セキュリティ

ITマネジメント（内部統制）

キーワードは、多段防御と分離・無害化

巧妙化、複雑化する マルウェア対策の最新ソリューションとは

マルウェアの種類は多彩で、新種が発生するとそれを改変した亜種も大量に登場します。これらは巧妙化、複雑化が進んでおり、マルウェア検知には、セキュリティ対策ソフトによる「検知」だけではない防御手法が求められます。ここでは最新のマルウェア対策について、多段防御を実現する「WideAngle マネージドセキュリティサービス」や分離・無害化ソリューション「Menlo Security」を通じて紹介します。

流行するマルウェアは年ごとに変化している

現状、サイバー攻撃の9割近くがメールやインターネットを介したものになっており、ほとんどがマルウェア感染をきっかけとしています。マルウェアはサイバー攻撃者にとって常套手段で、種類や手法は日々進化しています。それは、2017年がランサムウェア、2018年がマイニングマルウェアと、流行したマルウェアが年ごとに変化していることでもわかります。

標的型攻撃に使用されるマルウェアは、狙ったターゲットのために特別に作られる「新種」ですが、すぐに亜種が登場し、スパムメールなどの“ばらまき型”攻撃に転用されます。また、標的型攻撃では侵入したマルウェアがC&C（コミュニケーション&コントロール）サーバーと通信し、マルウェアの追加や盗み出した情報の送信などを行いますが、この手法は他の攻撃でも一般的に使用されているのです。

セキュリティ対策ソフトの検知を回避するテクニックも次々に登場しています。例えば、ファイルの拡張子を偽装したり、ファイルが実行された際の動作を隠すようにしたり、脆弱性を悪用して不正な動作を行ったりします。仮想環境で疑わしいファイルを実行することでその動作を確認し、マルウェアかどうかを判断するサンドボックスが普及すると、仮想環境ではスリープ状態に入るマルウェアが登場しました。

こうした新しい手法が次々に生まれてくる現状に対応するため、即応性のあるセキュリティ対策が不可欠となっています。

検知、分析、監視が連携した「多段防御」が有効

巧妙化、複雑化、そして悪質化するマルウェア対策には、複数のセキュリティ対策による多段防御が有効です。例えば、NTT Comが提供する総合リスクマネジメントサービス「WideAngle」では、メールやWebに対する「コンテンツセキュリティ」、サンドボックスによる「リアルタイムマルウェア検知」、PCやモバイルなど端末のアクティビティに対する「エンドポイントスレットプロテクション」といった複数のセキュリティ対策が用意されています。

コンテンツセキュリティは、ユーザー環境のメールとWebの通信から悪意あるソフトウェアを検出しブロックします。「WideAngle」では、NTT Comがセキュリティ機器の管理および運用を行うので、最新の環境でマルウェアを検知することが可能です。ユーザーは管理や運用の手間から解放され、工数をかけることなく最新のマルウェア対策を行えます。

リアルタイムマルウェア検知は、コンテンツセキュリティなどによって疑わしいと判断されたファイルについて、ユーザーのPCを仮想環境に再現したサンドボックス上で実際にファイルを実行し、その動作を確認します。前述の仮想環境でスリープ状態に入ることでサンドボックスを回避するタイプのマルウェアにも対応。ここで危険と判断されたファイルについては、NTT ComのSOC(セキュリティオペレーションセンター)からユーザーへ通知が行われます。

エンドポイントスレットプロテクションは、EDR(Endpoint Detection and Response)とも呼ばれるしくみです。エンドポイントとなるPCにエージェントをインストールすることで、検知される情報を分析し、脅威と判断された場合は、SOCからの指示により端末をネットワークから即時隔離します。エンドポイントの分析にあたっては、SOC独自の知見で作成したカスタムシグネチャをエージェントに適用し脅威を早期に検知。加えて他のセキュリティメニューのログとの相関分析により、より精度の高い分析が可能です。

「WideAngle」では、メールを中心としたマルウェアに対して多段防御を構築することでセッキュリティ精度を高めています。また「WideAngle」は、機器の管理や運用、監視に至るまでNTT Comにアウトソースできるマネージドセキュリティサービスです。セキュリティ担当者のいない会社においても、高度なセキュリティ対策を実現することができます。

Web 経由のマルウェアを遮断する「分離・無害化」で、防御をより堅牢に

これらの「検知」技術に加え、NTT Comではマルウェアが仕込まれた悪意のあるWebサイトから、利用者のPCを分離・無害化して守る「Menlo Security(メンロー・セキュリティ)」を提供しています。「Menlo Security」は、すべてのWebコンテンツをエンドポイントから分離されたクラウド上で実行。その際に特許技術で独自のHTML5コードへ変換することで無害化します。利用者のPCには無害化されたHTML5コードが転送されるので、たとえアクセスしたWebサイトに不正なプログラムが仕込まれていたとしても、利用者のPCに影響を及ぼすことはありません。

「Menlo Security」は、標的型攻撃のようなメールの添付ファイルを利用した攻撃にも効果を発揮します。マイクロソフトの「Office 365」を利用している場合は、メールに添付されているファイルを無害化して表示します。またメールに記載されたURLのリンク先が悪意のあるWebサイトであった場合でも、無害化して表示するので、悪意のあるインターネット攻撃からPCを守ります。「WideAngle」による多段防御と「Menlo Security」による分離・無害化技術を組み合わせることで、防御の層がより厚くなり、巧妙化、複雑化するマルウェアに対する堅牢なセキュリティの実現につながります。

関連サービス

WideAngle マネージドセキュリティサービス	ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。 セキュリティ運用基盤（SIEM）とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。
Menlo Security	インターネット分離・無害化の技術で、従来の検知技術による多層防御では防ぎきれなかった新種のマルウェア攻撃やゼロデイ攻撃も防ぎ、安全で自由なWeb閲覧を実現します。