2015/8/26
私情協大学セキュリティ研究講習会

S1-02「SJK 大学事務局マルウェア感染の疑い（内部通知)」対応フロー（解答例）

私情協大学セキュリティ研究講習会

Ⅰ．通知者の確認

① 内部の者から、「2 日ほど前に、メールに添付されたファイルを開いて、マルウェアに感染したかもしれない」、との電話連絡がありました。連絡を受け付ける際には、どのような情報を収集しますか？

（マ）

氏名、所属部署、架電時刻、メール受信日時、開封日時を確認する。

Ⅱ．一次対応（状況把握とログ保全）

① 通知のあった標的型サイバー攻撃メールの調査を行うにあたって、該当のメールからはどのような情報を収集するべきでしょうか？また、注意点を挙げなさい。

（テ）

オリジナルのメールヘッダー、題名、本文、添付ファイル名、添付ファイルを収集する。 該当のメールを転送すると、メールヘッダーが書き換わったり、２次被害が発生したりするので注意する。

② 同様の被害（同様のメール受信）が発生していないか調べるには、どのようなシステムのログを調査するべきでしょうか？

（テ）

該当のメールを転送したメールサーバーの通信ログから、同メールが複数宛てに転送されていないか調査する。 宛先が判明した場合には、題名、添付ファイル名等の情報を付加して、添付ファイルを開かないように通知する。 また、学内サイトなどに注意喚起する文書を掲載し、各部署の責任者へ通知する。

③ 通知者から該当のメールおよび添付ファイルを、どのような方法で入手しますか？また、その添付ファイルがマルウェアとしての挙動を示すか調査するためには、どのような作業を行いますか？

最終的に、このメールと添付ファイルは、どのように処分しますか？

（テ）

メールヘッダと本文は印刷および PFD ファイル、添付ファイルは専用の USB メモリで取得する。 テスト時には、仮想環境（VirtualBox）上の Windows とメーラー（または Firefox）を使って開封する。 調査終了後、専用機の仮想環境上で該当メールを保存し、端末およびメールシステムからは削除する。

④ ③の調査で、該当の添付ファイルはマルウェアであると確認されました。（テ）は（マ）への報告を行ってください。

（テ）→（マ）

該当メールの転送時刻、受信時刻 添付ファイルの開梱によるプロセスの起動やレジストリ書き換えの発生など不審な挙動の概要、ウイルス対策ソフトの未検知 → 標的型攻撃マルウェアと判断 同メールの転送先一覧

⑤ インシデントのレベルを判定して下さい。

（マ）

レベル 1

⑥ ⑤で判断したインシデントレベルに合せて、緊急措置を発動して下さい。

（マ）→（テ）

レベル 1 のインシデントに対して、該当端末の注意観測を指示。

⑦ ⑥の緊急措置発令に対し、技術的にはどのような対応をとりますか？

（テ）

業務用に代替器を貸出し、該当の端末は起動したまま、ネットワークトラフィックログを収集する。また、所属 VLAN の端末の監査ログ（ネットワークログオン）も収集する。（残っていれば）F/W の過去ログも保全する。 管理者パスワードの変更を行う。内部ネットワーク構成、制御の見直し。 アンチウイルスソフトベンダーに検体を送り緊急検知パターンファイルの作成依頼

⑧ CIO への（一次）報告内容を整理して下さい。

（マ）

部署、部署責任者、利用者名、感染日時
想定される脅威（流出が予想されるデータの機密レベル、停止する可能性のあるシステム）
学内告知状況
今後の調査方針（部署か？事務局全体か？全学か？また、セキュリティベンダーへの依頼を行うか否か？）

⑨ 二次対応として技術的に必要な事項を挙げて下さい。

（テ）→（マ）

端末のフォレンジックレベルの設定
端末の痕跡調査の範囲の決定
教学系ネットワークと管理系ネットワーク間の通信監視
ネットワークログオン監査ログの収集

データセキュリティの確保（機密度の高いデータの暗号化・隔離）
システム緊急停止時の代替サービス手段の確保

Ⅲ．二次対応（詳細な調査と封じ込め）

① 今回の場合は、内部拡散の有無については、どの範囲で調査しますか？

（テ）

事務系ネットワークと管理系ネットワーク

② 端末のフォレンジック調査は、何を証明するためにセキュリティベンダーに依頼しますか？費用の試算はどの位になりますか？また、どの予算からの出費になりますか？

（マ）

いつ、どの情報の流出の可能性があったのか。 外部の第 3 者の犯行であること（内部犯行でないこと）。

③ ②の要求を技術的な要求仕様にすると、どのような項目になりますか？

（テ）

要求として、 ・メモリ、HDD の正確な保全 ・不審なファイル作成やプロセス起動・通信状況調査、ネットワークログオンや媒体による拡散の有無、トリガーとなったマルウェアの特定 ・タイムライン解析による侵入・拡散の進行状況調査 を依頼する。70～150 万円/台程度を CIO 予算から捻出。その間の代替器は情セ貸

④ 攻撃の封じ込めは、どのようにして行いますか？

（テ）

セキュリティベンダーの調査結果を待って、方策を検討する。 特に、学内 LAN と切り離した代替サービスが可能なシステムを暫定構築することで、感染が疑われる VLAN からの拡散防止策を併行して行っていく。

Ⅳ．事後対応計画

① 再発防止策として必要と思われる内容を列挙しなさい。

（テ）

VLAN の精密化と封じ込め措置
ユーザーの啓蒙と不審メール対応マニュアル作成

（マ）

データセキュリティ（暗号化等）の確保と運用規程への反映
緊急措置判断の条件の精密化と運用規程への反映
ユーザーの啓蒙と不審メール対応マニュアル作成
情報共有システムの活用

② 報告・公示は、誰宛てに行いますか？

（マ）

インシデント報告書→CIO、セキュリティ委員会

CIO は、学長、理事長、広報への説明