

Google Minor Typographic Error Attack (Googkle)

分類 Other (Minor Typographic Error)
再現性 リモート

技術解説

1) 概要

「Google.com」のスペルミスが悪用したサイト「Googkle.com」に Internet Explorer (以下「IE」という。) を使用してアクセスすることにより、自動的に多数のウィルスやスパイウェアをホスト上にインストールされる可能性がある。

「Googkle.com」では、「http://www.googkle.com/」を含めた多数の URL へのリンクが存在している。リンクのほとんどはウィルスやスパイウェアなどの URL であり、ここからホスト上にダウンロード、実行させられたウィルスやスパイウェアにより、以下のような影響がある可能性がある。

- ホスト上にバックドアを仕掛けられる
- メールのリレー配信を行う
- ホストから複数の外部のメールサーバに対してアクセスを行う
- ホストのレジストリ情報を書き換えられる
- IE のホームの設定を書き換えられる
- Windows Media Player のファイルを書き換えられる
- その他

「http://www.googkle.com/」は、2005年4月28日以前に存在し、2005年4月29日頃に「googkle.com」が DNS エントリから削除された。2005年5月20日現在、当該サイトへのアクセスは不可能であることから、今後、「http://www.googkle.com/」による被害は少ないと考えられる。ただし、本件で悪用されたウィルスやスパイウェアなどへの URL は 2005年5月20日現在、引き続き存在しているため、当該サイトと同様にスペルミスが悪用する手法を用いた攻撃に利用される可能性があると考えられる。

対策方法

1) 対策

Internet Explorer の ActiveX の設定を無効にすることにより、この問題の対策が可能である。

ActiveX の無効方法：

1. [ツール] -> [インターネットオプション] を開く。
2. [セキュリティ] タブへ移動し、インターネットゾーンの [レベルのカスタマイズ] を開く。
3. [ActiveX コントロールとプラグイン] の項目全てで [無効にする] を選択する。

また、Windows Update を実施することにより、この問題の影響を抑えることが可能である。

Windows Update :
<http://windowsupdate.microsoft.com/>

2) Advisory情報

F-Secure ウィルス情報 Google :
<http://www.f-secure.co.jp/v-descs/v-descs3/google.htm>
F-Secure Virus Descriptions : Google :
<http://www.f-secure.com/v-descs/google.shtml>

検証有無

結果 ○:成功、×:失敗、-:未検証

OS	アプリケーション	バージョン	結果
Windows 2000 Advanced Server SP なし (J)	Internet Explorer	6.0 SP1	○
上記以外の組み合わせ			-

検証結果

1) 検証環境

OS	アプリケーション	備考
Windows 2000 Advanced Server SP なし (J)	Internet Explorer 6.0 SP1	SP1 以外の修正プログラムを適用していない。

2) 検証手順

1. Internet Explorer を使用して、「<http://www.google.com/>」へアクセスする。
2. ターゲットホストの挙動を確認する。

3) 検証結果

ターゲットホストにて、以下の事象を確認した。

- 二つのポップアップウィンドウが起動された
- Windows Media Player が起動した
- 外部に存在する多数のメールサーバの 25 番ポートに対してアクセスした
- 徐々にホストの動作が遅くなり、最終的にはキーボード、マウスからの応答を受け付けなくなり、サービス不能状態に陥った
- ハードウェアリセットからの再起動後、ホスト上では IE の履歴に閲覧した際の URL が残るものの、Temporary Internet Files フォルダにあるはずの参照したファイルは全て消されていた。

再起動後、引き続き検証を実施しようとしたが、キャッシュが消され、また当該サイトの DNS エントリが削除されていたため、検証が困難な状況となった。また、「www.google.com」が登録されていた IP アドレスにアクセスをしたが、アクセス不可能であった。

痕跡

1) ログ

ターゲットホストのイベントログには何も出力されなかった。

2) 痕跡

IE の履歴に参照した URL が残る他、Temporary Internet Files フォルダに、参照した HTML ファイルが残った。また、ダウンロードされたウイルスにより、以下のような痕跡が残される可能性が高いと考えられる。

- レジストリの書き換え
- IE のホームの書き換え
- Windows Media Player のファイルの書き換え
- 悪意あるファイルのダウンロード
- バックドアの作成
- メールのリレー配信
- その他