セキュリティ対策ベンダーに騙されるな

BluePlanet-works 吉澤

イントロ） マルウェア／コンピュータウィルスの既知・未知とは何だろう

セキュリティ対策ベンダーは、よくこういう事を言います。

「既知のマルウェアは100%止めます。
　未知のマルウェアですら70%止めます。
　未知ですよ。未知！！　どうですか。すごいでしょう！」

ところで、既知／未知は誰が、どうやって決めるの？

【答】
　誰が　　：セキュリティ対策ベンダー
どの様に　：①どこかで、着弾／発症／発覚しマルウェアと認識される。
　　②**パターンファイルが用意できると既知**になり、
　　用意できていないと未知とする。

⇒既知を１００%止めるって当たり前じゃないの？

疑問1）未知のマルウェアを70%止めるとどうなるのか

未知のマルウェアは、珍しいの？

世の中に出てきた瞬間は、すべて未知。
その中の96%のマルウェアは、1度しか使われないとの報告があります。
4%が再利用されます。
既知が攻撃に使われる方が珍しい。

では、既知の4%を100%止めて、未知の96%の７0%を止めることは、すごいことなの？

止められる　：４％＊１００％　＋　９６％＊７０％＝７１．２％
止められない：９６％＊３０％＝２８．８％

⇒１００個のマルウェアが来たら、２９個にやられちゃうの？
お金を払ってて、それかい（怒）

疑問2）パターンファイルは攻撃に間に合うのか

マルウェアが発見されてから、パターンファイルを作って間に合うの？

マルウェアは放出されてから**４時間で感染のピークは終わる**。

パターンファイルが展開されるにはどんな段取りが必要なの？

セキュリティ対策ベンダー：発見、認識、解析、作成、配布
顧客企業　　：検証、配布、更新

⇒PCのパターンファイルの更新は、どんなに早くても１日後。
間に合わないんじゃないの？

疑問3）次世代型製品は未知を止めると言われているが

そうは言っても、次世代型と言われる未知に強い製品もあるけど？

既知となった
マルウェア情報
＝過去の情報

クラウド上の膨大な
脅威データベース

AI・機械学習の為の
教師データ

振る舞い検知の為の
スコアリングパターン解析

⇒結局 過去の情報に依存している。
未知と言っても亜種には対応できるが、純粋な新規は無理だ！！

では、どうすれば良いのか？

Blue Planet-works
Safety for the Connected World

続きは投票で！

または、

OPENスクエア　田中昭造　検索