Student Name: Jonathan Lunger
Title: MidRiver Health

Case Overview

Title: MidRiver Health

Background: On April 9th, 2025, the MidRiver Health Security Operations Center (SOC) detected unusual activity originating from the Finance VLAN. At **19:04 EST**, outbound HTTPS traffic spiked from workstation **FIN-WS-077**, a system assigned to Finance employee **jmartin**. This activity occurred immediately after an **unrecognized VPN login** associated with jmartin's account, raising concerns of possible credential compromise and unauthorized access into the internal network.

Following this alert, the SOC isolated a collection of host logs, VPN authentication entries, DNS records, firewall egress logs, NetFlow summaries, and IDS alerts for further review. Because the affected workstation resides in the Finance VLAN, which regularly handles sensitive financial and operational data, the potential impact of this incident required immediate escalation.

Objective:

1. **Reconstruct the sequence of events** surrounding the anomalous VPN login and subsequent network activity.

2. **Identify the initial attack vector**, the systems affected, and any unauthorized processes or connections initiated from FIN-WS-077.

3. **Determine whether data exfiltration occurred**, and if so, quantify its scope, destination, and method.

4. **Correlate evidence across all log sources** to validate findings and ensure the conclusions are defensible.

5. **Develop actionable remediation and prevention recommendations** to reduce future risk to the Finance VLAN and broader MidRiver Health environment.

Scope:

This investigation is limited to analyzing the activity of **FIN-WS-077 (10.20.30.77)** and user **jmartin** on **April 9th, 2025**, based solely on the logs provided in Appendix A. The scope includes reviewing VPN authentication events, host activity, DNS queries, firewall egress traffic, NetFlow summaries, IDS alerts, and SOC notifications to determine whether unauthorized access occurred and whether data was exfiltrated.

Methodology:

To understand what happened on FIN-WS-077, I started by checking the VPN authentication log (A1). This is where I confirmed that jmartin's account logged in from an unusual external IP, **203.0.113.45**, at **19:03:58** with MFA approved (A1-31). Right after that, the VPN assigned him the Finance VLAN address **10.20.30.77** at **19:04:03** (A1-32). These two entries set the starting point for the rest of the investigation.

Next, I reviewed the Windows Security Log for FIN-WS-077 (A3) to see what happened on the host right after the login. A few events stood out. At **19:04:22**, the system assigned **special privileges** to jmartin (A3-18), which is unusual for a normal Finance user. Then at **19:04:40**, another entry showed **SeRestorePrivilege** being granted to svcbackup (A3-19). I also noted two key process events: **updater.exe** running at **19:05:20** (A3-21), followed by a hidden **encoded PowerShell command** at **19:06:05** (A3-23). These events helped show what activity took place on the machine right after the suspicious login.

After reviewing host activity, I looked at DNS logs (A4) to see what domains FIN-WS-077 tried to reach. Starting at **19:05:33**, the workstation began querying multiple subdomains under *support-sync.com*, such as **cdn-docs.support-sync.com** (A4-28) and **api.support-sync.com** (A4-29). These queries indicated the system was reaching out to external infrastructure it normally wouldn't contact.

From there, I checked firewall egress logs (A5) to see what outbound connections were made. Two entries from 10.20.30.77 showed major data transfers: **1.86GB** to **44.231.25.18** at **19:05:39** (A5-22) and **312MB** to **44.231.25.17** at **19:06:11** (A5-23). To confirm these numbers, I compared them with the NetFlow summary (A6), which showed the same high-volume traffic to those destinations (A6-1, A6-2).

I then reviewed IDS alerts (A7) to see if anything lined up with the events above. Two alerts did: one for **large outbound TLS data** at **19:05:42** (A7-12) and another for **multiple suspicious DNS lookups** at **19:05:56** (A7-13). Both alerts matched what I had already seen in the DNS and firewall logs.

Finally, I checked the SOC memo (A9) to verify when the SOC first noticed the issue. They flagged the unusual VPN login at **19:04:11** (A9-1) and then the outbound HTTPS spike at **19:06:03** (A9-2). These helped validate the timeline I built from the logs.

Using all timestamps from Appendix A, I lined up the events in order to create a clear timeline from the login through the outbound activity.

Executive Summary

Case Title: *MidRiver Health*

Background: On April 9, 2025, the SOC detected unusual activity coming from the Finance VLAN. One workstation, FIN-WS-077, suddenly generated a large spike in outbound HTTPS traffic. Around the same time, the user assigned to that workstation, jmartin, logged into the VPN from an unfamiliar, non-US IP address. Because this behavior didn't match his normal activity, the SOC flagged it as a potential account compromise and escalated the case for investigation.

Objective:

The goal of this investigation is to determine:

- Whether jmartin's VPN login was legitimate or the result of credential theft.
- What activity occurred on FIN-WS-077 immediately before and after the VPN login?
- Whether any sensitive data was accessed, staged, or exfiltrated from the Finance VLAN.
- The scope and impact of the incident, including any lateral movement or privilege escalation.
- What evidence supports or contradicts the possibility of data theft?
- What controls or policy updates should be implemented to prevent similar incidents?

This report walks through the investigative steps, the tools and filters that would be used, the timeline reconstruction, and the final findings based on the logs provided.

Evidence: Evidence collected is listed below and originates from the file **Appendix A – Evidence Logs file**

Findings: The analysis revealed multiple important findings that help form a complete picture of the incident:

Investigative Narrative: On April 9, 2025, user **jmartin** received an email claiming to be from IT Support with a "Mandatory VPN Client Update" (A8-1–A8-5). The email arrived at **18:57:01**, only minutes before the incident (A8-4). The included link pointed to *support-sync.com*, a domain that later appears throughout the malicious traffic.

At **19:03:58**, someone using jmartin's credentials logged into the corporate VPN from the external IP **203.0.113.45**, which the SOC flagged as unusual and outside the user's normal geography (A1-31; A9-1). The VPN successfully authenticated the login and assigned the session the internal address **10.20.30.77**, mapping it to workstation **FIN-WS-077** (A1-32; A2-15).

Within seconds of the VPN session beginning, privilege-related events were recorded on FIN-WS-077. At **19:04:22**, jmartin's account received special privileges (A3-18), and at **19:04:40**, the system granted **SeRestorePrivilege** to the service account *svcbackup* (A3-19). These actions indicate that the attacker gained elevated local control shortly after connecting.

At **19:05:37**, a suspicious binary named **updater.exe** executed under jmartin's profile (A3-21). This was followed by a hidden PowerShell process containing a base64-encoded command at **19:06:05** (A3-23), strongly suggesting malware deployment or command execution. Moments later, updater.exe terminated cleanly (A3-24), consistent with a dropper handing off control to another payload.

During the same minute, FIN-WS-077 began issuing DNS queries to multiple *support-sync* subdomains, including **cdn-docs.support-sync.com** (A4-28) and **api.support-sync.com** (A4-29). These domains were not seen elsewhere in the organization and fit the pattern of attacker-controlled infrastructure.

Immediately afterward, massive outbound HTTPS transfers began from **10.20.30.77**. At **19:05:39**, the firewall recorded **1.86 GB** sent to **44.231.25.18** under the SNI *cdn-docs.support-sync.com* (A5-22). A second large transfer of **312 MB** to *api.support-sync.com* occurred at **19:06:11** (A5-23). NetFlow confirms sustained exfiltration, showing **2.01 GB** to 44.231.25.18 (A6-1) and **346 MB** to 44.231.25.17 (A6-2), all originating from FIN-WS-077.

The IDS triggered multiple high-severity alerts tied to this host, including "Large Outbound Data Volume to Newly Observed Domain" at **19:05:42** (A7-12), "Suspicious User-Agent 'SyncClient/1.4.2'" at **19:06:15** (A7-15), and "JA3 fingerprint similarity" at **19:22:57** (A7-26). These collectively support that the traffic was automated, non-standard, and consistent with data exfiltration.

Finally, at **19:12:07**, the Windows Audit Log was cleared (A3-31), an action often taken by attackers attempting to remove traces of their activity. The VPN session ended at **19:12:55** with **2.2 GB** outbound (A1-36), closing the attacker's window of access.

Phase 1:Initial Alert and verification

Phase 1 began with reviewing the SOC alerts that triggered the investigation. At **19:04:11**, the SOC reported an unusual VPN login under jmartin's account (A9-1), followed two minutes later by a spike in outbound HTTPS traffic from internal address **10.20.30.77** (A9-2). Checking the VPN logs confirmed that jmartin's account successfully authenticated at **19:03:58** from external IP **203.0.113.45**, a location outside the user's normal region (A1-31). Once authenticated, the VPN assigned the session internal address **10.20.30.77** (A1-32), which the DHCP table identifies as workstation **FIN-WS-077** (A2-15). This meant the traffic spike and the unusual login were tied to the same device. Looking back a few minutes earlier, jmartin received an email from **it-alerts@support-sync.com** at **18:57:01** with a fake "Mandatory VPN Client Update" message and a link to **support-sync.com** (A8-1–A8-5). The timing—only six minutes before the suspicious login—suggests phishing was the likely entry point. Verifying the outbound traffic confirmed the concern: at **19:05:39**, FIN-WS-077 sent **1.86 GB** of data to *cdn-docs.support-sync.com* (A5-22), followed by another **312 MB** to a related domain at **19:06:11** (A5-23). Because the login came from an unfamiliar external IP, the workstation was correctly identified, and a massive data transfer occurred immediately afterward. Phase 1 validates that this is a confirmed security incident requiring deeper investigation.

Phase 2: Activity Timeline

After confirming that FIN-WS-077 was the workstation involved, the next step was to reconstruct its activity around the time of the incident using the Windows Security Log. The timeline shows that immediately after the suspicious VPN login at 19:03:58 (A1-31), the workstation recorded a significant privilege-related event: at **19:04:22**, jmartin's account received special privileges (A3-18), and only seconds later at **19:04:40**, the service account *svcbackup* was assigned **SeRestorePrivilege** (A3-19), a powerful right typically used by administrative processes. These privilege changes suggest the attacker gained elevated access on the system very early in the intrusion. Shortly afterward, at **19:05:37**, a new process named **updater.exe** launched from jmartin's user directory (A3-21); this is unusual because it originated from a temporary folder rather than an approved software path. Less than 30 seconds later, at **19:06:05**, a hidden PowerShell process executed using **-nop -w hidden -enc**, parameters commonly associated with encoded malicious commands (A3-23). The updater.exe process exited almost immediately after the PowerShell execution at **19:06:07**. Finally, at **19:12:07**, the system's audit logs were cleared (A3-31), an action that strongly suggests the attacker attempted to remove evidence of their activity before the VPN session ended at **19:12:55** (A1-36). This timeline establishes that privilege escalation, malware execution, command execution, and log tampering all occurred on FIN-WS-077 within minutes of the attacker gaining access, confirming that the workstation was fully compromised.

Phase 3: Network Traffic Analysis

Network traffic from FIN-WS-077 shows a clear pattern of malicious activity beginning immediately after the suspicious processes launched on the host. The first signs appear in the DNS resolver logs, where FIN-WS-077 begins querying multiple support-sync subdomains starting at 19:05:33, including cdn-docs.support-sync.com (A4-28), api.support-sync.com at 19:05:34 (A4-29), and additional domains such as telemetry.support-sync.com (A4-36) and suspicious-subdomain.support-sync.com at 19:14:12 (A4-50). These domains did not appear anywhere else in the environment and are tied directly to the phishing email sent earlier (A8-1–A8-5), reinforcing that they belong to attacker infrastructure. Only seconds after these DNS requests, the firewall logs show the start of large outbound HTTPS transfers from FIN-WS-077. At 19:05:39, the workstation sent 1.86 GB of encrypted traffic to 44.231.25.18 under the SNI cdn-docs.support-sync.com (A5-22), followed shortly afterward at 19:06:11 by 312 MB sent to 44.231.25.17 under api.support-sync.com (A5-23). NetFlow data confirms these transfers were not brief spikes but sustained exfiltration sessions, recording 2.01 GB from 10.20.30.77 to 44.231.25.18 (A6-1) and 346 MB to 44.231.25.17 (A6-2). The IDS detected multiple high-severity alerts during this period, including “Large Outbound Data Volume to Newly Observed Domain” at 19:05:42 (A7-12), “Suspicious DNS pattern” at 19:05:56 (A7-13), and a suspicious User-Agent string linked to SyncClient/1.4.2 at 19:06:15 (A7-15), all sourced from 10.20.30.77. These alerts, combined with the DNS activity and firewall volume, confirm that the workstation was actively communicating with attacker-controlled domains and transmitting large amounts of encrypted data off the network. Altogether, the DNS timeline, firewall logs, NetFlow records, and IDS alerts align perfectly to show that FIN-WS-077 was used to exfiltrate data shortly after the attacker took control of the system

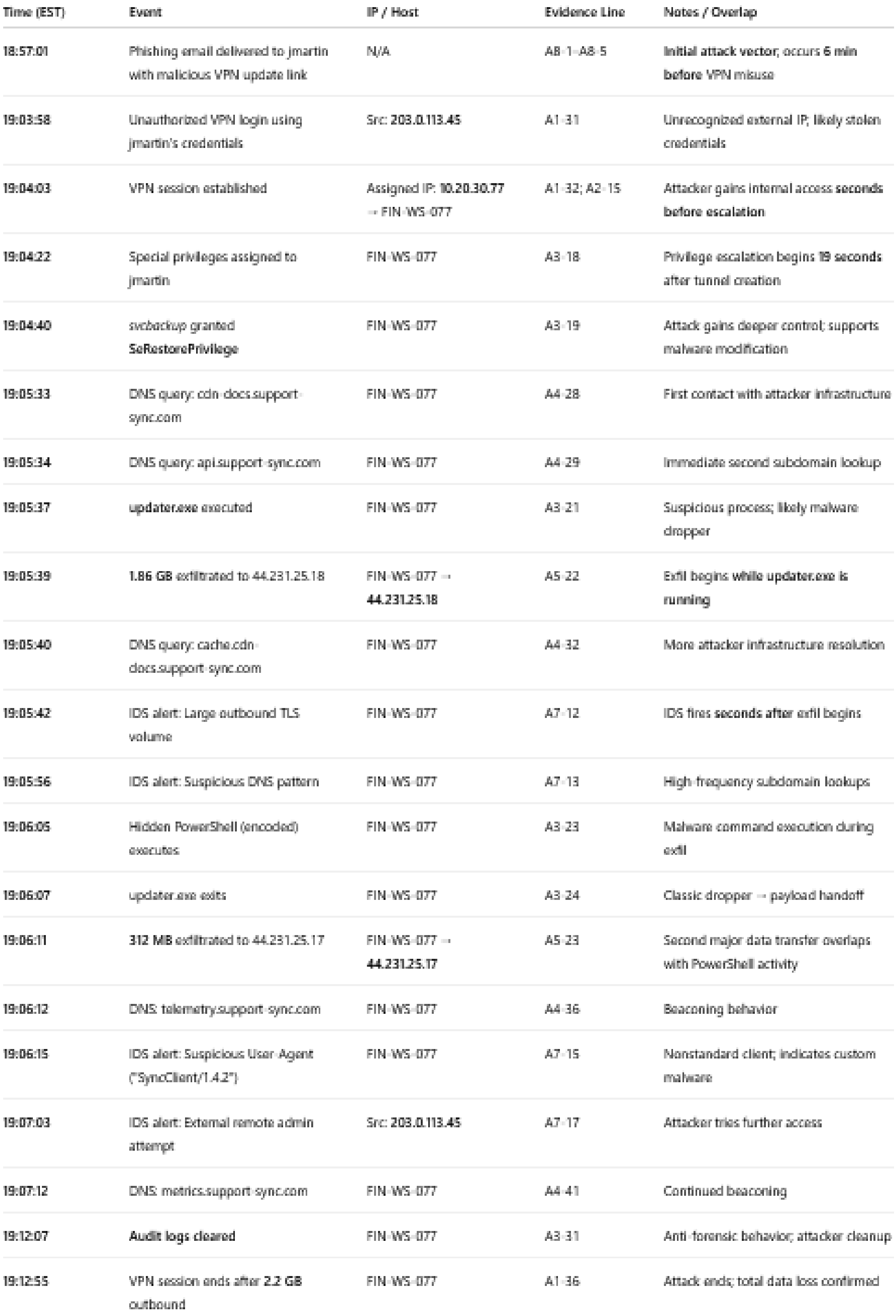
Phase 4: Attack Chain Correlation & Validation

By correlating all available logs, the full attack becomes clear. The intrusion started when employees, including jmartin, received a phishing email impersonating IT Support at 18:57:01, instructing them to install a fake “Mandatory VPN Client Update” from *support-sync.com* (A8-1–A8-5). This phishing campaign served as the initial attack vector, allowing the attacker to harvest credentials. Just six minutes later, those stolen credentials were used to log into the corporate VPN from the external IP 203.0.113.45 at 19:03:58 (A1-31), immediately triggering an SOC alert for unusual access (A9-1). The VPN then assigned the attacker to internal workstation FIN-WS-077 via 10.20.30.77 (A1-32; A2-15), giving them entry into the Finance VLAN. Within seconds of establishing the session, the attacker escalated privileges on the host: jmartin’s account received elevated rights at 19:04:22 (A3-18), and *svcbackup* was granted SeRestorePrivilege at 19:04:40 (A3-19). These rapid privilege changes enabled unauthorized tool execution. Immediately afterward, suspicious processes began running, including updater.exe launched from a temporary directory at 19:05:37 (A3-21) and a hidden, encoded PowerShell command at 19:06:05 (A3-23), strongly suggesting malware deployment. At the same time, FIN-WS-077 started querying multiple malicious *support-sync* subdomains, including cdn-docs.support-sync.com and api.support-sync.com (A4-28, A4-29), which directly match the phishing link used earlier. Seconds later, the workstation initiated massive outbound encrypted transfers, sending 1.86 GB at 19:05:39 (A5-22) and an additional 312 MB at 19:06:11 (A5-23), with NetFlow confirming a total of more than 2.3 GB sent to attacker-controlled servers (A6-1, A6-2). IDS alerts further reinforced the malicious nature of this traffic, flagging a large-volume TLS transfer, suspicious DNS bursts, an abnormal User-Agent string, and a malicious JA3 fingerprint—all tied to 10.20.30.77 (A7-12, A7-13, A7-15, A7-26). Before disconnecting, the attacker cleared the Windows audit logs at 19:12:07 (A3-31), a clear attempt to cover their tracks, and then ended the VPN session at 19:12:55 after sending 2.2 GB outbound (A1-36). Taken together, the evidence shows a complete attack chain: phishing > credential theft > unauthorized VPN access > privilege escalation > malware execution > DNS beaconing > large-scale data exfiltration > log clearing > disconnect.

Phase 5: Recommendations & Containment

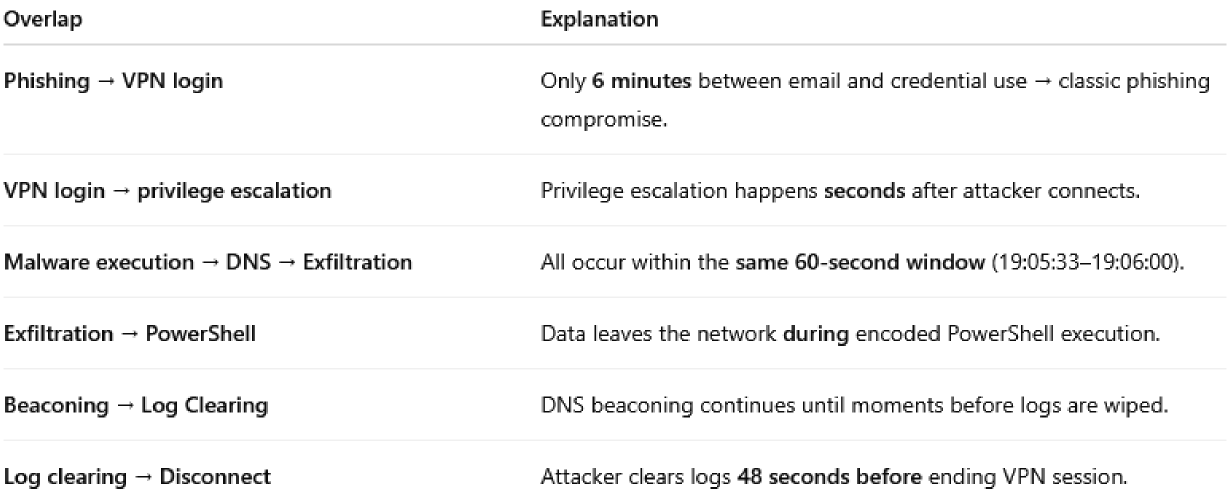
To contain this incident and prevent similar attacks in the future, the first step should be to disable jmartin's account, reset his credentials, and isolate FIN-WS-077 from the network so no more data can leave the Finance VLAN. The VPN session tied to the attacker should be terminated, and MFA should be reissued for anyone who may have been targeted by the same phishing email. In the short term, the organization should block *support-sync.com* and the related IP addresses, tighten egress filtering so workstations cannot send large amounts of data to unknown external sites, and turn on alerts for unusual privilege changes or audit log clearing, since those were early warning signs in this attack. Longer-term improvements should include better phishing awareness and stronger controls around VPN access, such as restricting logins from outside the country or requiring extra verification when a login seems unusual. The company should also encourage employees to take phishing reporting seriously by offering incentives. Many businesses now reward staff with small bonuses, recognition points, or monthly drawings when they report suspicious emails successfully. Programs like this greatly improve user engagement and make employees more likely to report phishing attempts before attackers can take advantage of them. Altogether, these steps would help stop this attack from continuing and make the environment more resilient going forward.

TimeLine:



Time (EST)	Event	IP / Host	Evidence Line	Notes / Overlap
18:57:01	Phishing email delivered to jmartin with malicious VPN update link	N/A	A8-1–A8-5	**Initial attack vector**; occurs **6 min before** VPN misuse
19:03:58	Unauthorized VPN login using jmartin's credentials	Src: **203.0.113.45**	A1-31	Unrecognized external IP; likely stolen credentials
19:04:03	VPN session established	Assigned IP: **10.20.30.77** → FIN-WS-077	A1-32; A2-15	Attacker gains internal access **seconds before escalation**
19:04:22	Special privileges assigned to jmartin	FIN-WS-077	A3-18	Privilege escalation begins **19 seconds** after tunnel creation
19:04:40	*svcbackup* granted **SeRestorePrivilege**	FIN-WS-077	A3-19	Attack gains deeper control; supports malware modification
19:05:33	DNS query: cdn-docs.support-sync.com	FIN-WS-077	A4-28	First contact with attacker infrastructure
19:05:34	DNS query: api.support-sync.com	FIN-WS-077	A4-29	Immediate second subdomain lookup
19:05:37	**updater.exe** executed	FIN-WS-077	A3-21	Suspicious process; likely malware dropper
19:05:39	**1.86 GB** exfiltrated to 44.231.25.18	FIN-WS-077 → **44.231.25.18**	A5-22	Exfil begins **while updater.exe is running**
19:05:40	DNS query: cache.cdn-docs.support-sync.com	FIN-WS-077	A4-32	More attacker infrastructure resolution
19:05:42	IDS alert: Large outbound TLS volume	FIN-WS-077	A7-12	IDS fires **seconds after** exfil begins
19:05:56	IDS alert: Suspicious DNS pattern	FIN-WS-077	A7-13	High-frequency subdomain lookups
19:06:05	Hidden PowerShell (encoded) executes	FIN-WS-077	A3-23	Malware command execution during exfil
19:06:07	updater.exe exits	FIN-WS-077	A3-24	Classic dropper → payload handoff
19:06:11	**312 MB** exfiltrated to 44.231.25.17	FIN-WS-077 → **44.231.25.17**	A5-23	Second major data transfer overlaps with PowerShell activity
19:06:12	DNS: telemetry.support-sync.com	FIN-WS-077	A4-36	Beaconing behavior
19:06:15	IDS alert: Suspicious User-Agent ("SyncClient/1.4.2")	FIN-WS-077	A7-15	Nonstandard client; indicates custom malware
19:07:03	IDS alert: External remote admin attempt	Src: **203.0.113.45**	A7-17	Attacker tries further access
19:07:12	DNS: metrics.support-sync.com	FIN-WS-077	A4-41	Continued beaconing
19:12:07	**Audit logs cleared**	FIN-WS-077	A3-31	Anti-forensic behavior; attacker cleanup
19:12:55	VPN session ends after **2.2 GB** outbound	FIN-WS-077	A1-36	Attack ends; total data loss confirmed

Key overlaps:



Overlap	Explanation
Phishing → VPN login	Only **6 minutes** between email and credential use → classic phishing compromise.
VPN login → privilege escalation	Privilege escalation happens **seconds** after attacker connects.
Malware execution → DNS → Exfiltration	All occur within the **same 60-second window** (19:05:33–19:06:00).
Exfiltration → PowerShell	Data leaves the network **during** encoded PowerShell execution.
Beaconing → Log Clearing	DNS beaconing continues until moments before logs are wiped.
Log clearing → Disconnect	Attacker clears logs **48 seconds before** ending VPN session.

How Wireshark Would Assist the Investigation:

If packet captures were available, Wireshark would make it much easier to confirm exactly what happened during the attack. Since jmartin was given the address 10.20.30.77, I could filter all of his traffic with a simple query like ip.addr = = 10.20.30.77 and instantly see everything his workstation sent or received during the incident window. I could also filter by time or look for his username to stay focused on the events between 19:04 and 19:15. Even though the traffic was encrypted, Wireshark would still show patterns, destinations, and data sizes, which would help confirm whether this was true data exfiltration or possibly the early stages of ransomware. With packet captures, I'd get a much clearer picture of what was transferred and how the attacker's tools behaved.

How Splunk would Assist the Investigation:

If these logs were loaded into Splunk, it would make the investigation a lot easier because everything involving jmartin would show up in one place instead of digging through each log manually. I could start with a simple search like index=fw "jmartin" and quickly see any firewall activity tied to him or his workstation. Then I could narrow the time to the incident window, from 19:00 to 19:15, which would line up his unusual VPN login at 19:04 (A1-31), the new privileges assigned to his account on the workstation (A3-18 and A3-19), and the big spike in outbound traffic from 10.20.30.77. Splunk would basically let me connect the VPN logs, Windows logs, and firewall activity all at once, which makes it much clearer how the attacker moved and whether they were just stealing data or trying to set up something like ransomware. This would give me a solid picture of what happened without having to jump between different log files.

How Windows Event Viewer Would Assist the Investigation:

If I had access to the workstation, Windows Event Viewer would help me confirm exactly what happened on FIN WS 077 during the incident. I would focus on the events around 19:04 when jmartin logged in and received special privileges (A3-18 and A3-19), and then look at the processes that started right after, like updater.exe launching at 19:05:37 (A3-21) and the encoded PowerShell command at 19:06:05 (A3-23). Event Viewer would also let me verify whether the installed service SyncClientService at 19:08 (A3-27) was legitimate or part of the attacker's activity. Reviewing these logs on the actual machine would help me understand whether the attacker was only exfiltrating data or also preparing the system for something more serious, like ransomware.

Filtering Out Unrelated Events:

While I was going through the logs, there were a bunch of entries that looked like normal day-to-day activity, like Teams starting up or random Windows services running. At first glance it almost feels like these events could blend in with what the attacker was doing, but once I lined the timestamps up with the actual attack window, none of them matched the privilege escalation, DNS lookups, or the big outbound traffic. Because the times didn't line up at all, I treated those entries as just normal background noise that happens on any workstation. They didn't have anything to do with the malicious activity, so I ruled them out as distractors and focused only on the events that fit the main timeline.

Conclusion

Based on everything in the logs, this incident clearly started with a phishing email that targeted employees in the Finance department. In jmartin's case, the attacker didn't waste any time — they sent the fake "VPN update" email, and within minutes, they were logging into the corporate VPN using his stolen credentials. Once the attacker connected to FIN-WS-077, they moved extremely fast. They escalated privileges almost immediately and even assigned **SeRestorePrivilege**, which raised a red flag for me because attackers often try to tamper with restore points when preparing for ransomware. That privilege doesn't usually show up in normal user activity, so combined with the hidden, encoded PowerShell command that ran shortly afterward, there's a real possibility this wasn't just about stealing data but could have been a setup for something like ransomware or system modification.

From there, FIN-WS-077 started talking to multiple suspicious support-sync subdomains and pushed out over 2GB of encrypted data. Since everything was sent over HTTPS, we can't see the exact contents of what left the network, but if we had packet captures instead of just logs, I could load the traffic into Wireshark and analyze the TLS handshakes, SNI fields, flow lengths, and even try to decrypt the payloads if session keys were available. With full PCAPs, we could also look at the binary patterns of the exfiltrated data to determine whether it was documents, database exports, or even partial ransomware payloads being downloaded or staged.

Even though the evidence strongly points to data exfiltration, the privilege escalation, encoded commands, and the fact that audit logs were cleared near the end all line up with behaviors seen in ransomware pre-staging. So while we can confirm that account compromise and data theft definitely occurred, the possibility of ransomware deployment shouldn't be ignored. With full forensic images or decrypted TLS streams, we could say more, but based on what we have, the attacker clearly had the access and tools needed to take this attack further.

Appendix A – Evidence Logs (Noisy Dataset)

All times Eastern, 24-hour clock. Line numbers and section labels included for citation (A1–A9).

A1. VPN Authentication Log

```
1. Apr 09 05:45:07 vpn01 AUTH User=svcbackup SrcIP=10.20.5.10 Device=Server MFA=svc Result=APPROVED

2. Apr 09 06:12:01 vpn01 AUTH User=sysadmin SrcIP=198.51.100.10 Device=WinServer MFA=svc Result=APPROVED

3. Apr 09 06:42:55 vpn01 AUTH User=intern1 SrcIP=198.51.100.99 Device=Android MFA=push Result=APPROVED

4. Apr 09 07:18:14 vpn01 AUTH User=tmiller SrcIP=198.51.100.42 Device=MacOS MFA=push Result=APPROVED

5. Apr 09 07:21:39 vpn01 NOTICE SessionEstablished CN=tmiller Tunnel=CorpVLAN AssignedIP=10.20.40.22

6. Apr 09 07:59:11 vpn01 AUTH User=kbrown SrcIP=198.51.100.55 Device=Win10 MFA=push Result=APPROVED

7. Apr 09 08:01:48 vpn01 NOTICE SessionEstablished CN=kbrown Tunnel=FinanceVLAN AssignedIP=10.20.30.88

8. Apr 09 08:32:14 vpn01 AUTH User=jmartin SrcIP=198.51.100.27 Device=iPhone MFA=push Result=APPROVED

9. Apr 09 08:33:00 vpn01 NOTICE SessionEstablished CN=jmartin Tunnel=FinanceVLAN AssignedIP=10.20.30.77

10. Apr 09 08:59:12 vpn01 NOTICE SessionTerminated CN=jmartin Duration=00:26:05 BytesOut=18MB

11. Apr 09 09:05:43 vpn01 AUTH User=kbrown SrcIP=198.51.100.55 Device=Win10 MFA=push Result=APPROVED

12. Apr 09 09:06:02 vpn01 FAIL User=unknown SrcIP=203.0.113.22 Reason=InvalidCreds

13. Apr 09 09:07:11 vpn01 AUTH User=alex SrcIP=198.51.100.60 Device=Android MFA=push Result=APPROVED
```

```
14. Apr 09 09:11:15 vpn01 NOTICE SessionEstablished CN=alex Tunnel=CorpVLAN
AssignedIP=10.20.41.13

15. Apr 09 09:42:01 vpn01 NOTICE SessionTerminated CN=tmiller Duration=02:20:18
BytesOut=1.8GB

16. Apr 09 10:12:58 vpn01 AUTH User=contract1 SrcIP=203.0.113.78 Device=Win10
MFA=push Result=APPROVED

17. Apr 09 10:13:22 vpn01 FAIL User=contract1 SrcIP=203.0.113.78 Reason=MFAExpired

18. Apr 09 11:12:04 vpn01 AUTH User=tmiller SrcIP=198.51.100.42 Device=MacOS MFA=push
Result=APPROVED

19. Apr 09 11:45:58 vpn01 AUTH User=sysmaint SrcIP=10.20.5.10 Device=Server MFA=svc
Result=APPROVED

20. Apr 09 12:03:21 vpn01 FAIL User=unknown SrcIP=203.0.113.45 Reason=InvalidCreds

21. Apr 09 12:04:02 vpn01 FAIL User=unknown SrcIP=203.0.113.45 Reason=InvalidCreds

22. Apr 09 13:22:07 vpn01 AUTH User=sysmaint SrcIP=10.20.5.10 Device=Server MFA=svc
Result=APPROVED

23. Apr 09 14:18:44 vpn01 AUTH User=alex SrcIP=198.51.100.60 Device=Android MFA=push
Result=APPROVED

24. Apr 09 16:39:10 vpn01 FAIL User=phishbot SrcIP=203.0.113.100 Reason=BlockedASN

25. Apr 09 17:41:09 vpn01 AUTH User=kbrown SrcIP=198.51.100.55 Device=Win10 MFA=push
Result=APPROVED

26. Apr 09 17:42:10 vpn01 NOTICE SessionEstablished CN=kbrown Tunnel=FinanceVLAN
AssignedIP=10.20.30.88

27. Apr 09 18:01:59 vpn01 NOTICE SessionTerminated CN=kbrown Duration=00:20:09
BytesOut=75MB

28. Apr 09 18:25:07 vpn01 FAIL User=testaccount SrcIP=203.0.113.201
Reason=LockedAccount

29. Apr 09 18:42:33 vpn01 AUTH User=intern2 SrcIP=198.51.100.99 Device=Android
MFA=push Result=APPROVED

30. Apr 09 18:55:44 vpn01 NOTICE SessionEstablished CN=intern2 Tunnel=CorpVLAN
AssignedIP=10.20.41.55
```

```
31. Apr 09 19:03:58 vpn01 AUTH User=jmartin SrcIP=203.0.113.45 Device=Win10 MFA=push
Result=APPROVED

32. Apr 09 19:04:03 vpn01 NOTICE SessionEstablished CN=jmartin Tunnel=FinanceVLAN
AssignedIP=10.20.30.77

33. Apr 09 19:04:18 vpn01 INFO HealthCheck Passed Tunnel=FinanceVLAN
Client=10.20.30.77 Latency=42ms

34. Apr 09 19:09:22 vpn01 NOTICE Keepalive Packet Received CN=jmartin

35. Apr 09 19:11:00 vpn01 INFO SyslogHeartbeat CN=tmiller Connected=TRUE

36. Apr 09 19:12:55 vpn01 NOTICE SessionTerminated CN=jmartin Duration=00:09:52
BytesOut=2.2GB

37. Apr 09 19:18:07 vpn01 NOTICE SessionEstablished CN=tmiller Tunnel=CorpVLAN
AssignedIP=10.20.40.22

38. Apr 09 19:21:44 vpn01 INFO CPU load average 63% Threads=215

39. Apr 09 19:28:13 vpn01 NOTICE SessionTerminated CN=intern2 Duration=00:32:29
BytesOut=90MB

40. Apr 09 19:55:33 vpn01 AUTH User=audit SrcIP=10.20.5.11 Device=Server MFA=svc
Result=APPROVED

41. Apr 09 20:03:14 vpn01 AUTH User=tmiller SrcIP=198.51.100.42 Device=MacOS MFA=push
Result=APPROVED

42. Apr 09 21:11:27 vpn01 AUTH User=tmiller SrcIP=198.51.100.42 Device=MacOS MFA=push
Result=APPROVED

43. Apr 09 21:35:01 vpn01 NOTICE SessionTerminated CN=tmiller Duration=00:24:14
BytesOut=510MB

44. Apr 09 22:12:15 vpn01 INFO DailySessionSummary ActiveUsers=8 Peak=22
```

A2. DHCP Lease Table (Finance VLAN)

```
1. 10.20.30.10  MAC=00:16:3E:00:10:AA  Host=FIN-WS-010  LeaseStart=2025-04-09 07:58:12

2. 10.20.30.12  MAC=00:16:3E:00:12:BB  Host=FIN-WS-012  LeaseStart=2025-04-09 08:00:11
```

3. 10.20.30.18 MAC=00:16:3E:00:18:CC Host=FIN-WS-018 LeaseStart=2025-04-09 07:57:59

4. 10.20.30.21 MAC=00:16:3E:00:21:22 Host=FIN-PRN-1   LeaseStart=2025-04-09 06:45:01

5. 10.20.30.25 MAC=00:16:3E:00:25:44 Host=FIN-MFP-01 LeaseStart=2025-04-09 06:45:02

6. 10.20.30.30 MAC=00:16:3E:00:30:33 Host=FIN-WS-030 LeaseStart=2025-04-09 08:02:54

7. 10.20.30.42 MAC=00:16:3E:00:42:66 Host=FIN-WS-042 LeaseStart=2025-04-09 08:15:22

8. 10.20.30.44 MAC=00:16:3E:00:42:66 Host=FIN-WS-042B LeaseStart=2025-04-09 09:45:12 (Duplicate MAC)

9. 10.20.30.55 MAC=00:16:3E:00:55:77 Host=FIN-WS-055 LeaseStart=2025-04-09 08:30:00

10. 10.20.30.61 MAC=00:16:3E:00:61:02 Host=FIN-PRINT-QA LeaseStart=2025-04-09 08:00:10

11. 10.20.30.66 MAC=00:16:3E:00:66:33 Host=CONF-LAP-1 LeaseStart=2025-04-09 09:02:23

12. 10.20.30.70 MAC=00:16:3E:00:70:11 Host=CONF-LAP-2 LeaseStart=2025-04-09 09:05:17

13. 10.20.30.71 MAC=00:16:3E:00:71:11 Host=CONF-LAP-3 LeaseStart=2025-04-09 09:06:10

14. 10.20.30.75 MAC=00:16:3E:00:75:18 Host=FIN-WS-075 LeaseStart=2025-04-09 09:07:00

15. 10.20.30.77 MAC=00:16:3E:3A:7B:11 Host=FIN-WS-077 LeaseStart=2025-04-09 17:55:01

16. 10.20.30.80 MAC=00:16:3E:00:80:08 Host=FIN-WS-080 LeaseStart=2025-04-09 09:01:02

17. 10.20.30.83 MAC=00:16:3E:00:83:83 Host=FIN-TEST-VM LeaseStart=2025-04-09 11:14:59

18. 10.20.30.85 MAC=00:16:3E:00:85:85 Host=FIN-ARCH-01 LeaseStart=2025-04-09 07:30:00

19. 10.20.30.88 MAC=00:16:3E:2C:88:02 Host=FIN-WS-088 LeaseStart=2025-04-09 08:01:02

20. 10.20.30.90 MAC=00:16:3E:00:90:99 Host=FIN-GUEST-1 LeaseStart=2025-04-09 09:00:01

21. 10.20.30.91 MAC=00:16:3E:00:91:91 Host=FIN-GUEST-2 LeaseStart=2025-04-09 09:00:05

22. 10.20.30.92 MAC=00:16:3E:00:92:92 Host=FIN-GUEST-3 LeaseStart=2025-04-09 09:00:06

```
23. 10.20.30.94 MAC=00:16:3E:00:94:94  Host=FIN-GUEST-4 LeaseStart=2025-04-09 09:00:07

24. 10.20.30.95 MAC=00:16:3E:AA:95:22  Host=FIN-WS-095  LeaseStart=2025-04-09 09:15:42

25. 10.20.30.97 MAC=00:16:3E:00:97:97  Host=FIN-LAB-TEST LeaseStart=2025-04-09 14:30:00

26. 10.20.30.99 MAC=00:16:3E:BB:99:33  Host=FIN-WS-099  LeaseStart=2025-04-09 10:00:00

27. 10.20.30.100 MAC=00:16:3E:00:10:AA Host=FIN-MFP-ARCHIVE LeaseStart=2025-04-09 07:59:55

28. 10.20.30.101 MAC=00:16:3E:00:10:AA Host=FIN-MFP-ARCHIVE LeaseStart=2025-04-08 22:14:00 (Expired)

29. 10.20.30.109 MAC=00:16:3E:00:10:BB Host=FIN-OLDLAP-01 LeaseStart=2025-04-08 20:45:00 (Expired)

30. 10.20.30.120 MAC=00:16:3E:00:12:12 Host=FIN-SMARTTV LeaseStart=2025-04-09 08:50:10
```

A3. Windows Security Log – FIN-WS-077

A3. Windows Security Log – FIN-WS-077 (Expanded / Noisy Version)

```
1. 07:02:11  4624  Interactive logon  Account=helpdesk      Source=10.20.5.10

2. 08:12:03  4624  LogonType=2        Account=jmartin       Source=LOCAL

3. 09:30:22  6005  EventLog started   Service=WindowsEventLog

4. 10:11:03  4688  New process: C:\Windows\System32\svchost.exe -k netsvcs Parent=services.exe

5. 11:54:12  1102  Audit log cleared  Account=adminuser

6. 12:10:05  4698  Scheduled task created  Task=BackupJob Account=svcbackup

7. 13:22:14  4624  LogonType=2        Account=kbrown        Source=LOCAL

8. 15:01:09  4625  Failed logon       Account=guest         Source=LOCAL Reason=BadPassword

9. 16:12:35  4670  Permissions on an object were changed  Account=svcadmin
```

```
10. 17:32:08  4647  User initiated logoff  Account=jmartin

11. 18:05:43  4624  Network logon     Account=crmsvc        Source=10.20.5.12

12. 18:36:50  4624  LogonType=2       Account=intern2       Source=LOCAL

13. 18:58:27  4624  LogonType=3       Account=jmartin       Source=10.20.5.10

14. 19:00:11  4648  A network logon was attempted  Account=svcbackup  Source=10.20.5.10

15. 19:01:05  4624  LogonType=2       Account=remoteuser Source=LOCAL

16. 19:02:43  4624  Account lockout cleared  Account=kbrown

17. 19:03:50  4624  LogonType=3       Account=svcmonitor  Source=10.20.5.10

18. 19:04:22  4672  Special privileges assigned to new logon  Account=jmartin

19. 19:04:40  4704  A user right was assigned  Account=svcbackup  Right=SeRestorePrivilege

20. 19:05:12  4688  New process: C:\Program Files\Microsoft Office\Teams\Teams.exe
Parent=explorer.exe

21. 19:05:37  4688  New process: C:\Users\jmartin\AppData\Local\Temp\updater.exe
Parent=Teams.exe

22. 19:05:39  5156  WFPEVENT  Allowed  Application=updater.exe  Dest=44.231.25.18:443

23. 19:06:05  4688  New process:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -nop -w hidden -enc
SQBmACgA  Parent=updater.exe

24. 19:06:07  4689  Process exited: updater.exe  ExitCode=0x0

25. 19:06:20  4625  Failed logon      Account=svcsvc        Source=LOCAL
Reason=BadPassword

26. 19:07:01  4634  An account was logged off  Account=remoteuser

27. 19:08:12  4697  A service was installed  Service=SyncClientService  Account=LocalSystem

28. 19:09:02  4625  Failed logon      Account=svcsvc        Source=LOCAL
Reason=BadPassword

29. 19:10:11  4673  A privileged service was called  Account=svcbackup

30. 19:11:02  4648  A network logon was attempted  Account=adminuser  Source=10.20.5.10
```

```
31. 19:12:07  1102  Audit log cleared  Account=system

32. 19:12:25  4624  LogonType=10   Account=remoteuser Source=203.0.113.66

33. 19:12:55  4634  An account was logged off  Account=jmartin

34. 19:14:18  4688  New process: C:\Program Files\Common Files\updatehelper.exe
Parent=svchost.exe

35. 19:20:02  4624  LogonType=2    Account=helpdesk     Source=LOCAL

36. 19:22:45  4624  LogonType=10   Account=systembackup Source=LOCAL

37. 19:30:11  1102  Audit log cleared  Account=adminuser

38. 20:01:01  4624  Interactive logon  Account=helpdesk    Source=10.20.5.10

39. 20:05:59  4688  New process: C:\Windows\System32\svchost.exe -k netsvcs
Parent=services.exe

40. 20:15:47  4624  LogonType=2    Account=kbrown       Source=LOCAL
```

A4. DNS Resolver Log (10.20.1.53)

```
1. 06:58:12  FIN-WS-018  Query A   internal-timesheet.midriverhealth.org          → 10.20.5.61

2. 07:12:01  FIN-WS-012  Query A   statuspage.midriverhealth.org          → 34.120.4.16

3. 08:13:09  FIN-WS-030  Query A   payroll.midriverhealth.org             → 10.20.5.60

4. 08:45:20  FIN-WS-042  Query A   updates.microsoft.com                  → 20.190.129.2

5. 09:03:11  FIN-WS-042  Query A   docs.google.com                        → 172.217.3.14

6. 09:46:22  FIN-WS-088  Query A   updates.microsoft.com                  → 20.190.129.2

7. 10:12:01  FIN-WS-077  Query A   microsoft.com                          → 20.112.52.29

8. 10:35:09  FIN-WS-099  Query A   doubleclick.net                  → 172.217.8.14

9. 11:05:44  FIN-WS-099  Query A   ads.example-ad.net                     → 198.51.100.200
```

```
10. 12:11:00  FIN-WS-055  Query PTR  10.20.30.55                    →
FIN-WS-055.midriverhealth.local

11. 12:33:17  FIN-WS-030  Query A   zoom.us                    → 170.114.52.33

12. 13:05:48  FIN-WS-095  Query A   zoom.us                    → 170.114.52.33

13. 13:33:12  FIN-WS-080  Query A   onedrive.live.com                 → 20.224.72.12

14. 14:01:02  FIN-WS-018  Query A   internal-timesheet.midriverhealth.org        → 10.20.5.61
(cache hit)

15. 15:02:44  FIN-WS-012  Query TXT spf.payroll.midriverhealth.org       → "v=spf1
include:spf.protection.outlook.com -all"

16. 15:17:03  FIN-WS-012  Query A   statuspage.midriverhealth.org       → 34.120.4.16
(TTL=3600)

17. 15:56:30  FIN-WS-099  Query A   analytics.tracker.example          → 52.216.8.9

18. 16:12:20  FIN-WS-012  Query AAAA statuspage.midriverhealth.org    →
2607:f8b0:4005:803::200e

19. 17:02:55  FIN-WS-030  Query A   finance.yahoo.com                 → 23.75.3.10

20. 17:25:10  FIN-WS-055  Query A   s3.amazonaws.com                  → 52.216.0.0

21. 17:55:01  FIN-WS-077  Query A   dhcp.lease-check.midriverhealth.local       → 10.20.1.1

22. 18:54:12  FIN-WS-077  Query A   teams.microsoft.com               → 13.107.6.171

23. 18:56:35  FIN-WS-030  Query A   finance.yahoo.com                 → 23.75.3.10

24. 18:59:03  FIN-WS-099  Query A   cdn.fastly.net                    → 151.101.1.195

25. 19:02:14  FIN-WS-055  Query A   microsoft.com                     → 20.112.52.29

26. 19:04:10  FIN-WS-012  Query A   auth.portal.midriverhealth.org       → 10.20.5.45

27. 19:05:20  FIN-WS-042  Query A   adobe.com                         → 192.147.130.34

28. 19:05:33  FIN-WS-077  Query A   cdn-docs.support-sync.com                  →
44.231.25.18

29. 19:05:34  FIN-WS-077  Query A   api.support-sync.com              → 44.231.25.17
```

```
30. 19:05:36  FIN-WS-077  Query TXT cdn-docs.support-sync.com         → "v=spf1
include:_spf.support-sync.com ~all"  (suspicious: new TXT)

31. 19:05:37  FIN-WS-030  Query A   ct-reports.support-sync.com       → 44.231.25.19

32. 19:05:40  FIN-WS-077  Query A   cache.cdn-docs.support-sync.com          →
44.231.25.20

33. 19:05:44  FIN-WS-042  Query A   ct-reports.support-sync.com       → NXDOMAIN

34. 19:05:47  FIN-WS-095  Query A   ct-reports.support-sync.com       → 44.231.25.19

35. 19:06:01  FIN-WS-088  Query A   wsj.com                       → 18.164.63.20

36. 19:06:12  FIN-WS-077  Query A   telemetry.support-sync.com        → 44.231.25.21

37. 19:06:15  FIN-WS-077  Query A   api.support-sync.com              → 44.231.25.17
(cache hit)

38. 19:06:20  FIN-WS-077  Query PTR  44.231.25.18                     →
host-44-231-25-18.hostingprovider.net

39. 19:06:38  FIN-WS-055  Query A   s3.amazonaws.com                  → 52.216.0.0

40. 19:07:05  FIN-WS-099  Query A   adserver.example-ad.net           → 198.51.100.200

41. 19:07:12  FIN-WS-077  Query A   metrics.support-sync.com          → 44.231.25.22

42. 19:08:41  FIN-WS-012  Query A   adobe.com                         → 192.147.130.34

43. 19:09:55  FIN-WS-018  Query A   auth.google.com                   → 172.217.14.197

44. 19:10:03  FIN-WS-077  Query TXT api.support-sync.com              → "dkim=none;
dmarc=none; spf=softfail"

45. 19:10:18  FIN-WS-077  Query A   ct-reports.support-sync.com       → 44.231.25.19
(now resolving)

46. 19:11:12  FIN-WS-077  Query A   ct-reports.support-sync.com       → 44.231.25.19
(repeat)

47. 19:11:45  FIN-WS-099  Query A   doubleclick.net                   → 172.217.8.14

48. 19:12:50  FIN-WS-077  Query A   backup.midriverhealth.s3.amazonaws.com → 52.216.0.1
```

```
49. 19:13:05  FIN-WS-055  Query A   microsoft.com                        → 20.112.52.29

50. 19:14:12  FIN-WS-077  Query A   suspicious-subdomain.support-sync.com    →
44.231.26.7  (low TTL)

51. 19:15:22  FIN-WS-018  Query A   onedrive.live.com                    → 20.224.72.12

52. 19:18:07  FIN-WS-042  Query A   auth.portal.midriverhealth.org         → 10.20.5.45  (cache
hit)

53. 19:19:31  FIN-WS-077  Query TXT support-sync.com              → "registration=2025-04-01;
country=US"

54. 19:21:00  FIN-WS-077  Query A   ct-reports.support-sync.com          → 44.231.25.19
(repeat)

55. 19:24:11  FIN-WS-055  Query A   doubleclick.net                      → 172.217.8.14

56. 19:25:50  FIN-WS-099  Query PTR  10.20.30.99                         →
FIN-WS-099.midriverhealth.local

57. 19:28:01  FIN-WS-077  Query A   telemetry.support-sync.com           → NXDOMAIN

58. 19:30:12  FIN-WS-030  Query A   partners.examplecorp.com             → 54.239.28.85

59. 19:34:05  FIN-WS-077  Query A   ct-reports.support-sync.com          → 44.231.25.19
(repeat)

60. 19:42:18  FIN-WS-018  Query A   internal-timesheet.midriverhealth.org         → 10.20.5.61
(cache hit)
```

A5. Firewall Egress Log (fw-east01)

```
1. 18:21:58  ALLOW  Src=10.20.30.12  Dst=172.217.3.110  Port=443  Proto=TLS
SNI=google.com                  BytesOut=2.1MB   BytesIn=1.8MB

2. 18:22:05  ALLOW  Src=10.20.30.30  Dst=20.190.129.2   Port=443  Proto=TLS
SNI=updates.microsoft.com        BytesOut=18MB   BytesIn=11MB

3. 18:30:40  ALLOW  Src=10.20.30.88  Dst=23.46.21.20    Port=443  Proto=TLS
SNI=finance.yahoo.com            BytesOut=3.2MB   BytesIn=2.7MB
```

```
4. 18:42:17  ALLOW  Src=10.20.30.99  Dst=52.216.80.11   Port=443  Proto=TLS
SNI=dropbox.com                BytesOut=84MB        BytesIn=23MB

5. 18:46:03  ALLOW  Src=10.20.30.30  Dst=13.107.6.171   Port=443  Proto=TLS
SNI=teams.microsoft.com          BytesOut=22MB    BytesIn=31MB

6. 18:50:01  ALLOW  Src=10.20.30.12  Dst=151.101.1.195  Port=443  Proto=TLS
SNI=cdn.fastly.net               BytesOut=2.8MB   BytesIn=1.6MB

7. 18:53:50  ALLOW  Src=10.20.30.55  Dst=52.96.58.34    Port=443  Proto=TLS
SNI=outlook.office365.com        BytesOut=4.5MB   BytesIn=4.2MB

8. 18:55:09  ALLOW  Src=10.20.30.88  Dst=23.46.21.20    Port=443  Proto=TLS
SNI=finance.yahoo.com            BytesOut=3.3MB   BytesIn=2.6MB

9. 18:57:02  ALLOW  Src=10.20.30.18  Dst=104.244.42.1   Port=443  Proto=TLS
SNI=twitter.com                  BytesOut=1.2MB   BytesIn=1.1MB

10. 18:58:14 ALLOW  Src=10.20.30.77  Dst=52.112.52.29   Port=443  Proto=TLS
SNI=microsoft.com                BytesOut=7.4MB   BytesIn=6.3MB

11. 18:59:20 ALLOW  Src=10.20.30.95  Dst=151.101.1.195  Port=443  Proto=TLS
SNI=cdn.fastly.net              BytesOut=2.4MB   BytesIn=1.9MB

12. 19:00:13 ALLOW  Src=10.20.30.30  Dst=52.96.58.34    Port=443  Proto=TLS
SNI=outlook.office365.com        BytesOut=5.1MB   BytesIn=4.7MB

13. 19:00:25 ALLOW  Src=10.20.30.77  Dst=18.164.63.20   Port=443  Proto=TLS  SNI=wsj.com
BytesOut=16MB        BytesIn=12MB

14. 19:01:37 ALLOW  Src=10.20.30.88  Dst=13.107.6.171   Port=443  Proto=TLS
SNI=teams.microsoft.com          BytesOut=12MB    BytesIn=9MB

15. 19:02:55 ALLOW  Src=10.20.30.12  Dst=52.216.0.0     Port=443  Proto=TLS
SNI=s3.amazonaws.com             BytesOut=27MB   BytesIn=21MB

16. 19:03:01 ALLOW  Src=10.20.30.55  Dst=44.231.25.19   Port=443  Proto=TLS
SNI=ct-reports.support-sync.com   BytesOut=28MB BytesIn=3MB

17. 19:03:42 ALLOW  Src=10.20.30.95  Dst=104.244.42.1   Port=443  Proto=TLS
SNI=twitter.com                 BytesOut=1.2MB   BytesIn=1.1MB

18. 19:04:05 ALLOW  Src=10.20.30.18  Dst=172.217.8.14   Port=443  Proto=TLS
SNI=doubleclick.net             BytesOut=6.5MB   BytesIn=3.9MB

19. 19:04:29 ALLOW  Src=10.20.30.42  Dst=192.147.130.34 Port=443  Proto=TLS
SNI=adobe.com                    BytesOut=4.8MB   BytesIn=5.0MB
```

```
20. 19:05:10 ALLOW  Src=10.20.30.18  Dst=20.224.72.12   Port=443  Proto=TLS
SNI=onedrive.live.com            BytesOut=24MB       BytesIn=18MB

21. 19:05:33 ALLOW  Src=10.20.30.55  Dst=44.231.25.19   Port=443  Proto=TLS
SNI=ct-reports.support-sync.com   BytesOut=51MB BytesIn=7MB

22. 19:05:39 ALLOW  Src=10.20.30.77  Dst=44.231.25.18   Port=443  Proto=TLS
SNI=cdn-docs.support-sync.com     BytesOut=1.86GB  BytesIn=41MB

23. 19:06:11 ALLOW  Src=10.20.30.77  Dst=44.231.25.17   Port=443  Proto=TLS
SNI=api.support-sync.com          BytesOut=312MB   BytesIn=15MB

24. 19:06:29 ALLOW  Src=10.20.30.30  Dst=52.96.58.34    Port=443  Proto=TLS
SNI=outlook.office365.com         BytesOut=4.3MB   BytesIn=4.1MB

25. 19:06:38 ALLOW  Src=10.20.30.12  Dst=44.231.25.21   Port=443  Proto=TLS
SNI=telemetry.support-sync.com    BytesOut=12MB BytesIn=2MB

26. 19:07:05 ALLOW  Src=10.20.30.99  Dst=198.51.100.200 Port=443  Proto=TLS
SNI=adserver.example-ad.net       BytesOut=2.8MB   BytesIn=2.2MB

27. 19:07:22 ALLOW  Src=10.20.30.88  Dst=20.82.128.44   Port=443  Proto=TLS
SNI=onedrive.live.com            BytesOut=18MB       BytesIn=8MB

28. 19:07:40 ALLOW  Src=10.20.30.55  Dst=44.231.25.19   Port=443  Proto=TLS
SNI=ct-reports.support-sync.com   BytesOut=43MB BytesIn=5MB

29. 19:08:22 ALLOW  Src=10.20.30.77  Dst=44.231.25.18   Port=443  Proto=TLS
SNI=cdn-docs.support-sync.com     BytesOut=119MB   BytesIn=6MB

30. 19:09:09 ALLOW  Src=10.20.30.42  Dst=23.75.3.10     Port=443  Proto=TLS
SNI=finance.yahoo.com             BytesOut=2.8MB   BytesIn=2.1MB

31. 19:10:12 ALLOW  Src=10.20.30.18  Dst=20.224.72.12   Port=443  Proto=TLS
SNI=onedrive.live.com            BytesOut=6MB        BytesIn=5MB

32. 19:10:27 ALLOW  Src=10.20.30.77  Dst=44.231.26.7    Port=443  Proto=TLS
SNI=suspicious-subdomain.support-sync.com BytesOut=84MB BytesIn=1MB

33. 19:12:05 ALLOW  Src=10.20.30.18  Dst=172.217.8.14   Port=443  Proto=TLS
SNI=doubleclick.net               BytesOut=3.4MB   BytesIn=2.7MB

34. 19:13:42 ALLOW  Src=10.20.30.95  Dst=172.217.8.14   Port=443  Proto=TLS
SNI=doubleclick.net               BytesOut=2.2MB   BytesIn=1.5MB

35. 19:14:25 ALLOW  Src=10.20.30.99  Dst=151.101.1.195  Port=443  Proto=TLS
SNI=cdn.fastly.net                BytesOut=1.5MB   BytesIn=1.1MB
```

```
36. 19:18:09 ALLOW  Src=10.20.30.30  Dst=52.96.58.34    Port=443  Proto=TLS
SNI=outlook.office365.com        BytesOut=3.7MB   BytesIn=3.5MB

37. 19:22:15 ALLOW  Src=10.20.30.88  Dst=20.82.128.44   Port=443  Proto=TLS
SNI=onedrive.live.com            BytesOut=15MB      BytesIn=8MB

38. 19:26:40 ALLOW  Src=10.20.30.55  Dst=44.231.25.19   Port=443  Proto=TLS
SNI=ct-reports.support-sync.com   BytesOut=32MB BytesIn=4MB

39. 19:31:50 ALLOW  Src=10.20.30.42  Dst=13.107.6.171   Port=443  Proto=TLS
SNI=teams.microsoft.com          BytesOut=5.8MB   BytesIn=8.1MB

40. 19:35:02 ALLOW  Src=10.20.30.12  Dst=52.216.0.0     Port=443  Proto=TLS
SNI=s3.amazonaws.com             BytesOut=25MB  BytesIn=17MB

41. 19:41:25 ALLOW  Src=10.20.30.77  Dst=52.112.52.29   Port=443  Proto=TLS
SNI=microsoft.com                BytesOut=8MB         BytesIn=6MB

42. 19:55:33 ALLOW  Src=10.20.30.55  Dst=44.231.25.19   Port=443  Proto=TLS
SNI=ct-reports.support-sync.com   BytesOut=47MB BytesIn=6MB

43. 20:01:09 ALLOW  Src=10.20.30.12  Dst=52.216.0.1     Port=443  Proto=TLS
SNI=s3.amazonaws.com             BytesOut=22MB  BytesIn=19MB

44. 20:12:50 ALLOW  Src=10.20.30.95  Dst=20.224.72.12   Port=443  Proto=TLS
SNI=onedrive.live.com            BytesOut=15MB      BytesIn=11MB

45. 20:15:12 ALLOW  Src=10.20.30.18  Dst=151.101.1.195  Port=443  Proto=TLS
SNI=cdn.fastly.net               BytesOut=3.1MB   BytesIn=2.9MB
```

A6. NetFlow Summary (18:55–19:15)

```
1. 10.20.30.77 → 44.231.25.18       Flows=4,128   BytesOut=2.01GB   BytesIn=43MB
Proto=TCP/TLS

2. 10.20.30.77 → 44.231.25.17       Flows=1,203   BytesOut=346MB      BytesIn=16MB
Proto=TCP/TLS

3. 10.20.30.30 → 52.96.58.34        Flows=243     BytesOut=4.6MB      BytesIn=4.3MB
Proto=TCP/TLS

4. 10.20.30.12 → 172.217.3.110   Flows=45         BytesOut=2.1MB      BytesIn=1.8MB
Proto=TCP/TLS
```

5. 10.20.30.88 → 23.46.21.20 Flows=64 BytesOut=3.2MB BytesIn=2.7MB
Proto=TCP/TLS

6. 10.20.30.95 → 104.244.42.1 Flows=15 BytesOut=1.2MB BytesIn=1.1MB
Proto=TCP/TLS

7. 10.20.30.55 → 44.231.25.19 Flows=312 BytesOut=180MB BytesIn=12MB
Proto=TCP/TLS

8. 10.20.30.42 → 13.107.246.40 Flows=78 BytesOut=1.0MB BytesIn=900KB
Proto=TCP/TLS

9. 10.20.30.99 → 172.67.180.38 Flows=201 BytesOut=1.9MB BytesIn=1.6MB
Proto=TCP/TLS

10. 10.20.30.18 → 151.101.1.195 Flows=92 BytesOut=6.5MB BytesIn=3.9MB
Proto=TCP/TLS

11. 10.20.30.12 → 52.216.0.0 Flows=34 BytesOut=27MB BytesIn=21MB
Proto=TCP/TLS

12. 10.20.30.77 → 52.112.52.29 Flows=6 BytesOut=15MB BytesIn=11MB
Proto=TCP/TLS

13. 10.20.30.30 → 44.231.25.19 Flows=9 BytesOut=48MB BytesIn=4MB
Proto=TCP/TLS

14. 10.20.30.55 → 52.216.0.0 Flows=12 BytesOut=22MB BytesIn=18MB
Proto=TCP/TLS

15. 10.20.30.80 → 13.107.42.16 Flows=27 BytesOut=6.2MB BytesIn=5.9MB
Proto=TCP/TLS

16. 10.20.30.77 → 44.231.26.7 Flows=18 BytesOut=84MB BytesIn=1MB
Proto=TCP/TLS

17. 10.20.30.95 → 172.217.8.14 Flows=11 BytesOut=2.2MB BytesIn=1.5MB
Proto=TCP/TLS

18. 10.20.30.30 → 20.224.72.12 Flows=7 BytesOut=4.3MB BytesIn=4.1MB
Proto=TCP/TLS

19. 10.20.30.88 → 20.82.128.44 Flows=33 BytesOut=18MB BytesIn=8MB
Proto=TCP/TLS

20. 10.20.30.42 → 23.75.3.10 Flows=14 BytesOut=2.8MB BytesIn=2.1MB Proto=TCP/TLS

21. 10.20.30.12 → 44.231.25.21 Flows=5 BytesOut=12MB BytesIn=2MB Proto=TCP/TLS

22. 10.20.30.77 → 44.231.25.20 Flows=102 BytesOut=119MB BytesIn=6MB Proto=TCP/TLS

23. 10.20.30.99 → 198.51.100.200 Flows=4 BytesOut=2.8MB BytesIn=2.2MB Proto=TCP/TLS

24. 10.20.30.55 → 44.231.25.19 Flows=47 BytesOut=32MB BytesIn=4MB Proto=TCP/TLS

25. 10.20.30.18 → 172.217.8.14 Flows=38 BytesOut=3.4MB BytesIn=2.7MB Proto=TCP/TLS

26. 10.20.30.77 → 44.231.25.22 Flows=22 BytesOut=67MB BytesIn=2MB Proto=TCP/TLS

27. 10.20.30.30 → 52.96.58.34 Flows=11 BytesOut=4.6MB BytesIn=4.3MB Proto=TCP/TLS

28. 10.20.30.12 → 172.67.180.38 Flows=19 BytesOut=1.2MB BytesIn=1.1MB Proto=TCP/TLS

29. 10.20.30.77 → 44.231.25.19 Flows=5 BytesOut=51MB BytesIn=7MB Proto=TCP/TLS

30. 10.20.30.88 → 151.101.1.195 Flows=3 BytesOut=1.5MB BytesIn=1.1MB Proto=TCP/TLS

31. 10.20.30.95 → 13.107.6.171 Flows=8 BytesOut=5.8MB BytesIn=8.1MB Proto=TCP/TLS

32. 10.20.30.42 → 52.216.0.1 Flows=2 BytesOut=25MB BytesIn=17MB Proto=TCP/TLS

33. 10.20.30.77 → 52.112.52.29 Flows=3 BytesOut=8MB BytesIn=6MB Proto=TCP/TLS

34. 10.20.30.30 → 44.231.25.18 Flows=2 BytesOut=1.9MB BytesIn=120KB Proto=TCP/TLS

35. 10.20.30.99 → 172.217.3.110 Flows=6 BytesOut=1.1MB BytesIn=900KB
Proto=TCP/TLS

36. 10.20.30.77 → 44.231.25.18 Flows=14 BytesOut=1.2GB BytesIn=10MB
Proto=TCP/TLS (aggregate of short-lived sessions)

37. 10.20.30.77 → 44.231.25.17 Flows=9 BytesOut=234MB BytesIn=6MB
Proto=TCP/TLS (additional flows not in primary capture)

A7. IDS Alerts (Snort)

1. 10:22:44 [1:1000003:2] DNS query to known ad domain "doubleclick.net"
Src=10.20.30.88 Dst=8.8.8.8 Priority=3

2. 11:18:57 [1:2019501:1] SMB negotiation from non-standard port
Src=10.20.30.30 Dst=10.20.5.12 Priority=2

3. 12:04:19 [1:1000012:1] Outdated TLS version detected Src=10.20.30.12
Dst=192.147.130.34 Priority=3

4. 12:17:25 [1:1000018:1] HTTP connection to known CDN "cdn.fastly.net"
Src=10.20.30.95 Dst=151.101.1.195 Priority=3

5. 13:02:33 [1:1000020:1] DNS query to dynamic domain "dynupdate.example.com"
Src=10.20.30.42 Dst=8.8.8.8 Priority=2

6. 13:45:51 [1:2001222:3] TLS certificate self-signed Src=10.20.30.55
Dst=44.231.25.19 Priority=2

7. 14:02:12 [1:2001555:1] Excessive outbound HTTP requests Src=10.20.30.99
Dst=198.51.100.200 Priority=3

8. 15:09:40 [1:2023011:1] Outdated TLS version detected Src=10.20.30.12
Dst=192.147.130.34 Priority=3

9. 16:17:13 [1:2023300:2] Invalid DNS response length Src=10.20.30.18
Dst=8.8.8.8 Priority=3

10. 17:08:21 [1:1000104:2] Possible TOR handshake attempt
Src=10.20.30.30 Dst=185.220.101.1 Priority=1

11. 18:25:54 [1:1000115:1] TLS certificate mismatch Src=10.20.30.55
Dst=44.231.25.19 Priority=2

```
12. 19:05:42  [1:2024001:3]  **TLS Large Outbound Data Volume to Newly Observed Domain**
Src=10.20.30.77  Dst=44.231.25.18  Priority=1

13. 19:05:56  [1:2024003:1]  Suspicious DNS pattern - multiple subdomain lookups
Src=10.20.30.77  Dst=10.20.1.53      Priority=2

14. 19:06:09  [1:2003032:4]  SMB negotiation from non-standard port
Src=10.20.30.30  Dst=10.20.5.12      Priority=2

15. 19:06:15  [1:2024005:1]  **Suspicious User-Agent "SyncClient/1.4.2"**
Src=10.20.30.77  Dst=44.231.25.17  Priority=1

16. 19:06:27  [1:2024007:1]  Unrecognized TLS certificate issuer                  Src=10.20.30.77
Dst=44.231.25.18  Priority=2

17. 19:07:03  [1:2024010:2]  External Remote Admin Attempt                        Src=203.0.113.45
Dst=vpn.midriverhealth.org Priority=1

18. 19:08:45  [1:2024100:1]  TLS connection to newly registered domain
"telemetry.support-sync.com" Src=10.20.30.77 Dst=44.231.25.21 Priority=2

19. 19:09:11  [1:2024200:1]  HTTPS traffic volume anomaly (spike 250%)
Src=10.20.30.88  Dst=20.82.128.44  Priority=3

20. 19:10:15  [1:2024215:1]  Potential credential posting via HTTP POST
Src=10.20.30.99  Dst=198.51.100.200 Priority=2

21. 19:11:22  [1:2024301:1]  TLS session reuse count exceeded threshold
Src=10.20.30.77  Dst=44.231.25.18  Priority=2

22. 19:12:05  [1:2024400:1]  Multiple failed TLS handshakes detected
Src=10.20.30.12  Dst=52.216.0.0      Priority=3

23. 19:14:17  [1:2024500:1]  Abnormal packet timing variation                    Src=10.20.30.30
Dst=52.96.58.34   Priority=3

24. 19:18:04  [1:2024600:1]  TLS connection closed abnormally                     Src=10.20.30.55
Dst=44.231.25.19  Priority=2

25. 19:20:12  [1:2024701:1]  DNS query to newly observed TLD ".info"
Src=10.20.30.18  Dst=8.8.8.8           Priority=3

26. 19:22:57  [1:2024802:1]  Suspicious JA3 fingerprint similarity (95%)            Src=10.20.30.77
Dst=44.231.25.18  Priority=2

27. 19:25:10  [1:2024901:1]  TLS handshake version downgrade attempt
Src=10.20.30.12  Dst=20.190.129.2  Priority=3
```

```
28. 19:28:36  [1:2025001:1]  Excessive DNS queries (100+ / min)                  Src=10.20.30.99
Dst=10.20.1.53          Priority=3

29. 19:31:09  [1:2025100:1]  Possible beacon interval detected (periodic TLS traffic)
Src=10.20.30.77  Dst=44.231.25.17  Priority=2

30. 19:35:44  [1:2025200:1]  TLS SNI length anomaly                              Src=10.20.30.30
Dst=52.96.58.34   Priority=3
```

A8. Email Headers

1. From: IT Support <it-alerts@support-sync.com>

2. To: jmartin@midriverhealth.org

3. Subject: Mandatory VPN Client Update

4. Date: Wed, 9 Apr 2025 18:57:01 -0400

5. Body: Please install the latest security update. https://support-sync.com/update

A9. SOC Alert Memo

1. 19:04:11 Alert Unusual VPN login – jmartin – SrcIP 203.0.113.45

2. 19:06:03 Alert HTTPS spike – 10.20.30.77 → cdn-docs.support-sync.com

3. 19:07:21 Case opened – Analyst S. Patel – Finance VLAN scope