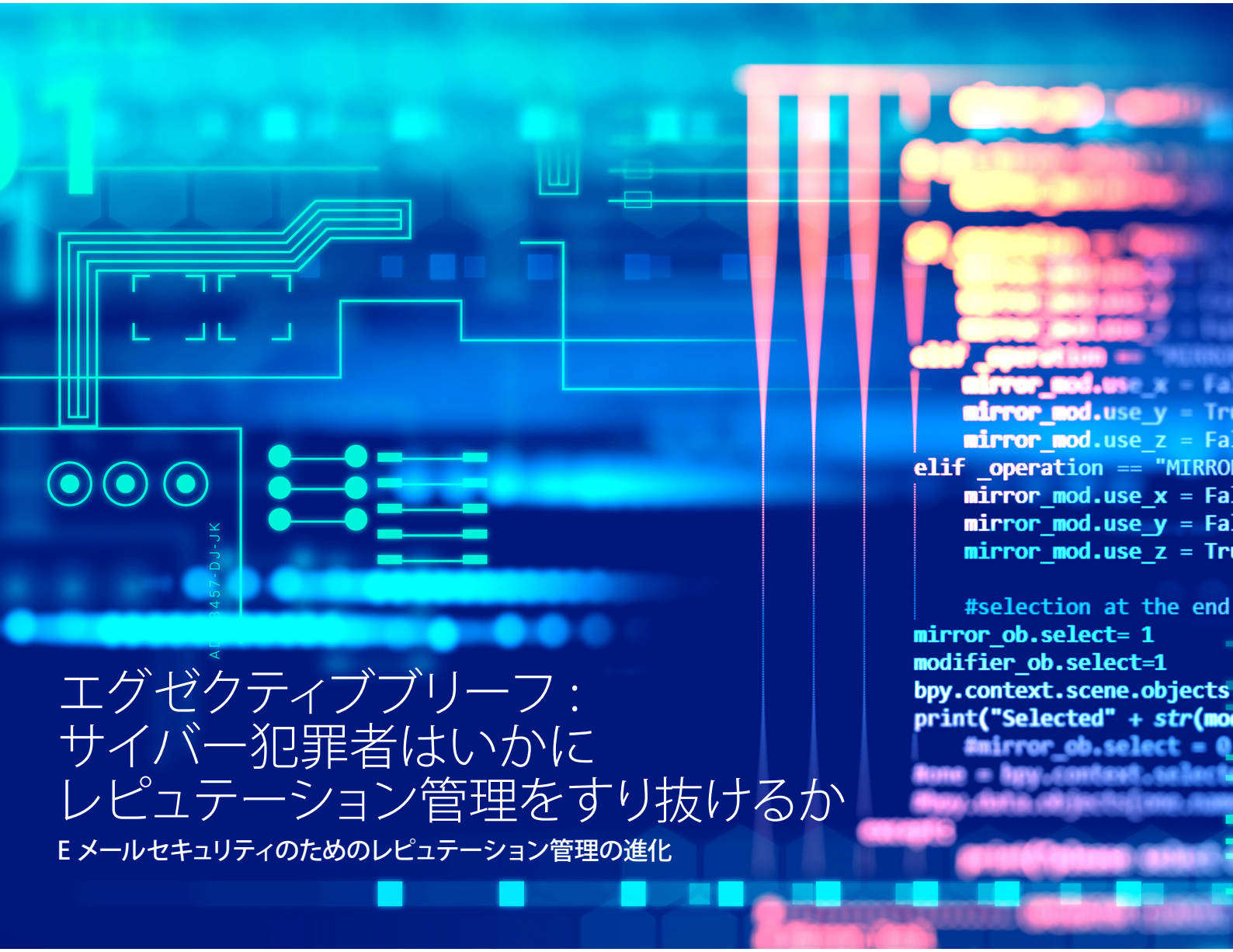
SONICWALL



エグゼクティブブリーフ：サイバー犯罪者はいかにレピュテーション管理をすり抜けるか

E メールセキュリティのためのレピュテーション管理の進化

要旨

テクノロジーの進歩に伴って、サイバー犯罪者は次々と新たな戦術を開発し、新たな攻撃を仕掛けてきます。1997 年に RBL (リアルタイムブラックホールリスト) が開発され、今日の DNSBL (DNS ベースのブラックホールリスト) フォーマットの基礎となりました。しかし、サイバー犯罪者は、IP レピュテーション管理システムを弱体化させ、このシステムをすり抜ける攻撃を仕掛けてきます。そのため、セキュリティ専門家は、常に前進して先を見越し、先手を打ってこうした攻撃を食い止める必要があります。

サイバー犯罪者はいかにして IP ベースのレピュテーション管理をすり抜けるか

IP レピュテーションシステムの普及に伴って、ハッカーは IP レピュテーションシステムを弱体化させることにますます多くのリソースをつぎ込むようになっています。こうした攻撃者は、信頼できるソースを装い、企業の E メールシステムや従業員を悪用することを目的として、スパムよりもフィッシングメールを使うことが多くなっています。フィッシング詐欺師は信頼できるパートナーや友人になりすまします。そして、フィッシングメールでは、レピュテーションが高い企業の正規のメールサーバーの侵害や、Yahoo®、Gmail® などの ISP や ASP の Web メールアカウントへの侵入が中心となります。こうして、サイバー犯罪者は、侵害した正規の企業のサーバーからの無害な E メールに混ぜて有害な E メールを送信することによって、従来の IP レピュテーションシステムでのリスティングを回避したり、遅らせたりすることができます。

サイバー犯罪者は自分の IP アドレスは操作しても、フィッシングやスパムメッセージのすべての機能を一様に操作することはしません。他の営利組織とは異なり、サイバー犯罪者は複雑さを減らすことでオーバーヘッドを削減します。彼らは IP アドレスの他に、コンテンツ、レ

将来のEメール脅威に備えるには、過去の教訓を理解する必要があります。

イアウト、ハイパーリンク、画像も再利用する傾向があります。そこに、防御のためのチャンスがあります。IP アドレスだけではなく、レピュテーションを特定し、管理するための追加の防御層を導入するのです。

これまでの経緯：レピュテーション管理の進化

当初、E メールレピュテーション管理システムは、RBL (リアルタイムブラックホールリスト) として始まりました。最初の RBL は、1997 年　に、MAPS (Mail Abuse Prevention System: メール濫用防止機構) 用のものとして Paul Vixie によって開発されました。Vixie は、「ブラックホール」という言葉を、受信トラフィックを転送せずに破棄する (この場合は、スパムを直接送信または有効化したサイトからの E メールトラフィックを破棄する) ネットワークリンクの意味で使いました。当初、RBL は、このサービスのサブスクライバとなっているシステムの管理者に BGP (ボーダーゲートウェイプロトコル) を使って送られる、疑わしいサイトのリストで構成されていました。サブスクライバは、その後、このリストを適用して、それらのサイトからの TCP/IP トラフィックをブロックすることができました。

RBL レピュテーションは、スパム管理を大きく前進させることになりましたが、固有の課題も生じていました。MAPS では、正確さを期するために、疑わしいサイトをリストに公開する前にサイトを入念に検証しました。これは誤判定を減らすのに役立ちましたが、その反面、サブスクライバが攻撃に迅速に対処しようとしても大幅に遅れをとることになりました。やがて、MAPS は E メールソフトウェアと統合できる RBL クライアントを開発し、管理者が独自の RBL をカスタマイズしてサーバーベースで受信 E メールを拒否できるようになりました。

MAPS RBL によって、DNSBL (DNS ベースのブラックホールリスト) フォーマット開発の基礎が築かれました。DNS (ドメインネームシステム) インターネットサービスは、DNS サーバーを使って、ドメイン名 / ホスト名から IP アドレスへの変換 (正引き DNS) と IP アドレスからその関連するドメイン名 / ホスト名への変換 (逆引き DNS) を実行します。DNSBL は、単なる目立たないリストでは終わらずに、IP アドレスを動的に追加し、削除するための、複数の標準が追加されました。DNSBL サービスプロバイダは、その後、標準化されたフォーマットを使い、IDNS (インターネットドメインネームサービス) を介して、更新されたリストを配信することができました。初期の DNSBL 開発者は、悪用される可能性があるオープンリレーまたはプロキシを送信元のメールサーバーが使用しているかどうか、スパムをおびき出して収集し、特定および分析することを目的とする「ハニーポット」システムにメールサーバーがスパムを送信しているかどうか、などの基準を追加しました。

今日では、利用可能な DNSBL サービスは多数あり、ほとんどの E メールサーバーがこれらのサービスに問い合わせて IP アドレスのレピュテーションを検証することができます。しかし、リストへの IP アドレスの追加、削除、保持に適用されている標準はサービス間で異なります。また、一部のサービスでは、危険な可能性がある IP アドレスがリストに含まれていなかったり、正当なアドレスが誤ってリストに含まれていたりすることもあります。

結論

E メールは、サイバー犯罪者が攻撃の実行に使い続けている重大な脅威ベクトルです。これまでに成し遂げられた組織のネットワークに対する攻撃の大半で、フィッシングメールが攻撃のゼロ地点となっていることが判明しています。スピアフィッシングやホエール攻撃の増加によって、有害な E メールと正当な商用通信との判別がますます難しくなっています。こうした状況から、現在のレピュテーション管理を見直して、新たな E メール脅威に対する防御力があるかどうかを確認することがきわめて重要になります。

詳細について。弊社のソリューションブリーフ、「高度なレピュテーション管理による E メール脅威対策」をお読みください。

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com