スパマーになっていませんか？
～ ゾンビ感染から組織を守る ～

A Sophos positioning paper
March 2006

ハイジャックされたコンピュータ（つまりゾンビマシン）は、ネットワークの中に隠れて、スパムを送信し、組織の機密を盗み、また他の深刻な犯罪に利用されます。このポジショニングペーパーでは、組織が絶えずさらされている急速に蔓延するゾンビマシンからの攻撃や、信頼性の高いゲートウェイ/エンドポイント保護のあるネットワークにおいても、マシンをゾンビ化されてしまう危険性などについて説明します。また、ゾンビマシン検出用のツールで組織を保護する必要性について説明します。

攻撃にさらされる組織のマシン

ゾンビマシンとは、知らない間にウイルスに感染し、許可されていないユーザーやリモートユーザーが制御できるようになっているコンピュータのことです。コンピュータがいったんゾンビ化されると、ハッカーは何千もの感染コンピュータが含まれるネットワークに接続して、さまざまな種類の犯罪を実行ために利用します。ゾンビコンピュータのネットワークは、ハイジャックされた企業がまったく意識しないうちに、スパムやウイルス、フィッシング詐欺メール、アダルトコンテンツなどを送信するために使われます。ソフォスは、全スパムの60%以上が、ハイジャックされたコンピュータから送信されていると推計しています。ゾンビマシンは、投資コンサルティング会社から大学や老人ホームまで、さまざまなタイプの組織で発見されています。ゾンビマシンはビジネスの混乱を招き、ネットワーク障害、情報窃取、組織の信用失墜の原因となります。

- **ビジネスの混乱：** システム管理者は、ドメインネームサーバーブロックリスト（DNSBL）に組織がスパマーとして表示されるまで、ネットワーク上にゾンビマシンがいることに気づかないことがあります。企業のメール配信を停止させ、それにより通常のビジネス機能を低下させます。
- **ネットワーク障害：** ゾンビマシンは組織内にある他のコンピュータに絶えず感染しようとし、組織内のネットワーク機能を低下させます。また、不法コピーのソフトウェアやビデオを保存するためにも利用され、他の組織にもハッキングを行って、ネットワークのリソースをさらに消費します。
- **情報窃取：** 顧客データベースや銀行のアカウントパスワードなどの個人情報は、ゾンビマシンによって盗まれる危険にさらされています。ゾンビマシンは、情報をハッカーに送信する前に、（キーロガーのような）スパイウェアをインストールしてキーボード上で行われる操作を全て把握することができるため、暗号化でさえ情報の保護対策にはなりません。
- **信用の失墜：** 組織がスパムを送信したり、他の犯罪を助成したりしていると思わせるゾンビマシンの不法行為は、踏み台として悪用された組織の評価やブランド価値を傷つけます。たとえば、ゾンビネットワークは、何千ものコンピュータが一斉に Web サイトにアクセスするような分散サービス拒否（DDOS）攻撃を仕掛けるために頻繁に利用され、サーバーに過負荷をかけて、シャットダウンを引き起こします。

速い、そして見えない

ゾンビマシンは一般に、エンドユーザーに知られないまま機能し、組織に引き起こすダメージは、知らない間に蓄積していきます。たとえば多くのゾンビマシンは、スパムを送信するために、非常に短期間の間だけ「活動」し、再び休止することによってその存在を隠すようにプログラムされています。

この文書は、2005 年 11 月に米国ソフォスで発行された『Are you a spammer? Why stopping zombies dead in their tracks is essential』を翻訳し、編集したものです。

セキュリティ対策が全く行われていないコンピュータをインターネットに接続すると、約50%のコンピュータが12分以内にゾンビ化される可能性があります。

ゾンビマシンは、気づかれずに機能するだけでなく、極めて速く作成されます。ソフォスのリサーチでは、ウイルス対策保護やファイアウォールがなくパッチが適用されていないコンピュータがインターネットに接続すると、約50%のコンピュータが12分以内にゾンビ化されることが示されています。図1に攻撃のスピードについて示します。Windows XP が起動されインターネットに接続されている無防備なコンピュータ上で、ウイルス感染の可能性が時間とともに増加していく様子が、グラフに表されています。

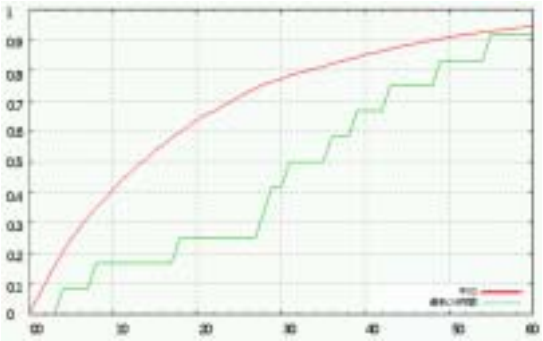

図1 インターネットに接続した無防備なコンピュータの感染確率

増加する脅威

セゾンビネットワークは、その作成スピードの速さと潜伏性で、犯罪者達の非常に手ごろなビジネスツールになっています。アドウェアをインストールしたり、スパイウェアやフィッシング詐欺によって機密情報を盗んだりすることにより、ゾンビマシンで多額の利益を得ることができます。悪質なダイヤラーをインストールしてユーザーに多額の電話代を請求したり、DDOS 攻撃の脅威を使って組織から金銭をゆすり取るためにゾンビマシンを利用することも可能です。

ゾンビネットワーク自身を売りに出すことさえも可能です。スパマーのフォーラムでは、2万台のコンピュータを含むネットワークのレポート1件が、2千ドルから3千ドルで売りに出されています。[1]

しかし、ゾンビマシンによって収入を得る最も一般的な方法は、スパムを送信することです。スパム対策の方法は、DNSBL を使用し、送信者認証情報（レピュテーション）に基づいてスパムメールを阻止することで、かなりの効果的があがっています。ゾンビネットワークは、レピュテーションで「問題がない」と評価されている送信者のコンピュータをハイジャックしてスパムを送信することにより、ブロック（阻止）リストに対抗します。スパムを送信し続けるには、識別あるいは駆除されてしまったゾンビマシンやブロックリストに載ったゾンビマシンと入れ替えるために、絶えず新しいゾンビマシンを作成して供給する必要があります。

スパム対策技術が継続的に進歩するのに対抗して、スパマーはさらにゾンビマシンを作成し続けます。近年の急速なゾンビウイルス数の増加は、世界各地に展開する脅威解析センターであるソフォスラボ（SophosLabs™）が確認した最新の300のウイルスのうち、3分の1以上がゾンビの機能を持っていることにも示されています。

コンピュータをゾンビマシンにする方法

コンピュータは、ボット（自動化されたプログラム）がインストールされるとゾンビマシンになり、ハッカーに制御を許し、ゾンビネットワーク（またはボットネット）の一部となります。ボットをインストールするためには、コンピュータ上でインターネットポートを開けることが必要です。バックドア（開いたインターネットポート）は、コンピュータに感染したウイルスやワーム、トロイの木馬によって開かれます。バックドアが開かれると、多くの場合、同じウイルスによってボットがインストールされ、コンピュータはゾンビマシンとなります。あるいは、コンピュータにアクセス可能な開いたポートを検索して侵入したハッカーが、ボットをインストールすることもあります。

ウイルスがコンピュータに感染し、コンピュータをゾンビ化する最も一般的な方法の1つに、OS の脆弱性を悪用する手口があります。

また、ウイルス性ペイロードが含まれるメールの受信者を欺いて添付ファイルを開かせたり、あるいはリンクをクリックさせることによりウイルスを起動させるという、ソーシャルエンジニアリングの手法も利用して蔓延しま

す。ゾンビ化したマシンを稼動させる最も一般的な方法は、チャットルームをモニターするようにプログラムすることです。ハッカーが特定のコマンドをチャットルームに入力すると、ゾンビは「活動を開始」し、その指示を実行します。また、ゾンビマシンは事前にプログラムされた指示を実行することも可能です。たとえば 2005年5月には、Sober-Q トロイの木馬と Sober-N ワームが同時に動作して世界中のコンピュータに感染し、ハイジャックしたコンピュータがドイツ選挙の最中に国粋主義的な内容のスパムを送信するようプログラムしました。[2]

ゾンビ攻撃に対する防御

ネットワーク上でコンピュータの制御を奪おうとするハッカーへの最も有効な対策は、迅速で信頼性の高いゾンビマシン検出システムで、エンドポイント/ゲートウェイソリューションを補強することです。しかし、その基盤には、クライアントマシンや、ワークグループ、ゲートウェイ、そしてリモートシステムの統合的な保護が必要となります。

ゲートウェイ防御

メールゲートウェイは、ゾンビマシン作成型を含むメール送信型ウイルスに対するネットワーク防御の最前線です。Sophos PureMessage™ は、ウイルスファミリーのさまざまな亜種とスパムキャンペーン* の両方を自動的に検出するユニークな手法であるGenotype™（遺伝子型）検出テクノロジーを搭載した、信頼性の高いゲートウェイ保護の統合ソリューションを提供します。

＊ スパムキャンペーン：同一の内容を含んでいる一連のスパム。フィルタリングによる検出を避けるため、形態を変えて配信される。

メールゲートウェイの確保だけでは充分でありません。ウイルスはゲートウェイを迂回し、他の多様なルートを経由してネットワークを攻撃することができます。

しかし、メールゲートウェイの確保だけでは充分でありません。ウイルスはゲートウェイを迂回し、他の多様なルートを経由してネットワークを攻撃することができます。

- インターネット — Sasser や Rbot などのワームにはゾンビ機能が含まれており、メール経由では蔓延しません。そのかわり、OS またはブラウザの脆弱性を悪用し、インターネット経由でクライアントマシンに直接蔓延します。
- モバイル機器 — 従業員によって社外に持ち出され、再び持ち込まれる USB フラッシュドライブや CD、モバイル PC などの機器を経由して、ウイルスがクライアントマシンに感染し、ネットワーク全体に蔓延することが可能です。
- インスタントメッセージ — IM アプリケーションはメールゲートウェイを迂回し、別の侵入ルートをウイルスに提供します。
- 不正な SMTP サーバー — ウイルスの中には、メールゲートウェイを迂回するために自身に内蔵した SMTP サーバーを使用して他のネットワークに蔓延するものもあります。Bofra がこの例として挙げられます。さらに、ゾンビマシンはネットワーク上に作成された後、自身の SMTP サーバーを使用して感染マシンから直接スパムを送信し、送信メールフィルタリングシステムによる検出を避けることもあります。

エンドポイント保護とセキュリティポリシー

安全に保護されているはずの組織内のコンピュータでさえもゾンビ化される危険があります。ゲートウェイ保護だけでなく、Sophos Anti-Virus™ のようなエンドポイントウイルス対策ソリューションをネットワークで使用することが不可欠です。

また、良質なエンドポイント/ゲートウェイ保護を、適切なセキュリティポリシーでバックアップすることも不可欠です。システムに対する絶え間ない攻撃により、セキュリティのほんのわずかな空間的、時間的なギャップをついて、マシンがゾンビ化されてしまう可能性もあります。すべてのエンドポイントが保護されていても、すべてのマシンの OS にパッチが完全には適用されていないなど、セキュリティ対策のわずかな不備により、コンピュータのハイジャックは可能となります。これは、大規模で分散化されているネットワークでは特に大きな問題となります。自宅のシステムから VPN 経由で社内ネットワークにアクセスする従業員や、自身のコン

ピュータをシステムに持ち込むゲストユーザーによって、ウイルスが組織に持ち込こまれることもあります。このように複雑な環境下では、保護の不十分な、あるいは頻繁にアップデートされないコンピューター台で、ネットワークをゾンビ化される危険が生じるため、すべてのマシンへの迅速なアップデートの適用が非常に重要です。また、セキュリティのベストプラクティスに関するエンドユーザー教育の実施、共有ファイルおよび感染している恐れのある Web サイトへのアクセス制限の設定といった、企業ポリシーの導入も重要な役割を担います。その他、クライアントファイアウォールを使用して、通信に不要な送受信ポートを閉じることも、ハッカー侵入防止策となります。

まとめ

ゾンビネットワークが犯罪者にとってより魅力的になるにつれ、ハイジャッされる企業のコンピュータ数は増加していきます。ゾンビマシンは検知しにくく、ビジネスに多大な被害をもたらします。コンピュータへの攻撃は迅速で絶え間なく、さまざまなソースからもたらされ、ネットワークのあらゆる侵入口で起こります。ゾンビに対する第1の防御として必要とされるのは、統合されたゲートウェイ/エンドポイントソリューションです。

ソフォスラボは、1日24時間、スパムやウイルス脅威に対する監視を行い、世界各地に展開するスパムトラップのネットワークを通じて、何百万ものメッセージを毎日分析しています。スパムトラップはスパムだけを受信するように設計されたメールアドレスで、スパム対策ソリューションのテストや、チューニング、開発などに使われています。ソフォスの PureMessage や Sophos Anti-Virus はその技術力を最大限に活かした Genotype(遺伝子型)検出テクノロジーにより、未知のセキュリティ脅威にもすばやく対応します。また、ソフォスラボが 24 時間体制で多様なセキュリティ脅威の解析を行い、迅速にアップデートをご提供して、セキュリティギャップを最小限に抑え、組織の安全を確保します。

その他、ソフォス製品およびソフォス製品を使ってネットワークを保護する方法の詳細につきましては、ソフォスのサイトをご参照ください。www.sophos.com

出展

1. How zombie networks fuel cybercrime, Celeste Biever, New Scientist, November 2004,
2. ソフォスの Genotype（遺伝子型）テクノロジー、スパムを送信する Sober-Q トロイの木馬をプロアクティブに阻止、ソフォス株式会社、2005年5月16日 、www.sophos.co.jp/pressoffice/news/articles/2005/05/va_soberq.

ソフォスとは

ソフォスは法人向けに統合脅威管理ソリューションを提供する世界的なリーディングカンパニーです。グローバル企業、SMB市場、教育機関、政府機関、金融業、製造業など、あらゆる規模、分野の組織をセキュリティ脅威から保護し、世界150カ国以上で3,500万人以上のお客様にご導入いただいております。セキュリティ分野で20年以上におよぶ実績と経験をベースに、セキュリティ解析センターが複雑な脅威に迅速に対応し、常時最新の対策をご提供しています。その高品質な技術力とサービスは多くのお客様から高い評価をいただいております。

ソフォス株式会社
〒231-0062　神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800　　E-mail. sales@sophos.co.jp

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.CO.JP