

脆弱性を狙った脅威の分析と対策について Vol.4

2010年7月29日

独立行政法人 情報処理推進機構
セキュリティセンター(IPA/ISEC)

独立行政法人 情報処理推進機構（略称 IPA、理事長：藤江 一正）は、2009 年度における脆弱性を狙った脅威の一例を分析し、対策をまとめました。

文書閲覧ソフトウェアの古い脆弱性を狙った標的型攻撃

～ 「不審メール 110 番」に届けられた標的型攻撃の分析・対策について ～

1. はじめに

IPA は「情報窃取を目的として特定の組織に送られる不審なメール（標的型攻撃）」に対して、「不審メール 110 番」を設置して情報を収集し、対策方法を提供しています。この度、2010 年 3 月に不審メール 110 番に相談のあった標的型攻撃の解析を行った結果、攻撃から 4 年前に発見された脆弱性が悪用されていたことが分かり、古い脆弱性が未だに攻撃に利用されている現状が浮かび上がりました。

本攻撃の場合、万が一添付ファイルを開いたとしても、定期的なバージョンアップを行っていればマルウェアへの感染を防ぐことが可能です。

本レポートでは、定期的なバージョンアップに有効なコンテンツを紹介するとともに、2009 年度に解析した 2 件の標的型攻撃に対して、攻撃に利用された脆弱性等について比較し、傾向をまとめました。2 件の標的型攻撃はいずれも文書ファイルを装ったマルウェアを脆弱性のある文書閲覧ソフトで開かせ、マルウェアに感染させるという手口を利用していました。

標的型攻撃は特定の組織を標的とするため被害情報が表に出て来づらく、被害に気付にくい攻撃です。あなたの知らないうちに標的型攻撃の被害に合わないために、近年の標的型攻撃に関する動向と対策を確認しておきましょう。

¹ 不審メール 110 番
<http://www.ipa.go.jp/security/virus/fushin110.html>

2. 攻撃の概要

以下に、前述の「標的型攻撃メール」による攻撃の分析結果を記載します。

2.1 「標的型攻撃メール」による攻撃

前述の「標的型攻撃メール」の特徴は以下の通りです。

受信者に心当たりのない個人名

フリーメールのアドレス

受信者が業務用で加入しているメーリングリスト

当時話題になっていたニュースを連想させる件名

受信者に添付ファイルを開くよう仕向ける文章

実在の団体名

フリーメールのアドレス

本文と関連がありそうな名前の DOC ファイル。実態はマルウェア。

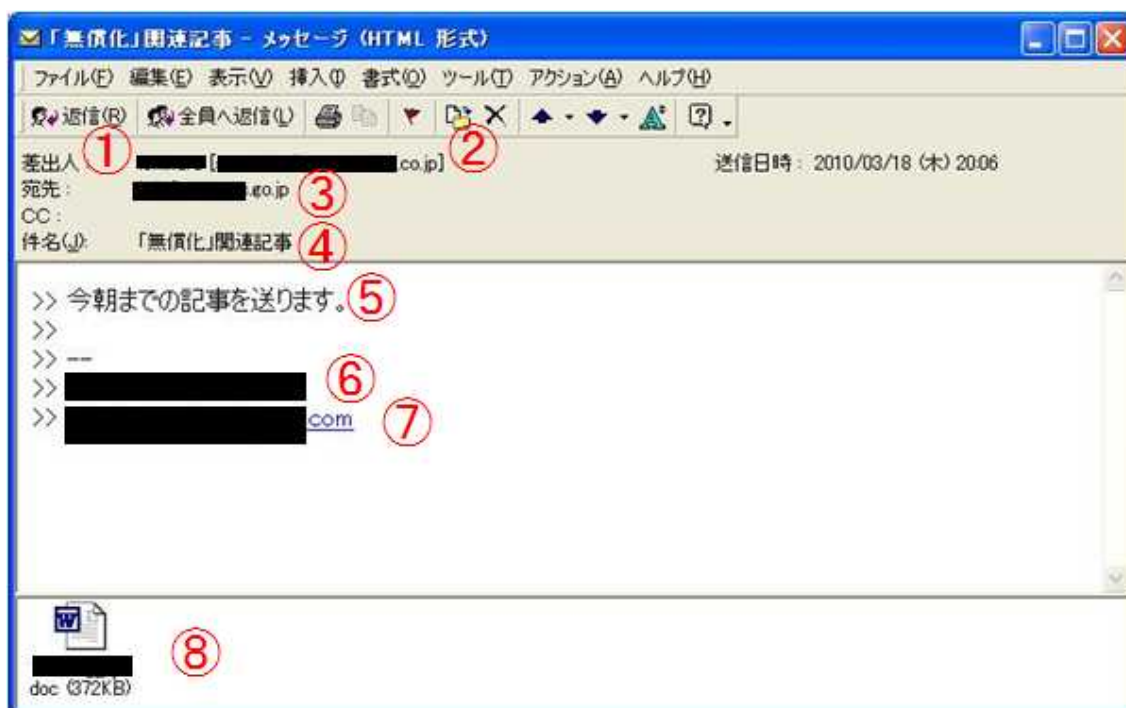


図 1. 標的型攻撃メール (メーラー : Outlook2000)

今回解析した「標的型攻撃メール」の受信者へのヒアリングによると、の差出人名との送信元アドレスの名前が違っている、メーリングリストの業務とは関係ない内容である等の点に違和感を感じ、添付ファイルを開くことはしなかったとのことでした。

3. 攻撃の分析

「標的型攻撃メール」に添付された悪意のある DOC ファイルの中に埋め込まれていたマルウェアの動作について記載します。

3.1. 攻撃の全体像

脆弱性のあるソフトウェアで悪意のある DOC ファイルを開き、攻撃が成功した場合、図 2 のような動作を行います。

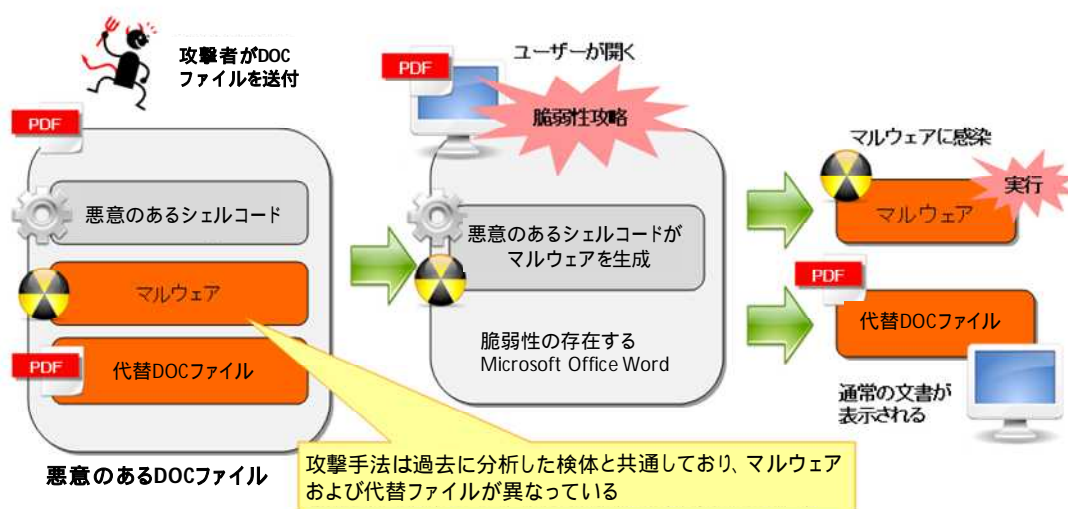


図 2 . 攻撃の全体像

悪意のある DOC ファイル内には、悪意のあるシェルコードが含まれています。悪意のあるシェルコードは、ファイル実行時に自動的にメモリ上に展開され、ファイルに存在する CVE-2006-2492(JVNDB-2006-000296²)の脆弱性を利用し、攻撃を実行します。これにより、悪意のある DOC ファイル内に含まれるマルウェアがファイルシステム上に生成され、実行されます。

本マルウェアは、インターネット上に存在する攻撃者が用意したサーバと通信し、ファイルをダウンロードし実行する機能を持ちます。

3.2 攻撃に悪用された脆弱性

今回の攻撃では、CVE-2006-2492(JVNDB-2006-000296)の脆弱性が利用されていました。本脆弱性は、本攻撃が行われた当時から約 4 年前の 2006 年 5 月 19 日に発見されており、攻撃当時には Microsoft 社から既に対策²が公開されていました。

² JVNDB-2006-000296

<http://jvndb.jvn.jp/ja/contents/2006/JVNDB-2006-000296.html>

² Microsoft DOC の脆弱性により、リモートでコードが実行される (917336) (MS06-027)

4. 2009 年度に解析した 2 つの標的型攻撃の比較

IPA は 2009 年度の調査において、2 つの標的型攻撃の解析を行いました。1 件目の標的型攻撃の解析結果は「脆弱性を狙った脅威の分析と対策について Vol.3」³として 6 月に公開しています。2 件目の標的型攻撃の解析結果は本レポートで紹介しています。

2009 年度調査の総括として、以下に 2 件の標的型攻撃に利用されている脆弱性等について比較を行い、傾向をまとめました。

4.1 利用された脆弱性に関する比較

表 1 は、標的型攻撃に利用されている脆弱性に関する比較です。

表 1. 利用された脆弱性の比較

	Vol.3 (2010 年 6 月公開)	Vol.4 (2010 年 7 月公開)
利用された脆弱性	CVE-2009-4324(JVNDB-2009-002451)	CVE-2006-2492(JVNDB-2006-000296)
脆弱性を利用されたソフトウェア	Adobe Reader	Microsoft Word
脆弱性の発見日	2009/12/16	2006/5/19
バッチの発行日	2010/1/12	2006/6/14
標的型攻撃メールの受信日	2009/12/25	2010/3/18

Vol.3 の標的型攻撃では「Adobe Reader および Acrobat における解放済みメモリを使用する脆弱性 (CVE-2009-4324(JVNDB-2009-002451))」が利用されており、Vol.4 の標的型攻撃では、「Microsoft Word における不正なオブジェクトポイントによるメモリ破壊の脆弱性 (CVE-2006-2492(JVNDB-2006-000296))」が利用されていました。

2 件の標的型攻撃では、一般に広く使用されておりメールに添付される頻度も高い文書閲覧ソフトウェアの脆弱性が攻撃に利用されていました。従来は、Microsoft Word のような Microsoft Office の脆弱性を利用した攻撃が多いと言われてきましたが、最近の傾向としては Adobe Reader の脆弱性を利用した攻撃が多い⁴とされています。2008 年度に解析した 2 件の標的型攻撃と、Vol.3 の標的型攻撃はいずれも Adobe Reader の脆弱性を利用していました。しかし、Vol.4 のような Microsoft Office の脆弱性を利用した攻撃も依然行われており注意が必要です。

<http://www.microsoft.com/japan/technet/security/bulletin/MS06-027.msp>

³ 脆弱性を狙った脅威の分析と対策について Vol.3

<http://www.ipa.go.jp/security/vuln/report/newthreat201006.html>

⁴ PDF Most Common File Type in Targeted Attacks

<http://www.f-secure.com/weblog/archives/00001676.html>

どちらの脆弱性も、発見からパッチの発行までに約 1 カ月かかっています。脆弱性の発見からパッチが発行されるまでの間は Vol.3 で紹介したような汎用的な対策を行うことが必要です。

Vol.3 の標的型攻撃は、攻撃時点ではまだパッチが発行されていないゼロデイ攻撃でした。これに対して、Vol.4 の標的型攻撃では約 4 年前に発見された脆弱性が利用されており、この点で 2 件の標的型攻撃は対照的です。定期的なバージョンアップを実施していないユーザが一定数存在することは、攻撃者を含めて広く知られており、そのため、発見から 4 年が経過した古い脆弱性でも依然として攻撃に利用されています。パソコンの利用者は、基本的なセキュリティ対策であるバージョンアップを確実に実施する必要があります。また、ゼロデイ攻撃にも対応するため、Vol.3 で紹介したような更新プログラムが存在しない脆弱性への対策も併用することが望ましいと言えます。

4.2 類似点

以下に、2009 年度に解析した 2 件の標的型攻撃の類似点をまとめました。

A)送信・通信方法の類似点

- ・送信には無料のメールサービスを利用
- ・接続先ホストが同一
- ・バックドア通信方法として、独自プロトコルとダウンロード機能を利用
- ・接続先ポート番号には、一般に利用されていないポート番号を利用

B)メールの特徴

- ・差出人を詐称している
- ・日本語や日本の時事に精通している人間がメール本文を作成したと思われる
- ・攻撃メールの内容は標的に特化したものではなく汎用的な内容を利用する
- ・受信者から不審メールとして扱われ攻撃に失敗しやすい

C)マルウェアの特徴

- ・中国語 OS 環境で作成している
- ・マルウェア作成者の身元がわからないようプロパティ情報を削除している
- ・Web 上などで公開されている内容を利用してダミーのドキュメントファイルを偽装のために開く
- ・ウイルス対策ソフトによる検出回避のためか、一度作成したマルウェアを改良して再利用している
- ・インストールするバックドアの機能は最低限に絞り攻撃意図をわからないようにする
- ・バックドアに利用するサーバは利用可能な時間を制限し、その制御のために DNS を

変更する

- ・使用するポート番号やプロトコルは独自のものを使用する

これらの類似点の他にも、頻繁に同じメーリングリストに標的型攻撃を送っている等の特徴があり、2つの標的型攻撃の送信者が同一人物であることを示唆しています。

5. リスク要件リファレンスモデルによる脅威の分類

NISC（内閣官房情報セキュリティセンター）が作成したリスク要件リファレンスモデルでは、実際に確認された脅威の振る舞いの分類から、脆弱性を利用した脅威を6つのパターンに分類しています（表2参照）。

2009年度に解析した2件の標的型攻撃は、パターン2の「標的型メール攻撃(情報搾取)」にあたります。「標的型メール攻撃(情報搾取)」振る舞いパターンの詳細については、以下をご参照下さい。

「リスク要件リファレンスモデル作業部会報告書」(P30)

http://www.nisc.go.jp/inquiry/pdf/2-1_RM-model_Open.pdf

表2. リスク要件リファレンスモデルによる脅威の分類

パターン1	正規 Web 閲覧によるマルウェア感染(情報搾取)
パターン2	標的型メール攻撃(情報搾取)
パターン3	正規 Web 改竄による誘導
パターン4	媒体介在マルウェア感染
パターン5	複合 DDoS 攻撃(攻撃基盤)
パターン6	通常 DDoS 攻撃

(「リスク要件リファレンスモデル作業部会報告書」 P27 から引用)

リスク要件リファレンスモデルは、脅威の全容を把握したうえで、組織における影響を把握し、コストに見合ったセキュリティ対策を講じるための方法論です。自組織に適したセキュリティ対策を考える際の参考にしましょう。

6 . 対策

Vol.4 で解析した標的型攻撃は、攻撃当時には既にパッチが発行されており、定期的なバージョンアップを行っていれば攻撃を防ぐことが可能な攻撃でした。以下に、定期的なバージョンアップに役立つコンテンツを紹介します。

Vol.3 の標的型攻撃のようなゼロデイ攻撃への対策は「脆弱性を狙った脅威の分析と対策について Vol.3」で紹介していますので、そちらもご参照の上、以下の対策と併用することを推奨します。

6.1 定期的なバージョンアップ

定期的なバージョンアップを行うことにより、万が一添付ファイルを開いてしまった場合でも、マルウェア感染を防ぐことができます。

以下に、定期的なバージョンアップに役立つコンテンツを紹介します。

A) Microsoft Update⁵

Microsoft Update の実施により、利用している PC に入っている Windows、プログラム、ハードウェア、またはデバイスに更新プログラムの適用が必要かどうかを確認することができます。定期的を確認し、更新プログラムが配信されていないか確認しましょう。

B) MyJVN バージョンチェッカ⁶

IPA が公開している MyJVN バージョンチェッカは、PC にインストールされているソフトウェア製品のバージョンが最新であるかを簡単な操作で確認するツールです。MyJVN バージョンチェッカは Adobe Reader 等の 9 つの製品のバージョンを確認することができます。ソフトウェアが最新のバージョンになっていなかった場合は、最新のバージョンにするための情報も見ることができます。

⁵ Microsoft Update

<http://www.update.microsoft.com/microsoftupdate/v6/default.aspx?ln=ja>

⁶ MyJVN バージョンチェッカ

<http://jvndb.jvn.jp/apis/myjvn/#VCCHECK>

7. さいごに

2009 年度に解析した 2 件の標的型攻撃は、それぞれ発見から間もない脆弱性と、発見から 4 年が経過した脆弱性が利用されていました。これらの攻撃への対策として、定期的にソフトウェアのバージョンアップ情報を確認し常に最新の状態にするとともに、ゼロデイ攻撃へも対応できるよう、汎用的な対策も併せて実施しましょう。

IPA は、本レポートのような標的型攻撃に対する情報発信や、「不審メール 110 番」による相談受付等を行い、標的型攻撃への知識の普及と対策の促進に取り組んでいます。標的型攻撃と思われる不審なメールを受信した際は、不審メール 110 番への情報提供にご協力下さい。

IPA は今後も、標的型攻撃等の脆弱性を利用した新たな脅威に対して調査・分析を実施し、対策を発表します。