Phishing – h.harris – 08/07/2025

Caso conduzido individualmente no simulador SOC da plataforma TryHackMe. Atuei como analista SOC N1, realizando todas as etapas de triagem, investigação, verificação de reputação, correlação de eventos e documentação final.

📝 Descrição:

Recebido alerta referente a um e-mail de phishing enviado ao usuário h.harris@thetrydaily.thm com o assunto:
"Your Amazon Package Couldn't Be Delivered – Action Required".

O remetente urgents@amazon.biz utilizava typosquatting, simulando a Amazon para induzir o usuário a clicar em um link encurtado malicioso: hxxp://bit.ly/3shKx3da12340

🔑 Entidades afetadas:

- Usuário: h.harris@thetrydaily.thm
- SourceIP (host): 10.20.2.17

🧠 Análise:

A investigação inicial no Splunk confirmou que o usuário clicou no link presente no e-mail de Phishing. O tráfego foi registrado nos logs de proxy/firewall, mostrando uma tentativa de conexão ao IP 67.199.248.11, via protocolo HTTP (porta 80).

A tentativa de acesso foi bloqueada pela política de firewall, impedindo que o conteúdo fosse carregado.

O domínio do remetente (amazon.biz) é um typosquatted domain, com aparência similar ao legítimo amazon.com, mas sem relação com a empresa verdadeira.

O IP de destino (67.199.248.11) foi posteriormente analisado no VirusTotal e identificado como malicioso por múltiplos motores, associado a campanhas de phishing e domínios de redirecionamento.

Dessa forma, mesmo com a contenção, o alerta foi corretamente classificado como True Positive, pois houve interação com um conteúdo malicioso real.

🛠️ Ação tomada:

- Alerta classificado como True Positive
- Conexão maliciosa bloqueada pelo firewall
- Usuário acessou o link, porém sem carga de conteúdo confirmada
- Caso documentado e encerrado sem escalonamento, conforme playbook

Escalonamento:

Não foi necessário escalar, pois:
- O acesso ao IP foi bloqueado automaticamente.
- Nenhum conteúdo foi baixado.
- Nenhum processo ou execução adicional foi detectado.

Recomendações:

- Reforçar campanhas de conscientização contra phishing
- Monitorar reincidência de links encurtados e domínios falsos
- Acompanhar comportamento do host 10.20.2.17 nas 24h seguintes

Evidências/IOC:

Type	Value	Description
Domain	amazon.biz	Typosquatting domain
IP	67.199.248.11	Malicious destination IP
URL	hxxp://bit.ly/3shKx3da12340	Phishing redirect
Sender	urgents@amazon.biz	Fake Amazon sender