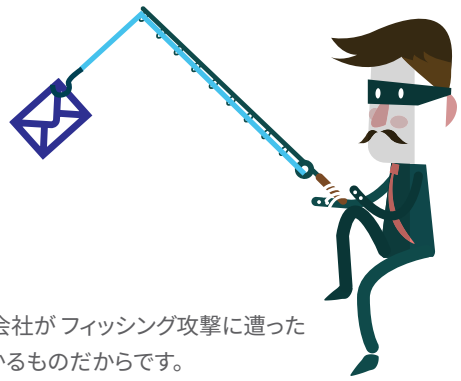
ハッカーの戦略を見破れ

WatchGuard Total Security Suite



はじめに

フィッシング攻撃は、今でも中堅規模企業にとって大きな心配の種となっています。実際、昨年だけで76%の会社が フィッシング攻撃に遭ったと報告しています。[1] これは驚くことではありません。この類の攻撃は単純な方法で実行でき、成功すれば儲かるものだからです。

とはいえ、IT管理者の皆様には朗報があります。フィッシングについて少し学習し、何重かの防御を施せば、フィッシング攻撃から組織を守ることができるのです。

フィッシングとは?

フィッシング攻撃とは、送信者を詐称して電子メールを送りつけ、対象者から機密情報を盗み出す行為のことをいいます。犯人がよく用いるのは、もっともらしく恐れを抱かせたり、好奇心をあおったり、緊急を装ったりして、対象者が添付ファイルを開くように、または悪意のあるリンクをクリックするように仕向けるという戦術です。

さらに巧妙なハッカーはスピアフィッシング攻撃を行うこともあります。この攻撃では、対象者についての特定の情報が含まれる電子メールが用いられます。多くの場合、攻撃者は対象者についてLinkedInなどのソーシャルメディアや企業のウェブサイトを調査して、対象者が確実にクリックする完璧な電子メールを巧妙に作り上げます。

フィッシング攻撃からの防御

効果の高いフィッシング対策プログラムには、保護、教育、評価、レポートという4つの要素があります。これら4つのステップをうまく連携させる事で、セキュリティ技術を活用しつつ、スタッフ自身が攻撃への防御策としての役割を果たす事が可能です。

フィッシング対策プログラムの最初のポイントは、簡単にクリックしかねないユーザと攻撃者の間にセキュリティ対策を導入して、保護を強化するというものです。次のような方法があります。

- 悪意のある外部DNS要求を監視し、それらの要求へのアクセスをブロックして、社員が疑わしいリンクを経由して不正なサイトに到達できないようにする。
- ファイルの動作を監視するツールを使用して、悪意のあるファイルがネットワークを介して移動しないようにする。
- クラウドサンドボックスソリューションを使用して、疑わしいファイルを仮想環境で起動させ、悪意のあるファイルかどうかを判断する。悪意のあるファイルと判定されたら、そのファイルを隔離してネットワークを攻撃から防御します。

さらに、社員にフィッシングに関する教育を定期的に行うこと、同時にクリック率を評価することも重要です。利用できるトレーニングには有料/無料を問わず様々なものがあります。フィッシングに対する意識を高めるためのコンピューターベースのトレーニング、フィッシング電子メールのシミュレーション演習、さらにはスタッフへのフィッシングに関する教育ビデオを視聴させたり、ポスターを掲示したりするという簡単な方法もあります。社員が十分な訓練を受け、フィッシングに関する定期的なテストを実施している組織は、感染率が5%と大変低くなっています。[2]

スタッフに、教育の一環として、疑わしいと思える電子メールの転送先を伝えることは重要です。多くの場合、疑わしい電子メールはヘルプデスクまたはITサポートに転送します。こうしたフィッシングメールは、攻撃方法と対象者を理解するのに役立ちます。フィッシングメールを収集して注意を払うことによって、組織が攻撃されている方法（Office 365 フィッシング、偽の請求書など）、および対象になっているユーザー（営業、研究開発、人事など）に関する傾向を把握できます。攻撃者の手の内を知り、その情報をセキュリティプログラムに反映させ、保護を強化できます。

DNS

1 https://info.wombatsecurity.com/state-of-the-phish

2 https://siliconangle.com/blog/2017/11/30/phishing-attacks-cost-1-6m-average-enterprises-successfully-fighting-back/

WatchGuardによるフィッシング保護

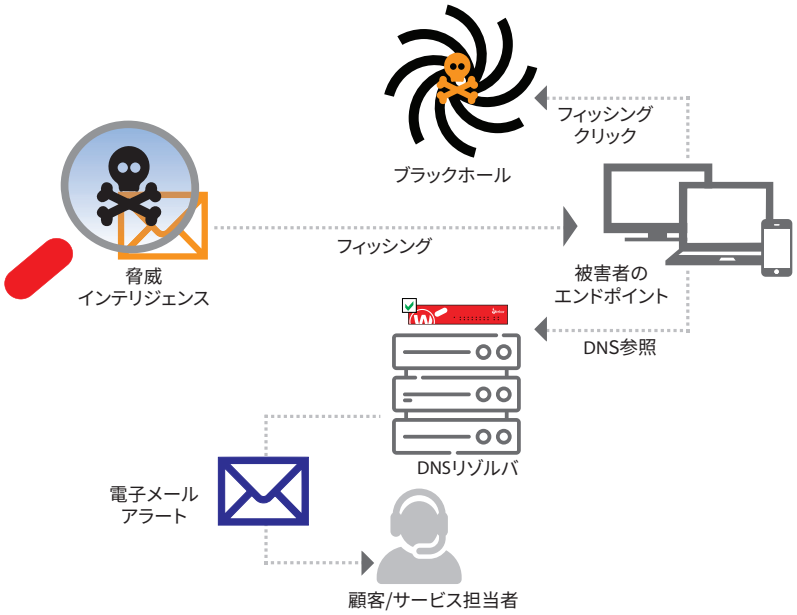
どの組織にも、フィッシングの被害に受けやすいユーザが存在するのも事実です。不審なリンクをクリックしたり、不審な添付ファイルを安易にダウンロードするスタッフはいないと自負する組織においても、適切なセキュリティサービスを導入しておく必要があります。フィッシング教育を最適なタイミングで実施するとともに、WatchGuard Total Security Suiteを使用することで、ユーザを攻撃から保護することが可能となります。

WatchGuard Gateway AntiVirusは、Firebox経由のファイルとトラフィックをスキャンして、既知のマルウェアとリスクウェアを特定します。シグネチャマッチングにより脅威が検知されると、接続がブロックされるか、ファイルが削除されます。これにより、フィッシング攻撃により、悪意のある添付ファイルが社員にダウンロードされるのを防ぐことができ、組織のセキュリティリスクを削減します。

WatchGuard APT Blockerは、ネットワークに到達するゼロデイ攻撃に関して、クラウドサンドボックス上で対象ファイルを実行し、脅威であるかどうかを正確に判別します。悪意があると判断されたファイルは隔離され、システム管理者にその脅威についてのアラートが送信されます。
では、巧妙に仕組まれたフィッシングや、十分なセキュリティに関する教育を受けていないユーザに対しては、どのように対処すれば良いのでしょうか?

WatchGuard DNSWatchは DNSレベルの検出機能を使用して、マルウェアの感染を特定して拡大を防ぐセキュリティレイヤを追加します。悪意のあるDNS要求は自動的に検知・ブロックされ、不審なサイトに誘導されることなく、ユーザは安全な場所にリダイレクトされます。さらに、パーソナライズされた機能を持つDNSWatchは、検知されたサイト、ブロックされたDNSに関する詳細レポートを提供します。

DNSWatchの特長の一つは、巧妙なフィッシング攻撃により不正サイトへのリンクをクリックしてしまった場合でも、ユーザは常に安全なサイトにリダイレクトされ、さらにリダイレクト先の安全なサイトにて、フィッシングに対するセキュリティ教育を補強することが可能なことです。
不正なリンクや添付ファイルをクリックしたその際に、ユーザにフィッシング対策について再教育の機会を提供する事で、インシデントの発生を防止する事が可能です。トレーニングサイトへのリダイレクトとともに、アラート機能やクリックした電子メールを転送する事も可能で、攻撃を受けたタイミングでアラートを受け取ることで、ユーザは多要素認証やパスワードマネージャーなどのセキュリティ機能の提案を受け入れやすくなり、セキュリティの強化への理解を得ることが可能となります。



WatchGuardについて

WatchGuard® Technologies, Inc.は、ネットワークセキュリティ、セキュア無線LAN、ネットワークインテリジェンス製品やサービスを全世界で80,000社以上のお客様に提供している業界のリーダーです。当社のミッションは、WatchGuardのシンプルかつ理想的なソリューションを分散型企業や中堅・中小企業で利用できるようにし、すべての企業がエンタープライズクラスのセキュリティ機能を確保できるようにすることです。

WatchGuardはワシントン州シアトルに本社を置き、北米、ヨーロッパ、アジア太平洋、南米に支社を展開しています。詳細については、WatchGuard.co.jpをご覧ください。

その他の情報、プロモーション、更新情報については、Facebook、LinkedInにて会社ページをご覧ください。また、最新の脅威に関するリアルタイムの情報や対処方法については、セキュリティブログ SecplicityJP (https://www.watchguard.co.jp/security-news) をご参照ください。

ウォッチガード・テクノロジージャパン株式会社 1.800.734.9905 〒 106-0041 東京都港区麻布台 1-11-9BPR プレイス神谷町 5 階 TEL:03.5797.7205 FAX:03.5797.7207 http://www.watchguard.co.jp/ jpnsales@watchguard.com

Part No. WGCE67085_032818