Monthly Research

POS マルウェアについて

株式会社ＦＦＲＩ
http://www.ffri.jp

Ver 1.00.01

アジェンダ

- POS マルウェアによる被害事例
- POS システムのセキュリティ研究事例
- POS システムがマルウェアに狙われる一因
- POS マルウェアの例 BlackPOS, Backoff
- POS マルウェアへの対策案
- まとめ

POS マルウェアによる被害事例

- 米国の小売大手 Target 社の大規模な情報漏洩事件
  - 発生期間は、2013 年の秋からクリスマス前までの間
  - 被害は、およそ 4,000 万人の顧客のクレジットカード情報に加えて、7,000 万人分の個人情報の漏洩
  - このサイバー攻撃は Kaptoxa と呼ばれ、BlackPOS という POS マルウェアを改良したと思われる Trojan.POSRAM が利用された
    - POS マルウェアとは、POS 端末上で動作するマルウェア
    - Target 社以外にも 6 社が被害に遭ったと言われている
  - この事件の結果、2014 年 5 月に Target 社の CEO が退任

POS システムのセキュリティ研究事例

- セキュリティ研究者も POS システムに着目している

- BlackHat USA 2014 では、新しいトピックとして POS システムのセキュリティに関する研究発表が 3 件あった。2013 年は POS システムに関する発表はなかった。
  - POINT OF SALE SYSTEM ARCHITECTURE AND SECURITY
    - 一般的な POS システムのアーキテクチャ、データフローと攻撃経路の解説
  - A JOURNEY TO PROTECT POINTS-OF-SALE
    - 一般的な POS システムの脆弱性およびメモリスクレイピング手法、POS システムの保護方法について説明
  - MISSION MPOSSIBLE
    - モバイル POS システムの脆弱性の解説、複数のアタックベクタからの攻撃、悪意のあるクレジットカードがリモートシェルをドロップする攻撃のデモ

POS システムがマルウェアに狙われる一因

- POS 端末の OS
  - 新規販売された POS 端末のシェア約 97% を占めるサプライヤー 8 社が Windows を採用
    - » 平成 25 年度　POS 端末サプライヤー別年間販売実績・シェア (DSS 研究所調べ)をもとに各サプライヤーの製品仕様を調査
  - 主に Windows Embedded POSReady が使われている
    - Windows Embedded Standard をもとにしたOS
    - PC 向け Windows と同じ脆弱性が存在しうる
    - Windows のソフトウェア開発技術でマルウェアを開発可能
- ネットワーク接続
  - マルウェアに感染しやすい Windows クライアントと同一のネットワークに接続されている可能性

POS マルウェアの例 BlackPOS の概要

- BlackPOS
  - アンダーグラウンドフォーラムで販売されている。作者はロシアに居るとされる。
  - Target 社への攻撃に使われたマルウェア Trojan.POSRAM は BlackPOS の亜種といわれている。
  - Trojan.POSRAM は発見された時、最新のアンチウイルスソフトで検知されなかった
  - Trojan.POSRAM の技術情報が、2014 年 1 月に米国土安全保障省(DHS)と複数の機関が共同で発表した「POS Malware Technical Analysis」というレポートに記載されている
    - 次頁以降、上記文書に記載されている技術情報を紹介する

POS マルウェア Trojan.POSRAM の動作

- Trojan.POSRAM(RAM スクレイパー)の動作概要
  - 攻撃者は何らかの方法で、POS 端末の接続された内部ネットワークに侵入し、POS 端末に Trojan.POSRAM を感染させた
  - POS システムのペイメントアプリがメモリに格納する復号された認証データ(カード番号, CVV等)を盗むために、マルウェアは以下のように RAM スクレイピングとデータの送信を行う
    - 下記の名前のペイメントアプリのプロセスをフックし、メモリ空間を監視し、抽出
      - pp.exe, PosW32.exe, pos.exe, epsenginesrv.exe
    - 抽出した認証データを .dll ファイルに保存する
    - 7 時間毎に時刻が午前 10 時～午後 5 時の間かどうかチェックし、もしそうであれば、内部ネットワークのテンポラリの共有フォルダに .dll ファイルの送信を試みる (TCP ポート 139, 443 または 80 を使用)
    - 上記によってインターネットにアクセスをしない POS 端末からデータを窃取

POS マルウェアと同時に使われたマルウェア

- Trojan.POSRAM に加えて以下の動作をするマルウェアが攻撃に使われた
  - ICMP Listener
    - Trojan.POSRAM からの共有フォルダへのデータ転送のログを記録するためのカスタム ICMPパケットを受信するサーバ
  - Shellcode Loader
    - ネットワーク経由で生のコードを受け取り、感染ホスト上で実行する
    - データ転送および実行を隠蔽し、ネットワーク制御とフォレンジックを妨害
  - Hacking Tools
    - ネットワーク探索、認証情報窃取、データベース操作、ポートフォワーディングなどを行うためのツール群

POS マルウェアの増加懸念

- ソースコードの流出による亜種の増加の懸念
  - 「POS Malware Technical Analysis」では、BlackPOS のソースコードが公開され、非常に簡単に入手可能になったため、POS マルウェアが間もなく爆発的に増加すると警告している。
  - また、今後 POS マルウェアの作成者は、バンキングマルウェアと同様に検知が難しいカスタムメイドのマルウェアを作成すると推測している。

- 別の POS マルウェア Backoff
  - 2014 年 7 月 31 日 US-CERT が Backoff という新しい POS マルウェアについて技術情報を公開し、警告を行った。
  - BlackPOS の亜種ではないと考えられる。
  - ここ数年で 7 つの POS システムベンダーがこのマルウェアに影響を受けていた顧客を確認した。シークレットサービスは 1,000 以上の米国企業が影響を受けていると推定している。

POS マルウェア Backoff の概要

- US-CERT のレポートには以下の技術情報が示されている。
  - 発見された時、最新のアンチウイルスソフトで検知されなかった
  - 3 種類の亜種(バージョン 1.4, 1.55, 1.56)があり、2013 年 10 月 ～ 2014 年 7月 までの間に変化が確認されている
  - 次の 4 つの機能を持っている
    - RAM スクレイピング
    - キーロガー (1.4 にはなし)
    - HTTP POST による C&C (C2) 通信
    - explorer.exe へのコードインジェクション (1.55 にはなし)

POS マルウェアへの対策案

- 現状分析
  - US-CERT やセキュリティベンダから公開されている技術情報をもとに
    - POS 端末および POS 端末と同一ネットワークの端末に不審なファイルやプロセスがないか調査する
    - POS 端末および POS 端末と同一ネットワークの端末から不審な通信が発生していないか調査する
    - 脆弱性診断の実施

- 予防
  - POS 端末のネットワークを一般的なクライアントネットワークと分離する
  - POS 端末と通信できる IP アドレスを限定する
  - POS 端末の OS にセキュリティ更新プログラムを適用する
    - Windows Update を行う

(参考情報) FFR yarai による POS マルウェアの検知

- 公開レポートに記載されている POS マルウェアのファイルハッシュ情報をもとに入手した検体を FFR yarai で静的スキャンした結果、以下の 6 つの検体を検知
  - 検知環境: FFR yarai 2.5.1192, Windows 7

SHA-1	種類
332548d0bc638c8948f3a429e79053003b4f6261	BlackPOS
9d99a2446aa54f00af0b049f54afa52617a6a473	BlackPOS
11b7430026c82097657c145dcedfa818bf1032d3	Backoff
98dbaeb6d46bd09eca002e1f2b6f3e76fd3222cd	Backoff
a6eb86b55148a7a491093f1f6af6a15c4b44b96c	Backoff
ab354242992af39f93520ac356ec12796e119151	Backoff

まとめ

- 昨年 POS マルウェアによる大規模な被害が米国で発生した

- セキュリティ研究者も POS システムに着目している
  - 今後、POS システムの新しい脆弱性が発見される可能性がある

- POS システムは今後さらにマルウェアに狙われていく恐れがある
  - 多くの POS システムは Windows 上で動作している
  - POS マルウェアは今後更なる増加が懸念される
    - 複数の種類の POS マルウェアの出現、BlackPOS のソースコード流出
  - 他の多くの企業が POS マルウェアの被害を受けていると推測されている
  - 日本国内でも同様の事案が発生する恐れがある
  - POS システムの現状調査や予防策の実施が推奨される

参考資料 1

- レジやPOSを狙うマルウェア
  - http://blog.kaspersky.co.jp/ram-scrapers-and-other-point-of-sale-malware/
- 米小売業者のカード情報流出、Target以外にも6社が被害に
  - http://itpro.nikkeibp.co.jp/article/IDG/20140121/531183/
- 7000万件に及ぶ情報漏洩事件の「その後」、株価復調もCEOの辞任に発展した米Target
  - http://it.impressbm.co.jp/articles/-/11538
- Point of Sale System Architecture and Security
  - https://www.blackhat.com/docs/us-14/materials/us-14-Zaichkowsky-Point-Of-Sale%20System-Architecture-And-Security.pdf
- A Journey To Protect Points Of Sale
  - https://www.blackhat.com/docs/us-14/materials/us-14-Valtman-A-Journey-To-Protect-Point-Of-Sale.pdf
- Mission mPOSsible
  - http://www.youtube.com/watch?v=iwOP1hoVJEE
- 平成25年度・POSシステム販売状況調査結果
  - http://dssr.jp/news.html

参考資料 2

- KAPTOXA Point of Sale Compromise
  - http://www.securitycurrent.com/resources/files/KAPTOXA-Point-of-Sale-Compromise.pdf
- POS Malware Technical Analysis
  - http://artemonsecurity.com/20140116_POS_Malware_Technical_Analysis.pdf
- Alert (TA14-212A) Backoff Point-of-Sale Malware
  - https://www.us-cert.gov/ncas/alerts/TA14-212A
- Backoff: New Point of Sale Malware
  - https://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware_0.pdf

Contact Information

E-Mail ：research—feedback@ffri.jp
Twitter：@FFRI_Research