アンラボ・セキュリティレター

Press Ahn

2014.3　Vol.03

「MDS」メモリ分析ベースの検知技術を搭載

行為分析を回避するマルウェアをスマートに検知

「MDS」メモリ分析ベース検知技術を搭載

多くのAPTソリューションベンダーでは、未知のマルウェア（unknown malware）を検知する対策としてシグネチャレス（signature-less）技術を強調している。これは仮想マシン（Virtual Machine）やサンドボックス（sandbox）ベースの行為分析技術を意味する。しかしサンドボックスベースの分析技術も、もはや効果的な方法とはいえない状況だ。最近の攻撃者は、自動化された行為分析システムを回避する、高度化されたマルウェア作成に力を入れている。マルウェアは日々想像以上の進化を遂げているのだ。

本コラムではサンドボックスベースの行為分析技術の限界と、これに代わるアンラボの対APTソリューションMDS（Malware Defense System 以下MDS）の新機能について紹介した。

サンドボックスの自動分析技術すら無力化する、高度なマルウェア

2012年11月、ASEC（AhnLab Security Emergency Response Center）に興味深いマルウェアサンプルが検知された。これは「韓国空軍のプレゼンスに対する評価と診断」という件名のメールに添付されたドキュメントファイルで、大韓民国空軍の目標や航空宇宙軍に対する社会の認識について詳細な内容が記載されており、メールの受信者が国防関連の重要文書であると信じ込ませるように見せかけていた。

これこそは攻撃者が標的を意識して仕掛けたAPT攻撃だった。そして添付されたドキュメントファイルも驚くほど巧妙に作成されていた。

ファイルの悪性可否を判断しにくくするためにヒープスプレー（[1]Heap Spray）をごく少量に抑え、ヒープスプレー検知を回避した上にソフトウェアの最新バージョンのみマルウェアが実行されるようになっており、バージョンが低いソフトウェアでは作動しなかったのである。

だがこのドキュメントファイルは、明らかに悪意ある行為を実行していた。はたしてこのファイルの秘密は何だろうか。

このファイルが作動するためには特定の条件が揃わなければならない。まず、内容を確認するためユーザーがドキュメントファイルを展開する。内容を読みながらスクロールバーを下に移動させ、2ページ目の「問題提起」という段落に到達した瞬間、「HncCtrl.exe」というファイルが自動作成された後に実行される。これは悪意ある不正ファイルであり、実行されると連続してまた別の不正ファイルが作成・実行されるのだ。これらのファイルはPCから個人情報を収集し、特定のメールアドレスに送信するようになっていた。つまり攻撃者は、特定のアクションがあってこそエクスプロイトが発動するようにマルウェアを設計したのである。これはドキュメントファイルを利用した最新APT攻撃タイプの一つで、自動化されたサンドボックス分析システムを回避する代表的なケースである。

1 ヒープスプレーとは、Windows が持っている不正プログラムの実行防止機能を回避し、攻撃成功率を高めるための手法。ヒープと呼ばれるメモリ領域に対して不正なプログラムをスプレーで塗りつぶすように大量に書き込み、不正プログラムが実行される可能性を高める。（出展： 情報技術辞典 平成 22 年版）

仮想環境の行為分析技術（Behavior Analysis in Sandbox）における限界

現在多くのAPTソリューションベンダーは、新種のマルウェア（unknown malware）を検知するためシグネチャに依存しないシグネチャレス（signature-less）技術の必要性を強調している。特に一部のベンダーでは「行為ベース分析」技術が、まるで新種のマルウェアを検知する唯一のシグネチャレス技術であるかのように主張している。だがこのサンドボックスなどの仮想環境ベースの行為分析技術を採用したソリューションだけで、日々高度化するマルウェアを十分に検知できるだろうか？　この問いに対する答えは「No」である。

ではサンドボックスベースの行為分析技術の限界は何か。同技術を採用した対APTソリューションの問題点について最新情報をまとめた。

サンドボックスベースの行為分析技術とは、分析対象をサンドボックスと呼ばれる限られた環境の中で実行させ、行為（behavior）の結果によって正常か脅威かを判断する技術だ。

だがこの技術を採用しているAPTソリューションが、100%機能を遂行するためには必ずマルウェアが作動しなければならない。つまり、マルウェアがサンドボックス分析環境下で常に意図している行為を予想したプロセス通りに動作してこそ検知できる。だが前述したように、最近では何ら行為も起動しないドキュメントファイルを利用した攻撃が増加し、自動化されたサンドボックスの分析システムを回避し始めた。

行為分析システムを回避する最新マルウェアの代表的な3つのタイプは次の通りである。

1. **特定のユーザーアクションを検知して悪意ある行為を実行するマルウェア**

   前述のケースから見るとマルウェアが潜むPDFファイルを展開するだけでは何も起こらず、ユーザーが特定のページにスクロールしてこそマルウェアの悪意ある行為が作動した。

   他にもPCがマルウェアに感染した状態でユーザがマウスをクリックしたり特定の方向に移動させるなど、入力デバイスの変化を検知した時に初めて作動したケースもある。興味深いのは、このケースではマルウェアに感染したことを警告するメッセージウィンドウが表示されたが、確認後に「OK」ボタンをクリックした場合のみ悪意ある行為が実行された。これらのマルウェアはユーザが特定のアクションを行うまでは疑わしい行為を見せないため、事前に検知するのが非常に難しい。

2. **自動化されたサンドボックスで制御が難しい「時間の制約」を利用するマルウェア**

   ほとんどのAPTソリューションは自動化された行為分析のため、仮想マシン（Virtual Machine）やサンドボックス（Sandbox）環境を使用する。しかしこれらの環境を起動するためにはハードウェアの限られたリソースを使用することになる。そしてサンプルの行為動作が終了するまで、1つのサンプルに対するダイナミック手法の分析時間を無限に使用することはできない。マルウェア作成者は、この点を突いて特定の時間に悪意ある作動を実行するスケジュール（scheduling）技法を使用する。これらの手法を利用するマルウェアを「時限爆弾マルウェア（time - bomb malware）」または「トロイの木馬ナップ（Trojan nap）」という。一部のAPTソリューションは時限爆弾手法に利用される「スリープ（sleep）API」など、特定のAPIを使用した場合は確実にマルウェアとして検知する。ただしAPIは通常のプログラムでも使用されるので、検知ミスが増加する可能性もある。

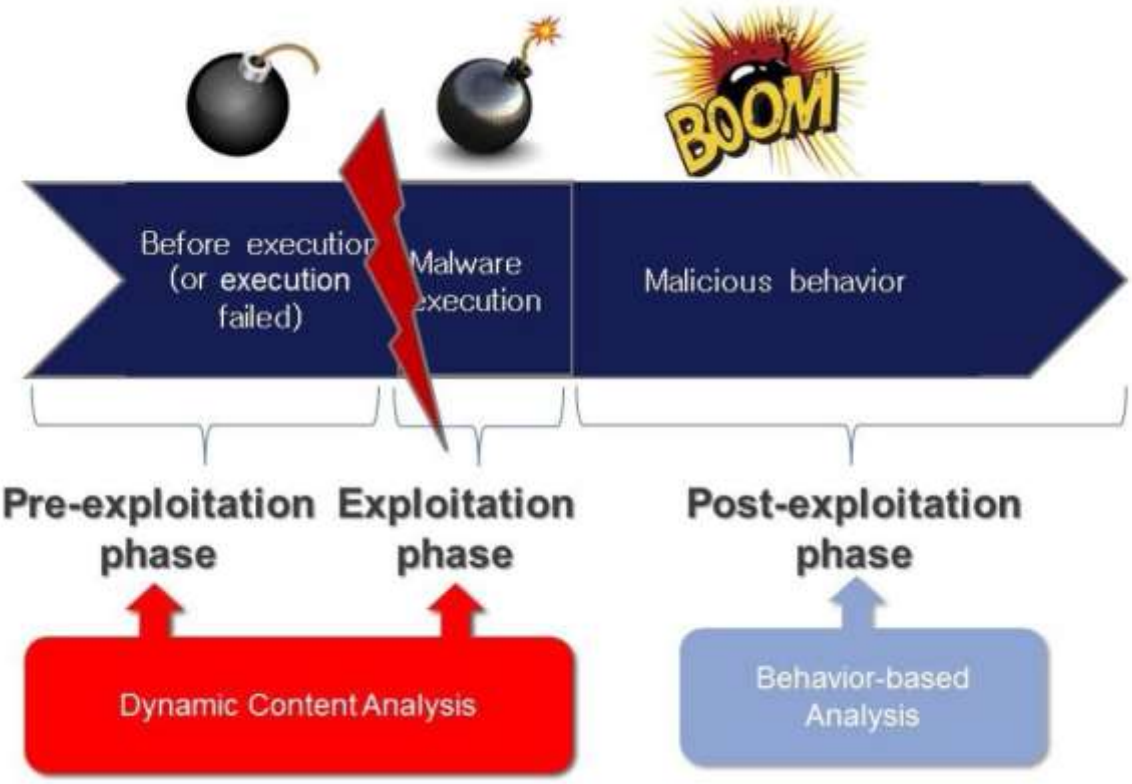
3. **仮想マシンまたはサンドボックスを認知して悪意ある動作を隠ぺいするマルウェア**

   攻撃者がインテリジェントなマルウェアを作成する理由は、APTソリューションの検知と分析を回避するためだけでなく、ダイナミック分析においても仮想マシンやサンドボックスが使用されるからだ。一部のAPTソリューションは実行中のプロセス、レジストリキーやレジストリ値、仮想ハードウェアなどの仮想マシンやサンドボックス内の様々な変化の試み自体を検知する。しかしマルウェアは逆に検知機能を認知し、悪意ある動作を実行しないように進化しているのだ。

MDS、メモリ分析ベースのエクスプロイト検知技術を搭載

MDSは高度化されたマルウェアを検知するため「ダイナミックコンテンツ分析（Dynamic Intelligent Content Analysis）」という新しい技術を適用した。これはメモリ領域でアセンブリコード（assembly code）ベースに分析する技術で、アンラボが開発した独自の技術である。

この技術はアプリケーションの脆弱性攻撃の段階（exploitation phase）からマルウェアか否か判断し、新たなゼロデイ（zero - day）脆弱性を突くマルウェアも検知が可能だ。



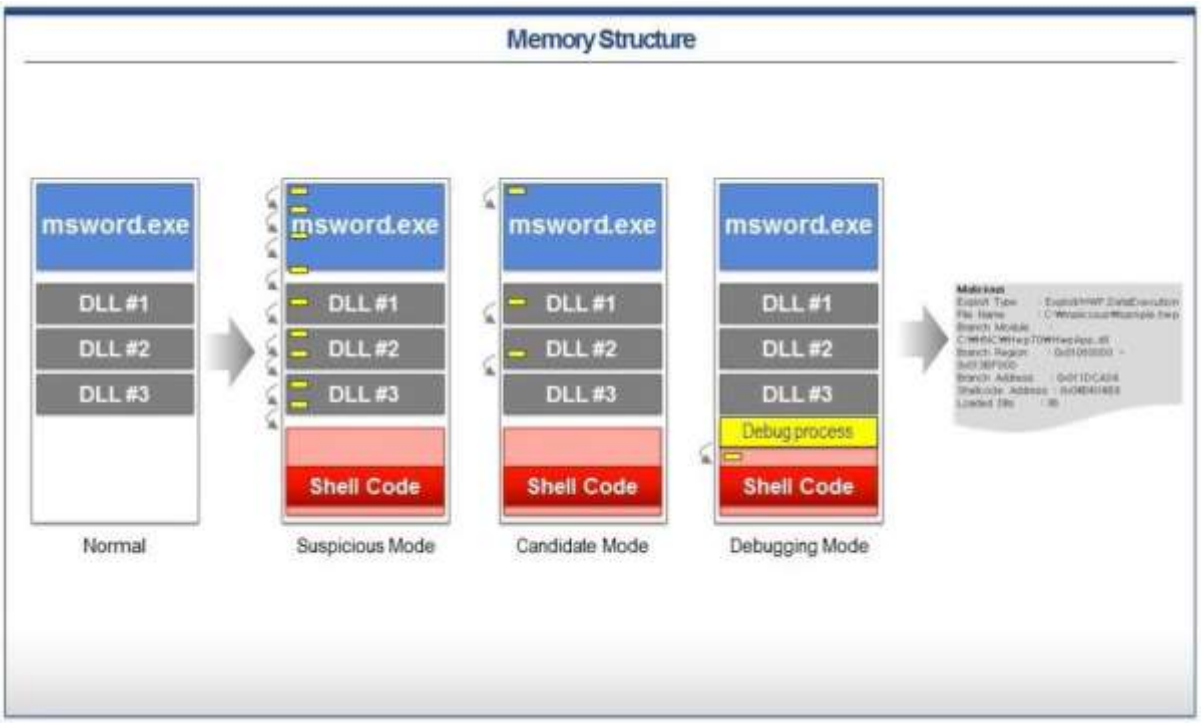
【図1】ダイナミックコンテンツ分析技術の概念

[図1]は、MDSのダイナミックコンテンツ分析技術の基本的な概念を図に表したものだ。特定のアプリケーションの脆弱性を攻撃するマルウェアが難なく設計通りに脆弱性をエクスプロイト（exploit）し、不正行為を実行すると仮定してみよう。このマルウェアが最終的に悪意ある行為を作動させるまでが「作動前（pre- exploitation phase）」段階であり、条件が揃った後にマルウェアが作動する「作動時点（exploitation phase）」段階に区分することができる。このマルウェアが作動前の段階で正常に動作しなかったり、マルウェアの作動時点で仮想マシンやサンドボックス環境を認識して何も反応しない場合は「行為ベース分析」技術は用無しになってしまう。

これにより悪意ある動作に関係なく、マルウェアの作動前段階またはマルウェアの作動時点においてもマルウェアを検知できる方法が必要となる。

この行為ベース分析技術の限界を克服し、エクスプロイトが発生する前の段階からマルウェアを検知するために開発されたのが、MDSのダイナミックコンテンツ分析技術なのだ。

MDS のダイナミックコンテンツ分析技術の仕組み



【図2】 Dynamic Intelligent Content Analysisの動作原理

[図2]はメモリ構造を簡単に図式化したもの。例えば、ここにバッファオーバーフロー（buffer overflow）攻撃に脆弱なマイクロソフトのWordファイルがあるとしよう。[図2]の左側「Normal」は、正常な Wordファイルを実行したときの状態だ。Normalファイルをクリックすると、メモリ上にはメインプログラムであるwinword.exeに関するダイナミック ライブラリファイルがロードされる。これが正常な状態であれば、DLL＃3まで処理されると通常のWordファイルが展開される。

では脆弱なWordファイルを攻撃するエクスプロイトが作動するとどんなことが起こるのか。最初はNormalの場合と同様プログラムが実行されるが、ある瞬間ダイナミックにデータを格納するヒープ（heap）と呼ばれる領域にシェルコードを保存しておく。その後バッファオーバーフローが発生するエクスプロイトタイミングに、正常であればDLL＃3に移動するEIPが、異常シェルコード領域にジャンプ（jump）することに。そしてシェルコードにコーディングされた悪意ある動作が生じることになる。

ダイナミックコンテンツ分析技術を搭載したMDSなら、こういった場合にはマルウェアを次のように検知できる。

分析対象プログラムがメモリ上にロードされた時点で「デバッグスレッド」を直接挿入し、異常メモリ領域への移動/ジャンプを検知する。ダイナミックコンテンツ分析技術は、通常のバッファオーバーフローはもちろんのことSEH（Structured Exception Handing）、RTL（Return-to-Lib）、ROP（Return-Oriented Programing）、ヒープスプレー（Heap spray）などマルウェアが利用する様々な脆弱性を攻撃（exploitation）する段階で検知できる。つまりMDSのダイナミックコンテンツ分析技術は、マルウェアの悪意ある動作タイプや発生可否に関係なくマルウェアを検知できる。

事前にAPTを遮断せよ

MDSのダイナミックコンテンツ分析技術は、アンラボが開発した十数余のアルゴリズムを基に完成させ独自の技術だ。

代表的なものとしては悪意ある非実行ファイルがエクスプロイトを作動させる前の段階でヒープスプレー（Heap Spray）を介してシェルコードを保存する手法、スタックオーバーフロー（Stack Overflow）を介してシェルコードを保存する手法、悪意あるスクリプトを含むメモリ領域にシェルコードを保存する手法などがある。特にMDSは、アプリケーションの脆弱性を攻撃する不正ファイル内のシェルコードの正確なメモリの開始ポイントを判断し、シェルコードのメモリダンプとそのアセンブリコードを視覚的に認識できるように表示する。メモリ分析を通じてシェルコードを検知してシェルコードの開始アドレスを正確に提供することは、MDSならではの差別化された特徴であり最も優れた技術である。

これまで紹介したMDSのダイナミックコンテンツ分析技術は、マルウェアのアナリストやセキュリティ研究者にとっては革新的な概念ではない。

しかしこれらの技術が自動化された分析システムに搭載され、大量のファイルを分析できるという点からマルウェアの分析と高度化されたAPT攻撃の猛攻を食い止めるための新境地を開いたと評価できる。

MDSは本技術を採用する環境や動作の実行条件など、潜在的な要因に影響を受けずにマルウェアを診断することができるため、APT攻撃を事前に遮断する強力な保護を実現できるだろう。

http://www.ahnlab.co.jp

http://global.ahnlab.com

http://www.ahnlab.com

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒101-002 東京都千代田区外神田4-14-1 秋葉原ＵＤＸ ８階北 | Tel：03-5209-8610 (代)