Przykładowa analiza incydentu phishingowego (SOC Simulator – TryHackMe)

Niniejszy dokument przedstawia przykładowe analizy incydentów phishingowych wykonane w środowisku SOC Simulator na platformie TryHackMe. Analizy obejmują zarówno przypadek skutecznie zablokowanego ataku, jak i incydent wymagający eskalacji po interakcji użytkownika z phishingową infrastrukturą. Celem jest zaprezentowanie procesu triage, klasyfikacji oraz reagowania na incydenty phishingowe.

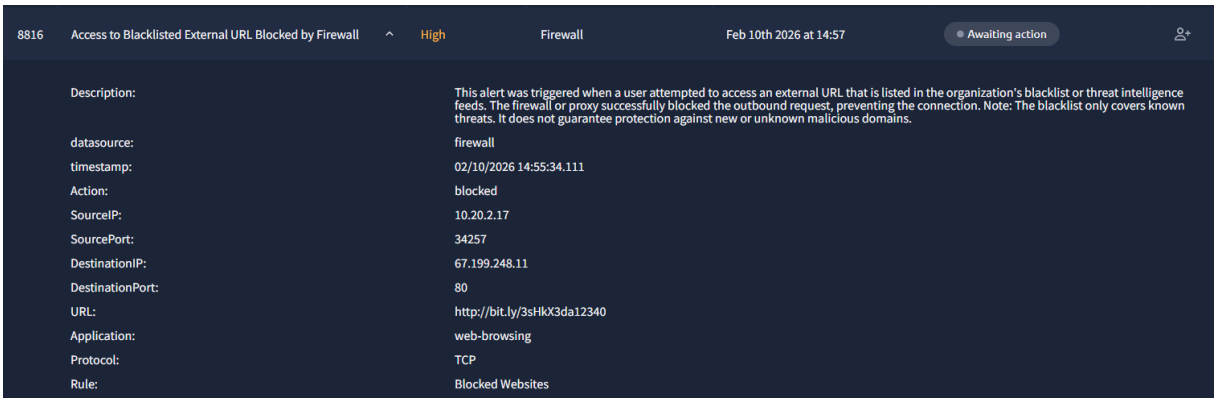
PRZYKŁAD 1

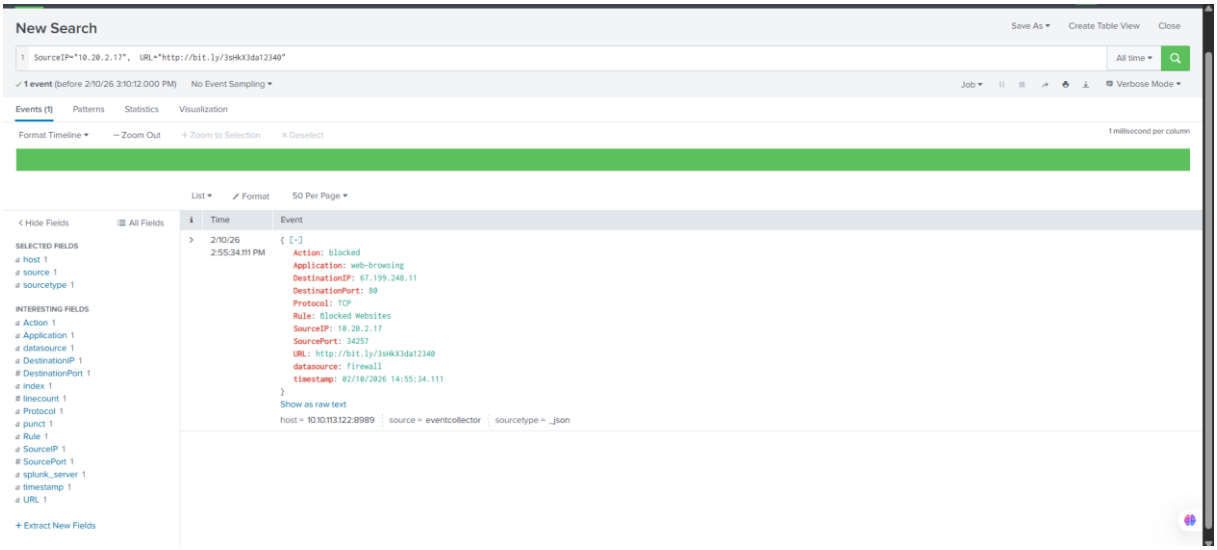
Phishing (True Positive, Prevented)

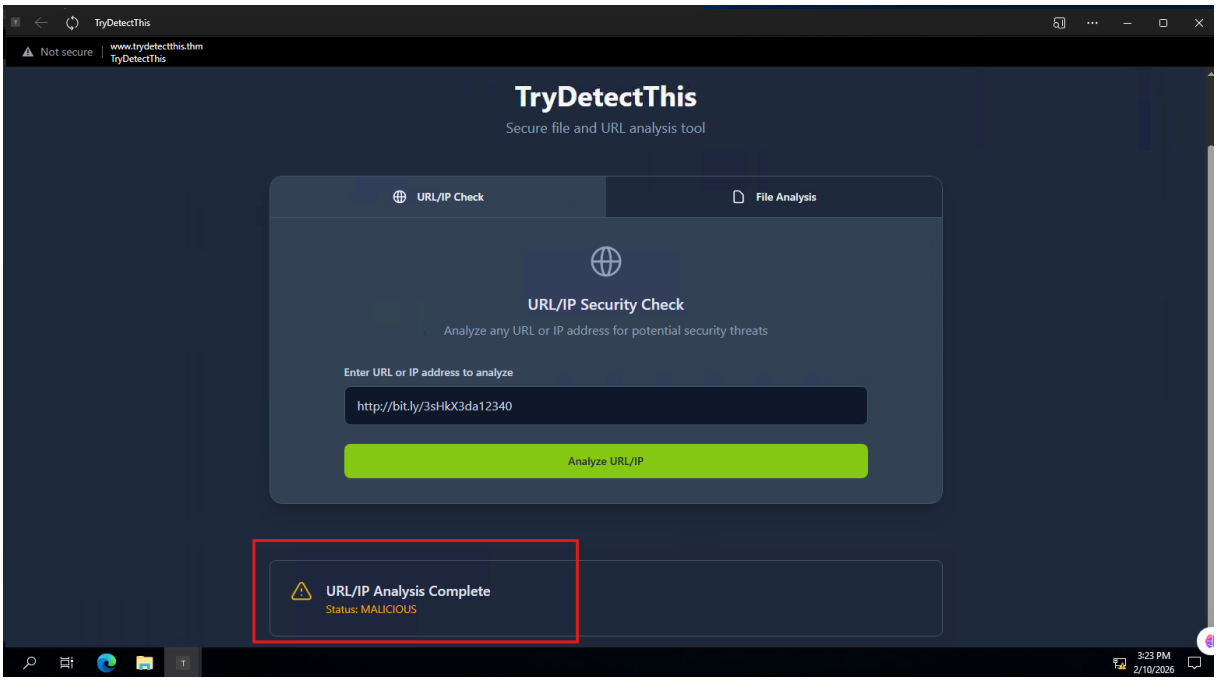
Alert ID: 8816
Alert Name: Access to Blacklisted External URL Blocked by Firewall
Severity: High
Data Source: Firewall

Time of activity

- 02/10/2026 14:55:34.111 – zarejestrowane zdarzenie firewall







Lista dotkniętych podmiotów:

- Endpoint użytkownika: 10.20.2.17
- Kontrola bezpieczeństwa: Firewall

Powód klasyfikacji jako True Positive

Użytkownik kliknął w niebezpieczny link zawarty w wiadomości phishingowej: hxxp[://]bit[.]ly/3sHkX3da12340

Firewall wygenerował alert „Access to Blacklisted External URL Blocked by Firewall”, potwierdzając, że URL znajdował się na liście zablokowanych adresów (blacklist / threat intelligence feed).

Połączenie wychodzące z hosta 10.20.2.17 do adresu IP 67.199.248.11 (port 80, TCP, web-browsing) zostało skutecznie zablokowane, co zapobiegło nawiązaniu połączenia oraz potencjalnej infekcji.

Ocena wpływu

• Interakcja użytkownika: Tak (kliknięto link)

• Połączenie wychodzące: Próba – Zablokowane

• Uruchomienie złośliwego oprogramowania: Nie

• Wyciek danych: Nie

• Naruszenie systemu: Nie

Eskalacja nie jest wymagana.
Zdarzenie zostało zatrzymane na poziomie sieciowym przez regułę „Blocked Websites”, a żadne oznaki kompromitacji endpointa nie zostały zaobserwowane.

Zalecane działania naprawcze

- Przypomnienie użytkownikowi zasad phishing awareness
- Utrzymanie IOC (URL/IP) na listach blokujących

Nie są wymagane żadne dalsze działania naprawcze, ponieważ w pełni zapobiegnięto icydentowi.

Lista wskaźników ataku (IOC)

- Złośliwy adres URL: hxxp[://]bit[.]ly/3sHkX3da12340
- Docelowy adres IP: 67.199.248.11
- Źródłowy adres IP (punkt końcowy): 10.20.2.17
- Protokół/Port: TCP/80
- Aplikacja: przeglądanie stron internetowych
- Reguła zapory sieciowej: Zablokowane witryny

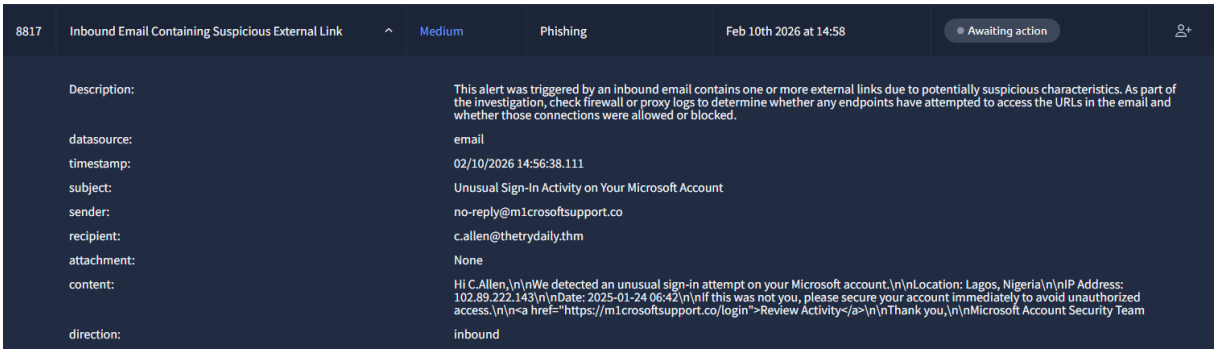
Wnioski końcowe

- Incydent został poprawnie sklasyfikowany jako **True Positive (phishing)** z potwierdzoną interakcją użytkownika.
- Złośliwy URL znajdował się na **blacklist / threat intelligence feed**, co umożliwiło jego skuteczne wykrycie.
- Połączenie wychodzące z hosta użytkownika zostało **zablokowane na poziomie firewalla**, zapobiegając infekcji oraz naruszeniu bezpieczeństwa.
- Nie zaobserwowano uruchomienia malware, eksfiltracji danych ani kompromitacji systemu.
- Mechanizmy ochronne zadziałały zgodnie z założeniami, dlatego **eskalacja oraz dalsze działania naprawcze nie były wymagane**.
- Incydent potwierdza skuteczność kontroli sieciowych oraz znaczenie świadomości użytkowników w kontekście ataków phishingowych.

PRZYKŁAD 2

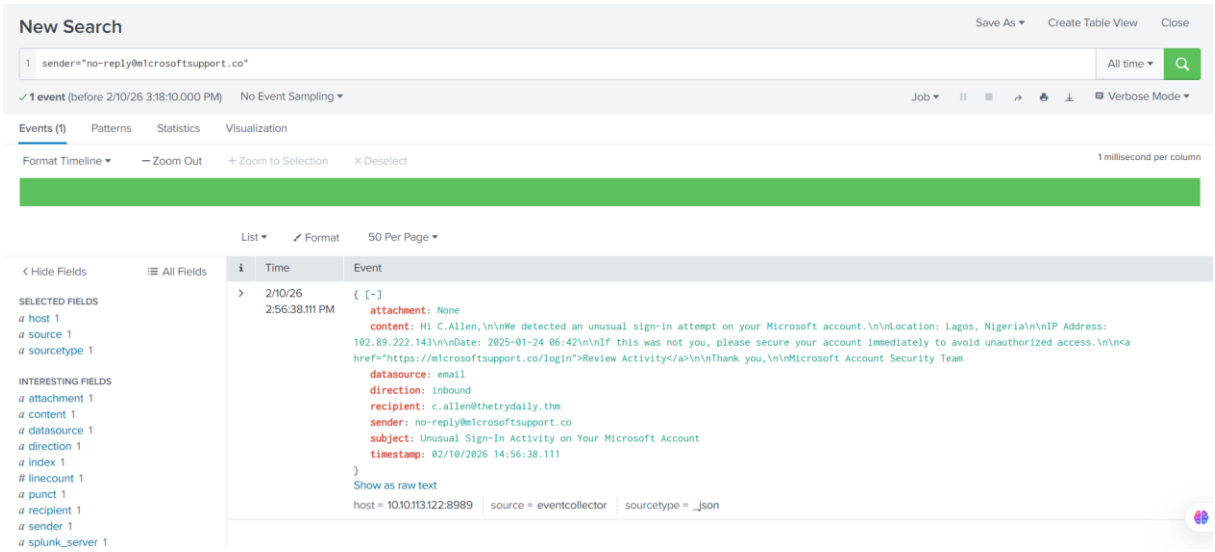
Incident Report – Phishing Email (True Positive, Escalated)

Alert ID: 8817
Alert Name: Inbound Email Containing Suspicious External Link
Severity: Medium
Category: Phishing
Data Source: Email

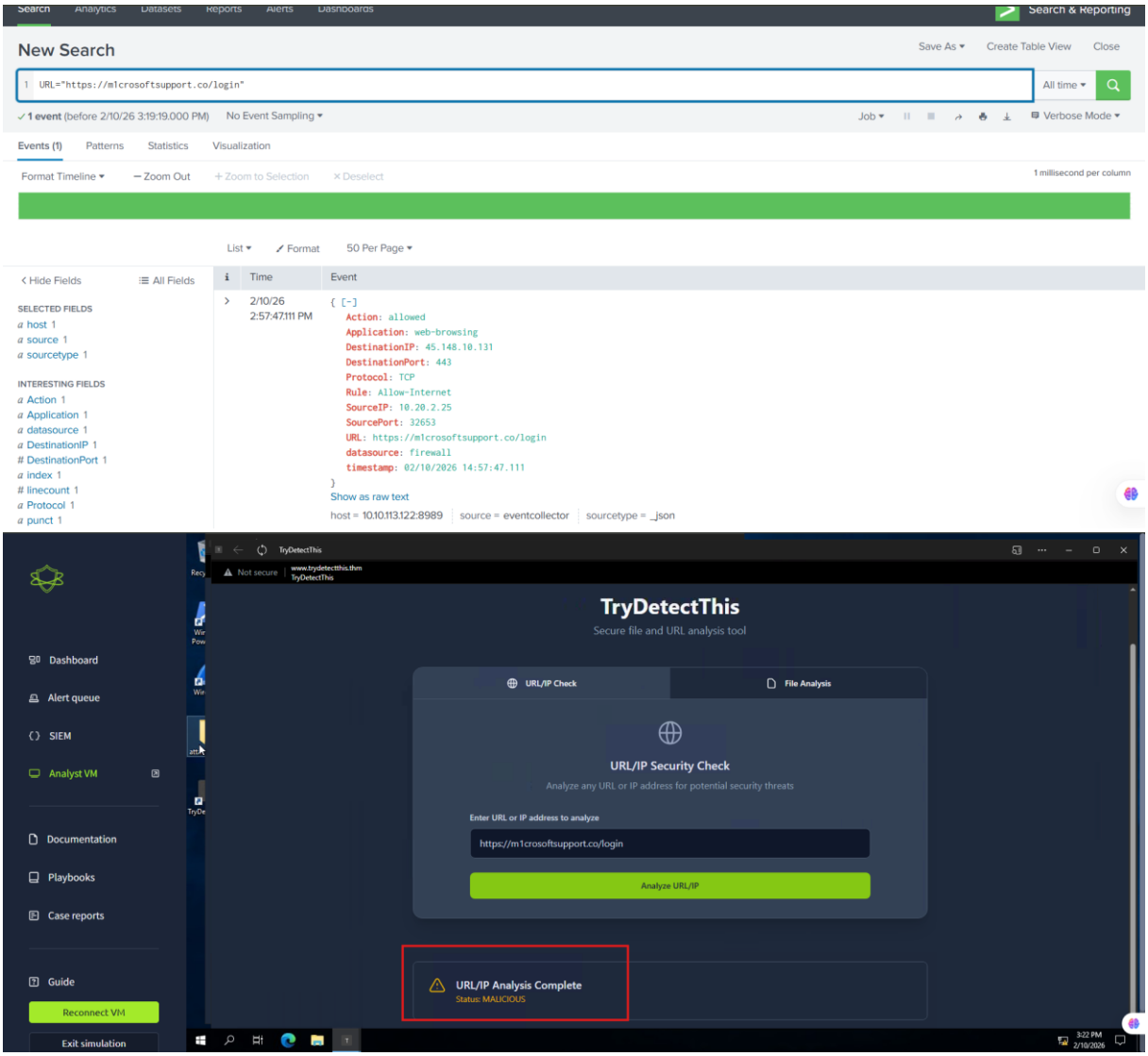


Time of Activity

- **Email received:** 02/10/2026 14:56:38.111



- **User interaction (link click):** 02/10/2026 10:10:35.959



Lista dotkniętych podmiotów:

- **Użytkownik:** c.allen@thetrydaily.thm
- **Endpoint:** 10.20.2.25

Powód klasyfikacji jako True Positive

Użytkownik **c.allen@thetrydaily.thm** otrzymał przychodzącą wiadomość e-mail od nadawcy **no-reply@m1crosoftsupport[.]co**, podszywającego się pod firmę Microsoft.

Wiadomość wykorzystywała techniki **social engineering** (informacja o nietypowym logowaniu, presja czasu) i zawierała zewnętrzny link prowadzący do fałszywej strony logowania: **hxxps[://]m1crosoftsupport[.]co/login**

Analiza logów potwierdziła, że użytkownik **kliknął w link**, a host **10.20.2.25** nawiązał połączenie z podejrzaną stroną o adresie IP **45.148.10.131**, co potwierdza rzeczywistą interakcję z phishingową infrastrukturą.

Ocena wpływu

- Interakcja użytkownika: Tak (kliknięto link)
- Dostęp do witryny phishingowej: Tak
- Krycie danych uwierzytelniających: Niepotwierdzone
- Dostarczenie złośliwego oprogramowania: Nie zaobserwowano
- Krycie systemu: Niepotwierdzone

Powód eskalacji alertu

Wymagana eskalacja.
Użytkownik uzyskał dostęp do phishingowej strony logowania, co stwarza potencjalne ryzyko przejęcia danych uwierzytelniających i wymaga dalszych działań zapobiegawczych.

Zalecane działania naprawcze

- Zablokować nadawcę: **no-reply@m1crosoftsupport[.]co**
- Zablokować domenę i URL w mechanizmach bezpieczeństwa sieciowego
- **Zresetować hasło** dla użytkownika (prewencyjnie)
- Uświadomić użytkownika w zakresie **phishingu**
- Monitorować logi pod kątem prób nieautoryzowanego logowania

---

Wskaźniki zagrożenia [Indicators of Compromise (IOCs)]

- **Nadawca:** no-reply@m1crosoftsupport[.]co
- **Złośliwy adres URL:** hxxps[://]m1crosoftsupport[.]co/login
- **Docelowy IP:** 45.148.10.131
- **Użytkownik:** c.allen@thetrydaily.thm
- **Endpoint:** 10.20.2.25

Status incydentu:

Otwarty – eskalowane w celu dalszego monitorowania i działań zapobiegawczych

---

Podsumowanie końcowe

Przedstawione analizy pokazują dwa scenariusze incydentów phishingowych w symulowanym środowisku SOC (TryHackMe SOC Simulator): jeden przypadek skutecznie zablokowany przez mechanizmy sieciowe, drugi wymagający eskalacji po interakcji użytkownika z podejrzanym linkiem.

Celem ćwiczenia było:

- Praktyczne stosowanie procedur **triage i klasyfikacji incydentów**,
- Analiza logów firewalla i systemu pocztowego,
- Identyfikacja **IOC (Indicators of Compromise)** i ocena ryzyka,
- Proponowanie odpowiednich działań naprawczych i prewencyjnych.

Analizy te demonstrują zrozumienie procesów **SOC**, umiejętność reagowania na incydenty oraz znaczenie połączenia kontroli technicznych i świadomości użytkowników w ograniczaniu skutków ataków phishingowych.