Phishing – c.allen – 08/07/2025

Caso conduzido individualmente no simulador SOC da plataforma TryHackMe. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, contenção e relatório.

Descrição:

Recebido alerta referente a um e-mail de phishing enviado ao usuário c.allen@thetrydaily.thm. O e-mail utilizava typosquatting no domínio (m1crosoftsupport.co) para simular comunicações legítimas da Microsoft, com o objetivo de capturar credenciais. O usuário acessou o link malicioso contido no e-mail.

Entidades afetadas:

- Usuário: c.allen@thetrydaily.thm
- SourceIP: 10.20.2.25

Análise:

- A análise inicial no Splunk confirmou o recebimento do e-mail e identificou que o link foi acessado pelo host 10.20.2.25, com tráfego permitido pelo firewall.
- IP de destino era 45.148.10.131.
- Consultas nas plataformas de threat intelligence indicaram que o domínio m1crosoftsupport.co ainda não constava em listas de reputação, mas o IP de destino (45.148.10.131) foi identificado como malicioso pelo VírusTotal.
- O domínio "m1crosoftsupport.co" é um caso clássico de typosquatting, se passando por um domínio legítimo da Microsoft com uma variação sutil no nome (trocando “i” por “1”).
- Como a comunicação foi permitida e o domínio é suspeito, foi classificado como um True Positive.

Ação tomada:

- Alerta classificado como True Positive
- Acesso confirmado nos logs; nenhum bloqueio identificado
- Potencial comprometimento considerado para investigação adicional
- Comunicado registrado no sistema de alertas e enviado ao time de resposta

Escalonamento:

O incidente foi escalado ao time N2 para investigação de possível comprometimento e ações corretivas.

Recomendações:

- Bloqueio do domínio m1crosoftsupport.co no firewall/proxy
- Verificação no host 10.20.2.25 por sinais de comprometimento
- Reset de credenciais do usuário

- Alerta ao usuário
- Revisão da política de filtragem de e-mails com typosquatting

Evidências/IOC:

Type	Value	Description
Domain	m1crosoftsupport.co	Typosquatting domain
IP	45.148.10.131	Destination IP
URL	https://m1crosoftsupport.co/login	Phishing login page
Sender	no-reply@m1crosoftsupport.co	Fake Microsoft sender