Web ベースの脅威から社内インフラを防御する シスコの最強セキュリティ対策

シスコ IT ケーススタディ／セキュリティ／IronPort S670 Web セキュリティ アプライアンス:
シスコは、従業員だけでなく、パートナー様やお客様も、どこからも、どんなデバイスからもアクセスできるサービスを提供できるボーダレス企業となるために、取り組みを続けています。社内サポート対象外の個人のデバイスも含む、あらゆるデバイスを利用可能にするという、シスコ IT のポリシーを実現するには、強力な Web セキュリティ対策が不可欠です。このため、シスコが社内に導入したのは、Cisco IronPort S670 Web セキュリティ アプライアンス（以下、WSA）でした。シグネチャ（過去に認識された攻撃パターン情報）によるマルウェア検知、Webレピュテーション（格付け）フィルタ、インライン型ファイルスキャンの機能を組み合わせることにより、強固な防御力を発揮します。WSA は、ノースキャロライナと東海岸の Research Triangle Park で利用開始後の3ヶ月間で、シグネチャ検知だけではすり抜けることもある有害オブジェクトを、3000万以上もブロックすることができました。このケーススタディは、高まるセキュリティ対策の要望に、シスコがどのように対処し成果を収めたかについて説明しています。シスコ IT が実際に体験したこの事例が、お客様が WSA の導入を検討される際のご参考になれば幸いです。

「WSA は、利用開始後わずか3ヶ月間で、全てのWeb トランザクションのうち1%をブロックすることができました。これは、数にして3000万以上の有害オブジェクトに相当します。ブロックされたトランザクションには、ボットネットコマンドの送信や受信、パスワードや個人情報の漏洩、マルウェアのダウンロードなどが含まれていました」

Jeff Bollinger, senior information security investigator

課題

2008年頃から、Web はハッカーたちの温床となっており[1)]、シスコ IT は Web からの攻撃が激増していることに憂慮しておりました。「リンクをクリックすることもなく、ただ閲覧するだけで、セキュリティの危機に晒されていたのです」シスコで情報セキュリティ調査を監督する Jeff Bollinger は、当時をこのように回想しています。

通常使われているブラックリストとホワイトリストでは、有害サイトのかなりの部分のブロックに失敗してしまいます。Websense Security Labs によると、有害コードを含む Web サイトの77%が合法サイトであり、危険性はあってもブラックリストには挙げられません。また、2008年後半には、ベスト100の人気サイトのうち70%が有害コンテンツをホストしているか、有害サイトへ誘導するリダイレクトが隠されていると報告されています[2)]。

1) Symantec, Internet Security Threat Report, 2011.
2) Websense Security Labs, “State of Internet Security, Q3 - Q4, 2008.”

シスコ IT は、様々なテクノロジを武器に Web ベースの脅威と闘ってきました。NetFlow でネットワークのトラフィックを統計分析しました。Cisco 侵入防御システム(IPS) やホストベースのCisco Security Agent で、マルウェア感染の兆候を示す異常な動作を発見しました。既知のウィルスは、ウィルス駆除ソフトで日常的に防御しました。

しかし、まだシグネチャのないデイゼロ攻撃（対策用ソフトウェアが提供される前に行われる攻撃）の脅威からも防御する必要がありました。「デイゼロ攻撃の発信元の検知率はゼロに近く、ホストを脅威から護るには、ウィルス駆除ソフトだけでは不十分でした」と、Bollinger。

また、業務に利用するデバイスを自由に選択できるようにするという AnyDevice 戦略を推進する過程で次のような変化が生じたこともリスクを高める要因となっており、対策を講じる必要に迫られていました:

- AnyDevice 戦略のポリシーにより、サポート対象外の個人のデバイスも業務に利用できるようになりました。しかし、このためリスクが高まったことも否定できません。「社内サポートの対象にならない個人のデバイスは防御力が低いと想定するべきなので、ネットワークの防御を徹底的に強化する必要がありました」と、Bollinger は指摘しています。
- SNS の利用者が増えていましたが、SNS サイトのリンクを経由してマルウェアが送られる被害も増えていました。[3)]
- スマートフォンの利用者が増えていましたが、そのOS はハッカーの攻撃対象として狙われていました。[4)]

このような脅威を撃退するため、Computer Security and Incident Response チーム（CSIRT) とシスコ IT は、ブラウザにロードされる前にブロックできるツールが必要と判断し、次の基準を満たすソリューションを検討しました。

- ネットワークのアプリケーション層の防御力を強化する。
- あらゆるデバイスを業務に利用可能にするために、本来はサポート対象外のエンドポイントも、シスコの責務を果たせるように防御する。
- Web ベースの脅威や攻撃の種類や攻撃量に関するデータを収集する。
- ブラウザの設定を変更せず、同じ環境を維持できるようにする。

ソリューション

シスコ IT は、WSA を活用することで、ユーザエクスペリエンスを損なうことなくデイゼロ攻撃の脅威から防御するという、目標を達成することができました。WSA は、まずレピュテーションフィルタやインライン型ファイルスキャンに基づいてWeb サイトの検査を行い、アクセスの可否を判断する、Web プロキシです。

WSA は、数多くのテクノロジを一元化するプラットフォームです。シスコはそれまで、Web レピュテーションフィルタ (WBRS) と、Webroot と McAfee のマルウェア駆除用スキャンエンジンの二つの機能を利用していました。シスコでは、他の多くの会社とちがい、WSA のフィルタ機能で、仕事に無関係なカテゴリのWeb サイトを全てブロックするわけではありません。例えば、ショッピングサイトやギャンブルサイトだからという理由でブロックされることはありません。従業員は常に生産性向上のため時間を有効に活用していると信頼するのが会社のポリシーだからです。「シスコは常に、従業員各自の Web アクセスに対して寛大なポリシーを貫いてきました。エンジニアリングや開発に専念できればそれでよいのです」（Bollinger）。

3) ITbusiness.ca, “Malware, Spam in 10 Percent of Facebook Links,” October 6, 2010.
4) PCWorld, “Six Biggest Rising Threats from Cybercriminals,” May 19, 2011.

WSA によるセキュリティ防御

リンクのクリックやURLへのアクセスを試みると、その接続要求が Web Cache Communication Protocol (WCCP) を経由して WSA のプールに送られます。WSA は、IronPort が提供するレピュテーション（格付け）サービス SenderBase のスコアに基づいて、そのサイト全体またはサイト内の個々のオブジェクトのロードの可否を判断します。Cisco IronPort メール セキュリティ ゲートウェイでも、SenderBase のスコアを基準にしています。

SenderBase は、最低評価-10～再高評価10のスコアで Web サイトを評価します。スコアが-10～-6の低評価サイトはスキャニングされず自動的にブロックされます。6～10点の高評価サイトは、スキャニングされずにアクセスを許可されます。

「実際、-6～6の中程度のスコアに該当するサイトが多いので、善悪を判断するデータが不足していると言えます」と、Bollinger は指摘しています。このスコアのサイトへのアクセスを試みると、ブラウザにロードされる前に WSA のマルウェアサービスがファイルやオブジェクトをスキャンします。このスキャンで、Webroot や McAfee のデータベースにあるマルウェアのシグネチャに一致する文字列や参照が発見される場合があります。Web ページに危険なバナーやリンクがある場合、そのオブジェクトはロードされませんが、他の部分はロードされます。図1に WSA の利用開始後3ヶ月間に実施されたレピュテーションフィルタの結果を示します。

全体が危険または有害なサイトの場合、安全のためにブロックされたことが知らされ、サポートが必要な場合のメールリンクを示す社内サイトのページへリダイレクトされます。

図1　WSA はレピュテーションフィルタのみで 0.5%のサイトをブロック、その後スキャンを行うことで さらに0.5%をブロック！

Web Reputation Actions (Volume)

Action	%	Transactions
Block	0.5%	13.8M
Scan Further: Malware Detected	0.5%	12.5M
Scan Further: Clean	73.1%	2.0G
Allow	26.0%	713.5M

WSA 導入計画

WSA は、三つの段階を経て世界中のシスコオフィスに導入されました。

POC（コンセプトの実証；Proof of Concept）： CSIRT はまず、ノースキャロライナにある Research Triangle Park (RTP) のシスコオフィスの一つのビルで、6ヶ月以上をかけて、300名を対象に POC を実施しました。WSA は、全てのWebサイトへのアクセス、また、Web からシスコ従業員が利用するデバイスへのリターントラフィックを調査しました。CSIRTは、各自のデスクトップの VLAN で、宛先ポート80/TCPのトラフィックが WCCP を経由して WSA へリダイレクトされるようにしました。WCCPを経由することで、WSA がユーザの Web トラフィックを調査します。この際、シスコ IT の手もユーザ自身の手も煩わせることなく、自動的に IronPort のプロキシをWebブラウザに使わせることができます。シスコ IT の AnyDevice 戦略に沿って、ブラウザ構成の変更は不要です。Bollinger の報告によると、「POCの実施期間に、マルウェアフィルタをすり抜けた有害トラフィックがレピュテーションフィルタでブロックされることが確証」され、また、この期間に機能停止が起こることもありませんでした。

試行運用： 次の段階では、2009年初頭から2011年初頭にかけて、対象をRTP オフィスの全従業員3000名に拡大しました。有線無線を問わず全てのWeb トラフィックが、4台の WSA のうちの1台へリダイレクトされました。この試行運用の期間中、全トラフィック中の1%がブロックされ、400万のオブジェクトを、ネットワーク感染や情報漏洩から防ぐことができました。

社内への導入： シスコ IT は、WSA の利用を、まずはインターネットへのトラフィックが RTP を経由するオフィスへ、そして他のもっと大規模なオフィスへと拡大していきました。「アクセスリストを変更し、ルータを WCCP 対応にして、WSA に転送可能にするだけで、利用者数を3,000名から30,000名に拡大することができました」と、Bollinger。現在、WSA はサンノゼ、カリフォルニア、バンガロールのシスコオフィスでも本番環境に利用されています。もちろん、Web リクエストがプロキシサーバ経由で送られるようになったという変化を、ユーザが意識することはありません。

デザインと設定箇所の決定

POC の段階では、CSIRT は、WSA を建屋のデスクトップゲートウェイスイッチに導入しました。WSA 2台で、POC の対象となる300名分の処理に必要な容量を十分に満たすことができました。「求められる容量は、対象ユーザ数だけでなく、レピュテーション、マルウェア駆除、認証など、WSA で利用可能なアプリケーションの数によっても様々でした」（Bollinger）。

試行運用段階では、シスコ IT は、デバイスの設置箇所について念入りに検討しました。インターネットのアクセスポイント全てにセキュリティ対策を施し、同時に管理用のアプライアンスの台数を減らすのは難題でした。

検討の結果、WSA をインターネットへのアクセスポイント全箇所に導入することになりましたが、各箇所に4～6台もあれば、シスコ社内の13万人のユーザを十分にサポートすることができました。最もトラフィックが集中する場所では、信頼できるネットワークに対してプロキシから除外するなど、シスコ IT が柔軟に計画することができました。

同じく WCCP を使用する Cisco Wide Area Application Services (WAAS) を妨害しないように、WSA はCisco WAAS の上流に導入されました。「必ずWAAS がトラフィックの最小化や加速化を完了した後に調査を始めることにしています」（Bollinger）。

WSAの構成方法

WSA を構成するには、次の方法があります：

リダイレクション： CSIRT は、WSA を透過的なプロキシとして、すなわちルータが Web ブラウザのトラフィックを WSA へリダイレクトできるように構成しました。これで、自宅など、社外で仕事をするときも、ユーザは通常通りに Web サイトへアクセスすることができ、ブラウザの設定を変更する必要はありません。

また、プロキシを明示する方法もあり、各ブラウザを手作業で構成して、ブラウザからプロキシサーバへ誘導するか否かを決めるファイルを指定します。「プロキシ指定（Explicit ）モードは、社内サポート対象のエンドポイントには適していますが、シスコでは、スマートフォンなどあらゆるデバイスの利用を認めています」と、Bollinger。指定モードはまた、社外で利用する際は、従業員がプロキシの設定を変更する必要があります。

Fail Open: WSA が処理に失敗した場合は、防御がない状態でブラウザの使用を継続することができます。利用時には違いを認識することができません。「WSA の Fail Open 機能は、とても重要です」（Bollinger）。また、必要な部門では、Fail-Closeシステムとして操作することも可能です。

サポート

WSA の導入、構成、パッチはシスコ IT のネットワーキングチームが担当します。

除外を含むセキュリティポリシーの管理は、CSIRT が担当します。例えば、セキュリティ調査担当者が、ブロックされたサイトにアクセスしたい場合、CSIRT が個別にアクセスを許可します。

Web ページをブロックするか決めかねる場合は、SenderBase のメールサポートチームがすぐにレピュテーションの調査に対応します。

成果

こうして、シスコでは、Web ベースの脅威を、過去最強レベルの防御力で撃退できるようになりました。WSA は、試行運用段階で、数多くのトロイの木馬型などのウィルスをブロックし、また、数万件の商用のトラッキングクッキーが従業員のデバイスに到達するのを防ぐことができました。

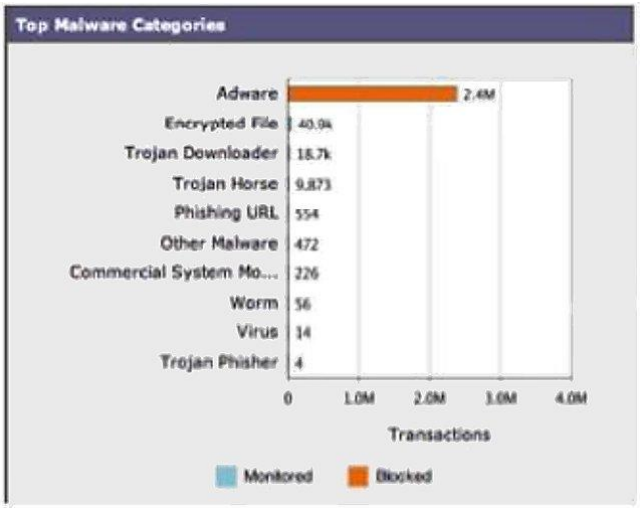
Bollinger によると、CSIRT は様々な実態がログで分析することができます。「ログを分析した結果、現在直面している最悪の脅威は水面下のハッキングサイトではなく、ブログ、フォーラム、Wiki など、毎日利用しているサイトにあるということがわかりました。何の気なしにサイトにアクセスするだけでシステムに異常が発生するのは日常茶飯事です。実際、Web サイトのほとんどが危険だと考えてよいでしょう」

WSA はまた、脆弱な業務用アプリケーションをデイゼロ攻撃から防御します。例えば、試行運用中、有害な.jpg ファイルが当時パッチのなかったActiveX の弱点を狙って攻撃してきたことがありました。その.jpg ファイルを含むサイトにアクセスしたら、ブラウザがクライアントにマルウェアをロードしてしまうところでした。ログデータによると、WSA がレピュテーションスコア -9 を示したその画像をブロックしていました。また、このログから、試行運用の対象外の地域では、脆弱なデバイスはその画像をロードしただけで感染してしまったことがわかりました。

3ヶ月間で3000万件以上をブロック

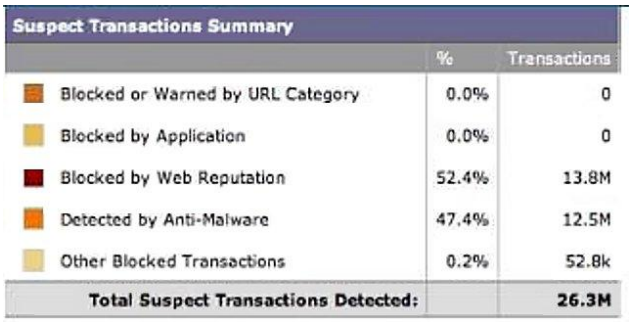
RTP と東海岸の本番環境で3ヶ月間、4台のWSA で300億件以上の Web トランザクションのセキュリティ検査を行いました。「WSA は、利用開始後わずか3ヶ月間で、全てのWeb トランザクションのうち1%をブロックすることができました。これは、数にして3000万以上の有害オブジェクトに相当します。ブロックされたトランザクションには、ボットネットコマンドの送信や受信、パスワードや個人情報の漏洩、マルウェアのダウンロードなどが含まれていました。WSA は、シスコのネットワークをマルウェア侵入から効果的に防御することができたといえます」と、Bollinger は報告しています。

図2 ブロックされたマルウェアのカテゴリ



東海岸の本番環境で1四半期間にシスコ従業員が接続要求した30億のオブジェクトのうち、52%がレピュテーションのスコアが低かったためにブロックされました（図3）。「WSA は、最近登録されたトップレベルドメインは特にスコアが低かったと報告しています。リストに挙げられたドメインは全て、マルウェアの配布や実行を試みていたのです。そして、WSA は、従業員が利用するデバイスから感染や情報漏えいを効果的に防いでくれました」（Bollinger）。

図3 レピュテーションスコアの低評価のため半数以上のサイトをブロック



Suspect Transactions Summary		
	%	Transactions
Blocked or Warned by URL Category	0.0%	0
Blocked by Application	0.0%	0
Blocked by Web Reputation	52.4%	13.8M
Detected by Anti-Malware	47.4%	12.5M
Other Blocked Transactions	0.2%	52.8k
Total Suspect Transactions Detected:		**26.3M**

ブロックされたオブジェクトの多くは、トラッキング用クッキーを含むバナー広告でした。他に、現在または過去に有害コードを配信したため、また、スパムキャンペーンの対象になったため、極端にレピュテーションスコアが低かったサイトもブロックされました。

IT のオーバーヘッドの軽減

ホワイトリストとブラックリストを社内で維持管理することは、スケーラブルな対策ではありません。

WSA では、これらのリストは SenderBase から数分毎に自動更新されています。「WSA が SenderBase に常時接続されているので、シグネチャの更新計画を立てる必要はありませんでした」と、Bollinger。オーバーヘッドが生じるのは、フェッチされたオブジェクトをログエントリーに保存する場合のみです。アクセスの可否に関わらず、シスコ IT では、必要とされない場合でもこの処理を行うことにしています。

CSIRT は、Cisco IronPort Eメール セキュリティ アプライアンスと同様、WSA にも Cisco IronPort M シリーズ セキュリティ管理アプライアンスを使用しています。

この事例で学んだこと

以上の経験に基づき、CSIRT とシスコ IT は、WSA の導入をご検討中のお客様に、次の事項を提案します。

- 接続要求した Web ページがブロックされたことを説明するページが表示された場合、その説明がわかりやすいか、必要な場合のサポートの受け方について知ることができるか、確認して下さい。シスコの場合、サポート用のメールリンクを提供します。
- WCCP サービスをリスタートする必要がある場合、プロキシサービスもリスタートしてください。ルータの WCCP のキャッシュとプロキシを同期させることができます。WSA の導入後に動作が遅くなったという報告もありましたが、プロキシサービスをリスタートすることで解決しました。
- アクセス制御リスト (ACL) で WCCP にリダイレクトする場合、リダイレクトさせたい全てのネットワークが対象になっているか確認してください。WSAでリダイレクトしたくないネットワークセグメントをバイパスさせるため、別のACLが必要な場合があります。
- ブラウジングのトラフィックが最もインターセプトしやすい箇所に WSA を導入しましょう。シスコでは、社内ネットワークとインターネット間のジャンクションに導入しています。また、必要なデバイスの台数を最小限にするために、外部へ転送されるトラフィックの全てが集まる集約ポイントに WCCP のリダイレクションを構成しています。モバイルワーカーの対応が必要な場合、無線ゲートウェイとリモートアクセスのネットワークを含めるようにしましょう。データセンターのサーバには通常、Web ベースの脅威から防御する必要はありませんが、防御する方が望ましい場合もあります。

次へのステップ

シスコ IT は、Cisco AnyConnect VPN クライアントに連携して ScanSafe クラウド セキュリティ サービスを利用することを検討しています。IT Customer Strategy and Success 担当部長 Jawahar Sivasankaran は、今後のセキュリティ対策について、次のように語っています。「ScanSafe は、WSA と同レベルのWeb セキュリティを、クラウドから提供することができます。これを利用して、社内からの接続要求はWSA へ自動転送され、社外からの接続要求は ScanSafe クラウドへ自動転送されるようにすることで、セキュリティをさらに強化していくという構想があります。さらに、ScanSafe を Cisco ISR G2 ルータと統合することで、今後もブランチオフィス戦略とクラウドコンピューティング戦略を発展させていく予定です」

詳しい情報はこちら

様々なビジネスソリューションに対するシスコ IT の取り組みについては、
シスコ IT 内の Cisco on Cisco ウェブサイト http://www.cisco.com/jp/go/ciscoit からご覧になれます。

Cisco IronPort Web セキュリティ アプライアンスについて詳しく知りたい方は、
http://www.cisco.com/web/JP/product/hs/security/ipweb/index.html をご参照ください。

付記

この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、この結果には様々な要因が関連していると考えられるため、同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。その場合、この免責事項は適用されないことがあります。

お問い合わせ先

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先:シスコ コンタクトセンター
0120-092-255(フリーコール、携帯・PHS 含む)
電話受付時間:平日10:00〜12:00、13:00〜17:00
http://www.cisco.com/jp/go/contactcenter