報道関係者各位　　2015年7月3日
プレスリリース　　グローバルセキュリティエキスパート株式会社

GSX 標的型メール訓練サービスにマルウェア感染調査を付加

～　セキュリティ教育訓練からマルウェア感染調査、

検知・防御までをソリューション連携する　～

この度、グローバルセキュリティエキスパート株式会社（本社：東京都港区新橋1-18-16、代表取締役社長：久慈 正一、http://www.gsx.co.jp）は、FireEyeの正式パートナーとして「標的型メール攻撃」から企業を守るために、FireEye製品との組み合わせソリューションを発表いたします。

一般的に標的型攻撃を含む、セキュリティ対策には多層防御が最も有効とされております。以下のような組み合わせをソリューション連携することで、

1. 人的抑止防御：標的型攻撃メールを開封しないように社員を訓練する、加えて開封した場合に迅速かつ適切な対応により、被害を最小限に抑える
2. システム的現状調査：マルウェアの脅威量や既にマルウェア感染しているかどうかの端末有無調査
3. システム的検知防御：解析エンジンによる標的型メール攻撃の検知及び防御【FireEye製品とのソリューション連携】

といった多層防御を実現することが可能になります。

◆標的型メール攻撃とは

標的型メール攻撃は、最も典型的なサイバー攻撃の手法です。重要な情報を盗み出す手段として、標的のクライアントPCをマルウェアに感染させる事を目的として、あらゆる騙しのテクニックを用いた攻撃メールを送信してきます。攻撃メールに含まれる、リンク先URLあるいは添付ファイルを開封するとマルウェアに感染します。

◆技術的対策＋人的対策＋プロセスによる包括的な対応の必要性

標的型メール攻撃への対策手段として、先ずは技術的な対策が求められます。マルウェア感染そのものを防ぐ、あるいは感染リスクを低減する為の対策である【入口対策】と、マルウェアに感染してしまった場合でも、外部への通信（≒情報流出）を水際で防ぐ為の対策である【出口対策】が急務とされています。

一方で、【入口対策】や【出口対策】などの技術的な対策を組み合わせることが非常に重要であるものの、それでもなお、100%のインシデント検知は未知のマルウェア対策ゆえ難しいと言われています。

そこで技術的な対策（導入したソリューションの機能性能）に依存しない、別の対策の実施が必要であると考えられます。それが、人的対策と不審メールの受信および開封時の対応プロセスです。

「マルウェアを開封し実行させない」「マルウェアを開封してもすぐに報告させる（適切な初動対応の徹底）」など、そもそもマルウェアを開封しなければ、感染することも無く、開封したとしても被害を極小化できるということです。

つまり、技術的対策、人的対策および不審メールの受信および開封時の対応プロセスを組合せた、多層的な対策が標的型メール攻撃に対して、最も有効な対策と言えます。

◆ GSX標的型メール訓練サービスについて

標的型攻撃を模擬した【訓練メール】を対象者に送信し、攻撃メールへの対応を教育訓練します。攻撃メールを模擬した実際には無害の"訓練メール"をGSXが対象者に送信します。訓練メールに含まれる、URLリンクあるいは添付ファイルを開封した対象者には、教育コンテンツが表示されると共に、開封した日時等のアクセスログがGSX訓練サーバ側に取得されます。最後に訓練結果を集計し、ログデーター式と共にご報告します。

実施イメージ

◆標的型メール訓練の実施効果とメリット

- 攻撃メールへのリスクレベルを評価把握できる
  実際に、どの程度のユーザが攻撃メールを開封してしまうか、現状のリスクレベルを調査把握する事が可能です。より踏み込んだ技術的な対策などの導入をご検討される場合、この結果を参考にすることが可能です。

- ユーザ端末のマルウェア感染率を大幅低減できる
  ユーザが攻撃メールを誤って開封してしまう確率が半分になれば、ユーザ端末のマルウェア感染リスクも半分になります。過去の実績では、継続的にあるいは複数回メール訓練を実施した場合、その開封率は半分~三分の一まで低減しています。

- 感染時の初動対応を徹底し、被害を最小化できる
  ユーザが攻撃メールを誤って開封してしまった場合でも、適切な初動対応ができれば被害を最小化することが可能です。教育コンテンツに、"LANケーブルを抜いてヘルプデスクへの報告"するルール等を記載することで、適切な初動対応についても教育訓練が可能です。

GSX
GLOBAL
SECURITY
EXPERTS

◆マルウェア感染調査について

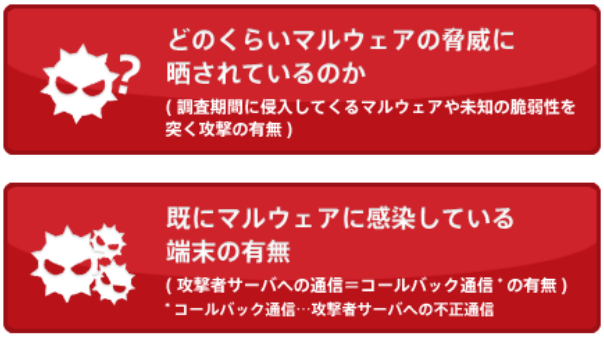
メールサーバのウイルス対策やスパムフィルタリング、またはエンドポイントのウイルス対策などについてはすでに大半の企業が取り組んでいると思われますが、未知のマルウェアが送りつけられるケースの多い標的型攻撃では、アンチウイルスソフトの導入に代表される従来型の技術対策だけですべてを防ぎきることは現実的に困難です。

標的型攻撃への対策、特に技術対策においては、一般的にはネットワークへのアプライアンスの導入や全クライアントへのソフトウェア導入などが必要です。GSXではこの足がかりとして、現状のマルウェア感染の有無を調査し、対策実施の優先度や重要度を改めて確認していただく「マルウェア感染調査」サービスを提供しています。

このサービスでは、ネットワーク・ゲートウェイに専用の調査機器（アプライアンス）を設置し、マルウェアへの感染状況を調査します。その後、

1. 侵入してきたマルウェアや未知の脆弱性を突く攻撃の有無
2. すでにマルウェアに感染している端末の有無（攻撃者サーバへの通信＝コールバック通信の有無）

についてレポートを作成、報告会を開催します。



◆標的型メール攻撃対策製品について

FireEye電子メール脅威対策プラットフォーム（ETP）は、電子メールを利用した高度なサイバー攻撃からネットワークを保護するクラウド型のソリューションです。電子メール脅威対策プラットフォームは、普及が進むクラウド型メール・サービスに欠けていた、高度なメール・セキュリティを提供します。

電子メールを利用した攻撃、特にスピア・フィッシング攻撃は、従来型のセキュリティ対策を容易に回避できるという理由から、現在でも、サイバー攻撃を開始する主要な手段として攻撃者に使用されています。このような攻撃は、組織宛ての電子メールをFireEye の電子メール脅威対策プラットフォームに転送するだけで防御できるようになります。

ETP では、最新の高度なサイバー攻撃を正確に検知するための専用技術FireEye Multi-VectorVirtual Execution™（MVX）エンジンを利用して、シグネチャ・マッチング技術には依存せずにすべての添付ファイルと本文中の URLを解析し、脅威をリアルタイムで検知してサイバー攻撃を防御します。

GSX
GLOBAL
SECURITY
EXPERTS

◆本リリースに関するファイア・アイ株式会社様からのエンドースメント

ファイア・アイ株式会社はグローバルセキュリティエキスパート株式会社によるGSX標的型メール訓練サービスにマルウェア感染調査が追加され、ファイア・アイのソリューションが貢献できることを心より歓迎いたします。グローバルセキュリティエキスパート株式会社の高度なコンサルティング能力とマルウェア対策で世界をリードするファイア・アイの製品が有機的に組み合わせることにより、特に標的型メール攻撃への防御力は飛躍的に高まるものと期待しております。

マルウェアによる攻撃は年々活発化、高度化する一方、2016年1月のマイナンバー制度の開始により、お客様が保有する個人情報を守る必要性は高まっています。特に、昨今の標的型攻撃の多くは、フィッシング・メールをきっかけにして起こっています。高度に組織化された標的型攻撃はツールのみで防ぎきれるものではなく、システムを運用する「人」のスキル、そして適切な「プロセス」が重要です。その意味でグローバルセキュリティエキスパート株式会社によるGSX標的型メール訓練サービスは「人」のスキル向上およびインシデント対応「プロセス」改善に大いに役立ちます。普段から「人」、「プロセス」、「技術ソリューション」の三方でしっかりと準備し、真の意味で総合的なセキュリティレベルを維持・向上することこそ進化するマルウェアへの最も有効な対策となります。

ファイア・アイ株式会社
執行役 社長
茂木 正之

■グローバルセキュリティエキスパート株式会社について

社名　：グローバルセキュリティエキスパート株式会社
本社　：〒105-0004 東京都港区新橋1-18-16　日本生命新橋ビル3F
代表者：代表取締役社長　久慈　正一
資本金：2億7,000 万円
コーポレートサイトURL：http://www.gsx.co.jp/
事業内容：
国内初の情報セキュリティ専門コンサルティング会社として2000年に設立され、脆弱性診断、コンサルティング、サイバーセキュリティサービスにいたる広範な情報セキュリティサービスを提供しています。

情報セキュリティポリシーの国際標準基準となった英国規格協会（BSI）のBS7799（現ISO27000）を日本に初めて紹介し、高品質な情報セキュリティコンサルテーションを行っています。

さらに、高い技術を有し、システムの脆弱性の検出のためにプラットフォーム診断やWebアプリケーション診断、スマホアプリセキュリティ診断などさまざまな脆弱性診断を行う【タイガーチームサービス（TIGER TEAM SERVICE）事業部】、標的型メール訓練サービスやマルウェア感染調査をはじめとする新しい脅威に対抗するサービス／ソリューションをご提案する【サイバーセキュリティサービス】、企業様のセキュリティポリシーの策定・リスクアセスメント・システム監査または、ISMSやPマーク取得支援、PCI DSS準拠認定支援、CSIRT構築運用支援などを行っている【コンサルティング事業部】を組織しています。

【サイバーセキュリティサービス】には、GSXサイバーセキュリティ研究所（GSX Cyber Security Research Institute）を擁し、セキュリティ製品評価やサイバー攻撃に関する情報収集及び分析、セキュリティインシデント対応要員の育成を進めており、問題指摘のみならず、インシデントに対する解決策までをワンストップで提供できる体制を整えています。

【本件に関するお問い合わせ先】

グローバルセキュリティエキスパート株式会社　事業開発部　マーケティング室

TEL　：03-3507-1360（代）　E-mail　：mktg@gsx.co.jp