マネージドセキュリティサービス 最前線

第6回 ー 実例ベースで考える ー

～マルウェア解析最前線からの報告～ Sandbox 技術＋αの対策

NTT コミュニケーションズ㈱　経営企画部
マネージドセキュリティサービス推進室長
与沢 和紀

NTT コムセキュリティ㈱
オペレーション＆コンサルティング部
市田 達也

弊社の WideAngle マネージドセキュリティサービス（MSS）では、Sandbox 技術を活用したメニュー「リアルタイムマルウェア検知（Real Time Malware Detection: RTMD）」を提供しているが、連載 6 回目となる今回は、昨今の観測されたマルウェアや事例を通して浮き彫りになった新たな課題と更なる取り組みの一部について紹介する。

企業を取り巻くマルウェア事情

先ず、読者の中には「マルウェアとは何？」と思われる方も当然いるはずなので、ここで改めて簡単に触れると、実はコンピュータウイルスのことであり、Malicious Software（悪意のあるソフトウェア）の略称である。マルウェアはユーザーが許可または意図しない、主に通信や内部システム情報の書き換えを行う不正プログラムともいえる。因みに、「マルウェアに感染している」というのは「不正プログラムが実行した、意図しないプロセスが動作した状態」を指す。

では、マルウェアに感染するとどうなるか？報道でご存じ方も多いと思うが、感染すると別コンピュータへの感染拡大や感染コンピュータ内の情報漏洩やスパムメール送信や DOS 等の外部への攻撃に加担するなど、被害者のみならず加害者にもなるという深刻な状況に陥る。しかし､1990 年代よりインターネットが普及して以来、少なくとも日本を含む先進国ではウイルス対策は常識という状況において、マルウェア感染によるセキュリティ事故が後を絶たないのは何故か。その疑問に答えるために、弊社における対応事例の一つを引用して説明したい。その従業員 1 万人規模の企業（メール総受信数：1,500 万通）における今年 1 月の事例では、添付ファイル付きメール 7 万 5,000 通のうち、1 万 3,000 通がマルウェア付きのものであった。弊社では、ウイルス対策を導入しているのだが、メール件数で 1 万 2,000 通、マルウェアの種類としては 700 種類もの数が検知されず、社内メールサーバに到達していたのである。従来のウイルス対策だけでは昨今のマルウェアは防ぎきれないのである。

マルウェアを検知・解析する仕組み

従来のウイルス対策とは、アンチウイルスソフトによるウイルススキャンのことである。ウイルススキャンは今までに発見された既知のマルウェアの辞書と見比べて検知するものであり、近年の巧妙化するマルウェアをリアルタイムに検知できるものではない。なぜならばマルウェアの中には自身のプログラムコードを暗号化（パッキング）するものが多数存在するためである。そこで我々はリアルタイムにそれらを検知するために、仮想環境による動的解析（Sandbox による解析）を採用している（図 1）。

被疑ファイルを仮想環境にて意図的に実行し、そのプログラムの挙動をトレースすることでマルウェアかどうかを判定する。代表的な判定ルールは、事前にマルウェアによくある挙動や挙動の遷移の悪性スコアを辞書として保持し、トレース結果がその悪性挙動にマッチした場合に悪性スコアを加点する。

【Sandboxの仕組み】

・シグネチャベースで検知できないマルウェアを発見するための技術

・社内ネットワークとは切り離した仮想環境に閉じ込めて、プログラムを実行

・プログラムを実行し、その挙動を監視することで、マルウェアかどうかを判定

・プログラムを複数の種類・バージョンのOS・ソフトウェアで実行

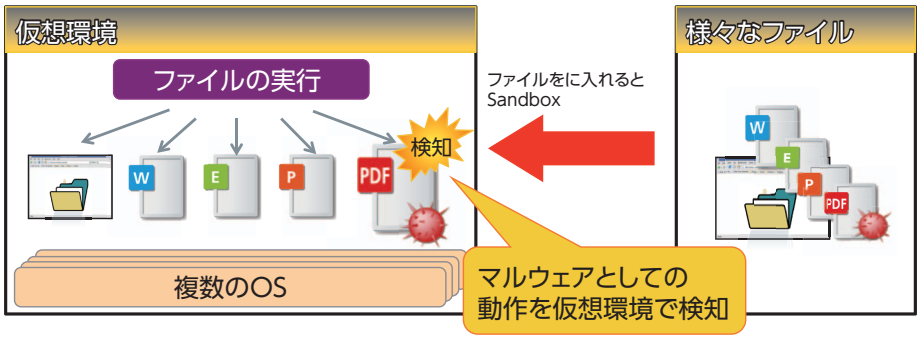

図 1　Sandbox の仕組み

その悪性スコアがマルウェアだと判定できる閾値を超えるとマルウェア判定がくだる。

本技術の主な優位点は、プログラムコードが暗号化されていても、コードではなく実行結果に基づき検知できるため、アンチウイルスベンダーのパターンファイルが存在しない未知のマルウェアを検知できる点と、仮想環境をお客さま環境に合わせることで、お客さまに影響のあるマルウェアを脅威通知できる点である。

逆に懸念点は、ファイルを実行し挙動を観測しなければならないため、ウイルススキャンに比べ解析に時間がかかる点と、ユーザー操作を要求するプログラムでは解析が途中終了し、あいまい判定をしてしまう点であるが、マルウェアが自身を停止させるSleep 挙動をスキップしたり、マルチウイルススキャンシステムやリスクアナリストの手動解析を併用することで時間的短縮及び検知精度の向上を実現している。

メール添付型マルウェアの事例

連載第 1 回目(2013 年 8 月号)及び第 2 回目(2013 年 10 月号）に記載したように、代表的なマルウェアの感染経路として、マルウェアがメール添付されるものがある。ユーザーが不用意にマルウェアファイルを開くと、マルウェアが実行され感染してしまう。このようなメールは、攻撃者によって、ユーザーがマルウェアファイルを開くように、送信元メールアドレスを偽装し、メール件名、ファイル名やメール本文の内容をユーザーの興味のある内容にて作成されている。

ここではグローバルリスクオペレーションセンターにて 2013 年末より、亜種も含め 200 種以上も検知された「UPATRE ダウンローダー」というマルウェアを紹介する。「UPATRE」はマルウェアの種別名で「ダウンローダー」というのはマルウェアの一般的な機能名である。添付メールの兆候としては、件名に「Voice Message from Unknown（xxx-xxx-xxx）」（xxx 部は電話番号）や「New Fax Message on dd/mm/yyyy」（dd/mm/yyyy）はメール送信日の日付）があり、ファイル名は「VoiceMail.exe」や PDF にアイコン偽装された「fax.pdf.exe」が多く見受けられた。このファイルを不注意に開いてしまうと後の被害は甚大だ。本マルウェアは自身ではレジストリの改ざん、ファイルの作成・削除や外部への感染拡大等の悪性挙動は持っていないが、代わりに追加マルウェ

アを攻撃者の用意したサーバからダウンロードする挙動を持つ。一つのファイル（マルウェア）で悪性挙動を多く含んでいるとそれだけセキュリティ製品に検知される可能性が高いため、一種の検知回避手段と言えるのだが、Sandbox では見逃さない。

このマルウェアに感染すると、（ときに直接マルウェア配布サーバにアクセスすることもあるが、）多くは HTTPS にて外部 C&C サーバと通信したのち、攻撃者の用意したマルウェア配布サーバから Zbot と言われる金融情報を窃取する別のマルウェアをダウンロードする。興味深いのは、ダウンロードされる別のマルウェアのいくつかは暗号化ファイルの拡張子「.enc」にてダウンロードされることだ。この手口はパターンマッチングで検知するアンチウイルス製品を回避できる可能性が高い。さらに、冒頭において Sandbox ではプログラムコードが暗号化されたマルウェアでも検出可能と書いたが、同拡張子のファイルは特殊であり、復号プログラムが実装されていない仮想環境においては Sandbox による解析でも検知できない可能性が考えられる。

このようなメール添付型マルウェアの事例では、Sandbox にてダウンローダーを検知し、トラブルの芽を早期に摘むことが重要であると分かるとともに、一旦感染してしまった場合を想定すると、後述する、悪性の高いマルウェアを追加ダウンロードする通信を遮断し、凶悪化を防止するための対策も必要であることにも気づかされる。

Web からマルウェア感染する事例

連載第 5 回目（2014 年 4 月号）に記載したような、Web サイトからのマルウェア感染事例（ドライブバイダウンロード）も数多く見られた。2013 年特に多かったのは、ユーザーが攻撃者によって改ざんされた一般 Web サイトにアクセスすると、攻撃者のサーバにリダイレクトされ、取得した htm ファイル内の JavaScript により、Java の圧縮ファイル（.jar）ファイルをダウンロードし意図せず実行させられるというものだ。これが Java の脆弱性を悪用した Exploit コードを含んでおり、さらに攻撃者のサーバから Zbot である Windows 実行ファイル（.exe）をダウンロードさせるものであった。このような場合、脆弱性を悪用したコードにより Web サイトにアクセスしただけでマルウェアをダウンロードし感染に至ってしまう。近年、一般的な Web サイトの改ざんが後を絶たない。ニュース等で報道されている通り、大手企業の Web サイトが改ざんされる事例も少なくないが、その他にも我々にて観測されたものとして、サークルや個人のブログサイト、インターネットショッピングのサイトがあった。このようなドライブバイダウンロードの基本的な対策としては、Web ブラウザや Java の最新セキュリティパッチの適用を定常的に、そして緊急性の高いものは迅速な適用を行うことであるが、脆弱性の存在や対応策が公表される前に攻撃が行われるゼロデイアタックや対応策が実施されるまでの間隙を突いた攻撃には、Zbot のような悪性プログラムを検出できる Sandbox が最良の策と言える。しかしながら、本事例においても、PC 端末が Zbot に感染してしまった場合も考慮すると、Sandbox だけでは不十分であり、後述する出口対策も含めて重要となってくる。

Sandbox 技術＋αの対策

本連載記事の前半で述べたように、従来のアンチウイルスソフトによるウイルススキャンだけでは、近年増加しているマルウェアを使った巧妙な攻撃への対策としては不十分であり、Sandbox は重要な検知技術となっている。実際、紹介した 2 つの事例では、アンチウイルス対策では検知できないダウンローダーや Zbot のダウンロードなど、攻撃の第一波を Sandbox が検出している。しかしながら、同事例では同時に、Sandbox 単体では一旦感染してしまった場合の悪性の高いマルウェアを追加ダウンロードする通信を「遮断」できないという課題も浮き彫りになっている。

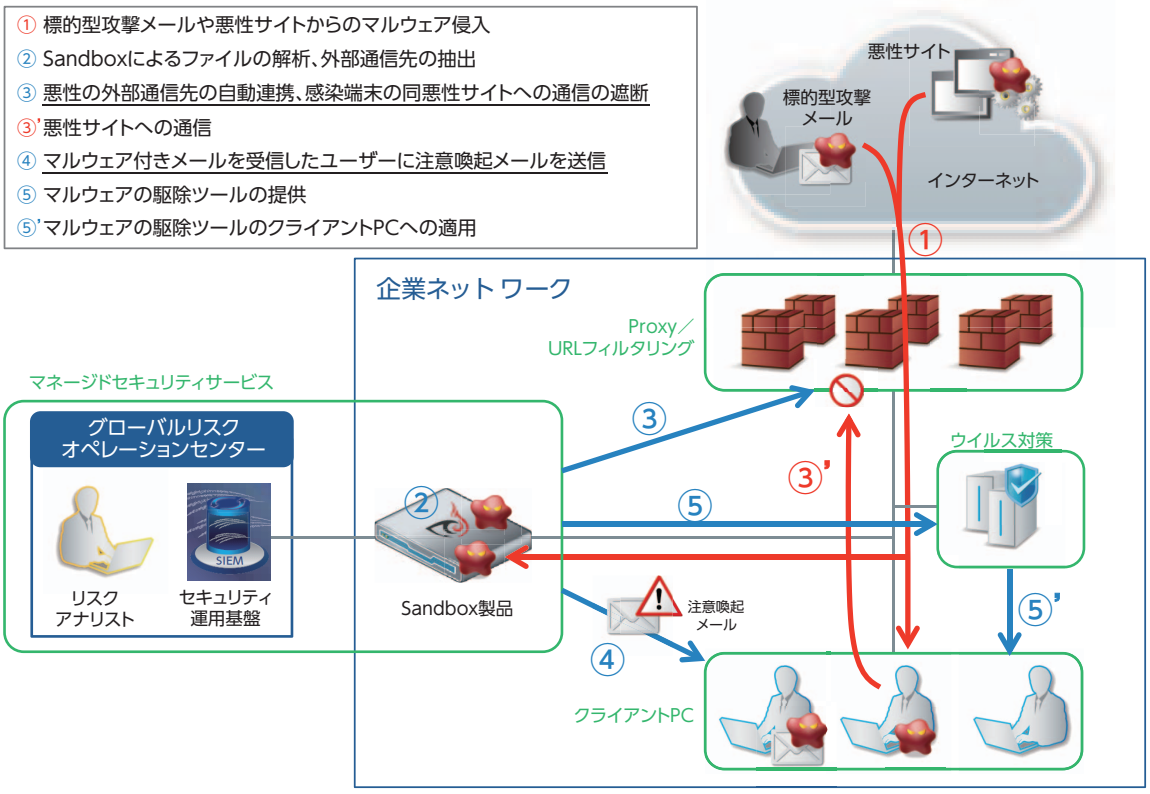

図 2　Proxy 等、他システムとの連携によるセキュリティ強化策

弊社の RTMD サービスでは、Sandbox 解析により未知のマルウェアを検知した時点で、その URL を遮断対象として Web プロキシや UTM に自動通知、連携防御するところまで進化させ、その課題に対応している(図 2)。これは、第二のマルウェアのダウンロードや、マルウェアの活動を最小限に抑える拡大防止及び出口対策である。また同時並行して Sandbox にて捕捉したマルウェアに対し、駆除パターンファイルを準備することで、マルウェアの活動の自由を奪った上で、遅くとも 1 週間以内に駆除できる環境が整えることが可能だ。

弊社では、Sandbox を活用した MSS を日本でいち早くサービス化し、検知精度の向上・効率化を実現するためのシステム的な対応(SIEM エンジンの開発)とリスクアナリストの分析ノウハウの蓄積を行ってきたが、総合での連携対策はこれまでの豊富な運用実績から生まれた対策である。

また、Sandbox でも検知しきれなかったマルウェアの侵入を、その後の感染拡大活動、例えば攻撃者サーバへのアクセスなどを検知し、結果として活動を遮断することを可能とする相関分析処理も、弊社開発の SIEM エンジンでは搭載しており、今回紹介した RTMD サービスのみならず、弊社の総合的な WideAngle セキュリティサービスを導入する意義が高い。相関分析処理に関する詳細は次回以降で紹介するが、今後も未知のマルウェア解析の最前線で、顧客企業の情報セキュリティを守り、信頼されるパートナーでありたいと願っている。

お問い合わせ先
NTT コミュニケーションズ㈱
経営企画部 マネージドセキュリティサービス推進室
E-mail：mss-sp-cp@ntt.com