20XX年X月XX日

解 析 調 査 報 告 書

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

調査概要:

本ウイルスについては主な感染経路として、Webやリムーバブルドライブからの可能性が高いと考えられます。
本ウイルスの検体は、●年前のパターンファイルでも
対応済みのものであるため、ウイルス対策が実施されていないマシンや、
ウイルス対策ソフトが適切に管理されていない
(アップデートされていない/動作していない)マシンが感染したことによるものと
考えられます。

受付番号		TK#〇〇〇〇〇〇(TK#△△△△△△)
検体ファイル基本情報		
1	ハッシュ値	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	解析対象ファイル名	「◆◆◆◆.exe」
ウイルス名		XXX_XXX_XXXX
通信の有無		有
プロトコル		TCP 80
脆弱性の利用		無
情報流出の有無		有
流出する情報		オンラインバンキング情報
通信を発生させる場合の接続先		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。

作成されるファイルにはシステム/隠しファイル属性が付与されています。

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:

脆弱性利用　外部通信

20XX年X月XX日

解 析 調 査 報 告 書

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

調査概要:

本ウイルスについては▼▼▼の脆弱性(CVE-2014-XXXX)を悪用して感染を広めようとします。主な感染経路といたしましては、メールからの可能性が高いと考えられます。
本ウイルスの検体は、●年前のパターンファイルでも対応済みのものであり、かつ▼▼▼の脆弱性においても、●年前にセキュリティパッチが公開されているため、ウイルス対策が実施されていないマシンや、ウイルス対策ソフトや▼▼▼の更新が適切に管理されていない(アップデートされていない/動作していない)マシンが感染したことによるものと考えられます。

IOS Support Desk 受付番号 (関連番号)		TK#〇〇〇〇〇〇(TK#△△△△△△)
検体ファイル基本情報		
1	ハッシュ値	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	解析対象ファイル名	「◆◆◆◆.exe」
ウイルス名		XXX_XXX_XXXX
通信の有無		有
プロトコル		TCP 80
脆弱性の利用		有
利用する脆弱性		CVE-2014-XXXX
情報流出の有無		無
通信を発生させる場合の接続先		XXX.XXX.XXXXX
ファイル情報		
以下のファイルが作成されます %system%¥XXXX.EXE(ウイルス自身のコピー)		
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_LOCAL_MACHINE¥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。 ※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:

Mail 感染　情報漏洩

20XX年X月XX日

解 析 調 査 報 告 書

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

調査概要:

本ウイルスについては主な感染経路として、メールからの可能性が高いと考えられます。
本ウイルスの検体は、●年前のパターンファイルでも対応済みのものであるため、ウイルス対策が実施されていないマシンや、ウイルス対策ソフトが適切に管理されていない(アップデートされていない/動作していない)マシンが感染したことによるものと考えられます。

IOS Support Desk 受付番号 (関連番号)		TK#〇〇〇〇〇〇(TK#△△△△△△)
検体ファイル基本情報		
1	ハッシュ値	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
	解析対象ファイル名	「◆◆◆◆.exe」
ウイルス名		XXX_XXX_XXXX
通信の有無		有
プロトコル		TCP 80
脆弱性の利用		無
情報流出の有無		有
流出する情報		下記コマンドで得られた情報
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
ファイル情報		
以下のファイルが作成されます %system%¥XXXX.EXE(ウイルス自身のコピー)		
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_LOCAL_MACHINE¥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。 ※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: