「今、現場で求められる Fast Forensics」

株式会社サイバーディフェンス研究所 杉山　一郎

・ここ１、２年でよく見られた標的型攻撃と対応してみて痛感したこと

組織のネットワークは人間の体と同じで、長く付き合えば付き合うほど変な癖（暗黙のルール等）や病を抱えがちである。そして、長期間あるいは深く潜伏した病や癖ほど完全に取り除くのが難しい。最近の標的型攻撃も同様で、完全に悪の根源を除去するのは非常に困難で、長期的な対応（治療）が必要だと感じる。そして、その対応にフォレンジック技術は欠かせないものではないかと感じる。

・攻撃のフェーズ

１、最初の侵入と継続的な活動を行うためのシステム変更
２、情報収集と横展開（組織横断）
３、外部へのデータ送信準備
４、データ送信、送信データの消去

・攻撃のフェーズやクライアントの状況を考慮したフォレンジック対応

× 関係する端末の完全コピー（完全なフォレンジックイメージの作成）が現実的に難しい。
※誤解のない様に言うと、完全コピーは実施できるのであれば実施した方がいい。

○ 早急な原因追求、侵入経路や継続的な活動拠点の把握を行うために、最低限のデータをコピーし、解析する。そして、解析により複数箇所で起きている独立した事象（点）を結ぶためのキー（プロセス、IP、タイムスタンプ等）を得、点をつなぎ全体の解明や次のアクションを起こす必要がある。
→一つのデバイスを深く見るのではなく、事象解決のための Fast Forensic が必要と考える。

・Fast Forensic で見るべき箇所は、各フェーズの特徴等から見えてくる。

1、 最初の侵入と継続的な活動を行うためのシステム変更
- ・ブラウザアクティビティの追跡（単に履歴だけでなく「どこからどの様に」の観点で）。
  ※最近のブラウザにはそれが備わっている事が多い
- ・ファイルアクセス、Java のキャッシュ等のユーザアクティビティ
- ・未知のサービス実行や、DLL の作成（Rundll32.exe の実行状況）等
- ・レガシーなレジストリ（Run キーや BHO 等）やタスクの設定
- ・USB デバイスの接続

・正規ファイルを装うファイルの存在
・Temp や AppData 等のディレクトリに存在する不審なファイル
等々

2、 情報収集と横展開（組織横断）
・PSEXEC や PSEXECSVC 等の SMB 経由での活動痕跡
・ハッシュダンプ（pwdump、wce 等）に代表されるグレーツールの痕跡
・検索やフォルダアクセスの痕跡（Recent、ShellBag 等）
・イベントログ（ログオン、プロセス作成、タスク等）
・ドメイン環境における情報収集（get-aduser 等）
等々

3、 外部へのデータ送信準備
・データの圧縮（典型的な例は RAR だが、最近は…）
・ファイル一覧の痕跡（DIR の実行および結果の痕跡等）
・データを集約するための拠点（各端末の相関分析から見えてくることや、責任所在が不明なテスト機などが多い）
等々

4、 データ送信、送信データの消去
・消去行為の痕跡（sdelete 等の実行、チェンジジャーナル、INDEX バッファのスラック等）
・データ転送ツール（RAT、PSCP、HTran 等）
・司令先（C&C）と他の通信の相関分析
等々

上記に加え、全てのフェーズでメモリフォレンジックやタイムライン解析を活用する。何も有効な情報が得られない場合、イメージ作成とディープなフォレンジックを実行する。

・Fast Forensic と従来のフォレンジック

従来のやり方（完全なディスクイメージの作成）が、フォレンジック的にはベストプラクティスだとしても、組織内部に深く侵入されている標的型攻撃に対応する現場では、その手法が毎回ベストプラクティスとは限らない。それより Fast Forensic するための対象を素早く保全する方にフォーカスし、その手法を更に発展させることも重要なのではと考えている。昨今のディスク容量の増大等も考慮すれば、なおさらと考える。もちろん可能であれば、グレーな端末はメモリ等をダンプの上、電源 OFF で隔離し、従来のフォレンジックに備えるのが望ましい。