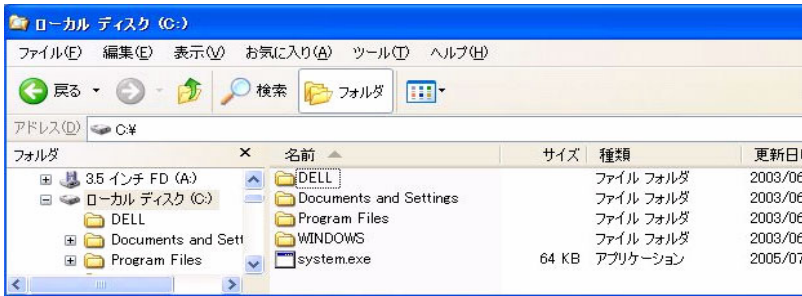
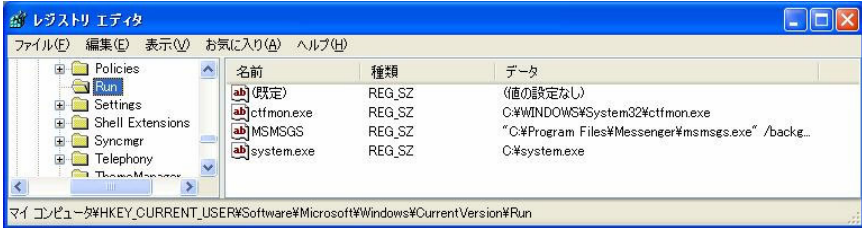


ウイルス解析報告書

ウイルス名	PWSteal.Jginko (別名 : Trojan-Spy.Win32.Banker.vt [Kaspersky Lab], PWS-Jginko [McAfee], TSPY_BANCOS.ANM [Trend Micro])
プログラム名及び容量(添付ファイル名)	プログラム名 : system.exe 容 量 : 65,536 バイト
種別	トロイの木馬
プログラム言語	C++
発症環境	Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP
発見日	2005 年 7 月 8 日
発見場所	日本
危険性	感染力が低い。危険度は 5 段階の 1(5 が最も危険)。
発症条件	プログラムを実行したとき。
ウイルスの活動、影響	このトロイの木馬は、日本の特定のオンラインバンクのアカウント情報を盗み取り、特定のサイトへ送信する。国内では、銀行を装い送付された CD をコンピュータに挿入したことによりプログラムが実行され、詐欺等の被害が認知されている。
被害の規模	シマンテック社に届出は寄せられていない。
亜種、変種の有無	同様のオンラインバンクのアカウント情報を盗み取る亜種が多数存在する。
ウイルスの動作概要	<p>このトロイの木馬が実行されると、次のことを行う。</p> <ol style="list-style-type: none"> 1. コンピュータ上でワームが複数同時に実行することを防ぐため、次のミュートクスを作成する。 kidou 2. ワーム自身を C:%system.exe としてコピーする。 <div style="text-align: center;">  </div> <ol style="list-style-type: none"> 3. レジストリを変更する。 Windows の起動時にトロイの木馬を実行するために、次の値を "system.exe" = "C:%system.exe" 次のレジストリキーに追加する。 HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run <div style="text-align: center;">  </div> <ol style="list-style-type: none"> 4. 自分自身あるいはコピーしたファイルを実行する際に、セキュリティの警告を表示しな

いようにするため、次のファイルの ZoneId(代替データストリームのファイル)を削除する。

C:¥system.exe:Zone.Identifier
[元のファイルのパス]:Zone.Identifier

5. Internet Explorer のウィンドウで、次の Web サイトへの接続を監視する。

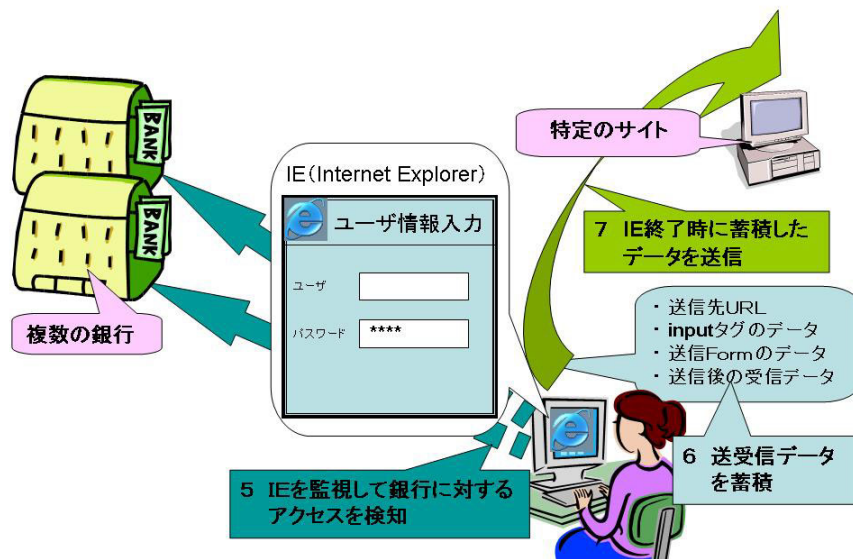
- resonabank.anser.or.jp
- btm.co.jp
- ebank.co.jp
- japannetbank.co.jp
- smbc.co.jp
- ebank.co.jp
- yu-cho.japanpost.jp
- ufjbank.co.jp
- mizuhobank.co.jp
- shinseibank.co.jp
- iy-bank.co.jp
- shinkinbanking.com
- shinkin-webfb-hokkaido.jp
- shinkin-webfb.jp
- paweb.anser.or.jp
- caweb.anser.or.jp
- hokugin.co.jp
- web-fb.com
- gunmabank.co.jp
- 105bank.com
- okbnetplaza.com
- suitebank.finemax.net
- ib-center.gr.jp
- cyber-biz.ne.jp

6. 5 の Web サイトへの接続を検出すると、スキャンを行い、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_InputVariable1
- 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

7. 収集したデータを特定の Web サイトに送信する。
8. アクセスした URL のリストを特定の Web サイトに送信する。
9. 動作概要図を下記に示す。



感染・発症防止方法

1. 予期せぬメールや不明なファイルが届いた場合には、安易に開封したり、添付ファイルを開かない。
2. インターネットからダウンロードしたファイルについては、必ずウイルススキャンを実行し、問題がないことが確認できるまでは絶対に起動しない。
3. 定期的にウイルススキャンを実行する。

ウイルスの駆除方法

手動による修復を行う場合、コンピュータに関する高度な知識が必要とされ、間違えるとコンピュータが正常に起動しなくなる場合もある。

	<ol style="list-style-type: none">1. 収集したデータの送信を防ぐため、感染したコンピュータをネットワークから切り離す。2. システムの復元オプションを無効にする。(Windows Me/XP)3. コンピュータをセーフモード(WindowsNT では VGA モード)で再起動する。4. 感染ファイルを削除する。 C:¥system.exe5. レジストリに行われた変更を元に戻す。 次のレジストリキーから HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Run 次の値を削除する。 "system.exe" = "C:¥system.exe" <p>各操作については Microsoft のホームページ、付属のマニュアル等を参照すること。</p>
その他	平成 17 年末現在で 1 件(国内 1 件)の届出がシマンテック社に寄せられている。