ワームとの戦いに勝利するには

DefensePro ホワイトペーパー

Avi Chesla, ラドウェア社セキュリティ担当副社長

North America

Radware Inc.

575 Corporate Dr., Lobby 1
Mahwah, NJ 07430
Tel: (888) 234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.
Tel Aviv 69710, Israel
Tel: 972 3 766 8666

www.radware.com

要旨

ワームは、人手を介さずにファイルを感染させる自己増殖型のプログラムです。この種のプログラムは多くの場合、大規模な DDoS 攻撃（分散型サービス拒否攻撃）を行ったり、企業の IT 運用を中断したりする目的で設計されており、収入の損失が生じます。過去数年にわたってインターネット上で拡散したワームは、世界中の企業の IT 運用に大きな損害を与えてきました。ワームによる DDoS 攻撃によって引き起こされた混乱が毎週のようにニュースになっています。IDC の企業調査 2005 は、ワーム、ウィルス、およびトロイの木馬が引き続き企業にとって最大のセキュリティ上の脅威であるとしています。ビジネスにおける大きな損害に加え、この種の攻撃による金銭的な損失は、何百万ドルにも上ります。セキュリティ製品を取り扱う数多くのベンダが、ワームの増殖の問題に取り組んできました。しかし現状では、どのソリューションも効果を上げていません。

ワームの拡散のメカニズム

ワームは通常、複数の代替可能な手段を使用して、ネットワークに侵入します。ワームは、企業のインターネット・ゲートウェイを通過して増殖するか、従業員が感染したノートパソコンをオフィスに持ち込むことによって企業内に入り込みます。多くの場合、オフィスから頻繁に外出する営業担当が、気付かないうちにワームの「ゾンビ」キャリアになっています。上記の方法で、ワームは自由にネットワーク内に入り込むことができるのです。ワームはいったんネットワーク内に侵入すると、自由かつ急速に拡散可能で、指数関数的に自己増殖します。自己増殖による大量のパケットがネットワーク内に溢れ、正当なトラフィックがブロックされてしまいます。ファイアウォール、スイッチ、ルータ、さらにはサーバおよびエンドステーションなどの企業のリソースが使用不可能になり、ビジネスが中断されてしまいます。

ネットワーク攻撃者がもたらした最大の革新の 1 つは、ネットワーク管理者が効果的な防止手段を実施する時間がないほど急速に拡散するワームです。たとえば、2003 年に発生した SQL スラマーは、約 10 分間でインターネット全体に拡散しました。このワームは、インターネットに接続されたホストの 15%に感染することに成功しました。ネットワーク管理者は、このワームの拡散の急速さに不意打ちされたのでした。

ではワームは、どのようにして広大なインターネットでこのように急速に自己増殖できるのでしょうか。SQL スラマーの場合、コネクションレスプロトコルの UDP（User Datagram Protocol）によって拡散しました。また、このワームは比較的小さなペイロードを使用しており、脆弱性の存在するホストに感染するために 1 パケットも必要としませんでした。こうしてこのワームは、すぐに数多くのホストに難なく増殖することができたのです。

TCP（Transmission Control Protocol）などコネクション型のプロトコルを使用するワームの増殖は通常、より遅いものとなります。コネクション型のプロトコルでは、ワームはホストからより多くのリソースを必要とし、たとえば通常、複数の通信スレッドを開放します。この場合、感染したそれぞれのホストは、他のホストを感染させるために、その対象ホストと完全な 3 方向ハンドシェイクを完了させる必要もあります。そのため、ワームの拡散速度は遅くなります。

コネクション型のプロトコルを使用するワームの拡散速度は速くはありませんが、攻撃による副産物があります。たとえば、SYN パケットの増加は、それ自体が DDoS 攻撃になります。コネクションレスプロトコルを使用して拡散するワームでは、こうした効果を上げることはできません。

世界最速のワーム

SQL スラマーは、これまでで最速の増殖速度を持つワームです。このワームによるトラフィック量は膨大であるため、多くの企業ネットワークおよびインターネット・サービス・プロバイダ（ISP）のネットワークコアで混雑が引き起こされました。インターネットに接続されたルータ、スイッチ、ファイアウォールなど多くのネットワーク・コンポーネントがサービス拒否状態に陥りました。

ワームとの戦いに勝利するには

自己増殖型ワーム

自己増殖型ワームとは、人間の手を介さずに拡散するワームのことです。自己増殖型ワームは通常、ランダムな IP アドレス生成テクニック（つまり、スキャニング）を使用することによって、脆弱性が存在する感染対象のホストを検出します。脆弱性の存在するホストを特定すると、ワームはそのホストで直ちにコードを実行し、悪意のあるコードでコンピュータを感染させます。次に、両方の感染したホストが同様のスキャニング・テクニックを開始して、他のホストを感染させます。このように、ワームは指数関数的に増殖していきます。

ランダムな IP アドレス生成テクニックは複数存在し、テクニックの効率によってワームの感染到達効率が異なります。

また、より高度なスキャニング・テクニックを使用するワームもあります。たとえば、Code Red II は、8 分の 3 の確率で感染したホストの IP アドレスの最初の 2 バイトを使用することにより、次の感染対象の IP アドレスをスキャンしました。そのため、IP 生成メカニズムはランダムではなく、決定性のパターンに従いました。ワームのスキャニング・アルゴリズムの解析はこのホワイトペーパーの対象ではありませんが、使用される増殖メカニズムがワームの感染到達効率に大きく影響する点は特筆に値します。

他の増殖方法

自己増殖するように設計されたプログラムのほかに、インターネット・メッセンジャー、P2P アプリケーション、および電子メール・サービスを使用して拡散するワームも多く存在します。これらのサービスには人手が介入するため（添付ファイルを開いたり、ハイパーリンクをクリックしたりするなど）、この種のワームの拡散速度は遅く、拡散効率が低い傾向があります [1]。

ワーム：防御の課題

ワームの増殖防止の目的を明らかにさせる必要があります。ワームを隔離できれば、正当な通信を妨害する能力は大幅に低下します。

数多くのセキュリティ・ベンダが、ワームによる攻撃をはじめ、ネットワーク攻撃を撃退する目的の製品を発売してきました。しかし、次に挙げるようないくつかの技術上の問題に直面しています。

- ***正当なトラフィックを妨害せずにワームの増殖をブロックする方法*** ：ワームは多くの場合うまく偽装していて通常のネットワーク・トラックに見えるため、これは容易ではありません。防御レベルを高くしすぎると、正当なトラフィックもブロックされてしまい、エンドユーザおよびネットワーク管理者が困ってしまいます。防御レベルを低くしすぎると、ワームは拡散しつづけます。

- ***新しい未知のワームの検出方法*** ：セキュリティ・デバイス・ベンダが「タグ付け」できないほどの速さでワームは増殖するようになってきています。そのため、セキュリティ製品は、検出技術として事前定義された攻撃シグネチャに頼ってばかりはいられません。

- ***製品の運用と保守を単純化する方法*** ：システムの誤設定は、誤検出や未検出の原因となります。IT 担当者の仕事量は既に非常に多いので、継続的にセキュリティ・デバイスを調整したり更新したりすることを期待するのには無理があります。そのため、ワームをブロックするデバイスは、保守要件が低い「接続するだけで防御できる」製品である必要があります。

---

[1] 一部のセキュリティ専門家は、ワームを自己複製型の悪意のあるコードとして定義し、ウィルスを人間の介入によって拡散される悪意のあるコードとして定義しています。

ワームとの戦いに勝利するには

・***製品の精度を高める方法*** ：上述のすべての理由から、ワームをブロックするデバイスは、ワームの増殖パターンを正確かつ迅速に特徴付け、自動的に粒度の細かい対策を開始できる必要があります。デバイスの防止技術は、正当なネットワーク・トラフィックに影響を及ぼさずに、ワームによって生成された接続のみをブロックできる非常に正確なものである必要があります。ブロック基準は、ソース IP アドレスだけではなく、ワームの拡散パターンを特徴付けるその他のパラメータ（宛先 IP、ポート番号、ペイロード情報、TTL など）にも基づく必要があります。

・***ワームの変化しつづける動作にリアルタイムでネットワークを適合化させる方法*** ：ワームへの対策は、変化しつづけるワームの動作にリアルタイムかつ動的に適合し、「スマートな」変異型ワームでも迅速かつ永続的に処理できる必要があります。

ワームの脅威の除去

ワーム封じ込めの目標は、危害を加えられる前にその増殖を阻むことです。現在ソリューションを発売しているほとんどのセキュリティ・ベンダは、反応性の対策（ワームに感染したシステムに対するパッチおよびアップグレード）を提供しています。もちろんこうしたソリューションは、ワームによる被害を受けたネットワークの修復にのみ有効であり、ワームの防止対策にはなりません。一方、別の少数のベンダでは、脆弱性のスキャニングおよび自動「アクティブ」パッチを採用した「積極的な」ソリューションを提供しています。この種の製品は、感染する前に脆弱性の存在するシステムにパッチを当てることで新しいワームに対処することを意図していますが、効果的なソリューションではありません。その理由は 2 つあります。まず、効果的であるためには、（ベンダが提供する）最新の脆弱性情報で更新する必要があります。今日のワームは、脆弱性が報告されるとすぐに拡散しはじめます。つまり、このような自動パッチ製品の自動更新は不可能です。2 つ目の理由として、これらのシステムは多くの場合、実行中のクリティカルなアプリケーションを一部中断してしまうため、常時ではなく限られたときにしか作動できません。

ネットワーク侵入防止システムは、静的なシグネチャを使用してワームを特徴付けるため、ワームによるネットワークへの影響を阻止することができません。前述のように、セキュリティ・デバイス・ベンダが「タグ付け」（ワームのシグネチャの作成）できないほどの速さでワームは増殖するため、シグネチャベースの侵入防止システムは、ワームに対して効果的ではありません。

ワーム駆除製品：DefensePro IPS

DefensePro は、前のセクションで取り上げた課題を設計上考慮し、ネットワーク・ワームの増殖をなくす上で非常に効果的な、これまでにない真に積極的で適合型の IPS 機能を組み込みました。DefensePro は、非常に精度が高くかつ簡単に使用できる、Adaptive Smart Dynamic Filters™ を採用しています。高度な統計解析、ファジーロジック、および新しいクローズド・フィードバック・フィルタリング・メカニズムを採用した DefensePro IPS デバイスは、侵入してくるワームを被害が生じる前に自動的かつ積極的に撃退し、防御します。この製品は、ワーム検出のためにシグネチャを使用せず、ユーザ定義の動作ポリシーや閾値にも依存しません。デバイスは、通常のトラフィックの変化にも適合するため、自然に進化していくネットワーク動作の影響を受けません。

DefensePro IPS を使用すれば、ネットワーク・ワームの阻止に加えて、システム管理者は感染したホストを特定することができます。DefensePro のトラフィック・フィルタは非常に粒度が細かく、変異型ワームにも適合できるため、感染した「ゾンビ」ホストは引き続き（ワーム・トラフィックではなく）正当なトラフィックを送信することができ、後からホストにパッチを当てたりアップグレードしたりすることができます。

つまり、DefensePro IPS ソリューションを使用すれば、使用および保守の非常に簡単なセキュリティ装置だけで、完全なビジネスの継続性を保証しながら、ワームの増殖を防止することができるのです。

ワームとの戦いに勝利するには

DefensePro IPS の仕組み

DefensePro は、ネットワーク・トラフィックに対して「インライン」に（通常はネットワークの周辺または重要なネットワーク・セグメントの間に）配置されるハードウェア装置です。
DefensePro は、次の 3 つの自動同期プロセスを使用して、ワーム防止を最適化します。

- **検出** – ワーム増殖のリアルタイムの検出
- **特徴付け** – ワーム増殖プロファイルの分類
- **緩和** – ワームの進化プロファイルをブロックする Adaptive, Smart, Dynamic Filters™ の起動

これらの各プロセスを以下に説明します。

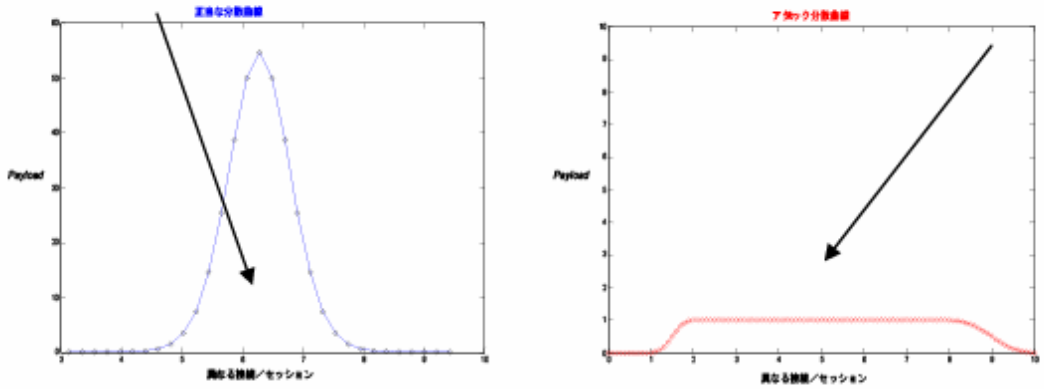
ワームの検出

ワームの検出は、ネットワーク内の接続全体でのホスト（つまり、保護されたネットワークに接続するユーザ）のペイロード分散の解析に基づいています。このユーザ分散曲線を表す解析パラメータが意思決定エンジン（ファジーロジック推論システム）に渡され、特定のトラフィックが攻撃である可能性を計算します。このシステムは時不変であり、低速ワームの拡散アクティビティも検出されます。

下の左の図は、正常なトラフィック動作パターンを示す正常なトラフィック分散曲線です。右の図は、攻撃（例：ワームの増殖）を示すトラフィックです。分散曲線は、多くのユーザのトラフィック・パラメータを高度に統計解析して、意思決定エンジンが生成します。下図では、統計解析によって得られたパターンが示されています。

分散曲線の例

正当なユーザ・プロファイル　　ワーム・プロファイル



Y 軸：ペイロード/接続、X 軸：接続 ID（各接続の宛先 IP およびポート）

意思決定エンジンの重要なタスクは、分散曲線が正常な行為、疑わしい行為、または攻撃行為を示すときを判断することです。この意思決定エンジンは、さまざまなワームのスキャニング・アクティビティに対してテストされており、無視できるほどの未検出および誤検出しか起こらないことが証明されています。

ワームとの戦いに勝利するには

ワームの特徴付け

IPS システムが提供すべきもっとも重要な機能の 1 つが、ワーム増殖動作を正確に特徴付けることです。特徴付けが正確であれば、対応する防止対策は、正当なネットワーク・トラフィックを阻害することなく、ワーム拡散動作を正確に捉えることができます。

DefensePro の特許出願中のテクノロジ・ブレークスルーの 1 つに、ワームが使用している現在の（および変異する可能性がある）増殖方法を動的に特徴付ける機能があります。このテクノロジは、ワーム・プロファイルを特徴付ける統計アルゴリズムの新たな実装を基盤としています。プロファイルには、ワーム発生元やエクスプロイトの対象となる脆弱性が存在するアプリケーションなどの情報が含まれます。

ワームのフィルタリング

前述のとおり、ネットワーク侵入防止システムの重要なタスクの 1 つは、ワームによるネットワークへの影響を緩和し、ネットワーク管理者がシステムのアップグレードやパッチ（すでに存在している場合）などの対応措置を実行して、すべての感染したホストを封じ込められるようにすることです。

DefensePro の緩和モジュールは、正当なトラフィックを（感染したホストからのものであっても）通過させる一方で、ワームのアクティビティを効果的に防止するフィルタを生成します。

緩和モジュールは、特徴付けモジュールが生成したワームのプロファイルによって、防止対策を生成します。これらの防止対策によって、トラフィックをブロックしたり速度制限したりすることができます。どのような場合でも、ブロックまたは速度制限は、ワームの拡散プロファイルに一致するトラフィックにのみ適用されます。

クローズド・フィードバック

DefensePro は、ワーム対策の効果を継続的に評価し、結果に応じて対策を調整することで防止対策を最適化するクローズド・フィードバック・テクノロジを内蔵しています。

クローズド・フィードバック・メカニズムは、次の手順で防止対策を最適化します。

- **手順 1** – 最初の防止対策（フィルタ）は、ワームを分類するもっとも広い基準で作成されます。たとえば、ワームが脆弱性のあるポートを 2、3 偵察する場合は、最初の防止対策では、もっとも集中的に偵察されているポートを対象とした感染ホストからのアクティビティのみをブロック（または速度制限）します。

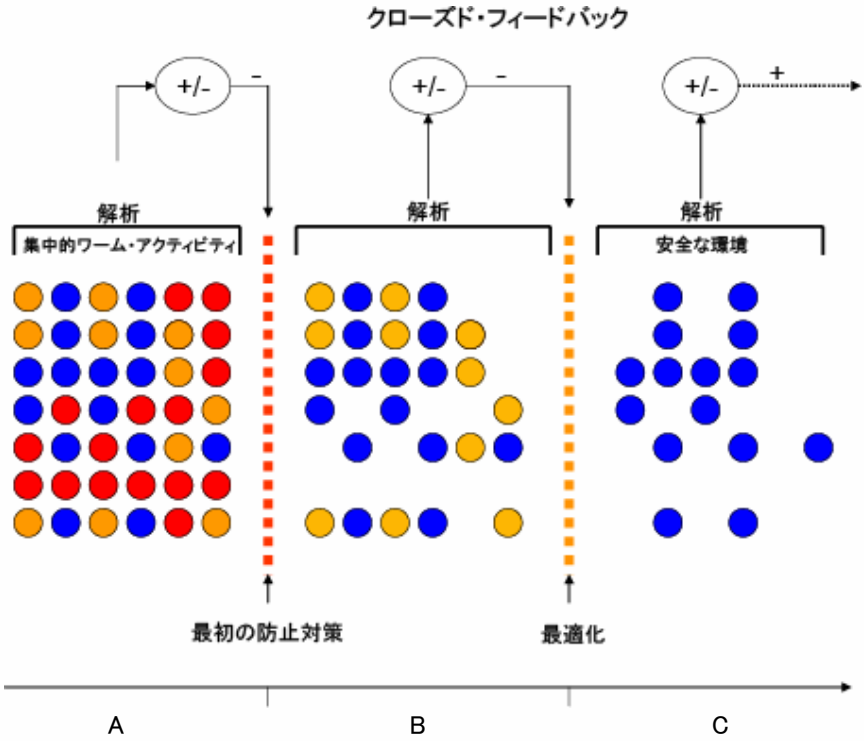
- **クローズド・フィードバックの確認** – クローズド・フィードバック・メカニズムは、最初の対策の効果（ネットワークが「妨害されずに」機能できるレベルまで十分にワームのアクティビティがフィルタされているか）を評価します。最初の対策が成功した場合、そのフィルタが維持されます。ここで、ネットワーク管理者は感染したシステムに対してパッチおよびアップグレードを実行できます。

- **クローズド・フィードバックの最適化** – 最初の対策の効果が十分ではなかった場合（ワーム増殖アクティビティがまだネットワークの運用を妨害している場合）、クローズド・フィードバック・メカニズムは、前段階のフィルタに加えて、粒度が粗い追加フィルタを組み込みます。フィードバック・プロセスは、攻撃が制御されるまで継続されます。この間、正当なトラフィックは影響を受けません。

- **クローズド・フィードバック動的フィルタ** – クローズド・フィードバック・メカニズムは、継続的に動作します。ワームの拡散プロファイルが変わった場合、クローズド・フィードバック・メカニズムは、そのワームの新しい特徴に最適化された新たな防止プロファイルを生成します。

クローズド・フィードバックによるワームのフィルタリング – 例

次の図は、正当なトラフィックに影響を与えずに、ワームの拡散アクティビティが緩和されるまでの、クローズド・フィードバック処理の仕組みを説明したものです。



上図の説明:

A – 赤色とオレンジ色のボールは、ワームの拡散アクティビティを示しています。赤色のボールは、より集中的な拡散アクティビティです。青色のボールは、正当なトラフィックです。

B – ワームに対する最初のフィルタが有効化(赤いボールを撃退)されると、クローズド・フィードバック・メカニズムは、残りのワームの拡散アクティビティ(オレンジ色のボール)がネットワーク処理を妨害する方法を評価します。粒度の粗い基準にしたがって、前段階の対策に加えて、追加防止策を有効化します。

C – 図中では、防止対策は効果的であるとみなされ、これ以上対策は実施されません。

要約

ワームは、収入の損失および評判の低下という形で、組織に大きな損害をもたらします。これまで、既存のネットワーク・セキュリティ・ソリューションでは、ワームは効果的に制御されていませんでした。

DefensePro は、ワームの増殖を防止する、現在もっとも効果的でシンプルな製品です。
DefensePro は、人手を介さずに、ワームの拡散アクティビティを検出し、特徴付け、防止します。
DefensePro は、感染したシステムを特定して保護するため、ビジネスの継続性を保証すると同時に、システム管理者には対応策(システムに対するパッチおよびアップグレード)を実施する時間的余裕を提供します。
DefensePro を使用すれば、今日の組織を脅かすワームなどのネットワーク攻撃を正確に防御することができます。