セキュリティあるあるLT

Security.any #01

hogehuga
脆弱性対応勉強会

本発表について

短いネタを複数開示します。 基本的に特定可能な情報はないので、ご自由に取り扱いください。

この資料は `TLP：GREEN` としています。

TLP v2

- TRAFFIC LIGHT PROTOCOL (TLP)
  - https://www.first.org/tlp/docs/v2/tlp-v2_ja.pdf
- 機密となりうる情報の広範な共有と、より効果的な連携の促進を目的に作られた。
  - TLP:RED
    - 受信者個人の目と耳に向けた共有に限られ、その先の公開はない。
  - TLP:AMBER
    - 限定公開、…Need to know の原則に基づき、…共有できる。
  - TLP:GREEN
    - 限定公開、情報の受信者はコミュニティ内に情報を共有できる。
  - TLP:CLEAR
    - 情報の受信者は、全世界に向けて情報を共有できる。公開に制限はない。

whoami

hogehuga

- Work: 脆弱性管理、セキュリティコンサルタント、研究員(?)
- Private: 脆弱性対応勉強会 主催者
- 発表履歴
  - Hardening Designers Conference2024
  - InternetWeek Shocase福岡
  - InternetWeek2024
  - NCA Annual Conference2024
  - etc
- 水風呂、バイク(VTwinMagna,ADV160,JC92GROM)、戦場の絆(サ終)、etc

セキュリティあるある、ショートショート

きょうのお品書き

1項 1-2分以下の時間しかありません。

- Case.1 転職初日に遮断される
- Case.2 誤送信を指摘したのに
- Case.3 フィッシング訓練で他人を釣る
- Case.4 フィッシング調査でミイラ取りが…

Case.1 転職初日に遮断される

概要

- 私、2024-07-01に転職しました。初出社です。
- 昼頃に、転職先で業務用にノートPCを貸与されました。
- 夕方ごろに、突然ネットワーク切断され、要注意人物にマークされました(?)

解説

- 社内ネットワークはどうなってるか、知りたいよね？
  - install Ubuntu.WSL2, nmap etc...
  - ラテラルムーブメント検出用のIPを弄繰り回してしまった...
    - 確かに、環境を知るために攻撃者のような動きはしました...
  - 何か検知した☞EDRで不正規な挙動検知した☞ごめんなさい🙇☞許す(回復)

Case.2 誤送信を指摘したのに

概要

- ある日、見知らぬ送信元からメールが来ていた。誰よ？
- 中を見ると、何らかの巨大プラントの設計図(物理/ネットワーク)などだった。
- 「同じ苗字のだれかと間違えて誤送信してね？」と送信者に伝えたら、「間違いならそうだろう。消去するように。」と言われて、以降メールが来なくなった。

解説

- 誤送信者のみに連絡したので、他の人はたぶん知らないままで、漏洩が隠蔽されたのでは...
- えっなんで上から目線なの？と思ったけど、こっちは会社名を背負っているので耐えた。CC先にバレて怒られてほしい。

Case.3 フィッシング訓練で他人を釣る

概要

- 会社のフィッシング訓練メールが来てました。そんなの一目で分かるじゃん。
- リンクURLが社員番号みたいだね。見知らぬ引数あるけど、書き換えてsubmit。
- 無事、フィッシングURLに引っ掛かったとして、再教育の羽目になりました。

解説

- 引っかかって踏むURLが、難読化(?)された何かと、社員を特定するIDっぽいものでした。
- 書き換えたらいけるかな、と思ったら、難読化されている方に詳細があったみたいです。
- 無事、3連続フィッシングに引っかかった人、になりました。

Case.4 フィッシング調査でミイラ取りが...

概要

- iPhoneのキャリアメール(@i.softbank.jp)に、流行りのフィッシングメールが来ました。
- 調査用に複数来てくれたらいいなぁ、と思いつつリンク先にアクセスしました。
- 無事、1日50通以上着弾するようになりました(キャリアメールもう使えないよ)

解説

- ちゃんと、調査用に作ったアカウントでやらないと、フィッシングメールまみれでメールが使えなくなります...
  - jp-t.ne.jp☞t.vodafone.ne.jp☞i.softbank.jpと引きついでたアカウントだったのに...

まとめ

以上、あるあるでした。

皆様におかれましても、いろいろ気を付けましょう。

- 自社のネットワーク構成、自分で調べちゃだめよ？
- 誤送信の指摘、送信者だけでよい？
- 他人に成りすましてフィッシングを食らっちゃだめよ？
- 調査用アカウントの利用は計画的に。