マルウェア Emotet に対するメールセキュリティ機能の提案

Proposed Email Security Features for Emotet Malware

堀口 幸佑† 坂﨑 尚生†
Kosuke HORIGUCHI† Hisao SAKAZAKI†
† 玉川大学工学部ソフトウェアサイエンス学科
† Faculty of Engineering, Tamagawa University

1. はじめに

近年、標的型攻撃メールの被害にあう企業が増え、社会問題にまで発展している。特に Emotet と呼ばれるマルウェアは、標的型攻撃メールの手法の一つでファイルレスという特徴を持っている[1]。その故、既存のウイルス対策ソフトでは検知することができない。本研究では Emotet に注目し、感染防止に向けたメールセキュリティ機能を考案する。

2. Emotet の概要

Emotet には、ばらまき型と返信型の二種類の形式が存在する。ばらまき型は、一般的なスパムメールと同様に企業や組織を装って不特定多数の宛先に同じ内容のメールを一括で送信するものである。返信型は、感染端末に実際に送信されたメールの本文を引用し、その返信メールを装うことで新たな感染者を増やす手法である。返信メールには Word ファイルが添付されており、Word ファイルを開くと不正なマクロより PowerShell が起動し Emotet 本体がダウンロードされる。一般にマルウェア対策は「感染防止」「感染確認[2]」「感染後の対策[3][4]」に分類することが出来る。Emotet の感染防止対策としては、現状、注意喚起を促すような運用的対策が多い。

3. Emotet 感染対策の検討

本研究では、Emotet の返信型の動作に着目した。Emotet の返信型は、過去の送信メールに擬態する。そこで返信内容の不自然さを検知する方法を検討した。より具体的には、添付ファイル付きの返信メールの正常性を判定するために「過去に同じ本文のメールが送られていないか」「メールの返信時間間隔が不自然ではないか」等、通常の返信内容とは異なるようなチェックポイントを検討した（表 1 参照）。このチェックポイントを用いて送信済メールと返信メールとを比較することで、返信型 Emotet による攻撃の可能性を検知する。一方、上記検知機能は感染の可能性を検知する機能である。返信メールの感染の可能性が高くても「添付ファイルを開かなかったら、仕事に支障をきたすかもしれない」というユーザ心理を拭うことは難しい。添付ファイルを開封するか否かは、最終的にはユーザの手に委ねられている。そこで本研究では、感染の可能性があるファイルを必要に応じて安全に確認する仕組みとして Sandbox との連携も検討した。

4. 返信メールの調査

送信メールと返信メールとの関係を調べるために研究室の 3 名の学生に対し、「返信メールの件数と割合」「送信から返信までの時間差」「返信メールの添付の有無・種類」等

表 1 検討したチェックポイントの例

返信元が過去に自分に添付ファイルを送った頻度および必要性
・いままであまりファイル付きメールを返信されたことがない
・添付ファイルがなくても通じる返信内容であった etc.
普段の添付ファイルの形式の違い
・普段 PDF の添付が多いのに何故か Word であった etc.
返信時間の差が開き過ぎていないか
・既に終了した会議の日程調整の内容
・一年前のメールへの返信 etc.
メールサーバの転送経路が過去の経路と一致しているか
・一旦、外国を経由して返信メールが到達している etc.
返信文とその原文の間に整合性が成り立っているか
・遊びの話のメールを引用して仕事の話が返信されている etc.
そもそも返信を必要とするメールか
・「了解」と一言書いたメールに対しての長文の返信 etc.

約一年間のメール履歴を調査した。結果、学生 3 人の調査であるが、全体割合の 6～10%程度が返信メールであった。また、送信メールから返信メールを受信するまでの時間差は、最大24 日、3 人の平均を取ると約18.25 時間であった。

5. プロトタイプシステムの開発

本研究では、前記方針に基づき Emotet に対するメールセキュリティ機能を設計し、プロトタイプシステムを開発した。検知機能の実装においては、自身が送信したメールを保管するデータベースを設け、送信メールから 10 日以上を経過した返信メールにアラートを挙げた。尚、10 日という値は、先の調査結果を基に目安として算出した。プロトタイプシステムでは、表 1 のチェックポイントの内、一つだけの実装となったが、外部メールサーバと連携し、チェックポイントに応じたメールを検知することができた。また安全機能においては、フリーの Sandbox 環境である Sandboxie との連携を検討した。

謝辞

ご助言を頂いた株式会社日立製作所研究開発グループ 主任研究員 川口信隆氏に感謝する。

参考文献

[1] Emotet と呼ばれるウイルスへの感染を狙うメールについて，独立行政法人情報処理推進機構セキュリティセンター，https://www.ipa.go.jp/security/announce/20191202.html
[2] EmoCheck, https://github.com/JPCERTCC/EmoCheck/releases
[3] 三須 剛史，桃井 達明，疑似 C&C サーバを用いた IoT マルウェア駆除手法の提案，SCIS2019，3E2-2.
[4] 古門良介ら，ランサムウェア感染時の復旧対策ツールの開発，SCIS2020，4F1-4.