暴露型ウイルスやスパイウェアによる情報漏えい

2007年2月14日

株式会社セキュアブレイン

星澤裕二

暴露型ウイルスとは

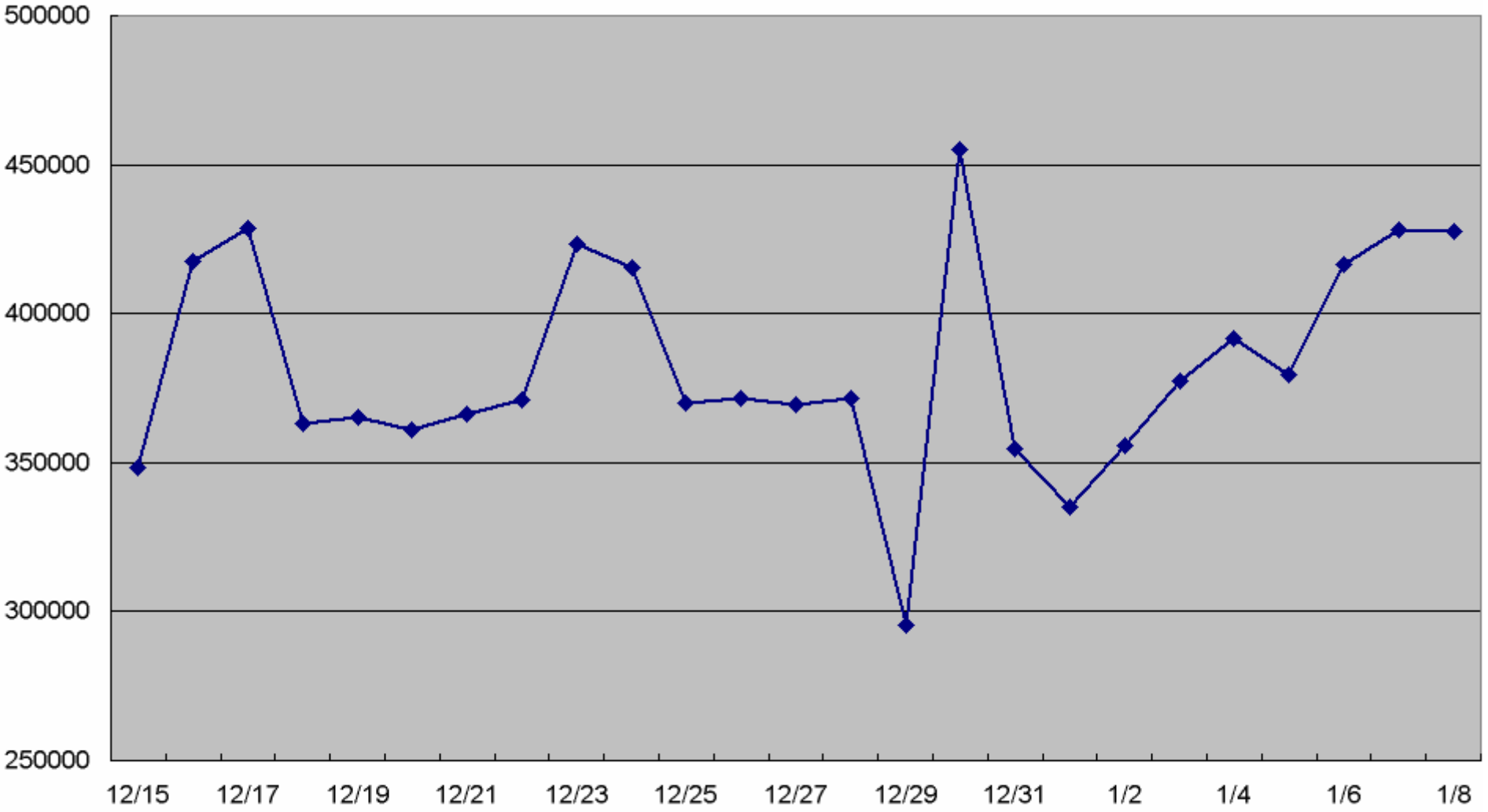
- 暴露型ウイルスとは、PC内の情報をP2Pネットワークやインターネット上に公開するマルウェアの総称
  - 次のような情報が公開されてしまう。公開される情報はマルウェアにより異なる。
    - マイドキュメントやデスクトップ上のファイル
    - デスクトップのスクリーンショット
    - Officeファイル
    - OutlookやOutlook Expressのメール
    - IEのお気に入りや履歴
    - Winnyの検索履歴
    - ハードディスク内の全データ
- データが流出してしまった場合、完全に回収することは不可能

WinnyやShareを悪用するマルウェア

- ワーム
  - W32.Antinny.AX, W32.Antinny.BF, W32.Antinny.K, W32.Antinny.Q, W32.HLLW.Antinny, W32.HLLW.Antinny.E, W32.HLLW.Antinny.G, W32.Yawmo
- トロイの木馬
  - Backdoor.Doroku, Backdoor.Hesive.F, Infostealer.Kurofoo, Infostealer.Kurofoo.B, PWSteal.Kurofoo, Trojan.Deoplive, Trojan.Exponny, Trojan.Exponny.B, Trojan.Upbit, Trojan.Leega, Trojan.Upchan, Trojan.Kakkeys, Trojan.Kakkeys.B, Trojan.Kakkeys.C, Trojan.Kakkeys.D, Trojan.Nullpos, Trojan.Nullpos.B, Trojan.Welomoch, Trojan.Remojin
- ハッキングツール
  - Hacktool.YMDSearch

- 出典: 株式会社シマンテック「Winny による機密情報漏えいについて (2006/8/16)」 http://www.symantec.com/region/jp/winny/

Winnyノード数



Winnyノード数推移 2006/12/15-2007/1/8

出典: ネットエージェント株式会社「Winnyノード数推移」
http://www.onepointwall.jp/winny/winny-node.htm

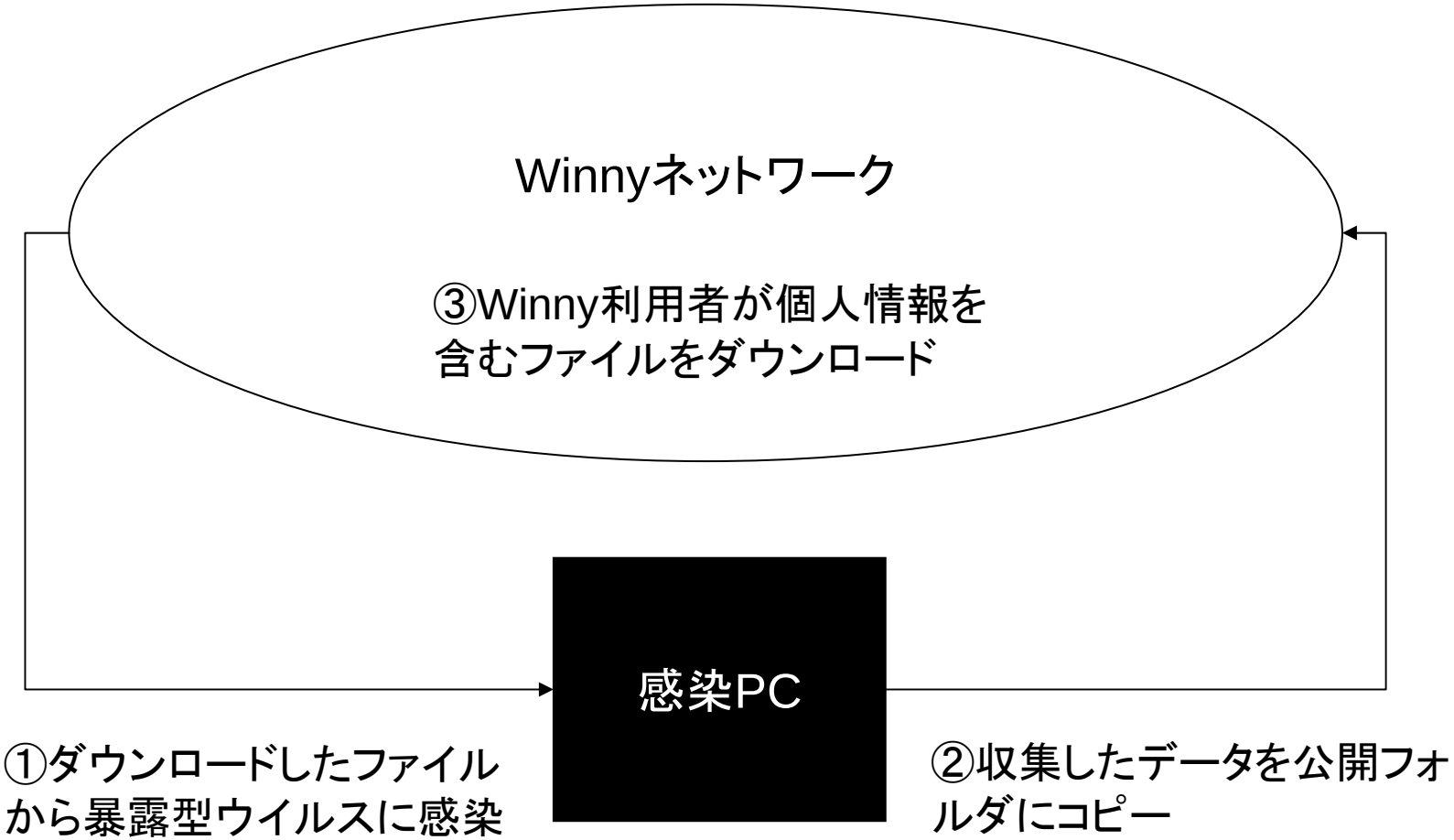
2006年Winnyによる情報流出事件の一部 (1/2)

- 北陸電力
  - 12月15日
  - 富山新港火力発電所の燃料貯蔵量に関する情報など
  - http://www.rikuden.co.jp/press/attach/06121502.pdf
- NTT西日本
  - 12月5日
  - 鹿児島支店と宮崎支店が持つ顧客情報3,140件、および電話番号約21万件
  - http://www.ntt-west.co.jp/news/0612/061205a.html
- 東北電力
  - 10月6日
  - 「送電業務総合支援システム」開発に関わるシステム設計書およびレビュー報告書の一部
  - http://www.tohoku-epco.co.jp/whats/news/2006/10/06.html
- 中部電力
  - 8月31日
  - 四日市LNGセンターの点検記録のフォーマットと記録の一部など
  - http://www.chuden.co.jp/corpo/publicity/press2006/0831_2.html
- 三菱重工業
  - 8月23日
  - 関西電力の原子力2次系配管の情報
  - http://www.mhi-ir.jp/frmpage/060823_genshi.html

2006年Winnyによる情報流出事件の一部 (2/2)

- 仙台市水道局
  - 8月8日
  - 水道メーターの交換業務委託に関する書類、水道メーター交換台帳、集合住宅代表者リスト、予算関係書などの行政情報440ファイル。この中には、2,011人分の氏名、住所、電話番号のほか、189社分の法人名、所在地、電話番号が含まれていた
  - http://internet.watch.impress.co.jp/cda/news/2006/08/08/12939.html
- JR北海道
  - 8月2日
  - 青函トンネル工務所管内における過去の道床交換工事の工事関係書類・見積査定書（2004年度分2件、2005年度分2件）と、2006年9月に発注を予定していた作成中の工事関係書類（2件）
  - http://www.jrhokkaido.co.jp/press/2006/060803.pdf
- 東京電力
  - 5月18日
  - 原子力発電所の運転員がプラントの運転管理を行なうための研修用資料
  - http://www.tepco.co.jp/cc/press/06051803-j.html
- ANA
  - 3月15日
  - 空港施設に入るための暗証番号など
  - http://internet.watch.impress.co.jp/cda/news/2006/03/15/11258.html

Winnyと暴露型ウイルス



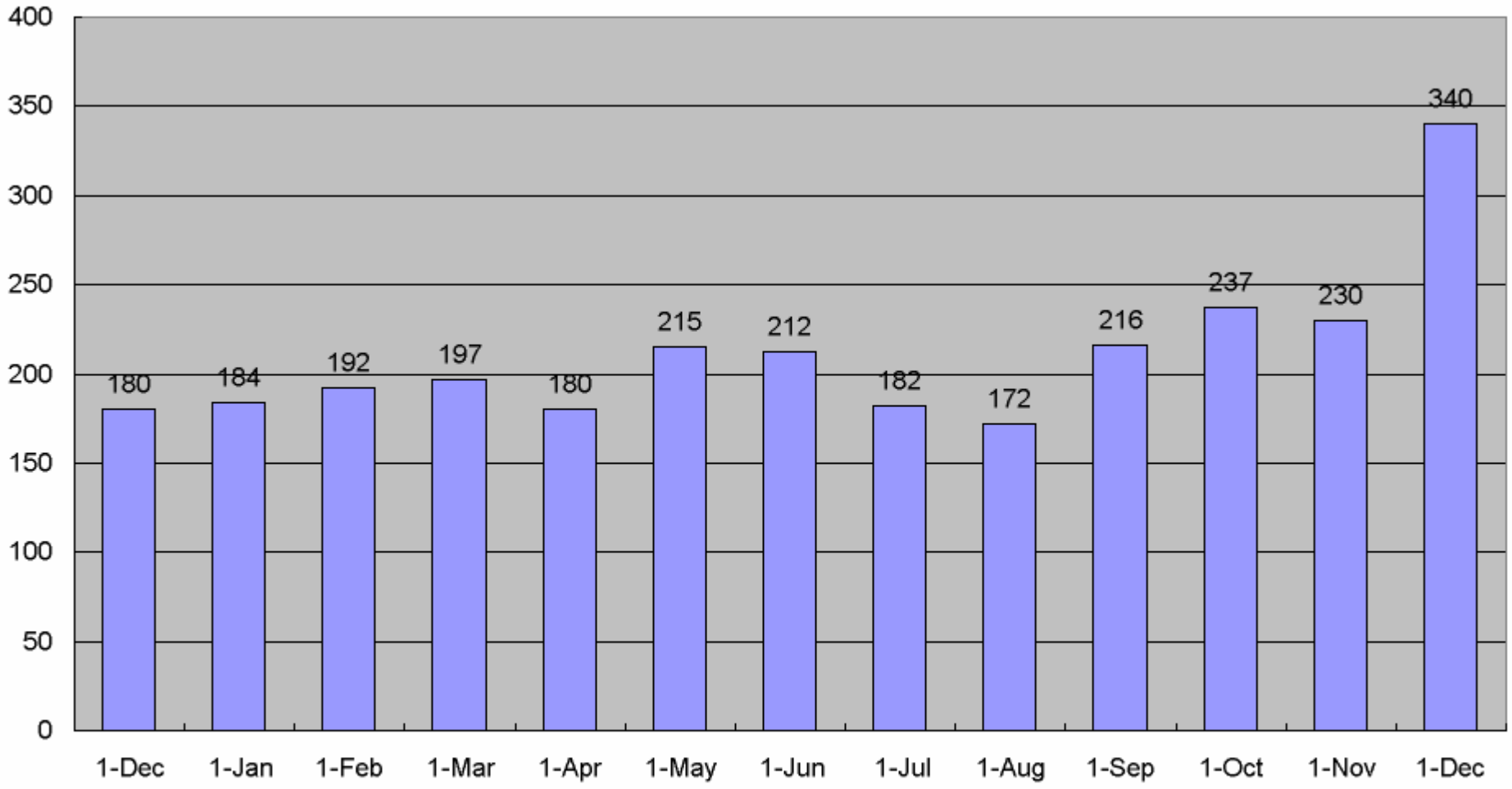
Winny以外を利用する暴露型

- 山田ウイルス
  - 感染PCをWebサーバとして動作させ、スクリーンショットを含むハードディスクの内容をインターネットに公開する
  - アクセスのためのアドレスを「2ちゃんねる」などのインターネット上の掲示板に書き込む
- 山田オルタナティブ
  - 感染PCがWebサーバとして動作させ、ハードディスクのすべての内容を公開
- W32.Antinny.BF (WORM_ANTINNY.AW)
  - OfficeドキュメントやOutlook Expressの関連ファイルなどをアップロードフォルダに格納し、WinnyやShareのネットワーク上に公開

スパイウェアとは

- 現在、スパイウェアの業界標準的な定義はない
- 利用者や管理者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム等（IPAとJNSAスパイウェア対策啓発WGによる共同の定義）
- 広義のスパイウェアに分類されるPhishing-based Trojanによる逮捕者も

Phishing-based Trojan



Password Stealing Malicious Code Unique Applications

出典: Anti-Phishing Working Group「Phishing Trends Report」
http://www.antiphishing.org/reports/apwg_report_december_2006.pdf

スパイウェア事件

- 元インターネットカフェ従業員を不正アクセス行為で逮捕 (2006/6/13)
  - 被疑者は、インターネットカフェ従業員の立場を利用し、店内のパソコンに「キーロガー」を仕掛け、他人のID・パスワードを不正に取得した上、その入手したID・パスワードを利用して、オークションサイトにおいて数十回不正アクセス行為を繰り返していました。
  - 警視庁 ハイテク事件簿 http://www.keishicho.metro.tokyo.jp/jiken/kenkyo/jiken.htm#180613
- スパイウェアを使用したインターネットバンキングに対する不正アクセス禁止法違反等被疑者を逮捕 (2006/1/16)
  - 被疑者らは、スパイウェアを作成の上、某会社のネットバンキング用のID、パスワードを不正に入手して、他人の住居等の無線LANアクセスポイントを利用し、入手したID、パスワードを使い銀行のサーバに不正アクセスして、他人名義の口座等から自己が管理する口座に約1500万円を送金しました。
  - 警視庁 ハイテク事件簿 http://www.keishicho.metro.tokyo.jp/jiken/kenkyo/jiken.htm#180116

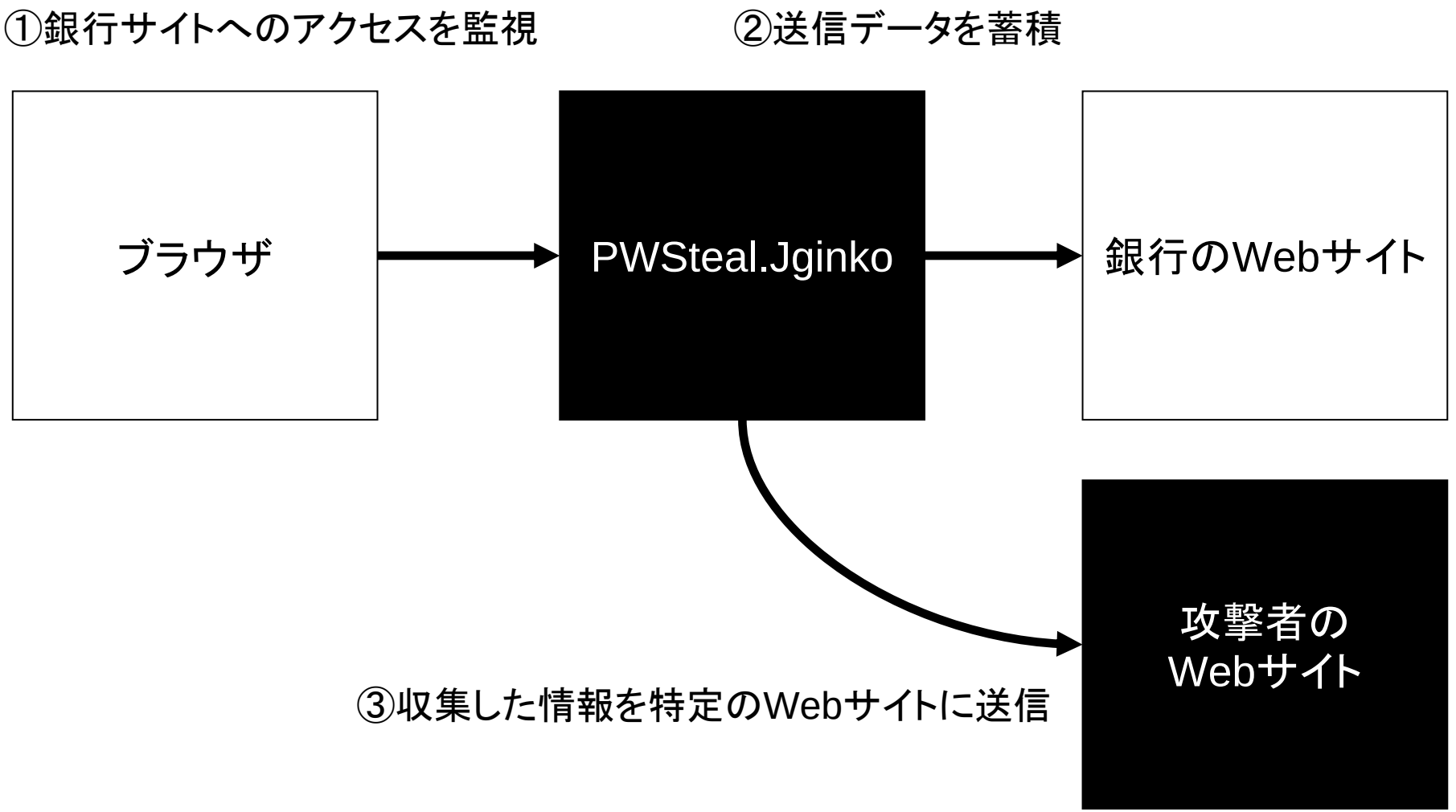
PWSteal.Jginko (1/3)

- PWSteal.Jginko(TSPY_BANCOS.ANM, PWS-Jginko)は、HTTPパケットを監視し、東京三菱銀行、イーバンク銀行、りそな銀行、三井住友銀行などのWebサイトで入力されたユーザ名、パスワードなどの情報を収集する
- 収集したデータとアクセスしたURLのリストを特定のWebサイトに送信する

PWSteal.Jginko (2/3)

- 次のWebサイトへのアクセスを監視する
  - resonabank.anser.or.jp, btm.co.jp, ebank.co.jp, japannetbank.co.jp, smbc.co.jp, ebank.co.jp, yu-cho.japanpost.jp, ufjbank.co.jp, mizuhobank.co.jp, shinseibank.co.jp, iy-bank.co.jp, shinkinbanking.com, shinkin-webfb-hokkaido.jp, shinkin-webfb.jp, paweb.anser.or.jp, caweb.anser.or.jp, hokugin.co.jp, web-fb.com, gunmabank.co.jp, 105bank.com, okbnetplaza.com, suitebank.finemax.net, ib-center.gr.jp, cyber-biz.ne.jp
- Webページ内で次の文字をtext入力フィールドのname属性として見つけると、入力されたデータ等を収集する
  - Pw, Ransu1, FurikomiKin, PASSWORD, PASSWD2_1, CHK_PASSWORD, password, recognitionPassword, passwordOLD, LOGIN_PASSWORD, USER_PASSWORD, OLD_PASSWORD, log_pass, PWD_PASSWORD, EWF_ENTRY_InputValiable1, AG00010, fldUserNumId, LgnPwd, i_pwd, BPW0020, i_acOneTime1, i_acFstCodenum, dat_0, S023, i_pwd, Pwd1, S007, WGLI020, Password, PIN, loginPassword, passwd, loginPwd, pw, logonPwd, KeiyakuNo, Anshu2, PWD_PINNUMBER, tb_conf, BPW0010
- 出典: @police PWSteal.Jginkoウイルス解析報告書
  - http://www.cyberpolice.go.jp/server/virus/pdf/PWSteal_Jginko.pdf

PWSteal.Jginko (3/3)



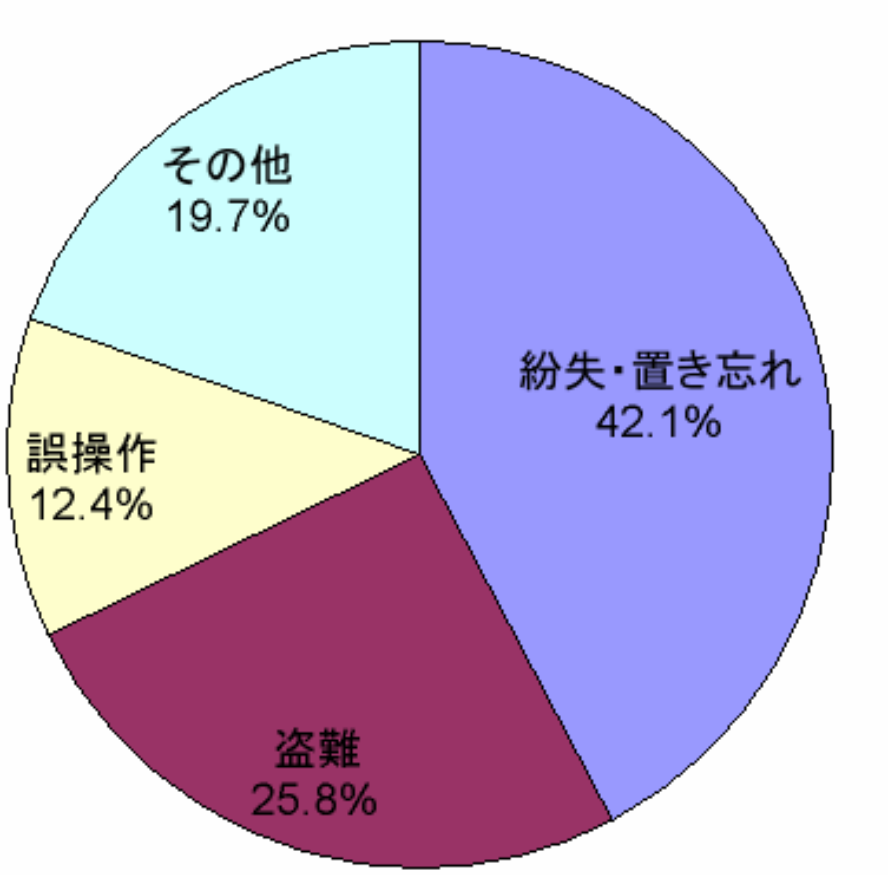
ボットやPhishingにも注意

- ボット
  - 遠隔操作により様々な情報を収集することができる
    - DOSコマンドの実行
    - キーボード入力の記録
    - コンピュータゲームのCDキーを盗む
    - メールアドレスの収集
    - システム情報の表示
    - トロイの木馬の更新版も含む、ファイルのダウンロードと実行
    - プロキシサーバとして動作
    - バックドアの管理
    - ネットワークに関する情報を送信
    - ファイルのダウンロードと実行
- Phishing
  - 人の心理を突き、うっかり個人情報を漏らしてしまうように仕向けるテクニック「ソーシャルエンジニアリング」を使う

しかし・・・

- Winnyの使用をやめ、ウイルス対策やスパイウェア対策をきちんとやったとしても情報が漏えいしてしまうことがある

その他の情報漏えい事件 (2/3)



個人情報漏えい原因の件数割合

出典: JNSA「2005年度情報セキュリティインシデントに関する調査報告書
http://www.jnsa.org/result/2005/20060803_pol01/index.html

その他の情報漏えい事件 (3/3)

- 紛失・置忘れ: 42.1%
  - 電車、飲食店など外部の場所に、PC、情報媒体等を紛失または置き忘れてしまった。
- 盗難: 25.8%
  - 車上荒らし、事務所荒らしなどにより、PC 等の情報媒体とともに機密情報が盗難された。
- 誤操作: 12.4%
  - あて先間違いによって、電子メール・FAX・郵便の誤送信が発生した。
- その他: 19.7%
  - 管理ミス、不正な情報持ち出し、設定ミス、内部犯罪・内部不正行為、目的外使用など。
    - Winnyに起因する情報漏えいについては一部を除き「管理ミス」や「不正な情報持ち出し」に分類

情報漏えい対策

- 情報漏えいを完全に防止することは難しい
- データ持ち出し禁止、セキュリティポリシー、物理セキュリティ、暗号化、パスワード、・・・
- 次のことを前提に対策を講じる
  - すべての攻撃を防御できるセキュリティ対策ソフトはない
  - PCやデータは盗まれるもの
  - 万全なセキュリティ対策はない

ご清聴ありがとうございました

株式会社セキュアブレイン
星澤裕二
Email: yuji_hoshizawa@securebrain.co.jp
Web: http://www.securebrain.co.jp/

参考情報

- IPA「Winny緊急相談窓口（Winny119番）」
  - http://www.ipa.go.jp/security/announce/20060320.html
- JNSA「スパイウェア対策啓発WG」
  - http://www.jnsa.org/spyware/index.html
- JNSA「2005年度 情報セキュリティインシデントに関する調査報告書」
  - http://www.jnsa.org/result/2005/20060803_pol01/index.html
- トレンドマイクロ「Winnyによる情報漏えい対策」
  - http://www.trendmicro.co.jp/security/winny/
- シマンテック「Winnyによる機密情報漏えいについて」
  - http://www.symantec.com/region/jp/winny/index.html