標的型サイバー攻撃警報システム「パケンチャー」の紹介

Advanced Persistent Threat Detection System “PACKENCHER”

明石 敬*
Kei Akashi

標的型サイバー攻撃警報システム「パケンチャー」は、近年、脅威を増している標的型サイバー攻撃の早期発見を目的として開発したシステムである。標的型サイバー攻撃の侵入の早期発見のため、詐称メールの可能性がある場合の警報メールを通知する。また、潜伏の早期発見のため、マルウェアによるバックドア通信を検知し、警報メールで通知する。さらに、パケンチャーやDynamic MSIESERのログをセキュリティ分析員により監視するサービスも提供する。

We developed Advanced Persistent Threat Detection System “PACKENCHER” for the purpose of early detection of APT attacks that recently increasing. “PACKENCHER” notifies by detecting a suspicious e-mail and suspicious backdoor’s communication. In addition, we provide detection services by security analyst used “PACKENCHER” and “Dynamic MSIESER”.

1. まえがき

近年、従来型の攻撃とは異なる手法による標的型サイバー攻撃は国内でも大手重工業の標的型サイバー攻撃の事例が大きく報道されて以降、後を絶たない。サイバー情報共有イニシアティブの情報によれば、2014年７月～９月の標的型サイバー攻撃件数は100件であり、前年同期の95件と同程度である。(1)

標的型サイバー攻撃とは、重要情報の不正な取得を目的として特定の企業や組織に対して行われるサイバー攻撃である。震災やオリンピック開催に乗じたタイトルや関係者を装った詐称メールを起点に不正に情報を搾取する手法（ソーシャルエンジニアリング）の利用により近年手口が巧妙化している。このような攻撃に対しては、従来のスパムフィルタやウィルス対策ソフトウェア等では防御することが困難であり、侵入、潜伏の早期段階において、疑わしきメールや外部への不正な通信をいち早く発見することが非常に重要である。

2. 標的型サイバー攻撃警報システム「パケンチャー」とは

当社製品である、標的型サイバー攻撃警報システムPACKENCHER（以下、本製品）は、標的型サイバー攻撃を早期に発見することを目的として開発された。標的型サイバー攻撃のきっかけとなる侵入の早期発見および侵入された後の潜伏の早期発見を行う機能を有する。それぞれ以下に述べる。

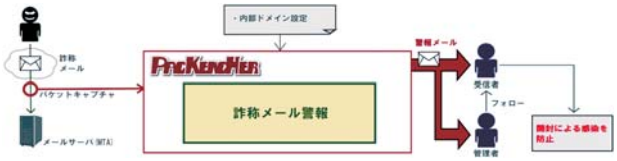

図１　侵入の早期発見

2.1 侵入の早期発見

本製品は、侵入の早期発見のために、メールを構成するパケットの内容を検査し、詐称メールの可能性がある場合に受信者および管理者宛てに注意喚起のメールを通知する。詐称メールの侵入経路となるメールサーバ（MTA）の前段に設置することにより、前述した検査を実施している。

侵入を早期発見するために、以下に挙げる機能を実現している。

（１）詐称メール検査

メール受信時に、外部から届かない内部ドメインの詐称や、海外経由で届かない国内ドメインの詐称など複数の検査を行い、標的型サイバー攻撃の可能性がある詐称メールを多角的に検知する。

（２）警報メール送信

詐称メールを検知した場合、検知した内容を警報メールとして管理者に、または管理者および受信者に直ちに送信する。

＊鎌倉事業部　ICTソリューション開発部

（3）自動学習

各検査に必要な情報は、過去に受信したデータを利用した機械学習を行い、検知精度の向上を図っている。

2.2　潜伏の早期発見

本製品は、潜伏の早期発見のために通信を構成するパケットの内容を検査し、判定基準に一致したホストについてレポート（CSV）を出力する。管理者はレポートを確認の上、疑わしき通信について調査・遮断を行う。バックドア感染PCの通信経路に設置することにより、前述した検査を実施している。

潜伏の早期発見するために、以下に挙げる機能を実現している。

（1）バックドア通信検査

統計を利用したURL長などの検査や機械的なアクセス、HTTPポートにおけるHTTP以外の通信、ロングセッション、ファイアーウォール等による遮断など、バックドア通信の可能性のある通信を多角的に検知する。

（2）レポート送信

検知した内容は、警報レポートとして管理画面および管理者にメールにて送信する。

（3）ホワイトリスト設定

バックドア通信の検知が不要である通信先については、ホワイトリストに設定することで検知対象から除外可能である。

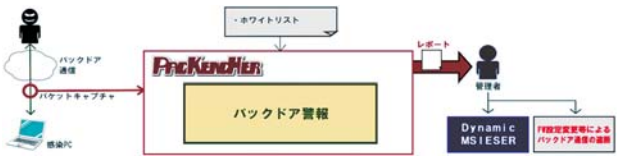

図２　潜伏の早期発見

3.　セキュリティログ分析サービスの紹介

当社では、本製品や当社ネットワークフォレンジック製品であるDynamic MSIESERのログおよび導入済みのWEBプロキシログをセキュリティ分析員が分析し、標的型サイバー攻撃に利用される詐称メールの検知やバックドア通信の検知を実施する「セキュリティログ分析サービス」を行っている。セキュリティに対して知見を有する分析員が定期的にログを監視することによって、優先的に確認すべきアラートイベントを特定することができ、情報システム部門やセキュリティ部門の詳細調査の効率化が図れる。

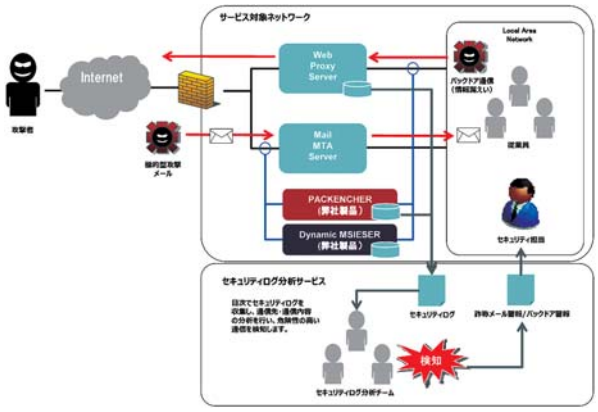

図３　セキュリティログ分析サービス

セキュリティログ分析サービスでは、表１に示す脅威を検知し、報告することができる。

表１　検知する通信

No.	通信	検知する通信
1	SMTP 通信	標的型サイバー攻撃メールによる通信
2		マス的なウィルスメール
3		スパムメール
4	HTTP 通信	バックドアによる通信
5		Web 改ざんによる攻撃
6		一般的なウィルスによる通信
7		匿名ソフトによる通信

4.　むすび

本稿では、標的型サイバー攻撃警報システム「パケンチャー」について述べ、パケンチャーを活用したセキュリティログ分析サービスについて説明した。

標的型サイバー攻撃は、従来型のアンチウィルスソフトやスパムフィルタといったセキュリティ製品では防ぎきれない。一方、本製品およびセキュリティログ分析サービスは、これら従来型のセキュリティ対策製品のカバーできない範囲を対象としたものであり、本製品・サービスを組み合わせることで、より一層のセキュリティレベルの向上が期待できるものである。本製品・サービスを活用頂ければ幸いである。

本製品・サービスの詳細については、下記窓口に問い合わせ頂きたい。

営業本部　ソリューション営業部　第一課
〒105-6132　東京都港区浜松町二丁目4番1号
世界貿易センタービル32階
TEL：03-3435-4737　FAX：03-3435-4745
E-MAIL : pk-info@mss.co.jp

参考文献

（1）サイバー情報共有イニシアティブ（J-CSIP）運用状況，IPA技術本部セキュリティセンター（2014年10月）

執筆者紹介

明石　敬
2007年入社。主に、製品事業、官公庁・民間企業の受託開発事業に携わる。2011年より情報セキュリティ製品・サービス関連業務に従事、現在に至る。