

RAPORT Z ANALIZY LOGÓW W SIEM

Analiza podejrzanego połączenia sieciowego i mechanizmu persistence w SIEM

Celem analizy było:

- zidentyfikowanie źródła i charakteru połączenia,
- ustalenie procesu odpowiedzialnego za ruch sieciowy,
- sprawdzenie potencjalnych mechanizmów persistence,
- ocena ryzyka i wpływu na środowisko.

Practice Scenario

You are an SOC Level 1 Analyst on shift and have received an alert indicating a suspicious network connection using port 5678 on the WIN-105 host. Your task is to conduct an investigation and determine whether this activity is suspicious.

The logs for this task are located in the Splunk index task4. Use the following query:

```
index=task4
```

Splunk Enterprise

Apps

SearchAnalyticsDatasetsReportsAlertsDashboards

New Search

1 index="task4" "ComputerName=WIN-105" DestinationPort=5678

✓ 1 event (before 15/02/2026 08:19:21.000) No Event Sampling

Events (1)PatternsStatisticsVisualization

Timeline formatZoom OutZoom to SelectionDeselect

FormatShow: 20 Per PageView: List

Hide FieldsAll Fields

+ Extract New Fields

	Time	Event
✓	14/08/2025 11:10:24 AM 11:10:24.000	08/14/2025 11:10:24 AM ... 1 line omitted ... EventCode=3 EventType=4 ComputerName=WIN-105 User=NOT_TRANSLATED Show all 33 lines

Event Actions

Type	Field	Value
Selected	DestinationPort	5678
	host	WIN-105
	source	WinEventLog:Microsoft-Windows-Sysmon/Operational
	sourcetype	WinEventLog
Event	ComputerName	WIN-105
	DestinationHostname	ip-10-10-114-80.eu-west-1.compute.internal
	DestinationIp	10.10.114.80

Time	Event
	<input type="checkbox"/> DestinationHostname ip-10-10-114-80.eu-west-1.compute.internal <input type="checkbox"/> DestinationIp 10.10.114.80 <input type="checkbox"/> DestinationIpv6 false <input type="checkbox"/> DestinationPortName rrac <input type="checkbox"/> EventCode 3 <input type="checkbox"/> EventType 4 <input type="checkbox"/> Image C:\Windows\Temp\SharePoint.exe <input type="checkbox"/> Initiated true <input type="checkbox"/> Keywords None <input type="checkbox"/> LogName Microsoft-Windows-Sysmon/Operational <input type="checkbox"/> Message Network connection detected: RuleName: - UtcTime: 2025-08-14 11:10:21.430 ProcessGuid: {c5d2b969-c41e-689d-dc02-000000002101} ProcessId: 1460 Image: C:\Windows\Temp\SharePoint.exe User: WIN-105\Ben Foster Protocol: tcp Initiated: true SourceIpv6: false SourceIp: 10.10.61.100 SourceHostname: WIN-105.eu-west-1.compute.internal SourcePort: 49798 SourcePortName: - DestinationIpv6: false DestinationIp: 10.10.114.80 DestinationHostname: ip-10-10-114-80.eu-west-1.compute.internal DestinationPort: 5678 DestinationPortName: rrac <input type="checkbox"/> OpCode Info <input type="checkbox"/> ProcessGuid {c5d2b969-c41e-689d-dc02-000000002101} <input type="checkbox"/> ProcessId 1460 <input type="checkbox"/> Protocol tcp <input type="checkbox"/> RecordNumber 7469 <input type="checkbox"/> RuleName - <input type="checkbox"/> Sid S-1-5-18 <input type="checkbox"/> SidType 0 <input type="checkbox"/> SourceHostname WIN-105.eu-west-1.compute.internal <input type="checkbox"/> SourceIp 10.10.61.100 <input type="checkbox"/> SourceIpv6 false <input type="checkbox"/> SourceName Microsoft-Windows-Sysmon <input type="checkbox"/> SourcePort 49798 <input type="checkbox"/> SourcePortName - <input type="checkbox"/> TaskCategory Network connection detected (rule: NetworkConnect) <input type="checkbox"/> Type Information <input type="checkbox"/> User NOT_TRANSLATED

Alert został wygenerowany na podstawie logów sieciowych pochodzących z Sysmon (zdarzenia Network Connection). Nietypowy był zarówno **port docelowy**, jak i fakt, że połączenie odbywało się **wewnątrz sieci LAN**.

Odnaleziony adres IP jest z grupy prywatnych. Oznacza to że połączenie zostało nawiązane m.in. poprzez: VPN, proxy lub z endpointu w tej samej sieci.

Analiza połączenia sieciowego

Zawężono zakres wyszukiwania do konkretnego hosta oraz portu docelowego.

Wynik analizy:

- Host źródłowy: 10.10.61.100
- Host docelowy: 10.10.114.80
- Połączenie: internal → internal (ta sama sieć)

Fakt, że komunikacja odbywała się pomiędzy dwoma hostami w tej samej sieci, **znacząco podnosi poziom ryzyka**, ponieważ może oznaczać, że atakujący:

- posiada już dostęp do środowiska,
- próbuje rozszerzyć kontrolę na kolejne endpointy. (tzw. Lateral Movement – ruch boczny)

Identyfikacja procesu inicjującego połączenie

Analiza **procesu, który zainicjował ruch sieciowy** wykazała, że połączenie zostało nawiązane przez plik:

C:\Windows\Temp\SharePoint.exe

Obserwacje:

- Nietypowa lokalizacja (folder Temp).
- Nazwa sugerująca legalną aplikację Microsoft SharePoint, jednak zawierająca **literówkę**.
- Brak zgodności z typowymi ścieżkami instalacyjnymi legalnych komponentów systemowych.

Na tej podstawie proces został zaklasyfikowany jako **wysoko podejrzany**.

The screenshot shows a Splunk search interface with the following search query: `index="task4" "ComputerName=WIN-105" DestinationPort=5678`. The results table shows one event from 2025-08-14 11:18:24. The process name is 'Office365 Install', the computer name is 'WIN-105', the destination IP is '10.10.114.80', the destination port is '5678', and the image path is 'C:\Windows\Temp\SharePoint.exe'.

Analiza pliku i reputacji

Znajomość hashu wywołanego procesu jest kluczowa w dziedzinie cyberbezpieczeństwa. Działa on jak unikalny cyfrowy odcisk palca konkretnej wersji pliku.

- Na przykład: Pozwala natychmiast sprawdzić, czy działający proces jest znanym wirusem, trojanem lub innym zagrożeniem. Bazy danych takie jak VirusTotal przechowują hashe milionów szkodliwych plików, umożliwiając ich błyskawiczne wykrycie. Antywirusy porównują hashe, dzięki czemu są w stanie zapobiec kompromitacji systemu.
- Dzięki hashowi można także potwierdzić, że uruchomiony program jest oryginalny i nie został zmodyfikowany przez napastnika (np. wstrzyknięcie kodu do legalnego pliku system32).

Dla zidentyfikowanego procesu pozyskano metadane oraz skróty kryptograficzne (w tym MD5).

The screenshot shows a Splunk search interface with the following search query: `index="task4" "ComputerName=WIN-105" "C:\Windows\Temp\SharePoint.exe"`. The results table shows multiple events. The first event is from 2025-08-14 11:18:22, with the command line `"C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\Temp\SharePoint.exe`. The second event is from 2025-08-14 11:18:22, with the command line `"C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\Temp\SharePoint.exe`. The third event is from 2025-08-14 11:18:24, with the command line `"C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\Temp\SharePoint.exe`. The fourth event is from 2025-08-14 11:11:57, with the command line `schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\System32\schtasks.exe`. The fifth event is from 2025-08-14 11:14:17, with the command line `schtasks /create /sc onlogon /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe" /ru "Ben Foster"` and the image path `C:\Windows\System32\schtasks.exe`. The sixth event is from 2025-08-14 11:14:39, with the command line `"C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\Temp\SharePoint.exe`. The seventh event is from 2025-08-14 11:15:08, with the command line `cmd.exe` and the image path `C:\Windows\System32\cmd.exe`. The eighth event is from 2025-08-14 11:15:09, with the command line `schtasks /create /sc once /at 15:30 /tn "Office365 Install" /tr "C:\Windows\Temp\SharePoint.exe"` and the image path `C:\Windows\System32\schtasks.exe`.

Hash pliku został wykorzystany do weryfikacji reputacji w publicznych bazach zagrożeń (m.in. VirusTotal).

Nie został on dopasowany do znanych próbek.

Nie wyklucza to złośliwego charakteru pliku.

Wnioski:

- Brak detekcji **nie oznacza bezpieczeństwa**.
- Plik może być:
 - malware typu **FUD (Fully Undetectable)**,
 - narzędziem stworzonym specjalnie pod dany atak (custom payload).

W połączeniu z nietypową lokalizacją i zachowaniem sieciowym, plik należy traktować jako **złośliwy**.

Analiza persistence

Dalsza analiza logów wykazała utworzenie **zaplanowanego zadania systemowego** o nazwie:

Office365 Install

Znaczenie:

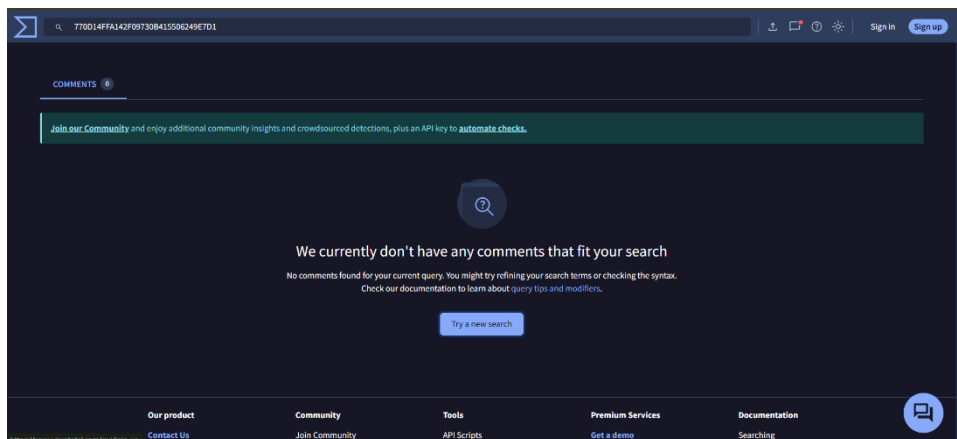
- Zaplanowanie zadania systemowego sugeruje legalne działanie administracyjne.
- Zadanie zostało powiązane czasowo z uruchomieniem podejrzanego procesu.
- Jest to klasyczny mechanizm **utrzymania dostępu (persistence)**

Ocena incydentu

Klasyfikacja: High Severity

Uzasadnienie:

- Podejrzany proces imitujący legalne oprogramowanie,
- Nawiązanie połączenia sieciowego wewnątrz LAN,
- Wykryty mechanizm persistence,
- Ryzyko lateral movement.



Rekomendowane działania (Response)

1. Natychmiastowa izolacja hosta 10.10.61.100.
2. Usunięcie zaplanowanego zadania i podejrzanego pliku.
3. Reset poświadczeń użytkownika powiązanego z hostem.
4. Przeskanowanie środowiska pod kątem:
 - podobnych nazw plików,
 - analogicznych zaplanowanych zadań,
 - komunikacji na port 5678.
5. Utworzenie reguły detekcyjnej w SIEM dla:
 - procesów uruchamianych z katalogu Temp,
 - nazw imitujących produkty Microsoft.

Podsumowanie

Analiza wykazała, że pojedynczy alert sieciowy może prowadzić do wykrycia **pełnego łańcucha ataku**, obejmującego:

- uruchomienie złośliwego procesu,
- komunikację sieciową,
- mechanizm persistence.

Case potwierdza znaczenie korelacji logów sieciowych i procesowych oraz pokazuje praktyczne podejście do analizy incydentów w środowisku SIEM.

Refleksja

W trakcie analizy:

- przećwiczyłam identyfikację **procesów podszywających się pod legalne oprogramowanie (masquerading)** na podstawie nazwy pliku, jego lokalizacji oraz obserwowanego zachowania,
- potwierdziłam, że **brak detekcji hasha w bazach reputacyjnych nie oznacza braku zagrożenia**, a ocena pliku musi uwzględniać kontekst jego działania oraz powiązania z innymi zdarzeniami,
- przeanalizowałam na rzeczywistych logach **typowe mechanizmy utrzymania dostępu (persistence)**, w szczególności wykorzystanie zaplanowanych zadań systemowych jako metody zapewnienia ponownego dostępu do systemu.