20XX年X月XX日

ウイルス診断レポート

株式会社〇〇〇　　御中

株式会社アイ・オー・エス
東京都港区芝5-20-14
三田鈴木ビル3階

受付番号	TK#〇〇〇〇〇〇(TK#△△△△△△)
診断結果　1	ウイルス判定　　白　　黒
診断結果　2	情報流出　　有　　無

上記診断結果に基づき、ウイルス判定の結果、黒かつウイルスの動きとして
情報漏洩有と診断された場合、下記詳細情報を必ずご確認下さい。

通信の有無	
プロトコル	
通信を発生させる場合の接続先	
流出する情報	
備考	

備考:

20XX年X月XX日

ウイルス診断レポート

株式会社〇〇〇　　御中

株式会社アイ・オー・エス
東京都港区芝5-20-14
三田鈴木ビル3階

受付番号	TK#〇〇〇〇〇〇（TK#△△△△△△）
診断結果　1	ウイルス判定　　白　（黒）
診断結果　2	情報流出　　（有）　　無

上記診断結果に基づき、ウイルス判定の結果、黒かつウイルスの動きとして
情報漏洩有と診断された場合、下記詳細情報を必ずご確認下さい。

通信の有無	有
プロトコル	TCP　80
通信を発生させる場合の接続先	XXX.XXX.XXXXX このウイルスは上記サイトに接続し、不正リモートユーザからの以下のコマンドを実行します。 ドライブ情報の取得 システム情報の取得 ファイル情報の取得 ファイルの実行 ファイルの削除 ファイルの作成 OSの再起動
流出する情報	オンラインバンキング情報
備考	

備考:

セキュリティー強化診断レポート

脆弱性の利用	有

利用される脆弱性の種類	XXX.XXX.XXXXX

ファイル情報

以下のファイルが作成されます

%temp%¥XXXX.EXE(ウイルス自身のコピー)
%temp%¥XXXX.DLL(ウイルスのコンポーネント)

また、物理ドライブ/リムーバブルドライブに以下のファイルを作成します。
autorun.inf
XXXXXX.bat(ウイルス自身のコピー)
※autorun機能により、ドライブアクセス時にウイルスが実行されるように仕組みます。

以下のファイルを削除します。

C:¥Windows¥System32¥drivers¥xxxxxx.sys

ウイルスは自身のコンポーネントを以下の正規プロセスに組み込みます。

explorer.exe

レジストリ情報

以下のレジストリが作成されます

キー：HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥Currentversion¥Run
値　：XXX = XXXXXXXXX
※このレジストリによりウイルスが起動時に実行されます。

以下のレジストリが変更されます。

キー：
HKEY_CURRENT_USER¥SOFTWARE¥MICROSOFT¥Windows¥CurrentVersion¥Explorer¥Advanced
値　：Hidden
変更前のデータ："1"
変更後のデータ："2"

キー：
HKEY_CURRENT_USER¥SOFTWARE¥MICROSOFT¥Windows¥CurrentVersion¥Explorer¥Advanced
値　：ShowSuperHidden
変更前のデータ："1"
変更後のデータ："0"

キー：
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥Folder¥Hidden¥SHOWALL
値　：CheckedValue
変更前のデータ："1"
変更後のデータ："0"

※この変更によりシステム/隠しファイルを非表示にします。

備考：