation in suspicious paths; handle duplication events
T1021.001 RDP Lateral Movement	Windows Security (4624/4625 type 10); firewall	New RDP to sensitive servers; logins outside normal hours; RDP across unexpected network zones
T1560.001 Archive via Utility	File monitoring; EDR	Sudden creation of large ZIP archives in research directories; mass file read followed by archive creation
T1071.001 / T1571 / T1573.002 HTTPS C2 on 8443	Proxy logs; NetFlow; TLS analytics (SNI/JA3)	TLS sessions to rare/new domains; HTTPS on non-standard port 8443; anomalous JA3/SNI/cert patterns
T1041 Exfiltration Over C2	DLP; proxy logs; NetFlow	Sustained outbound uploads to a single external endpoint; unusual data volume spikes from research segments

Define the Threat Scenario

This section covers step 1 of the lab instructions.

Brief description of the attack, APT group involved, and what happened based on the scenario.

A biotechnology firm focused on cancer research experienced a multi-stage intrusion attributed to APT10 (also tracked by MITRE as the group menuPass). The adversary's objective was to

steal sensitive intellectual property, including experimental datasets and drug formulation information. The intrusion began with a targeted spearphishing email delivering a macro-enabled Excel attachment. When the macro executed, it launched PowerShell to download and run a remote script that deployed a remote access tool (RAT). The attackers then dumped administrator credentials from memory, used those credentials to pivot via Remote Desktop Protocol (RDP) to secure research servers, staged data into a ZIP archive, and exfiltrated it over encrypted HTTPS to an external command-and-control (C2) domain on port 8443.

Map to MITRE ATT&CK Tactics and Identify Techniques

This section covers content for steps 2, 3, and 5 of the lab instructions

Complete the table as described in the lab instructions. Add additional table rows if needed.

Tactic	Technique Name	Technique ID	Description	IOCs
Initial Access	Spearphishing Attachment	T1566.001	Malicious macro-enabled Excel attachment delivered via targeted email.	Attachment: `financial_report_2024.xlsm`
Execution	User Execution: Malicious File	T1204.002	User opens the file and enables macros, triggering payload execution.	User-enabled macros in `financial_report_2024.xlsm`
Execution	Command and Scripting Interpreter: PowerShell	T1059.001	PowerShell used to download and execute remote script/tooling.	PowerShell to `hxxp://192.168.50.10/ratscript.ps1`
Command and Control	Ingress Tool Transfer	T1105	Tool/script transferred from external host into victim environment.	Download source: `192.168.50.10` (`ratscript.ps1`)

Command and Control	Remote Access Software	T1219	RAT provides remote control/interactive access for follow-on actions.	RAT executed after script download (from `ratscript.ps1`)
Credential Access	OS Credential Dumping: LSASS Memory	T1003.001	Credential dumping from memory to obtain administrator credentials.	`C:\Windows\Temp\dump.dat`
Lateral Movement	Remote Services: Remote Desktop Protocol	T1021.001	Stolen admin credentials used to access research servers via RDP.	Unauthorized RDP: `192.168.100.20` → `10.30.40.50`
Collection	Archive Collected Data: Archive via Utility	T1560.001	Sensitive research data compressed into ZIP for staging/exfil.	ZIP archive created (staging prior to exfiltration)
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	HTTPS used to blend attacker traffic with normal web traffic.	Outbound HTTPS to `biotechsecure-update.com`
Command and Control	Non-Standard Port	T1571	Uses uncommon port to evade basic filtering/monitoring.	Port `8443` outbound
Command and Control	Encrypted Channel: Asymmetric Cryptography	T1573.002	Encrypted channel reduces visibility into C2/exfil traffic.	Encrypted outbound to `biotechsecure-update.com:8443`
Exfiltration	Exfiltration Over C2 Channel	T1041	Data exfiltrated over the established C2 channel.	Outbound HTTPS exfil to `biotechsecure-update.com:8443`

Technique Analysis

This section covers content for step 4 of the lab.

Document your findings of each technique as described in step 4 of the lab instructions. You can document in a similar format as the example below or you can document each technique in a paragraph format.

Example:

Spearphishing Attachment (T1566.001)

- **How it works:** A malicious macro embedded in a Word document is sent via phishing email.
- **Execution:** User enables macros → Payload runs → Attacker gains access.
- **APT33 Behavior:** Frequently employs spearphishing in initial attacks.

Phishing: Spearphishing Attachment (T1566.001)

• How it works: A targeted email carries a weaponized attachment to deliver malware or trigger follow-on execution.

• In this incident: The attachment financial_report_2024.xlsm was used as the initial delivery vehicle.

• Why it is effective: Biotech and research organizations are high-value and often have mixed user technical maturity; convincing business-themed lures

increase macro enablement rates.

• Impact: Establishes a foothold and enables subsequent stages (PowerShell, tooling download).

User Execution: Malicious File (T1204.002)

• How it works: Adversary relies on a user opening a file and/or enabling content (macros) to start code execution.

• In this incident: The macro payload required the victim to open the Excel file and enable macros.

• Impact: Bypasses some perimeter controls by shifting execution to user action and trusted applications.

Command and Scripting Interpreter: PowerShell (T1059.001)

• How it works: PowerShell executes commands and scripts for download, execution, discovery, and defense evasion.

• In this incident: Macro triggered PowerShell to download and run ratscript.ps1 from an attacker-controlled host.

• Impact: Fileless or low-footprint execution, rapid staging, and easy living-off-the-land activity.

Ingress Tool Transfer (T1105)

• How it works: Tools/files are transferred from an external system into the victim environment over a network channel.

• In this incident: ratscript.ps1 (and the RAT stage) was fetched from 192.168.50.10.

• Impact: Enables modular tooling (download only what is needed, when needed).

Remote Access Software (T1219)

• How it works: A remote access tool provides interactive C2, remote command execution, and sometimes persistence.

• In this incident: The downloaded RAT enabled ongoing remote control to facilitate credential theft, lateral movement, and exfiltration.

• Impact: Provides a stable operator interface for long-dwell APT operations.

OS Credential Dumping: LSASS Memory (T1003.001)

• How it works: Attacker dumps LSASS process memory to extract password material/hashes and reuse them for access.

• In this incident: A memory dump artifact was found at C:\Windows\Temp\dump.dat.

• Impact: Enables privilege escalation and lateral movement using stolen admin credentials.

Remote Services: Remote Desktop Protocol (T1021.001)

• How it works: With valid credentials, adversaries use RDP to access other systems and operate interactively.

• In this incident: Unauthorized RDP sessions were observed to 10.30.40.50 from 192.168.100.20.

• Impact: Direct access to high-value research servers and ability to stage/collect data.

Archive Collected Data: Archive via Utility (T1560.001)

• How it works: Collected data is compressed (e.g., ZIP) to reduce size and package it for transfer.

• In this incident: Sensitive data and formulations were archived into a ZIP prior to exfiltration.

• Impact: Reduces transfer time, hides file structure, and simplifies staged exfiltration.

Application Layer Protocol: Web Protocols (T1071.001) + Non-Standard Port (T1571) + Encrypted Channel (T1573.002)

• How it works: C2/exfil uses HTTPS to blend into normal web traffic; non-standard ports can bypass simplistic rules; encryption conceals payloads.

• In this incident: Outbound HTTPS traffic to biotechsecure-update.com over port 8443 carried attacker traffic.

• Impact: Makes network inspection harder and increases the chance that traffic is allowed through egress controls.

Exfiltration Over C2 Channel (T1041)

• How it works: Data is exfiltrated over the same channel used for command and control to blend in.

• In this incident: ZIPped data was sent via the established HTTPS C2 path to biotechsecure-update.com:8443.

• Impact: Exfiltration may resemble routine encrypted outbound traffic and evade simplistic DLP rules

Mitigation Strategies

This section covers the content from step 6 of the lab.

Complete the sections of this table.

Technique ID	Mitigation Strategy	Justification	Potential Drawback
T1566.001	Email security gateway + attachment sandboxing; block/quarantine macro-enabled attachments from external senders; enforce DMARC/SPF/DKIM	Reduces phishing delivery success and detects weaponized attachments before users open them	May block legitimate macro workflows; tuning needed to reduce false positives
T1204.002	Disable Office macros from the internet (Mark-of-the-Web policy); Protected View; phishing awareness + simulations	Prevents common “enable macros” execution path and reduces user-triggered payloads	Some business teams rely on macros; training is not 100% effective
T1059.001	PowerShell hardening: Constrained Language Mode; AMSI; block unsigned scripts; WDAC/AppLocker rules; enable Script Block Logging	Limits attacker scripting and improves visibility into malicious PowerShell behavior	Can break admin automation/scripts; requires careful rollout and exceptions
T1105	Egress controls: force web traffic via proxy; block direct outbound to raw IPs; allowlist outbound destinations for sensitive segments	Disrupts tool download paths and adds inspection/control points	Operational overhead maintaining allowlists; may disrupt legitimate connections
T1219	Application allowlisting + EDR blocks on remote access tooling; restrict remote admin tools to approved set	Prevents unauthorized RAT/remote tools from executing and persisting	Allowlisting takes effort; custom malware may evade simple tool-name blocks
T1003.001	Enable Credential Guard / LSASS protection (RunAsPPL); ASR rules to block credential theft; reduce/admin logon exposure	Makes LSASS dumping harder and reduces credential material available to steal	Compatibility issues on older systems; needs testing and phased rollout

T1021.001	Lock down RDP: disable where unnecessary; MFA for admins; network segmentation + jump host; firewall allowlists; NLA	Stops lateral movement even with stolen creds and reduces attack paths to crown jewels	Adds friction to admin workflows; requires strong access governance
T1560.001	DLP + file activity monitoring; alert on large archive creation; least-privilege access to research repositories	Detects/limits data staging and reduces who can package sensitive datasets	DLP and monitoring require tuning; risk of noise/false positives
T1071.001	Secure web gateway/proxy with strong logging; DNS filtering; block rare/newly registered domains; (where permitted) TLS inspection in high-risk zones	Increases detection of suspicious HTTPS-based C2 and blocks malicious destinations	TLS inspection has privacy/legal/performance considerations
T1571	Block outbound non-standard ports by default; require approval for ports like 8443; alert on new outbound ports	Removes easy evasion via alternate ports and highlights abnormal outbound behavior	Some apps legitimately use 8443; exceptions must be managed
T1573.002	Encrypted traffic analytics (JA3/SNI/cert anomalies); enforce modern TLS policies; scoped TLS inspection where allowed	Flags suspicious encrypted channels even when content is unreadable	Analytics require baselining; inspection increases complexity and may be restricted
T1041	Exfil controls: DLP + netflow thresholds; alert on sustained outbound uploads; restrict outbound from research network; monitor unusual upload volumes	Detects and reduces data leaving via established C2 paths	Legitimate large uploads may trigger alerts; requires baselines and tuning

Monitoring and Validation

This section covers the content from step 7 of the lab.

Document how you would validate each Technique that you discovered for this attack and how you would monitor for similar attacks in the future.

The goal is to detect similar behavior early (delivery, execution, credential theft, movement, and exfiltration). Monitoring should combine endpoint telemetry (EDR/Sysmon), identity signals, and network controls (proxy, DNS, firewall, IDS). Validation can be performed through controlled simulations (purple teaming) and ATT&CK-aligned; tests.

Email delivery and attachment execution (T1566.001, T1204.002)

• Email gateway: flag macro-enabled attachments (.xlsm) from external senders; detonation results; DMARC failures.

• Endpoint: Office spawning child processes (Excel -> powershell.exe, cmd.exe) via EDR/Sysmon process creation telemetry.

• User awareness validation: periodic phishing simulations and reporting rate tracking.

PowerShell and tool transfer (T1059.001, T1105)

• PowerShell logging: enable Script Block Logging (Event ID 4104) and Module Logging; alert on suspicious web requests and encoded commands.

• Process telemetry: alert on powershell.exe downloading from raw IPs, unusual parent processes (Excel), or execution from temp directories.

• Proxy/firewall: alert on outbound connections to known-bad IPs/domains and blocked categories; enforce proxy usage for web egress.

RAT / interactive C2 (T1219, T1071.001, T1571, T1573.002)

• Network: detect new or rare domains (biotechsecure-update.com) and TLS connections to non-standard ports (e.g., 8443).

• TLS analytics: baseline SNI/JA3/JA3S fingerprints and alert on anomalies; consider TLS inspection for high-risk segments where appropriate.

• Endpoint: watch for suspicious services, scheduled tasks, or persistence artifacts created by remote access tooling.

Credential dumping (T1003.001)

• Endpoint: alert on LSASS access, handle duplication, or creation of dump artifacts in suspicious locations (e.g., C:\Windows\Temp\dump.dat).

• Hardening validation: confirm Credential Guard / LSASS protection (RunAsPPL) status on endpoints and admin workstations.

• Identity: alert on unusual privilege use, credential reset events, and rapid authentication to multiple systems.

Lateral movement via RDP (T1021.001)

• Windows Security logs: monitor logon events and RDP logons (e.g., Event IDs 4624/4625 with logon type 10) to sensitive servers.

• Network segmentation: alert on RDP traffic crossing unexpected network zones; enforce jump hosts and MFA for admin access.
• Behavioral: detect 'new admin workstation' accessing high-value servers or access outside normal hours.
Staging and exfiltration (T1560.001, T1041)
• File monitoring: alert on sudden creation of large archives (ZIP) in research directories and mass file reads before archive creation.
• DLP: monitor outbound transfers of sensitive file types and unusually large HTTPS uploads to rare destinations.
• Network: alert on sustained outbound data transfer to a single external endpoint, especially over 8443.

References

• MITRE ATT&CK; - APT10 (menuPass) group profile: https://attack.mitre.org/groups/G0045/
• MITRE ATT&CK; - T1566.001 Phishing: Spearphishing Attachment: https://attack.mitre.org/techniques/T1566/001/
• MITRE ATT&CK; - T1204.002 User Execution: Malicious File: https://attack.mitre.org/techniques/T1204/002/
• MITRE ATT&CK; - T1059.001 Command and Scripting Interpreter: PowerShell: https://attack.mitre.org/techniques/T1059/001/
• MITRE ATT&CK; - T1105 Ingress Tool Transfer: https://attack.mitre.org/techniques/T1105/
• MITRE ATT&CK; - T1219 Remote Access Software: https://attack.mitre.org/techniques/T1219/
• MITRE ATT&CK; - T1003.001 OS Credential Dumping: LSASS Memory: https://attack.mitre.org/techniques/T1003/001/
• MITRE ATT&CK; - T1021.001 Remote Desktop Protocol: https://attack.mitre.org/techniques/T1021/001/
• MITRE ATT&CK; - T1560.001 Archive via Utility: https://attack.mitre.org/techniques/T1560/001/
• MITRE ATT&CK; - T1071.001 Web Protocols: https://attack.mitre.org/techniques/T1071/001/
• MITRE ATT&CK; - T1571 Non-Standard Port: https://attack.mitre.org/techniques/T1571/
• MITRE ATT&CK; - T1573.002 Encrypted Channel: Asymmetric Cryptography: https://attack.mitre.org/techniques/T1573/002/
• MITRE ATT&CK; - T1041 Exfiltration Over C2 Channel: https://attack.mitre.org/techniques/T1041/