不正送金対策向け金融サイバーキルチェーン

Financial Cyber Kill Chain for countermeasures against financial frauds

岡田　周平・マネジメント分科会・情報セキュリティ大学院大学

Abstract : There are a variety kinds of financial frauds and the frauds consist of multiple attack phases. On the other hand, there are many defenders such as financial institutions, depositors and so on. Many things should be considered to take care of the attacks, for example who implement the countermeasures, what kind of financial frauds we can defense, what phases we can defense. It is crucial that necessary countermeasures are clarified and every parties reach an agreement on the plans, understand their roles and proceed with the necessary works. Based on the above, we propose an analysis framework called “Financial Cyber Kill Chain”. It aims to improve optimum defense analysis and common understanding among defenders. We consider these improvements strengthen overall countermeasures. Therefore we verify the efficacy and usefulness of our approach with several case studies and interview.

研究目的

・ 不正送金を狙う攻撃に対して、**預金者保護を徹底**するため**最適な防御に向けた分析及び対策を講ずる者（対策主体）の間における認識を共通化し、対策全体を強化**すること。

提案

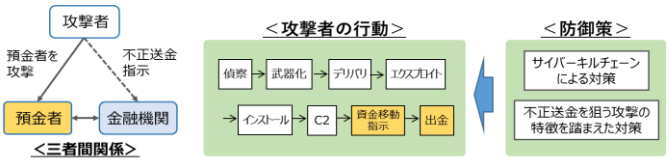
・ **不正送金を狙う攻撃に対する個々の対策の効果と限界を明確にする分析フレームワーク**を提案。 ⇒ **「金融サイバーキルチェーン」**
・ 提案手法は、不正送金を狙う攻撃者の行動を起点として、攻撃フェーズ及び対策を表現。

貢献

・ **金融機関をはじめとする各対策主体が導入すべき対策の理解、合意に向け、本フレームワークを基にした議論ができる。**
・ 提案内容について、**6個の事例を用いて、攻撃と対策の分析を行い、有効性を検証**。また、**2先に対してヒアリングを実施し、提案手法の有用性を検証。**
・ 本研究では、不正送金を狙う攻撃を対象に攻撃と対策の分析を行ったが、**提案手法は他の分野でも活用可能**と考える。
例）重要インフラ、オンラインマネー、イーコマース

1．金融サイバーキルチェーンのサマリ

【ポイント】APTを分析するサイバーキルチェーンの応用、各対策主体の役割の明確化



2．金融サイバーキルチェーンの特徴

・ **金融サイバーキルチェーン**は、攻撃分析表及び対策表のふたつの表から構成される。
・ **攻撃分析表**は、**定義した攻撃フェーズを基に、攻撃者の行動及び対策を具体的に記述**する。
・ **対策表**は、**攻撃フェーズ毎に、対策を対策主体別及び効果分類別に記述**する。
・ **想定する利用者**は、**金融機関をはじめとする各対策主体**である。

3．攻撃者の行動：2016年6月、スパイウェアの事例

#	発生事象	攻撃者フェーズ
1	2016年6月以前、攻撃者は、銀行や送信先メールアドレスを調査、識別、選択する等、情報収集を行ったと推測される。	偵察
2	攻撃者は、金融マルウェア（Bebloh）や送信用の電子メールを準備したと推測される。	武器化
3	2016年6月、攻撃者は、本銀行の預金者を含め、銀行を騙る電子メールを広く送信した。	デリバリ
4	2016年6月以降、一部の預金者は、電子メールの添付ファイル（ZIPファイル）を実行した。	エクスプロイト
5	当該預金者のPCは、金融マルウェアに感染し、金融マルウェアは継続的に当該PCを監視した。	インストール
6	当該預金者は、Webブラウザを通じて、本銀行のインターネットバンキングサービスにアクセスした。	C2
7	金融マルウェアは、アクセスを検知し、ログイン後、認証情報の入力を求める画面（偽画面）が表示されるような命令を追加する改ざんを行った上で、Webブラウザに渡した。	↑
8	預金者は、Webインジェクトに気付かず、認証情報を入力してしまった。	↑
9	資金移動指示には認証情報が必要であったが、攻撃者は当該情報も入手していたため、指示を行った可能性がある。	資金移動指示
10	攻撃者は、資金移動先口座から出金した可能性がある。	出金

4．分析事例：2016年6月、スパイウェアの事例（C2フェーズ）

#	発生事象	攻撃者フェーズ	対策主体：金融機関	預金者	他の金融機関	ISP	セキュリティベンダ	警察当局等
1	当該預金者は、Webブラウザを通じて、本銀行のインターネットバンキングサービスにアクセスした。	C2						
2	預金者は正規のWebサイトにアクセスしているため、【EV SSL証明書】は有効でなかった。	↑	✓	✓				
3	**【不正送金対策向けAV】は金融マルウェアを駆除できなかった、又は、駆除できたが、本対策を導入していなかった。**	↑	✓	✓				
4	金融マルウェアは、アクセスを検知し、ログイン後、認証情報の入力を求める画面（偽画面）が表示されるような命令を追加する改ざんを行った上で、Webブラウザに渡した。	↑						
5	預金者は、Webインジェクトに気付かず、認証情報を入力してしまった。	↑						
6	**金融マルウェアのC2通信について、【C2通信遮断】を行うことにより、一部の攻撃が阻止できた可能性がある。**	↑				✓	✓	

5．対策主体が講ずる対策の効果と限界を分析

・ 攻撃者は、本フェーズで攻撃先を選択し、金融マルウェアを準備
・ 各対策主体は、対策を講じていない

・ 攻撃者は、本フェーズで認証情報を盗取
・ 金融機関、**預金者**、ISP及びセキュリティベンダが対策を実施
・ 2個の対策（不正送金対策向けAV、C2通信遮断）が、効果を発揮

・ 攻撃者は、出金を実施
・ 金融機関、**預金者**、警察当局等が対策を実施
・ 5個の対策（取引メール通知、テイクダウン等）が、効果を発揮

・ 攻撃者は、本フェーズで銀行等を騙る電子メールを送信し、預金者PCを金融マルウェアに感染させる
・ 対策主体は、**預金者**が中心となっている
・ 3個の対策（用心深いユーザ、OS等の最新化、AV）が、効果を発揮

・ 攻撃者は、不正な資金移動を指示
・ 金融機関、**預金者**及びその他の金融機関が対策を実施
・ 2個の対策（OTP、IP等情報共有）が、効果を発揮
・ 預金者に頼らない対策が不足