運用管理の負荷軽減にもつながるTraps

こうしてTrapsは、パターンファイルとは全く異なる3つのアプローチによりエンドポイントを保護している。パターンファイルを使わない手法であるため、これまでのアンチウイルスソフトにありがちだったファイルスキャンや、パターンファイル更新といった負担がないという点もユーザーにとってのメリットだ。Trapsは実行されたファイルやプログラムを調べる仕組みのため、端末のCPUやメモリに対する負荷を軽減でき、またアップデートも機械学習エンジン更新などを月に1回程度行うだけなのでネットワーク負荷も抑えられるなど、管理者にとってもメリットがある。さらに、Trapsは全てのファイル実行を記録し、メモリダンプやアクセスしたURLなど後の分析に利用できる情報を収集できるため、もしインシデントが発生したときでも調査が容易になる。

加えて、パロアルトネットワークスは長年にわたって次世代ファイアウォールを提供してきたセキュリティベンダーでもある。WildFireのデータの充実ぶりは、まさにその裏付けがあってこそのものだ。Trapsと次世代ファイアウォールはもともとWildFireを介した脅威情報の連携が行われているが、最近では管理ツールも連携が進められており、ネットワークとエンドポイントの両方で検知したイベントの情報を一元的に把握できるようになっている。これにより、両製品を導入している組織ならネットワーク管理者とPCセキュリティ管理者の間で高度な情報を共有でき、より効果的な対応を取ることができるというわけだ。

《アンチウイルスソフトとTrapsの動作の違い》

	従来のアンチウイルスソフト	Traps
検出のタイミングとリソース負荷	・ディスクアクセスごとに検索 ・定期的なフルスキャン CPU/メモリなどのリソースを大量に消費	・プログラム実行時にスキャン CPU/メモリなどへの影響が少ない
アップデートのタイミングとネットワーク負荷	・日々のパターンファイル更新が必要 ・未アップデート端末の管理が必要 ネットワークリソースを日々大量に消費	・1ヶ月に1回程度のアップデート（機械学習エンジン更新等のため） ※ネットワーク接続時、WildFireとの連携はリアルタイムで可能 ネットワークリソースへの影響が少ない
インシデント発生時の調査	・インシデント発生時の時間や マルウェアの検出名の情報のみ インシデント発生時の調査が困難	・全てのファイル実行を記録 ・脆弱性攻撃/悪意の実行ファイル（exe） 検出時に関与するURL、メモリダンプ取得 インシデント発生時の調査を支援

企画・制作　朝日インタラクティブ株式会社　営業部

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/paloalto/sp/

C17K-24-02　2018.03

HITACHI
Inspire the Next

次世代エンドポイントセキュリティ製品

パロアルトネットワークス Traps ホワイトペーパー

paloalto NETWORKS

未知の脅威に対抗する新たなアプローチ 最新の次世代エンドポイントセキュリティとは?

**企業や公的機関の業務を阻害するなどの猛威を振るうサイバー攻撃の脅威。攻撃者は次々に新たな手口を取り入れており、ここ数年は既存技術の延長では対応が困難なものも増えてきた。これに対しセキュリティ業界でも、これまでにない新たなアプローチの研究を進めてきた。
その一つが、「次世代エンドポイントセキュリティ」と呼ばれる分野だ。未知の脅威に対していかにしてリアルタイムに対抗するか、その難題に立ち向かう新たなアプローチを紹介する。**

攻撃者は手口を高度化させ次々に新型マルウェアを作成 パターンファイルなどに頼った検知手法では限界に

これまで、PCなどの端末（エンドポイント）を保護するセキュリティといえば、長らくアンチウイルスソフトが主流だった。その主な手法は、メールの添付ファイルやWebサイトからダウンロードしたファイル、USBメモリなどを通じて外部から持ち込まれるファイルをスキャンして、悪意あるファイルかどうかを判別するというものだ。この基本的な判定基準はパターンファイル、つまりマルウェアと判定されたファイルの情報を基にしている。しかし、インターネット上では多種多様なマルウェア作成ツールが出回っており、特別な専門知識が無くても、これらを駆使して容易に新たなマルウェアを作り出すことができるようになってきている。そのため、パターンファイルの更新・配信サイクルによっては対策が間に合わず、検知から漏れてしまうといったケースが生じている。しかも、マルウェアは数が急増しているだけでなく、手口の高度化も進んでいる。標的となる企業にあわせて文面を工夫するなどして疑われにくくしたり、感染後には活動形態を変え、LAN上で別のPCやサーバへ感染を拡大させたりといった手口も広く使われている。そうした活動の末に、組織内から重要な情報を盗み出して別の相手に売りつけたり、ユーザーのデータを暗号化した上で身代金を要求（ランサムウェア）したりするなど、組織や個人に被害をもたらす。

このように攻撃が巧妙化しているなか、パターンファイルに頼った検知では限界であるという事実は、何年も前からセキュリティ業界の大きな課題となっていた。もちろんさまざまな対策が考えられており、例えばエンドポイントのみならず、ネットワーク上で侵入前や侵入後の活動を検知する技術が広まるなど、多層防御の取り組みが進められている。しかし一方で、一般的なオフィスワーカーの間では、PCを持ち出してのモバイルワークや在宅勤務などのリモートワークなど、社内ネットワークの保護を受けられない場面も増えている。USBメモリなどの直接的な侵入手口も含めると、やはりエンドポイントのセキュリティ機能強化も不可欠であることには変わりはない。

株式会社 日立ソリューションズ