CHECK POINT

セキュリティレポート

2024.3

Check Point SMB

YOU DESERVE THE BEST SECURITY

脆弱性を利用したマルウェア感染増

情報セキュリティ10大脅威 2024

脆弱性からの感染増

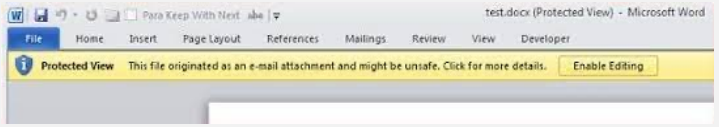
脆弱性及びパッチについて

チェック・ポイント・リサーチは、#MonikerLink（CVE-2024-21413）と呼ばれるMicrosoft Outlookのリモート・コード実行（RCE）の脆弱性を発見しました。

Microsoftは2月のパッチ・チューズデーでこの脆弱性に対処をしております。

この欠陥により、リモートの攻撃者は、Protected View プロトコルをバイパスする悪意のあるリンクを展開することが可能となり、認証情報の漏洩やRCE機能につながる可能性があります。

保護ビューとは

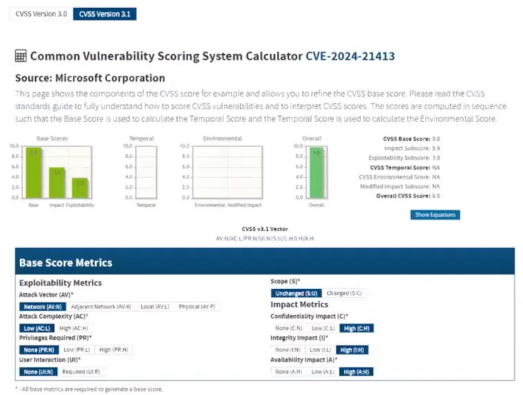


保護ビューは、セキュリティ上、安全でないとみなされるファイルを開く際に適用されるセキュリティ機能です。

保護ビューは、主に安全でないファイルを開く際に発生するセキュリティ機能であり、外部からのデータや悪意のあるコードが含まれている可能性がある場合にユーザーを保護します。

しかし、編集が必要な場合は保護ビューを解除する手順が必要です。これにより、ファイルを通常のモードで安全に編集・開くことができます。

- Microsoft Outlook の脆弱性(CVE-2024-21413 - 2024/2/16 公開)
  - CVSS 9.8
  - CPRの調査で発見 - #MonikerLinkと命名
  - 最新のWindows/Office Outlookを含めて確認
- 影響
  - Officeアプリケーションの保護ビューを回避
    - シングルクリックで攻撃を開始
  - 悪用のシナリオ
    - データ盗取
    - マルウェアのインストール
    - 特権昇格
    - ID盗取 ….



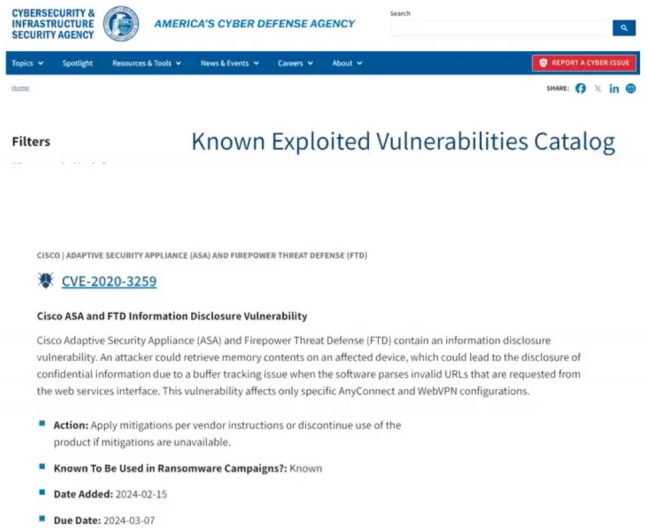
- Outlookがハイパーリンクを処理する方法を悪用
  - 特別に細工されたハイパーリンクを不適切に解析して COM オブジェクトにアクセスするWindows のコンポーネントオブジェクトモデル(COM)の不正使用
  - https://xx またはhttp://xx の場合はブラウザを起動
  - “Skype:SkypeName?call”Call me on Skype - 処理の中で安全でない警告表示
  - file:///¥¥10.10.111.111¥test¥test.rtf
  - file:///¥¥10.10.111.111¥test¥test.rtf!something
    - Outlookのセキュリティ制限を回避しリモートリソースへのアクセスを続行

保護ビューを回避

NTLM クレデンシャル情報が漏洩?

ランサムウェアランキング

- 1月の顕著な活動ランサムウェア第3位
  - 1位: LockBit3、2位: 2. 8base
- 2023年初めに確認
- WindowsとLinux両方のススステムを標的
- メール添付ファイルやVPNエンドポイントのエクスプロイト
- CISAがCisco ASA/FTD脆弱性悪用を警告
  - CVE-2020-3259(CVSSスコア: 7.5)



ランサムウェア感染は境界内のハードウェアに重大な損害を与えます。
脆弱性が多いネットワーク機器はしっかりと管理、監視が必要です。
しかし、都度それらを気にしなければならないストレスは大きいと思われます。

情報セキュリティ10大脅威 2024 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

サプライチェーンを深掘りしてみましょう!!

情報セキュリティ10大脅威 2024 [組織]
サプライチェーンを深掘りしてみましょう!!

パターン1

人手不足

⇩

DX化を進めざるを得ない

⇩

DX化を意識するあまり、セキュリティまで考える余裕がない

パターン2

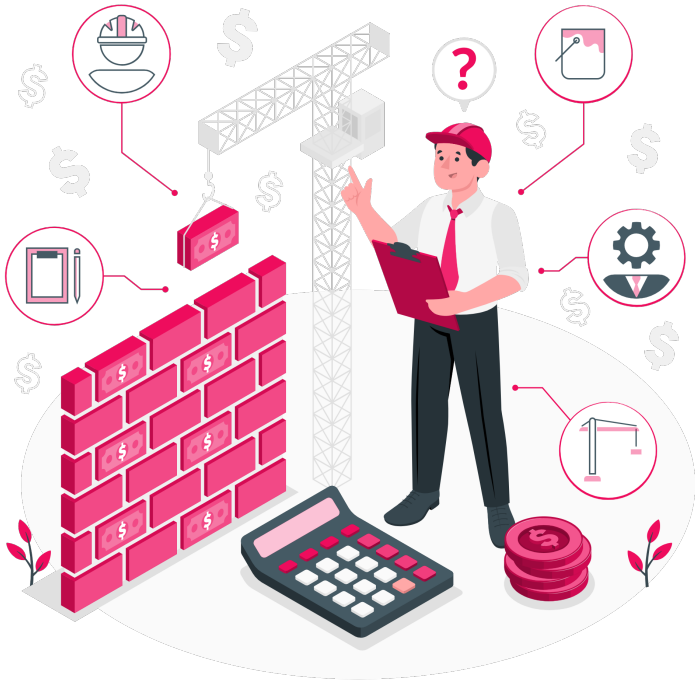
小さな会社だから必要ないという認識
（但し大手企業の下請け、孫請け）

⇩

自社を経由しマルウェアに自社と取引先が感染

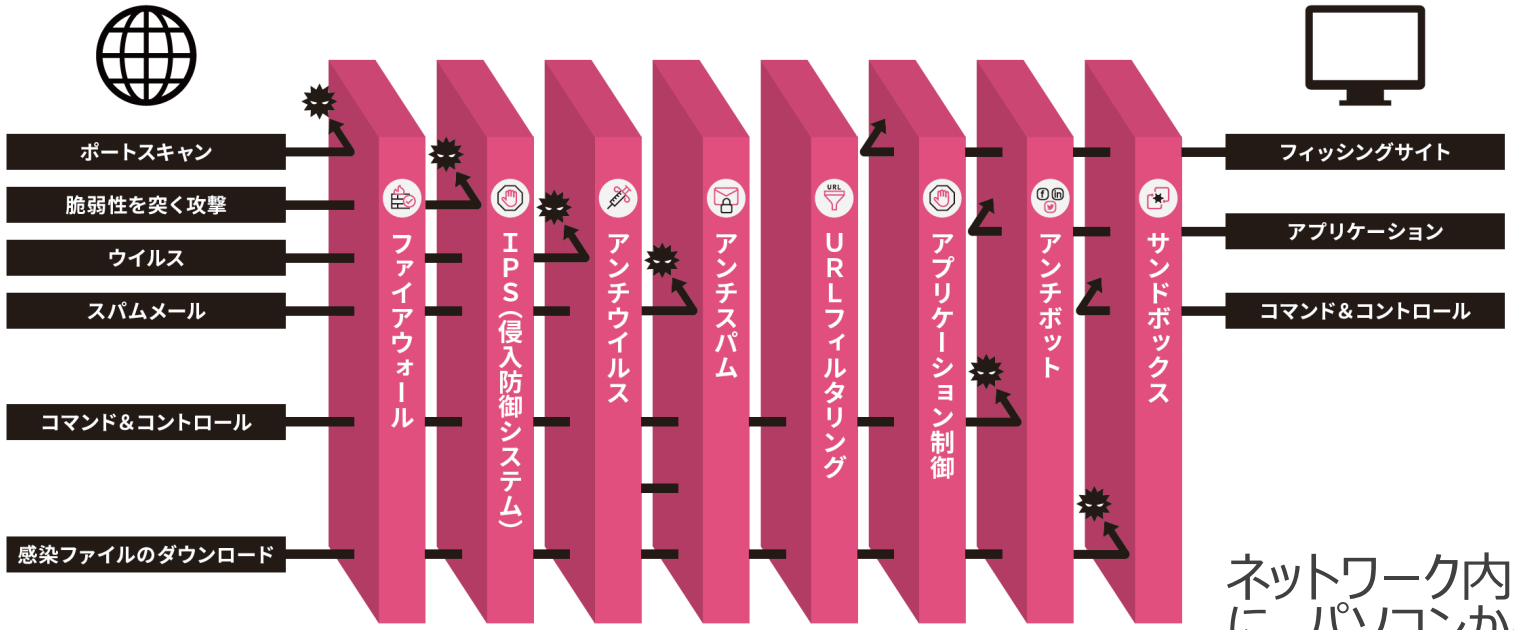
⇩

各取引先が損失を被る（損害賠償へ発展）



①オールインワンアプライアンス

複雑なサイバー攻撃を防ぐために必要な機能が1筐体に集約されたUTM！
（統合脅威管理：Unified Threat Management）



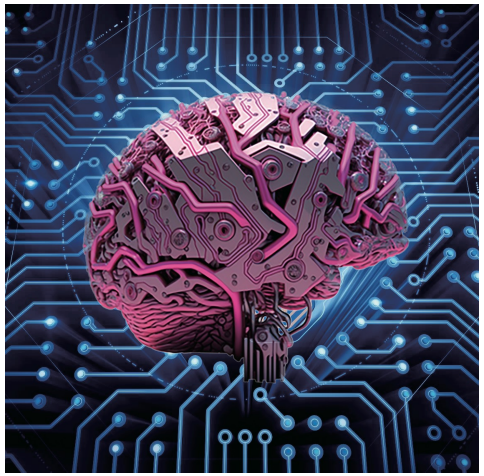
ネットワーク内にある、パソコンをUTMでブロックするとともに、パソコンからC＆C等へのアクセスを遮断します。

外部からの脅威と内部から実施するアクセスを

オールインワンで保護。

あらゆる脅威からの保護

様々なセキュリティ機能に関する脅威対策エンジン



THREATCLOUD

感染ホスト検出
サンドボックス静的解析
サンドボックス動的解析
メール静的解析
フィッシング対策AIエンジン
ネットワークAIエンジンアグリゲータ　などなど

◆世界中の約15万のセキュリティ・ゲートウェイを通過するトラフィックから日々脅威情報を収集
◆脅威情報を防御可能な情報に活用
◆リアルタイムに防御情報をアップデート

容易な導入と管理

クラウド管理によって導入から運用フェーズまでのコスト削減を実現

簡単デプロイ

- ✓ 事前定義された設定ウィザードにより数分でのセットアップが可能

モバイル・クラウド管理

- ✓ クラウドからの一括管理・設定変更が可能なため、保守運用のアウトソースが可能
- ✓ モバイル管理にも対応、インシデントをリアルタイムに確認可能

セキュリティレポート

- ✓ シンプルで直感的なレポートを標準で提供
- ✓ 通信量や検出したセキュリティ脅威等の情報を確認可能

Check Point1500Proシリーズラインナップ

10名規模の企業から400名まで幅広くサポート可能！

	1535	1555	1575	1595	1600	1800
参考ユーザー数 (NGTX全て有効時)	20	50	100	200	300	400
NGTX スループット ※エンタープライズトラフィック ※スマートアクセル有効	440Mbps	600Mbps	650Mbps	900Mbps	2.0Gbps	2.6Gbps
ファイアーウォール スループット ※試験環境トラフィック	1.5Gbps	2.0Gbps	4.8Gbps	6.4Gbps	8Gbps	17Gbps

※NGTX：サンドボックス含む全てのセキュリティ機能を有効にした状態

差別化ポイント！他社のUTMスループットは理想環境でセキュリティ機能を全て有効にしていない数値の場合が多いですが、チェック・ポイントのスループットは全てのセキュリティ機能を実環境で有効にした数値です

Summary

脅威に晒されそうな環境にならないために

確認・予測・対応策を

今一度お客様とご確認されてみてください!!

CHECK POINT

Thank You!

YOU DESERVE THE BEST SECURITY