5E-1

ユーザが意識しないHTTP通信の識別について

榊原裕之† 桜井鐘治†
†三菱電機株式会社 情報技術総合研究所

1. はじめに

近年，企業などの特定の組織に対する標的型攻撃が増えており，不審なメールにより組織に入り込んだマルウエアが活動し，機密情報が漏洩する事故が起こっている．この様な攻撃は，Advanced Persistent Threat (APT) と呼ばれる[1]．APT 攻撃におけるマルウエアによる情報漏洩は，組織の多くでインターネットとの通信が許可されているHTTP を用い，ユーザに気づかれないように行われる．本稿では，プロキシログや端末操作ログなどの各種ログを用い，ユーザが意識しない HTTP 通信を識別する方法について提案と考察を述べる．

2. APT攻撃について

APT 攻撃は，以下の段階に分類される[1]．

① 攻撃の準備段階

攻撃対象の組織(T)に関係のある別組織(X)を侵攻し組織 X のメール情報を取得する．

② 初期の潜入段階

攻撃者は①で取得したメール情報を用いて，組織 X を装い，標的型メールを組織 T に送信する．標的型メールには，ソフトウエアの脆弱性を攻撃する悪質なコードが文書ファイルを装い添付されている．或いは，マルウエアが配備された悪意のある Web サイトへの URL が記載されている．組織 T のメールの受信者は，巧妙な文面に騙されて標的型メールの添付ファイルを開いたり，記載された URL をクリックすることにより，ソフトウエアの脆弱性が攻撃されマルウエアに感染する．

③ 攻撃基盤を構築する段階

組織 T の端末に感染したマルウエアは，インターネット上の攻撃者と通信・制御され，別のマルウエアをダウンロードする．これは RAT(Remote Administration Tool)と呼ばれる．

④ システムを調査する段階

RAT は攻撃対象の組織 T における端末情報やネットワーク等のシステム情報を取得する．感染した端末に保存された他の端末へのアカウント情報を取得し，侵攻先を拡大する．また，システム情報にあわせて RAT をアップデートしたり別のマルウエアをダウンロードする場合がある．

⑤ 攻撃最終目的の遂行段階

RAT はファイルサーバや DB サーバにアクセスし機密情報を取得，攻撃者へ通信により漏洩する．

③～⑤における RAT と攻撃者の通信では，HTTP 等，組織においてインターネットとの通信が許可されているプロトコルが用いられる．従って，ブラウザ等のユーザによる通信と区別がつきにくい．

3. APT攻撃への対策

APT 攻撃への対策は，大きく分けると，標的型メールによるマルウエアの侵入（２章②）への対策，内部活動への対策（２章③，④），情報漏洩（２章⑤）への対策がある．各々への対策と課題を述べる．

3.1. 標的型メールへの対策と課題

攻撃の初期段階における標的型メールの検知やマルウエア感染を防止する．

■対策

(a)不審なメールをブロックするメールレピュテーション製品の導入

(b)ソフトウエアの脆弱性を解決するパッチ適用

(c)ユーザに対する教育で，不審なメールの添付ファイルへのアクセスや URL へのアクセスを禁止

■課題

(a)送信元メールアドレスが関係のある組織の場合はすり抜ける．

(b)出張／休暇による不在者の端末は即座にパッチ適用が難しい．パッチ適用が情報システムに与える影響を確認してから適用指示が出る場合は適用が遅延する．

(c)標的型メールの文面は巧妙であり，教育を受けても騙されたり，うっかりアクセスする可能性がある．

3.2. 内部活動への対策と課題

RAT による端末情報やアカウントの詐取，ネットワークの偵察等を検知／防止する．

■対策

(a)端末の不審な挙動を検知するソフトウエアの導入

(b)他端末へのアクセスアカウントの厳重な管理

(c)ネットワーク偵察行為の検知

(d)RAT の攻撃者との通信を検知／遮断

■課題

(a)検知精度が条件により変わる可能性があり，状

Detection of user-unaware HTTP communication
Hiroyuki Sakakibara†, Shoji Sakurai†
† Information Technology R&D Center, Mitsubishi Electric Corporation

況によってはすり抜ける可能性がある.
(b)他端末へのアクセスアカウントの管理を厳しくすると利便性が損なわれる場合がある. 例えば他端末へアクセスしたアカウント情報の一時的なキャッシュまで禁止すると利便性が損なわれる.
(c)偵察行為は目立たないように時間をかけて行われることがあり, 検知されにくい.
(d)3.3 情報漏洩への対策と課題における(c)で述べる.

3.3. 情報漏洩への対策と課題

情報漏洩を防止する.
■対策
(a) Web アクセス向け情報漏洩防止製品の導入
(b) 機密ファイルの暗号化／DB 暗号化
(c) RAT の攻撃者との通信を検知／遮断
■課題
(a)検知精度が条件により変わる可能性があり, 状況によってはすり抜ける可能性がある.
(b)ファイルが漏洩しても暗号化しておくことにより, 情報を漏洩させない方法であるが, ファイルサーバにおける個々のファイル全てを暗号化することは, 運用が難しい場合がある.
(c) RAT とブラウザが送出する HTTP リクエストにおける特徴の差異を用いて RAT の通信を検知する方法等がある[1]. RAT により通信の特徴が異なるため全ての RAT に適用できるわけではない.

以上の課題を鑑み, RAT の通信を早期に検知する 3.3(c)の対策を充実させることが最終的に情報漏洩の防止に繋がると判断した.

4. ユーザが意識しない HTTP 通信の検知

本稿では, RAT の通信の特徴に依存せず, 各種ログを使用しユーザが意識しない HTTP 通信を RAT の通信として検知する方式を検討した.

4.1. 検知方式

組織からインターネットへの許可された通信として HTTP があり, プロキシサーバを通過する. プロキシサーバを通過する通信は以下である.
(a) OS／ソフトウエアのアップデート等の通信
(b) ユーザのブラウザによる通信

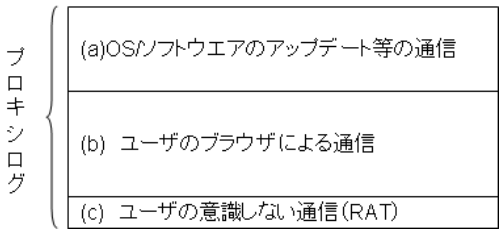

図 1 プロキシログの内訳

(c) RAT の通信
従って, プロキシログから, (a)と(b)を除外した残渣を(c)と判断することにした（図 1）.

■OS／ソフトウエアの通信の除外
組織において使用可能な OS やソフトウエアは予め決められていることがあるため, アクセス先の URL を予め知ることができる. これを含むプロキシログエントリを(a)として除外する.
■ユーザのブラウザによる通信の除外
(b)の通信の除外については, 以下の様に行う.

近年, 内部統制を目的とし, ユーザの端末上の操作を監視するためのソフトウエアが利用されている. ユーザの端末上でファイルのコピー／リネーム／媒体への書き出しを監視する機能がある. さらに, ブラウザでアクセスした URL（アドレスバー入力, リンククリック）を記録する機能を持つ. このようなソフトウエアのログ（端末操作ログと呼ぶ）を用いると, ブラウザによりアクセスした URL が判断できる.

あるサイトのトップページにブラウザでアクセスすると, 画像や動画等のコンテンツが自動でダウンロードされることがある. これらのダウンロードの HTTP 通信はプロキシログに記録されるため, (b)として判断する必要があるが, URL は端末操作ログには記録されない. そこで, 端末にローカルプロキシを導入し, アクセスした URL と取得したコンテンツを用いて判断する方法が考えられる. 以下の様な URL を(b)として判断する.
①端末操作ログに記録されたブラウザでアクセスした URL を 1 つ取得する.
②ローカルプロキシログにおけるアクセスした URL の記録から, ①の URL に一致するものを抽出する.
③②で一致した URL に対応する html コンテンツを取得する.
④③のコンテンツに記録された画像アクセス用の URL(img タグの src)や他のサイトへのリンク（a タグ）等を URL 抽出する.
⑤④で抽出した URL は①の URL にアクセスした結果ブラウザが自動で取得したか, 今後アクセスする可能性のある URL なので, (b)として判断する.
①～⑤を端末操作ログにおける URL について繰り返す. なお, 当処理は端末毎に実施する.

5. おわりに

APT 攻撃における情報漏洩対策として, プロキシログ, 端末操作ログ, ローカルプロキシログを用いた, RAT の通信を検知する方法を検討した. 今後, 実験により有効性について検証する予定である.

参考文献

[1]「新しいタイプの攻撃」の対策に向けた設計・運用ガイド 改訂第 2 版, IPA