セキュリティ

ITマネジメント（内部統制）

犯人は、マルウェア感染したゾンビPC！？

不正通信での情報漏えいは「自動ブロック」で防ぐ

標的型攻撃や不正送金、情報漏えいなどによる被害が後を絶ちません。こうした被害を防止するためには、マルウェアに感染させた「ゾンビPCやIoT機器」などを操って情報を盗み出すC&Cサーバとの通信を遮断する手段が有効です。そのひとつが、C&C（コマンド&コントロール）サーバとの通信を自動ブロックする「マルウェア不正通信ブロック」です。

標的型攻撃でも使用される「C&Cサーバ」

マルウェアを使ったサイバー攻撃では、一般的にC&Cサーバが使用されます。C&Cサーバは、サイバー攻撃者がマルウェアに指令を出したり、盗み出した情報を受け取ったりするためボットネットワークをコントロールする指令サーバのことです。ボットはマルウェアの一種で、PCやIoT機器などに感染し乗っ取っていまいます。かつては「ゾンビPC」とも呼ばれていましたが、サイバー攻撃者からの指令を受けると、いいように操られてしまうため、この名前がついたのでしょう。ボットと化したPCは指令サーバとの通信を可能にした上で、発見されないよう必要以上の動きを止め、静かに指示を待ちます。それゆえ、ユーザーが気づかないままPCがボットにされているケースが後を絶ちません。

サイバー攻撃の一種に「標的型攻撃」があります。標的型攻撃は非常に巧妙で、入念な準備と事前調査を行った上で実施されます。こうした攻撃の多くは、高度な技術を持つサイバー攻撃者グループによって行われているとされ、組織や国家に依頼を受けるケースもあるといいます。そのため資金も潤沢で、特定のターゲットを狙うためだけに新種のマルウェアが開発されることもしばしばです。このため、従来のパターンマッチングによるウイルス対策ソフトで検知するのは困難です。

そして、C&Cサーバは標的型攻撃でも使用されています。メールなどを通じてターゲットにマルウェアを侵入させることが成功した場合、サイバー攻撃者はC&Cサーバから乗っ取ったPCへ指令を出して次々にマルウェアを送り込み、感染を拡大させます。こうしてターゲットから重要な情報を盗み、C&Cサーバに送信させるのです。

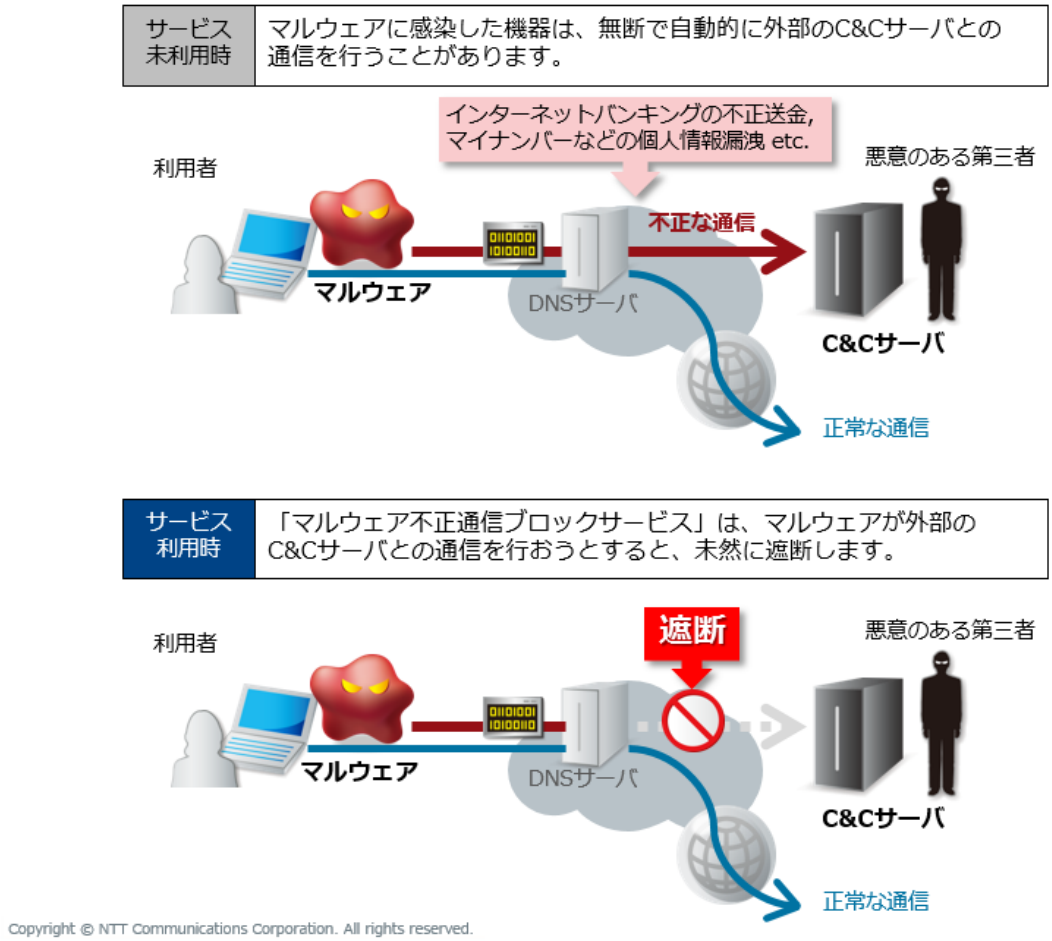
この際、指令や情報の送信にはWeb閲覧などに使用されるポート80（HTTP）が使用されるため、数多くやり取りされるWebの通信に紛れてしまい、検出は困難です。しかも、サイバー攻撃者はC&CサーバのIPアドレスを頻繁に変更します（10分ごとに変えていたというケースもあります）。これにより、IPアドレスを指定して通信を遮断する対策も難しくなります。

「マルウェア不正通信ブロック」で不正な通信を自動的に遮断

このように高度化する標的型攻撃への対策ですが、効果的なのは「入口対策」「内部対策」「出口対策」です。また、それぞれの対策を「多層化」「多段化」することで、より高い効果が得られるとされています。具体的には、入口対策ではゲートウェイにおけるファイアウォールやIPS（不正侵入防止システム）の設置、ウイルス対策などです。内部対策では、内部ネットワーク・通信の監視や、複数機器のログを分析するSIEM（セキュリティ情報イベント管理）など。出口対策では、ゲートウェイでの対策に加えデータの暗号化などが挙げられます。

しかし、これらの対策を全て行うと莫大なコストがかかりますし、管理や運用の負荷が大きくなるため、組織の規模によっては現実的ではありません。まずは、自社が漏らしてはいけない重要なデータは何かを洗い出し、それを守ることを第一に考え、最適なセキュリティ対策を構築することが肝要となります。

そのひとつが、秘密裏に機密データを盗み出すC&Cサーバの「不正通信」を検知し、自動的に遮断することです。例えば、NTT Comの提供する「マルウェア不正通信ブロック」は、OCNのネットワーク上でユーザーのPCやスマートフォンなどの端末がマルウェア感染したことで発生するC&Cサーバへの通信を検知し、自動的に遮断します。C&Cサーバへの通信を遮断することで、インターネットバンキングを悪用した不正送金や個人情報の盗難などマルウェア感染による被害を防止することができます。



このサービスは、NTT Comの参照用DNSサーバを利用しているユーザーに無料で自動適用されます。対象サービスとしては、OCNの接続サービスや、DNSサービス、「Arcstar Universal One」インターネット接続機能、Group-VPN インターネット接続サービスなどが該当します。

なお、「マルウェア不正通信ブロック」は、不正な通信を遮断するサービスです。C&Cサーバとの通信が検知された場合、PCなどの端末がマルウェアに感染している可能性がありますが、同サービスに駆除機能はないため、別途セキュリティ対策ソフトなどを使用して駆除する必要があります。

NTT Comでは、「WideAngle マネージドセキュリティサービス（MSS）」において、ネットワークに流れる不正通信や不正侵入などの脅威を検知、遮断する「NWセキュリティ」、Webサイトやメール添付ファイルに潜む脅威に対応した「リアルタイムマルウェア検知」などの機能も提供しています。これらを「マルウェア不正通信ブロック」を組み合わせることによって、より効果的な対策が可能になるでしょう。

関連サービス

マルウェア不正通信ブロック	NTTコミュニケーションズがDNSサーバーを提供するインターネット接続サービスにおいて、不正送金や個人情報漏えいなどによるお客さまの被害防止のために、悪意ある第三者が管理するC&Cサーバーとの通信を自動的にブロックします。
WideAngle マネージドセキュリティサービス	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが、ICT環境を24時間365日サポート。高度なセキュリティ監視により、実在するリスクと潜在リスクを可視化します。 また、「NWセキュリティ」をはじめとするセキュリティ対策パックメニューや、「リアルタイムマルウェア検知」などの機能をご用意、様々なご要望に応じて総合的なセキュリティソリューションを提供します。
WideAngle マネージドセキュリティサービス NWセキュリティ	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。
WideAngle マネージドセキュリティサービス リアルタイムマルウェア検知	アンチウイルスなど、従来のセキュリティ対策では検知できない、メールの添付ファイルやWebサイトに潜む未知の脅威を検知します。