ThreatSTOP™

顧客事例:

ボルチモア大学

～大量のマルウェアソースと感染を乗り越えて～

ub UNIVERSITY OF BALTIMORE

ボルチモア大学

米国メリーランド州ボルチモア

問題

- 人的リソースがブロックするIPアドレスの入力と、マルウェア感染への対処にさかれてしまう
- マルウェア感染のせいで、ホストのパフォーマンスが落ちる
- 大学のオープンな環境のため、重要なセキュリティの脆弱性による情報流失をしてしまう可能性がある

顧客概要

ボルチモア大学はメリーランド大学システムの一部で、ビジネス、公共政策、リベラルアーツ、科学を専攻する6400人ほどの学部生と大学院生が学んでいます。
法科大学院は国内第6位の規模を誇ります。
そのネットワークは、Juniper Service GatewayとCiscoのルータ、スイッチで守られた複数のデータセンターで構成されていました。
ThreatSTOP導入以前はシマンテックのアンチウイルスを第一段階のセキュリティ製品として使用していました。

問題の検証

他の多くの大学と同じく、ボルチモア大学も学習や知識の共有のためにオープンな勉強環境を整えており、それがセキュリティの問題を難しくしていました。
大学職員は、セキュリティ製品、ネットワーク製品、そしてデスクトップなどのリソースに対して、ブロックするIPアドレスのリストを手動で入力し、防御を乗り越えてきてしまったマルウェアによる感染をクリーニングする必要がありました。ユーザ自身も、学問に集中しなければいけないにもかかわらず、フィッシングや感染したホストに接続するWebサイトに対処し続けなければいけませんでした。

3つの課題

1. オープンな学習環境を維持しながらも、フィッシングや悪意を持つWebサイトとの接続を制限する

2. 手動で行っていたブロックするIPアドレスの入力・アップデートを合理化、自動化し、スタッフをマルウェア感染関連の仕事から解放する

3. サポート最終日を迎え、ThreatSTOPのIPアドレス情報をあまり入れることができないJuniper Netscreen Firewallをアップグレードする

ThreatSTOPの解決策

数ヶ月の評価のあと、ボルチモア大学は2011年ファイアウォールアップグレードプロジェクトとして、Juniper SRX Services GatewaysとThreatSTOPを選択しました。OpenDNSなど他の製品も検討されましたが、ボルチモア大学からの条件を満たすことが出来ませんでした。OpenDNSはドメイン名のみでブロックするので、悪意を持つIPアドレス経由でマリシャストラフィックを受けているボルチモア大学にとって、それだけでは精度が足りていませんでした。
選定の基準は以下の通りです:

1. Juniperに対して：SRX Firewallは機能性に優れており、将来増やすことにも対応できる。また、ボルチモア大学はJuniper製品に慣れているので、アップグレードによって引き起こされる問題は最小限ですむ

2. Juniperを選んだ一番の理由は、ThreatSTOPを簡単に導入することが出来、またThreatSTOPを機能面で完璧にサポートできるということ

3. ThreatSTOPに対して：自動でIPアドレス情報のアップデートが出来、またマルウェアの検挙率が高く、偽陽性が低い精度の高いリストを持っている

ThreatSTOPとJuniperのファイアウォールセットでのソリューションは、すぐに期待したとおりの結果をもたらしました。2011年10月のある1週間の間だけで、下記の結果を出しました。

アウトバウンドブロック (出口対策)

攻撃数	531,040
攻撃者数	3,149
1日平均ブロック数	78,880
トップ3の情報ソース	Russian Business Network, PhishTank, Parasites

インバウンドブロック (入口対策)

攻撃数	1,241,873
攻撃者数	148,434
1日平均ブロック数	155,234
一番多い情報ソース	中国

導入結果

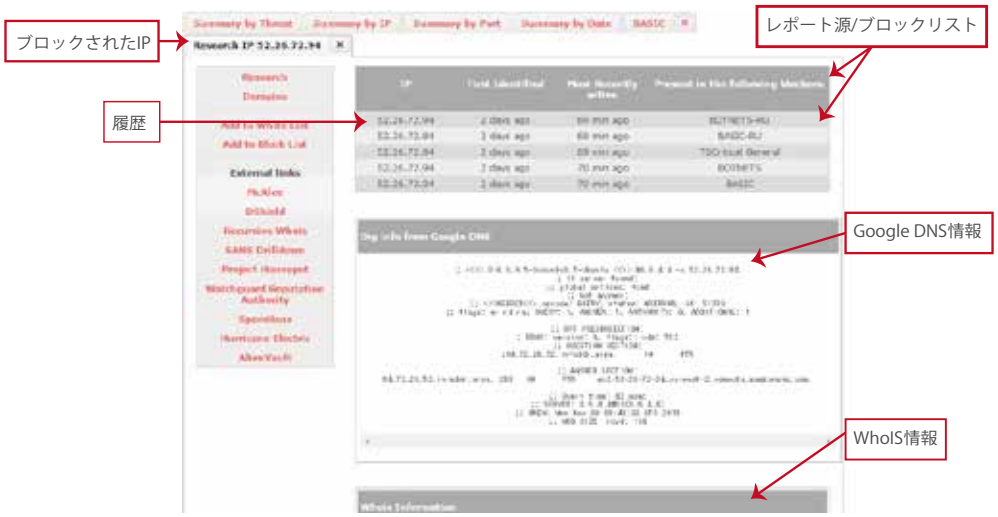
- ヘルプデスクへのマルウェア関連の相談は90%減少
- スタッフが何百時間も他の仕事に回すことが出来るようになった
- Juniper SRXに搭載したThreatSTOPがリアルタイムでマルウェアの侵入とボットネットを阻止
- ネットワークパフォーマンスの向上
- ボルチモア大学の学生・スタッフに対して、より安全な環境を提供できるようになった

ThreatSTOP

マルウェア関連の相談を90%削減

特権ユーザがボット化されてしまった時も、ThreatSTOPはボットがコールバックを実行し情報が流失してしまうのを防ぎました。
このおかげで、ボルチモア大学のITヘルプデスクのスタッフは、何かが発生する前に端末を検疫することが出来ました。

ThreatSTOPはWebベースのレポート機能も持っています。ファイアウォールのログファイルから作成されており、マルウェアの侵入を発見・分析することができます。また、必要であれば、マルウェアを侵入させようとした犯人を訴える際の資料として、それらの情報を使用することもできます。



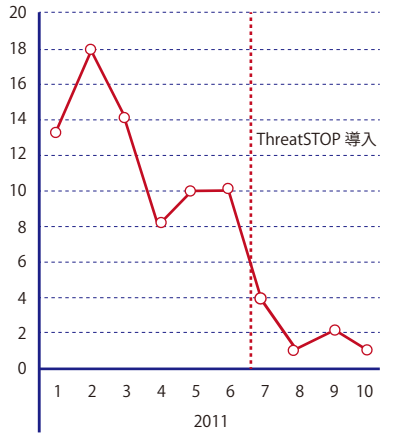
まとめ:

ThreatSTOPは高いマルウェア検挙率と正確性、素早いアップデートと即座の探知力を誇る、対ボットネット・マルウェアの最も効果的なソリューションです。既存のファイアウォールが様々な問題を解決できるようになります。一度シンプルなスクリプトよりインストールすれば、ThreatSTOPが既知の悪意を持つIPアドレスのリストを提供し、ファイアウォールの機能は強化されます。このリストは継続的にアップデートされ、DNSサーバを通して自動的にファイアウォールに提供されます。ThreatSTOPは既存の投資を強化し、更なる投資を不要にし、ハードウェアアップグレードの遅れ、ネットワークの再設定や再トレーニングを削減します。

メリット

- ヘルプデスクのチケットは劇的に減少しました。ThreatSTOPを導入する前は、月に10~18発行されていたのですが、現在では月に1~2となり、マルウェアチケットは90%も少なくなりました。

ヘルプデスクのマルウェア / ウィルス対応インシデント数



『かつてヘルプデスクチームは忙殺されていた。今は大切なリソースを守り、マルウェア関連の問題を終らせることができる』

Mike Connors
(情報セキュリティ分析担当者)

『マルウェアやウイルスのインシデント数減少のおかげで、チームが他の仕事に集中できるようになりました』

Dave Wells
(コールセンターマネージャー)

NVC NETWORK VALUE COMPONENTS

株式会社ネットワークバリューコンポネンツ

〒144-0035 東京都大田区南蒲田2-16-2
電話: 03-5714-2050 http://www.nvc.co.jp/

※本カタログに記載されているシステム名、製品名、社名などは各社の商標および登録商標です。
(threatstop_UBal_B5Y)