情報セキュリティにおける「欺し」を考える

情報セキュリティにおける心理学・行動科学的な考察

内田勝也¹

(¹ 情報セキュリティ大学院大学)

キーワード: 情報セキュリティ, 欺し, 情報セキュリティ心理学

Analysis of deception in information security

The approach of psychology and behavioral scientific in information security

Katsuya UCHIDA¹

(¹Institute of Information Security)

Key Words: Information Security, deception, Information Security psychology

目 的

現実世界では、「振込詐欺」や「催眠商法」等, 人が人を欺す例は数多くあり, また, お釈迦さまも「嘘も方便」と言っており, 神話の世界では, 神様が人間を欺したり, 動物が人間を欺す例もある。

情報通信技術の発展は, 人が人を欺すだけでなく, 人が機械を, 機械が人を, 機械が機械を欺す例も見られる。

また, 情報セキュリティにおける欺しでも, 多くの場合, 心理的, 行動科学的な観点からの攻撃が行われていると感じている。

そこで, 攻撃者(攻撃機器)と被害者(被害機器)について, インシデント解説や報道等を基に考察を行った。

方 法

情報セキュリティでの考えを, (1)ハードウェア/ソフトウェア, (2)人間, (3)ハードウェア/ソフトウェアと人間の両方に関係するものの3つに分類した。なお, ハードウェアとソフトウェアを一つとして扱うのは, コンピュータは, ソフトウェアはハードウェア内にある

「Stored Program 方式」が特徴であり, 現在ではコンピュータだけでなく, 多くの機器は, 機械的な制御からプログラム制御を行うことが主流になっており, 1つのものとして考えることにした。

そこで, 情報セキュリティの特徴を考慮し, 攻撃側と防御側をハードウェア/ソフトウェアと人間に分類するだけでなく, ハードウェア/ソフトウェアと人間の両方が絡む場合を含め, 3つに分類して, 考察を行った(図1)。

図1 攻撃者・被害者の分類

結 果

9分類された攻撃・防御について, その概要を以下に記す。

a) Hard/Soft ⇒ Hard/Soft

ネットワークに接続される機器全てにユニークな番号(Mac アドレス)が設定されているが, それを変更することによって, 防御側に誤認させる。

b) Hard/Soft ⇒ Hard/Soft + Human

本来の目的を隠し, 悪意のあるプログラムである「ト

ロイの木馬」ウイルスの多くは, 添付ファイルとして, 電子メールで送付され, 被害者がそれをクリックすると, 実行されるもので, 最近では, 金銭を要求する「ランサムウェア」(金銭要求のもの)はその典型例。

c) Hard/Soft ⇒ Human

スマートフォンのソフトウェア「Call ID」では, 発信者の性別や声を変えることができ, 他人になりすまし, 受信者を欺す。

d) Hard/Soft + Human ⇒ Hard/Soft

ファイル添付型の標的型攻撃は, メール添付ファイルを受信者がクリックするとパスワード等を盗取する。

e) Hard/Soft + Human ⇒ Hard/Soft + Human

URLを埋め込んだ標的型メールを送付し, URLをクリックさせ, そのウェブから悪意のあるプログラムをダウンロードさせて, 目的を達成する。

f) Hard/Soft + human ⇒ Human

ビッシング(Vishing: Voice Phishing)は, 自動応答電話を利用し, 途中から攻撃者が対応し, 悪意ある行為を行う。

g) Human ⇒ Hard/Soft

指紋や静脈を偽造し, 認証システムを欺すもの

h) Human ⇒ Hard/Soft + Human

社内の人間と思わせる言葉を使って金融機関に電話をかけ, 対応者(被害者)にコンピュータ操作をさせ, 別の支店でその口座から現金を引き出した。

i) Human ⇒ Human

宅配便や清掃業者等の制服を着用し, オフィス内に入り込み, 重要書類やノートPC等を盗取する。

考 察

ソフトウェアの高度化は機器の高度化に繋がり, 人間だけでなく, プログラマブル機器が機器や人間を欺すことも発生している。高齢者等への介護や癒やしロボットが活躍していることを考えれば, ロボットが加害者(?)になる可能性も否定できない。

今回は, 攻撃・防御の対象者(対象機器)毎の分類を試み, 実際に情報セキュリティ分野で発生した事案について, それぞれに当てはめたが, 数多くの事例を収集し, その特徴の分析を行い, また, それらの攻撃を防ぐ方法についても考察を重ねている。

引用文献

内田勝也・高橋正和(2004), 有害プログラム——その分類・メカニズム・対策 共立出版