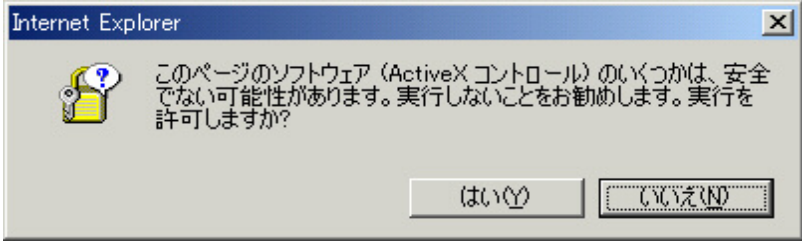
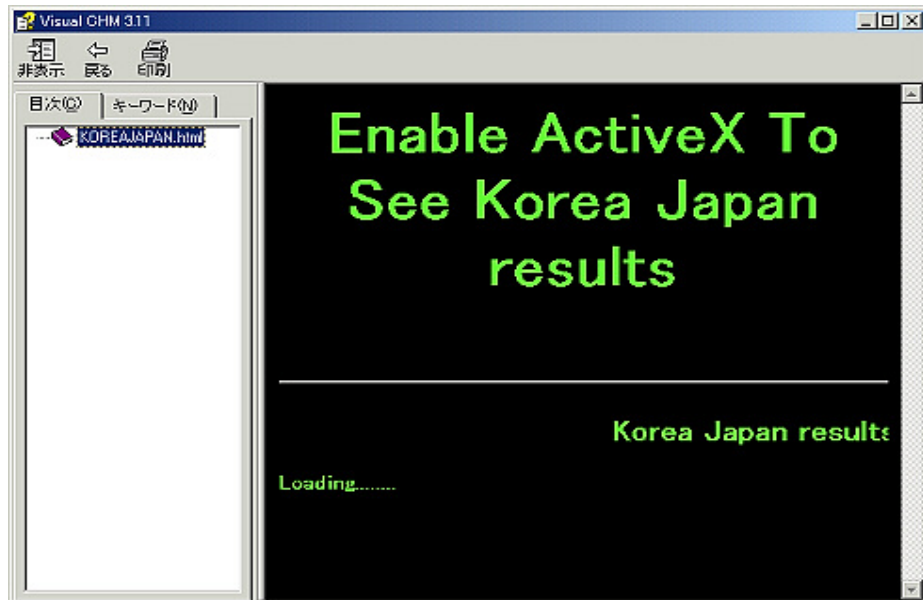


ウィルス解析報告書

ウイルス名	VBS/Chick.F (World Cup, I-Worm.Brit-G)
プログラム名及び容量 (添付ファイル名)	koreajapan.chm (12,170バイト)
種別	ワーム
プログラム言語:	VBS
発症環境	Windows9x/ME/NT/2000/XP (HTML形式ヘルプ利用可能環境)
発見日時	2002年6月7日
発見場所 (発信地)	不明
危険性	非常に低い(メール、IRCによる感染に失敗するためかなり低い。日本国内においてはさらに低い)
発症条件	発病はない
ウイルスの活動、 影響	<p>VBS/Chick.Fはワールドカップの最新試合結果を表示するユーティリティを装って、電子メールとIRC 経由で感染しようとするワームである。(実際にはバグのため、メール添付もIRC感染もない)</p> <p>このワームは、 件名: RE: Korea Japan Results 本文: Take a look at these results ... Regards, 感染したユーザーの名前</p> <p>このワームは、koreajapan.chmというファイルがその実体である。このファイルは「コンパイル済みHTMLヘルプ」であり、通常は複数のHTMLファイルや画像ファイルをまとめて一つにしたものであるが、このワームでは正体を隠蔽するためにこの形式をとっている。</p> <p>ワームファイルをダブルクリックすると以下の警告ダイアログが表示される。</p> <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;">  <p>Internet Explorer</p> <p> このページのソフトウェア (ActiveX コントロール) のいくつかは、安全でない可能性があります。実行しないことをお勧めします。実行を許可しますか?</p> <p style="text-align: right;"> <input type="button" value="はい(Y)"/> <input type="button" value="いいえ(N)"/> </p> </div> <p>これに「はい」と答えるとワーム本体が動作を開始する。このとき画面には次のようなウィンドウが表示されている。</p>



ワームを実行すると次のことが行われる。

1.ワームメールの発信(添付無し)

OutlookメールクライアントとExchangeメールサーバーの組み合わせを利用している環境では、アドレスリストにあるメールアドレスにワームメールが発信される。ただしバグにより肝心のワームファイルの添付に失敗する。

この組み合わせを採用している組織は日本ではかなり少ないため、どちらにしろ被害は広まらない。

これはVBS/Loveletterをはじめとするこのタイプのワームの伝染率からも伺える。

2.IRCクライアント利用者間での感染

IRC(インターネット中継チャット)クライアントのmIRCが利用されている場合、この自動運転ファイルが書き換えられる。ただしワームの転送は失敗するので感染はしない。なお、mIRCは日本語を通さないため、国内での利用者は殆どいない。

これらの状況からみて、このワームが感染を引き起こすことは考えにくい。

被害の規模

現在、アンチウイルスベンダーからは被害報告があったという報告はない。(2002年6月13日3時18分現在)

亜種、変種の有無

A型からF型までの亜種が確認されている。詳細は不明。

ウイルス動作概要

ワームを実行するとIEの設定にもよるが、「安全でないActiveXが実行されようとしている」という意味の警告がなされることがあるが、ワームはこれに対抗する処置として"Enable ActiveX To See Korea Japan results"というメッセージを表示し、ユーザーにActiveXを実行させることを促す。

ユーザーがActiveX実行を許可し、ワームの実行が次にうつるとWindowsフォルダ(通常はc:\windows)にワームのコピーをkoreajapan.chmの名前で作成しようとするが失敗する。これはコピー元となる自分自身のフルパス名作成に失敗しているからである。

OutlookメールクライアントとExchangeメールサーバーが使用されている環境では、バックグラウンドでOutlookを実行し、MAPIを用いてアドレスリストの最初のメールアドレスを取得し、これに宛ててワーム添付ファイルを送信しようとするが、上記でワームのコピーに失敗するため、添付原本が見つからずに添付に失敗する。

IRC(インターネット中継チャット)のクライアントである「mIRC」がC,D,Eドライブのどれかにインストールされている場合、ワームはこのフォルダにscript.iniという名前の自動運転ファイルを作成する。これは、mIRCを用いてチャットを行ったとき、あとから参加してきたユーザーに対しワームをDCC(直接接続転送)で送りつけるのが目的であるが、転送原本のkoreajapan.chmファイルが無いので失敗する。

ワームは最後にレジストリの

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersionにchmというキーを作成し、この値を1とする。ワームはワームメール転送前にこの値をチェックするので、以降はワームメールの送信は行われぬ。

感染・発症防止方法	koreajapan.chmファイルを開かない。(ただしメールでもIRCでも流通することは無いので通常は、入手することは無いと思われる。)
ウイルスの駆除方法	<p>< 確認 > レジストリの、HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion に chm というキーがあるか確認する。</p> <p>< 駆除 > koreajapan.chmという名前のファイルがドライブに存在する場合はこれを削除する。 必須ではないが、レジストリエディタなどで HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion にあるchmというキーを削除する。</p>
その他	バグの修正は比較的簡単なので、本来の仕様で動作するバージョンも流通する可能性はある。ただしその場合でも、特に日本国内ではさほど被害は出ないと思われる。 報告書作成 : 2002年6月20日現在

VBS_Chick.F フローチャート

