

# SOC Investigation Report

## Data Exfiltration via RDP Compromise Incident

**Report ID:** INC-2025-XXXX

**Analyst:** Gregory Sewalt

**Date:** 9/21/2025

**Incident Date:** 14-September-2025

---

### 1. Findings

#### Key Indicators of Compromise (IOCs):

- **Attack Source IP:** 159.26.106.84
- **Compromised Account:** slflare
- **Malicious File:** msupdate.exe
- **Persistence Mechanism:** Scheduled task creation for automated payload execution post-intrusion ("MicrosoftUpdateSync"), Microsoft Defender folder scan exclusion for ongoing detection avoidance (C:\Windows\Temp)
- **C2 Server:** 185.92.220.87
- **Exfiltration Destination:** 185.92.220.87.8081













#### KQL Queries Used:

##### Query 1 - Initial Access Detection:

```
DeviceLogonEvents
| where ActionType has_any ("LogonFailed", "LogonSuccess")
| where isnotempty (RemoteIP)
| where DeviceName contains "flare"
| where Timestamp between (datetime(2025-09-13 00:00:00) ..
datetime(2025-09-16 23:59:59))
| project Timestamp, DeviceName, ActionType, AccountName, RemoteIP
| order by Timestamp asc
```

**Results:** The query yielded extensive failed logon attempts from 9/12 up to 12:53:53 AM on 9/13 before dropping off completely until 9/16. The first successful logon attempt on 9-16 originated from IP 159.26.106.84 from account “slflare” at 11:40:57 AM.

### Attachments:

<input type="checkbox"/> Timestamp	DeviceName	ActionType	AccountName	RemoteIP
<input type="checkbox"/> > Sep 13, 2025 12:37:16 AM	 slflarewinsysmo	LogonFailed	slflarewinsysmo	(  ) 79.76.123.251
<input type="checkbox"/> > Sep 13, 2025 12:53:53 AM	 slflarewinsysmo	LogonFailed	slflarewinsysmo	(  ) 79.76.123.251
<input type="checkbox"/> > Sep 16, 2025 11:35:09 AM	 slflarewinsysmo	LogonFailed	slflarewinsysmo	(  ) 79.76.123.251
<input type="checkbox"/> > Sep 16, 2025 11:36:55 AM	 slflarewinsysmo	LogonFailed	slflare	(  ) 159.26.106.84
<input type="checkbox"/> > Sep 16, 2025 11:38:33 AM	 slflarewinsysmo	LogonFailed	slflare	(  ) 159.26.106.84
<input type="checkbox"/> > Sep 16, 2025 11:40:57 AM	 slflarewinsysmo	LogonSuccess	slflare	(  ) 159.26.106.84

### Query 2 - Malicious Execution:

```
DeviceProcessEvents
| where Timestamp between (datetime(2025-09-16 11:40:57) ..
datetime(2025-09-16 23:59:59))
| where DeviceName == "slflarewinsysmo"
| where AccountName == "slflare"
| where FileName endswith ".exe"
| where FolderPath has_any ("Download", "Temp", "Public")
| project Timestamp, FileName, FolderPath, InitiatingProcessFileName
| order by Timestamp asc
```

**Results:** The query yielded execution logs for two specific files, DismHost.exe and msupdate.exe. While both are potentially suspicious, msupdate.exe, executed at 12:38:40 PM, is particularly suspect due to it being initiated in powershell with the following command: "msupdate.exe" -ExecutionPolicy Bypass -File C:\Users\Public\update\_check.ps1 . Both this and its file path are highly irregular for a legitimate MS Update process.

### Attachments:

<input type="checkbox"/> Timestamp	FileName	FolderPath	InitiatingProcessFileName	ProcessCommandLine
<input type="checkbox"/> > Sep 16, 2025 12:01:40 PM	DismHost.exe	C:\Users\SLFlare\AppData...	cleanmgr.exe	dismhost.exe [7358A319...
<input type="checkbox"/> > Sep 16, 2025 12:38:40 PM	msupdate.exe	C:\Users\Public\msupda...	powershell.exe	"msupdate.exe" -Executi...
<input type="checkbox"/> > Sep 16, 2025 12:46:30 PM	DismHost.exe	C:\Users\SLFlare\AppData...	cleanmgr.exe	dismhost.exe [A456061...
<input type="checkbox"/> > Sep 16, 2025 4:29:35 PM	DismHost.exe	C:\Users\SLFlare\AppData...	cleanmgr.exe	dismhost.exe [ED5C93E...

### Query 3 - Persistence Detection:

```
DeviceRegistryEvents
| where DeviceName == "slflarewinsysmo"
| where Timestamp between (datetime(2025-09-16 13:38:40) ..
datetime(2025-09-16 12:50:59))
| where RegistryKey startswith
@"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Schedule\TaskCache\Tree"
| where ActionType == "RegistryValueSet" or ActionType ==
"RegistryKeyCreated"
| project Timestamp, ActionType, RegistryKey
| order by Timestamp asc
```

**Results:** Querying for registry events consistent with newly registered scheduled tasks (registry key creation and/or registry values being set) within the tightened timeframe yielded two Registry Key Creations, only one of which occurred post-malicious execution from Step 2. This zeroed in on the associated Registry Key Creation event occurring at 12:39:45 PM. Examination of the Registry Key resulted in discovery of the name of the scheduled task: "MicrosoftUpdateSync".

### Attachments:

<input type="checkbox"/> Timestamp	ActionType	RegistryKey
<input type="checkbox"/> > Sep 16, 2025 11:46:44 AM	RegistryKeyCreated	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\OneDrive Standalone Update Task-S-1-5-21-41595212...
<input type="checkbox"/> > Sep 16, 2025 12:39:45 PM	RegistryKeyCreated	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\MicrosoftUpdateSync


☐ **Additional Evidence** - Any supporting materials

### Query 4 - Ongoing Detection Avoidance:

```
DeviceRegistryEvents
| where DeviceName == "slflarewinsymo"
| where Timestamp between (datetime(2025-09-16 19:39:45) ..
datetime(2025-09-16 23:59:59))
| where RegistryKey startswith
@"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths"
| where ActionType in ("RegistryValueSet", "RegistryKeyCreated")
| project Timestamp, DeviceName, RegistryKey, RegistryValueName,
RegistryValueData
| order by Timestamp asc
```

**Results:** Querying for any registry key creation or modifications consistent with Microsoft Defender folder exclusion resulted in a Registry Value Set event at 12:39:48 PM with the folder “C:\Windows\Temp” set to be excluded from future scans.

## Attachments:






<input type="checkbox"/> Timestamp	DeviceName	ActionType	RegistryKey	RegistryValueName	RegistryValueData
<input type="checkbox"/> > Sep 16, 2025 12:39:48 PM	 slflarewinsymo	RegistryValueSet	HKEY_LOCAL_MACHINE...	C:\Windows\Temp	0

## Query 5 - Host Enumeration:

```
DeviceProcessEvents
| where Timestamp between (datetime(2025-09-16 19:39:48) ..
datetime(2025-09-16 23:59:59))
| where DeviceName == "slflarewinsymo"
| where AccountName == "slflare"
| where FileName in ("cmd.exe", "powershell.exe", "wmic.exe", "net.exe",
"systeminfo.exe", "ipconfig.exe", "whoami.exe", "tasklist.exe")
| where ProcessCommandLine has_any ("systeminfo","ipconfig","net
user","net
localgroup","whoami","tasklist","Get-ComputerInfo","Get-WmiObject","Get-Ne
tIPConfiguration")
| project Timestamp, DeviceName, AccountName, FileName,
ProcessCommandLine, InitiatingProcessFileName,
InitiatingProcessCommandLine
| order by Timestamp asc
```

**Results:** Querying for any host enumeration commands being executed from built-in Windows tools used for enumeration yeilded numerous Process Events, the earliest being executed at 12:40:28 PM by “cmd.exe” from within powershell with the command “"cmd.exe" /c systeminfo.”

**Attachments:**





<input type="checkbox"/>	Timestamp	DeviceName	AccountName	FileName	ProcessCommandLine	InitiatingProcessFileName	InitiatingProcessCommandL...
<input type="checkbox"/>	> Sep 16, 2025 12:40:28 PM	 slflarewinsysmo	slflare	cmd.exe	"cmd.exe" /c systeminfo	powershell.exe	powershell.exe
<input type="checkbox"/>	> Sep 16, 2025 12:40:28 PM	 slflarewinsysmo	slflare	systeminfo.exe	systeminfo	cmd.exe	"cmd.exe" /c systeminfo
<input type="checkbox"/>	> Sep 16, 2025 12:40:34 PM	 slflarewinsysmo	slflare	cmd.exe	"cmd.exe" /c "whoami /...	powershell.exe	powershell.exe
<input type="checkbox"/>	> Sep 16, 2025 12:40:34 PM	 slflarewinsysmo	slflare	whoami.exe	whoami /all	cmd.exe	"cmd.exe" /c "whoami /...
<input type="checkbox"/>	> Sep 16, 2025 12:40:35 PM	 slflarewinsysmo	slflare	cmd.exe	"cmd.exe" /c "net user"	powershell.exe	powershell.exe

**Query 6 - Data Archive Creation for Exfiltration:**

```
DeviceFileEvents
| where Timestamp between (datetime(2025-09-16 19:40:28) ..
datetime(2025-09-16 23:59:59))
| where ActionType == "FileCreated"
| where DeviceName == "slflarewinsysmo"
| where FileName has_any (".zip", ".rar", ".7z", ".7zip")
| where FolderPath has_any ("Temp", "AppData", "ProgramData")
| order by Timestamp asc
```

**Results:** Querying for any File Creation events yielded two instances of compressed archive creation apparently intended for data exfiltration, the earliest being created at 12:41:30 PM named “backup\_sync.zip”, and a second at 1:49:43 PM named “employee-data-20250916204931.zip”.

**Attachments:**











<input type="checkbox"/>	Timestamp	DeviceId	DeviceName	ActionType	FileName	FolderPath
<input type="checkbox"/>	> Sep 16, 2025 12:41:30 PM	 401039d292f73a34a4...	 slflarewinsysmo	FileCreated	backup_sync.zip	C:\Users\SLFlare\AppData\Local\Temp\backup_sync.zip
<input type="checkbox"/>	> Sep 16, 2025 1:49:43 PM	 401039d292f73a34a4...	 slflarewinsysmo	FileCreated	employee-data-20250916204931.zip	C:\ProgramData\employee-data-20250916204931.zip

**Query 7 - External Server Connection and Data Exfiltration:**

```
DeviceNetworkEvents
| where Timestamp between (datetime(2025-09-16 19:41:30) ..
datetime(2025-09-16 23:59:59))
| where DeviceName == "slflarewinsysmo"
| where InitiatingProcessFileName in ("powershell.exe", "svchost.exe")
| where isnotempty(RemoteIP)
| project Timestamp, DeviceName, InitiatingProcessFileName, RemoteIP,
RemotePort, RemoteUrl, Protocol
| order by Timestamp asc
```

**Results:** Querying for any Network Events indicative of external connection yielded two back-to-back connections from IP address 185.92.220.87, one through port 80 at 12:42:17 PM, the other through port 8081 at 12:42:26 PM. The first event was determined to have established the connection with the remote server, and the second event, due to its use of port 8081 (commonly used for data exfiltration) was determined to be the actual data exfiltration.

**Attachments:**

<input type="checkbox"/>	Timestamp	DeviceName	InitiatingProcessFileName	RemoteIP	RemotePort	RemoteUrl	Protocol
<input type="checkbox"/>	> Sep 16, 2025 12:42:17 PM	 slflarewinsysmo	powershell.exe	 185.92.220.87	80		Tcp
<input type="checkbox"/>	> Sep 16, 2025 12:42:26 PM	 slflarewinsysmo	powershell.exe	 185.92.220.87	8081		Tcp
<input type="checkbox"/>	> Sep 16, 2025 12:46:50 PM	 slflarewinsysmo	svchost.exe	 23.215.0.49	443	 oneclient.sfx.ms	Tcp
<input type="checkbox"/>	> Sep 16, 2025 12:47:15 PM	 slflarewinsysmo	svchost.exe	 132.196.74.212	443	 fe2cr.update.microso...	Tcp

---

## 2. Investigation Summary

**What Happened:**

On 16-September-2025, an external threat actor originating from IP 159.26.106.84 successfully compromised the account **slflare** via RDP brute force attacks. The attacker deployed a malicious executable (**msupdate.exe**) and established persistence through a scheduled task named “MicrosoftUpdateSync” while excluding **C:\Windows\Temp** from Microsoft Defender scans. Sensitive data was compressed into archive files and exfiltrated to the remote server at 185.92.220.87 over port 8081.

**Attack Timeline:**

- **Started:** 12-September-2025 20:34:18 UTC (initial failed logon attempts)
- **Successful Compromise:** 16-September-2025 11:40:57 UTC
- **Malicious Execution:** 16-September-2025 12:38:40 UTC

- **Persistence Established:** 16-September-2025 12:39:45 UTC
- **Data Exfiltration:** 16-September-2025 12:42:26 UTC
- **Ended:** 16-September-2025 12:42:26 UTC (last confirmed malicious activity)
- **Duration:** Approximately 3 days from initial reconnaissance/failures; ~1 hour from compromise to data exfiltration
- **Impact Level:** High

### 3. Who, What, When, Where, Why, How

#### Who:

- **Attacker:** External threat actor, IP 159.26.106.84
- **Victim Account:** slflare
- **Affected System:** slflarewinsymo (internal hostname), 10.0.0.15
- **Impact on Users:** Potential exposure of sensitive corporate data; no indication of user disruption beyond account compromise

#### What:

- **Attack Type:** RDP brute force leading to system compromise and data exfiltration
- **Malicious Activities:**
  - Repeated failed logon attempts to gain access
  - Successful RDP logon using compromised credentials
  - Execution of malicious payload (`msupdate.exe`) via PowerShell
  - Creation of persistence mechanism via scheduled task ("MicrosoftUpdateSync")
  - Exclusion of `C:\Windows\Temp` from Microsoft Defender scans to evade detection
  - Host reconnaissance using `cmd.exe` and `powershell.exe` (systeminfo, ipconfig, tasklist, etc.)
  - Compression of sensitive files into zip archives for exfiltration
  - Data exfiltration to external C2 server at 185.92.220.87 over port 8081

#### When:

- **First Malicious Activity:** 13-September-2025 00:00:00 UTC (failed logon attempts)
- **Successful Compromise:** 16-September-2025 11:40:57 UTC
- **Last Observed Activity:** 16-September-2025 12:42:26 UTC (data exfiltration)
- **Detection Time:** 16-September-2025 13:00:00 UTC (SOC alert timestamp, assume near real-time)
- **Total Attack Duration:** Approximately 3 days from initial reconnaissance; ~1 hour from compromise to data exfiltration
- **Is it still active?** No

### Where:

- **Target System:** slflarewinsysmo, internal network
- **Attack Origin:** IP 159.26.106.84; geographic location undetermined (likely external)
- **Network Segment:** Corporate network (internal host)
- **Affected Directories/Files:**
  - C:\Users\Public\update\_check.ps1 (malicious script)
  - C:\Windows\Temp (exfiltrated files temporarily stored here)
  - Created archives: backup\_sync.zip, employee-data-20250916204931.zip

### Why (Intent/Motive):

- **Likely Motive:** Data theft for financial or competitive gain
- **Target Value:** The compromised account had access to sensitive corporate data, which was collected and exfiltrated

### How:

- **Initial Access Method:** RDP brute force using compromised credentials
  - **Tools/Techniques Used:**
    - PowerShell for payload execution and host reconnaissance
    - Windows built-in tools (cmd.exe, powershell.exe, wmic.exe, net.exe, systeminfo.exe, ipconfig.exe, whoami.exe, tasklist.exe)
    - Custom malicious executable (msupdate.exe)
  - **Persistence Method:** Scheduled task creation ("MicrosoftUpdateSync")
  - **Data Collection Method:** Compression of files into zip archives within C:\Windows\Temp
  - **Communication Method:** Outbound connections to external C2 server (185.92.220.87) via ports 80 and 8081
- 

## 4. Recommendations

### Immediate Actions Needed:

- Disable the compromised account slflare and enforce a password reset for all privileged accounts
- Isolate affected host (slflarewinsysmo) from the network for forensic analysis
- Terminate any running malicious processes (msupdate.exe)
- Remove scheduled task "MicrosoftUpdateSync" and any related artifacts



- Run full Microsoft Defender scan and any endpoint detection remediation on the affected host
- Monitor for any additional outbound connections to 185.92.220.87

#### **Short-term Improvements (1-30 days):**

- Enforce MFA for all RDP accounts and high-privilege accounts
- Implement geo-restrictions or IP allowlists for RDP access
- Review and tighten firewall and network segmentation for sensitive systems
- Conduct credential audits for other accounts that may have been reused

#### **Long-term Security Enhancements:**

- Deploy Endpoint Detection & Response (EDR) solutions with behavioral analysis for anomaly detection
- Implement robust logging and monitoring for scheduled task creation and Defender exclusions
- Establish regular penetration testing and red-team exercises focusing on remote access vectors
- Conduct user awareness training on password hygiene and phishing resistance

#### **Detection Improvements (Optional):**

- **Monitoring Gaps Identified:** Lack of alerting on unusual Defender exclusions, scheduled task creation, and mass file archiving
- **Recommended Alerts:**
  - Alert on new scheduled task creation under unusual names
  - Alert on changes to Defender exclusions
  - Alert on creation of zip archives in sensitive directories (**Temp**, **AppData**, **ProgramData**)
- **Query Improvements:** Refine KQL queries to correlate RDP logins with subsequent process executions and network connections for faster detection

**Report Status:** Complete

**Next Review:** 9/29/2025

**Distribution:** Cyber Range