Check_NEWS Vol. 2
令和５年２月

必見!!

1月マルウェアランキング
今更聞けないIT特集__ウイルス対策ソフト（EPP）とEDRの違いって何？

EPPとEDRの違い!!

一言で言うとウィルス対策ソフト（EPP：Endpoint Protection Platform）は事前対策。EDR（Endpoint Detection and Response）は事後対策です。

	ウイルスソフト（EPP）	EDR
役目	マルウェアに感染しない様、水際対策をするためのもの。	感染を前提とし、感染後の被害を最小限に抑える。
方法	パターンマッチング方式による検出	各エンドポイントメーカーのレピュテーション検査
強み	定義ファイルに登録済みの脅威はほぼ検出ができる	異常や不審な挙動を検知する為、未知の脅威にも対応可能
弱み	定義ファイルに登録されいない脅威には、為す術がない。	侵入を前提としているため、未然には防げない。


広報れお

先月号のセキュリティレポートにて、概要だけ説明していたEPPとEDRの違い。（左記図）Endpoint対策として、ひと昔前はEPP、いわゆるウイルスソフトが主流でした。しかしながら、このEPPの仕組みのままでは、どうしても未然にマルウェアを防ぐことが出来なくなっているのです。サイバーセキュリティを施す中で、最後の砦となるのがEndpointセキュリティ。EPPとEDRの違いを知るだけで、少しでも**会社の情報を守る**という意識が芽生えていただけると幸いです。

ごあいさつ

私たちチェック・ポイント・ソフトウェア・テクノロジーズ株式会社は1993年に創業、世界各国に支店を持つグローバル企業であり、様々なインターネットシーンにおけるセキュリティ対策企業として、官公庁をはじめ数多くの企業様で採用をいただいており、私たちの企業ドメインとして今日に至っております。『サイバー攻撃は大手企業だけ』この様に思われている経営者様も少なくないと思います。『目に見えない脅威だからこそ』私たちはその先にある『財産』『人材』『資産』を守らなければなりません。『100%に近づく安心』これが私たちの使命であり、企業を守る役割と自負しております。

振る舞い検査

実社会でもそうですが、『見た目』だけで泥棒と判断することは難しくなりました。見た目だけでは判断出来ないマルウェアが『悪さ』をやりだしたからです。

広報れお

イメージ・・・

携帯に連絡があったらこのボタンを押す!!
このバイト楽だなー♪♪

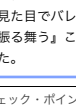
数日後


身分を明かさず支持


支持通りにボタンを押す

世の中に甚大な被害をもたらす・・・

このボタンって、みんなを不幸にするボタンだったの!?
私は何も知らなかったのにー!!!



よしよし!!うまくいったぞ!!

この様に、誰かに指示したり、または本人が見た目でバレない様にしながら、『悪意を振る舞う』ことで、被害が増えていきました。


広報れお

パターンマッチング検査

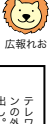
そもそも、**EPPではパソコンに侵入する前、未然に対策**しますが、EDRは違いますよね？
イメージ的にはEPPの方が良い気がします。


広報れお

そうですね!!従来の検出方法は
『パターンマッチング検査』です。こちらはパソコンに侵入する前に、怪しいと思われるものは退治せよ!!というものです。しかし、この方法では近年のマルウェアは防ぎきれなくなってしまいました。まずはパターンマッチングを説明します。

実社会に置き換えて考えてみましょう。
例えば、泥棒の特徴がサングラスにマスクをした人だと定義します。すると人々は見た目で判断し、サングラスとマスクをした人＝泥棒と判断し警察に通報することでしょう。


広報れお



EPPも同じ仕組みです。
EPPを作っている会社はそれぞれにパターンファイルを持っていて、『あやしい見た目』のパターンを数多く定義します。その定義に合ったマルウェアをPCに侵入する前に削除していくのです。


広報れお

今更聞けないITのこと

最近よく耳にする『ランサムウェア』ですが、これは実際に何をするのですか？
よく病院や教育機関などが被害に遭ったとニュースで見ます。今更誰に聞いて良いかわかりません。教えてください。

パソコンのファイルをロックし身代金を要求する悪質なマルウェア

広報れお

一度感染してしまうと、パソコンを初期化する以外復旧方法が無いと言われているランサムウェア。**『復旧させるためには身代金を払え』**と脅されますが、身代金を払ったところで解除される保証もありません。。。。

ランサムウェアに感染してしまったパソコン。こうなるとデータの閲覧はおろか、一切のパソコン操作が出来なくなってしまう。

広報れお

来月はランサムウェアについて特集します!!

1月マルウェアランキング

順位	マルウェア	11月比較
1	Qbot	↑
2	Lokibot	↑
3	AgentTesla	↑
4	Formbook	↔
5	XMRig	↓
6	Emotet	↓
7	Vidar	↑
8	GuLoader	↑
9	Nanocore	↓
10	njRAT	↑

順位	モバイルマルウェア
1	Anubis
2	Hiddad
3	AhMyth

2023年1月は前月と同様、Qbotがランキング一位となり、引き続き猛威を振るっていることがわかった。2位には2016年2月に初めて確認されたWindowsおよびAndroidを標的とするインフォスティーラ型マルウェアであるLokibotがランクインした。中東および北アフリカで大規模なフィッシングキャンペーンが展開された際に使われたリモートアクセス型のトロイの木馬であるnjRATやWindowsを標的とするインフォスティーラのVidarなどがトップ10に返り咲いている。サイバー犯罪者グループが個人情報の窃取を目的に、継続して信頼できるブランド名を悪用しマルウェアを拡散していることが確認されている。同社は、クリックするリンクが正規のURLであることに注意を払う必要があるとし、SSL証明書を示す南京錠のアイコンを確認するとともに、悪意のあるWebサイトであることを示唆する誤字脱字がないかどうかを確認するよう注意を喚起している。

このままではまずいと思ったEPP制作会社は、悪事をする『振る舞い』を察知し、『見た目』ではなく、『怪しい動き』をするファイルや、外部からの攻撃を待っていそうな『振る舞い』をするものを駆除するようになったのです。

広報れお

なるほど!!確かに『怪しそうだ』や『見た目が悪い』だけで判断されては、本当に必要な情報が弾かれてしまったり、本当に悪意あるものを間違って受け入れてしまうこともありますよね。

大事なことは守ること!!

広報れお

今までは、パターンにハマったものは駆除、ハマらないものはスルー。という状況でした。それであれば、一旦すべて受け入れて、怪しい挙動や振る舞いをおこないそうなファイルを検知、駆除または隔離しよう!!
という考えにいたりました。
これがEDRです。

広報れお

ちょっと宣伝になりますが、
Check Point社のEndpointセキュリティHarmonyエンドポイントでは、アンチウイルスやアンチbotはもちろんのこと、ゼロフィッシング対策、万が一ランサムウェアに感染しても自動復旧する機能を備えております。最後の砦はしっかりとしたEndpointを導入してみてはいかがでしょうか？

Harmony Endpoint 機能一覧
ファイアウォール、アプリケーションコントロール、VPN
アンチウイルス、アンチマルウェア
アンチランサムウェア、振る舞い検知、アンチボット、アンチエクスプロイト
フォレンジック、インシデント可視化、暗号化ファイルの復元
ゼロフィッシング、企業パスワードの再利用防止、 URLフィルタリング、SSL可視化
サンドボックス、 ファイル無害化

*詳しくは販売店様へお問い合わせください

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社 URL：https://checkpoint.com/jp
〒105-0001東京都港区虎ノ門1-2-8虎ノ門琴平タワー25F

CHECK POINT