FireEye

NVC NETWORK VALUE COMPONENTS

従来の IPS では検知できないゼロディマルウェアをブロックし、解析する
FireEye Malware Protection System

⚠ 既存システムでは止められない最新マルウェアが急増中

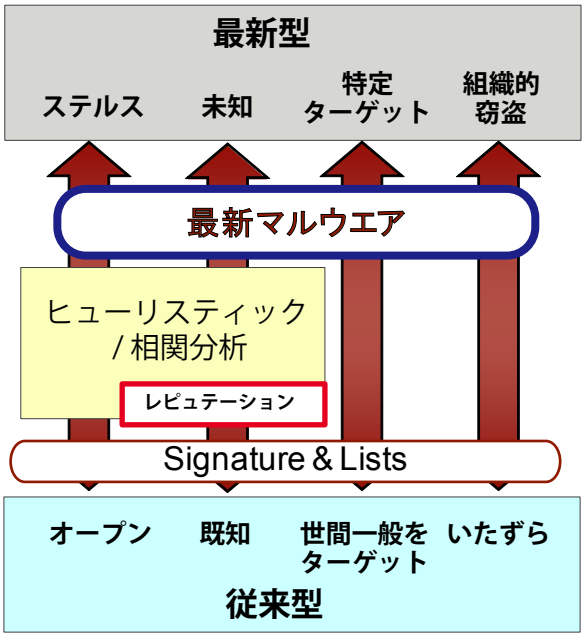
新たなマルウェアが1.44秒ごとに発生

90%のマルウェアが数時間以内に自己改変

▼IPS (侵入防止システム)、アンチウィルス
シグネチャのすり抜け
▼ URLフィルタ, レピュテーションフィルタのすり抜け
▼ヒューリスティック評価、相関分析、簡易
エミュレーションのすり抜け

サイバー攻撃の7割以上はターゲットを絞り、
75%は50台以下のコンピューターを標的設定

▼APT (Advanced Persistent Threat) 攻撃では
シグネチャベースだけでは防御が難しい



マルウェアを可視化して防御対策しませんか?

シグネチャに依存しない FireEye ゼロディ攻撃対策

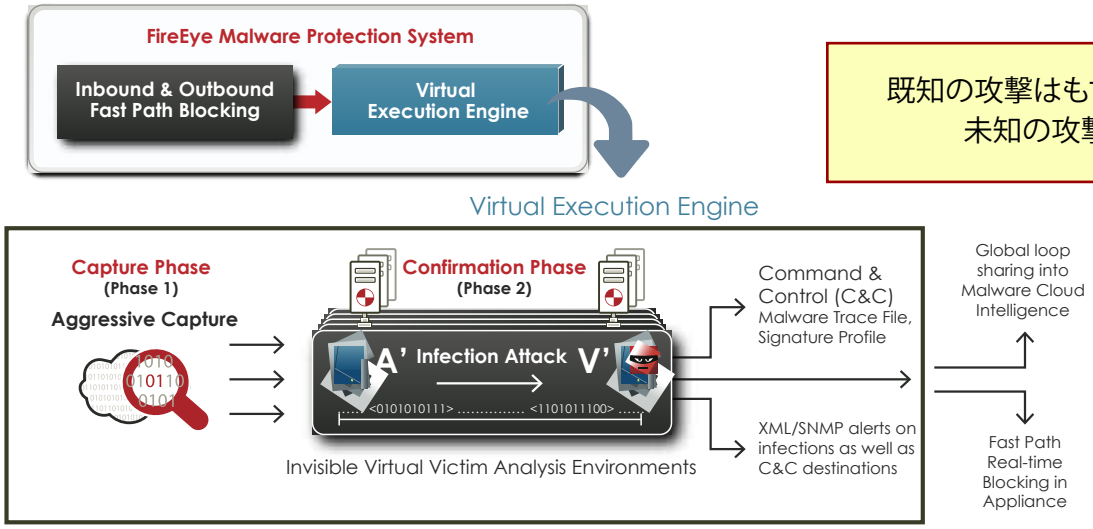
FireEye

標的型攻撃に対する多重のマルウェア対策

- ●入口/出口対策: 企業のゲートウェイを通過するすべての通信から 怪しいデータを検出
- ●出口対策: 情報流出を防ぐアウトバウンド・コールバックを停止
- ●可視化: トラフィックのふるまいから未知のマルウェアを検知し隔離分析
- ●仮想実行エンジン (Virtual Execution Engine) で動作確認するため誤検知削減
- ●マルウェア情報をクラウドでリアルタイムに共有

高いセキュリティ診断を
アプライアンス化

セキュリティ判断を実行する仮想環境を搭載した FireEye アプライアンス



既知の攻撃はもちろんブロック
未知の攻撃は解析

1) 既知の攻撃およびコールバックはマイクロ秒でブロック
2) インバウンドのトラフィックは、リアルタイムでヒューリスティック検知 (スタティックおよびダイナミック) をし【Phase 1】、疑わしいフローは隔離して、Virtual Execution Engineで解析【Phase 2】
3) 疑わしいコールバックをブロック
4) 監視された仮想環境でWindows OS, ブラウザ, プラグインを含めて、実際にマルウェアを動作させて検証し、マルウェアの動作を把握し、外部へのコールバックをブロック

◆ Web MPS (Malware Protection System) 製品仕様

	1300	2300	4000	7000
				
モニタリング用インタフェース	10/100/1000MBASE-T × 2		10/100/1000MBASE-T × 4	
管理用インタフェース	-		10/100/1000MBASE-T × 2	
パフォーマンス・レート	最大20Mbps	最大50Mbps	最大250Mbps	最大1Gps

◆ Email MPS (Malware Protection System) 製品仕様

	5000	8000
大きさ	2U 19インチラックマウント (43.8 cm x 71.1 cm x 9.0 cm)	
モニタリング用インタフェース	10/100/1000MBASE-T × 2	
管理用インタフェース	10/100/1000MBASE-T × 2	
パフォーマンス・レート	200,000 email/日	500,000 email/日

製造・販売元

FireEye

FireEye, Inc.

http://www.fireeye.com/

販売代理店

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

http://www.nvc.co.jp/

※本カタログに記載されているシステム名、製品名、社名などは各社の商標および登録商標です。
※仕様および型番号などは予告なく変更されることがあります。
(fireeye_v2_B1X)