

近年の標的型攻撃に関する調査研究

- 調査報告書 -

2008年3月

IPA[®] 独立行政法人 情報処理推進機構
セキュリティセンター

近年の標的型攻撃に関する調査研究

調査報告書

もくじ

もくじ	2
概要	4
1. はじめに	5
2. マルウェアの解析と脅威分析	5
3. 調査研究の範囲と調査方法	7
4. 標的型攻撃に利用されているセキュリティ脆弱性の実態調査・傾向分析	8
4.1 標的型攻撃に利用された脆弱性	8
4.2 標的型攻撃に利用された脆弱性を持つソフトウェアやコンポーネントの傾向	11
4.2.1. ファイル処理における脆弱性と標的型攻撃	11
4.2.2. ソフトウェアの知名度と標的型攻撃の関連性	13
5. 標的型攻撃に利用されていたセキュリティ脆弱性	14
5.1 標的型攻撃に利用された脆弱性	14
5.2 標的型攻撃に利用される可能性が高いソフトウェアの傾向	15
6. 標的型攻撃用マルウェアの実態調査・傾向分析	17
7. 近年の標的型攻撃で用いられるマルウェアの分析	17

近年の標的型攻撃に関する調査研究

調査報告書

7.1 マルウェアの解析と攻撃シーケンスの分析	18
7-1-1. TROJ_MDROPPER 系の攻撃シーケンス	18
7-1-2. TROJ_PPDROP 系の攻撃シーケンス	26
7.2 攻撃サイトの特徴	28
7.3 ボット型マルウェアと標的型攻撃マルウェアの共通仕様分析	31
7.4 標的型攻撃用マルウェアの検知手法	33
7.5 効率の良い脅威分析手法に関する検討	34
8.まとめ	35

概要

近年、特定の企業あるいは組織を標的とした標的型攻撃による被害が深刻化しているが、攻撃が見えにくくなっている事もあり、その実態が正確に把握しにくくなっている。標的型攻撃はマルウェア(悪意のあるソフトウェア)によるものが多数であるが、最近では、インターネット上のホストからプログラムや機械語コードをダウンロードする「ダウンローダ」を介して設置される多段型のマルウェア(以下、シーケンシャルマルウェア)が多発している。図1に、従来型マルウェアとシーケンシャルマルウェアの違いを示す。また、脆弱性(ぜいじゃくせい)を利用してマルウェアを設置させる例も多くなっており、さらに、検出や解析を困難にする手法も高度化している。本調査研究では、まず、実際に標的型攻撃に利用された脆弱性の実態調査を行い、傾向を分析する。つぎに、標的型攻撃に用いられるマルウェアの実態調査、傾向分析、攻撃シーケンス分析を行う。その上で、標的型攻撃及び近年のマルウェアの攻撃モデルを分析し、イントラネット内に潜伏したマルウェアの検知手法の検討、シーケンシャルマルウェアの動的解析手法の検討を行う。

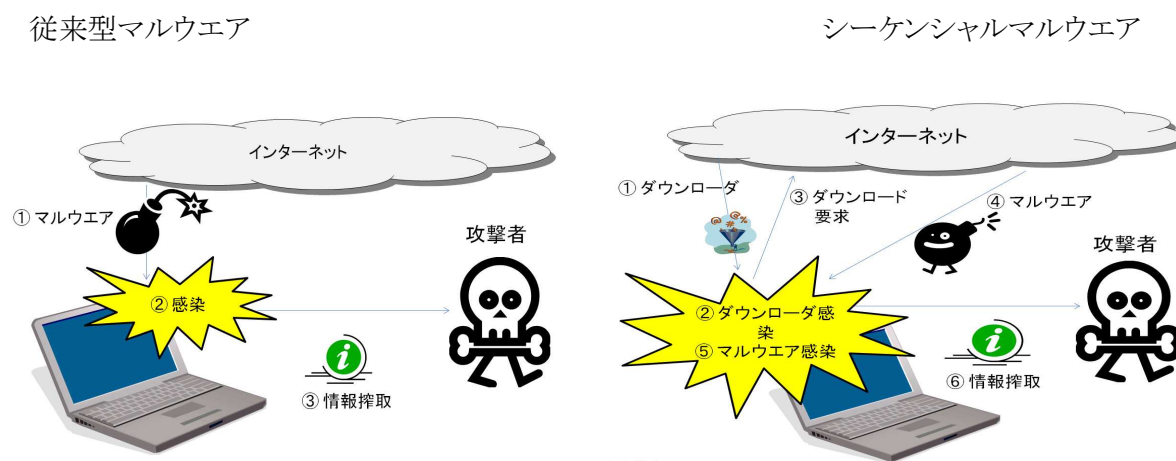


図1. 従来型マルウェアとシーケンシャルマルウェアの違い

近年の標的型攻撃に関する調査研究

調査報告書

1. はじめに

近年、特定の企業・組織を標的とした標的型攻撃による被害が深刻化している。標的型攻撃では攻撃対象が限定的であるため、攻撃発生前に情報を入手し、適切な対応を取る事が難しい。また、近年は解析や検出を困難にするための手法が高度化している。このため、アンチウイルスや IDP (Intrusion Detection and Prevention: 侵入検知防御) などのソリューションが有効に機能しないケースが発生しており、攻撃が見えにくく、適切に対応できない企業・組織が増えている。セキュリティベンダーでも攻撃が見えにくいため情報が得られにくく、実態を正確に把握するのは困難である。このため、企業・組織は十分な情報や技術的解決策を得られないという状況にある。更に、近年のマルウェアの詳細な挙動・仕組みに関する解析結果は公表されておらず、その脅威を正確に把握できない。

本調査研究は、このような近年の標的型攻撃とそれがもたらす脅威について詳細な調査研究を行い、実態を正確に把握し、対策に結びつけることを目的とする。

2. マルウェアの解析と脅威分析

近年のマルウェアは攻撃シーケンスが複雑化しており、それに伴ってマルウェアを構成するプログラムは肥大化している。アンチウイルスベンダーをはじめとするマルウェア対策システムの開発においては、いかに効率よく新種マルウェアを検出するための検出に利用可能なマルウェアの特徴パターン（以下、シグネチャ）を開発するかといった事柄が非常に重要となっている。

近年の標的型攻撃に関する調査研究

調査報告書

しかし、アンチウイルスベンダーでは、マルウェアの解析は基本的に検出シグネチャを開発するために行うものである。このため、近年の複雑化したシーケンシャルマルウェアにおいても、主要 API (Application Programming Interface) 呼び出しのトレース、ファイルシステムやレジストリのモニタリング、通信の分析など、自動化が可能となる部分に限定した解析に留まるケースが多い。こういったアプローチは、検出シグネチャを開発するという目的においては必要十分である。しかし、アンチウイルス製品は基本的に脅威分析を行うためのソリューションではなく、あくまでマルウェアの感染を防ぐことを目的としている。このため、マルウェアによる攻撃の脅威分析を正確に行うためには、自動化された解析手法だけでは十分でない。

マルウェアの自動解析では、コード(プログラム)の詳細を把握できないため、正確な挙動の分析ができない。状況に応じて実行パスや実行コードが変化し、挙動が変化する可能性があるが、自動分析では分析時以外の状況で何が起るのか予測できない。

また、自動解析では、APIトレースや各種リソースのモニタリングを行い、各要素の分析結果(ログ)を突き合わせて最終的に挙動を把握するが、呼びだされた API やその引数、リソース名など、末端の情報から正確な全体フローを作成する事は難しい。

通信においても、近年のマルウェアは通常何らかの暗号が施されている。このため、例えばファイル読み込み後にパケットを送信する API が呼ばれても、パケットが暗号化されている場合、読み込まれたファイルの内容が本当に送信されているのかどうか、また、他にどのような情報が一緒に送信されているのか、といった事が全て把握できない。

近年のマルウェアには、通常、攻撃対象システムにアクセスするためのプログラム(以下、バックドア)が実装されており、攻撃者からの指示によって様々な処理を行うが、実際にどのような事が行われる可能性があるのかといった事を分析する事は自動解析では難しい。

このように、正確な脅威分析を行うためには、マルウェアの全コードを網羅的に解析する必要がある。

近年の標的型攻撃に関する調査研究

調査報告書

3.調査研究の範囲と調査方法

以下の範囲で調査研究を行った。

a. 標的型攻撃用セキュリティ脆弱性の実態調査・傾向分析

標的型攻撃に利用された脆弱性をリストアップした。また、標的型攻撃に利用された脆弱性を持つソフトウェアやコンポーネントの傾向を分析した。

b. 標的型攻撃用セキュリティ脆弱性の分析

標的型攻撃に利用された脆弱性を、攻撃の入り口(以下、アタックベクタ)、脆弱性の性質、攻撃安定性、環境依存性などの観点から分析した。得られた分析結果から、今後の標的型攻撃に利用される可能性が高いソフトウェアやコンポーネント、および、それらに想定される未知の脆弱性の内容・傾向を分析した。

c. 標的型攻撃用マルウェア実態調査・傾向分析

近年の標的型攻撃に利用されたマルウェアの実態を調査し、傾向を分析した。また、標的型攻撃に利用されたマルウェアの検体を分析した。

d. 標的型攻撃用マルウェア分析

マルウェアを静的・動的に解析し、その構造と挙動、攻撃シーケンスを分析した。シーケンシャルマルウェアの攻撃ダウンロードサイトの特徴分析、および収集分析を行った。また、不特定多数を対象とする無差別攻撃型マルウェアであるボット型マルウェアと標的型攻撃マルウェアの共通仕様の分析を行った。標的型攻撃の攻撃モデルの分析整理を行った。標的型攻撃によりイントラ内に潜伏したマルウェアの検知手法の検討を行った。シーケンシャルマルウェア攻撃シーケンスに応じる動的解析手法の検討を行った。

マルウェア本体及び当該マルウェアが、攻撃者が用意したサーバからダウンロードしてくる攻撃コード等

近年の標的型攻撃に関する調査研究

調査報告書

を取得し解析した。解析方法は、ディスアセンブラツールによる静的解析、デバッガでトレースしながら挙動を解析するデバッグ解析、および、テスト環境下にて得られたマルウェア検体や攻撃コードを実行して挙動を解析する動的解析の 3 つのアプローチを取った。

4. 標的型攻撃に利用されているセキュリティ脆弱性の実態調査・傾向分析

4.1 標的型攻撃に利用された脆弱性

標的型攻撃の対象は、主に、サーバではなく企業などのイントラネット内 PC である場合が多い。後述するが、代表的な標的型攻撃の攻撃シーケンスの分析を行った結果、クライアント PC を攻撃対象としており、目的は主に情報搾取であると推測される。

イントラネット内のクライアント PC は基本的に外部から直接アクセスできない。このため、標的型攻撃における攻撃方法は、必然的に図2に示すような受動的攻撃が主流となっている。受動的攻撃は、図 3 に示すようなネットワークサービスに対して直接攻撃を行う能動的攻撃とは異なり、攻撃対象システムを利用するユーザーが何かしらの操作(e-mail 閲覧、web ページ閲覧、など)を行うことで初めて成立する。能動的攻撃の場合、攻撃対象のシステムを利用するユーザーの操作は不要であるが、攻撃対象システムに対してネットワーク的に到達可能である事が前提条件となり、イントラネット内のシステムを攻撃する事は難しくなる。しかし、受動的攻撃の場合、ユーザーの操作が必要となるが、e-mail などの手段で簡単に攻撃対象システムに到達できる。

受動的攻撃そのものは古くからファイアウォールで保護された企業イントラネット内などのシステムを攻撃する手段として用いられてきた。巧みな話術や騙しなどによる「社会的」な手段（以下、ソーシャルエンジニアリング）

近年の標的型攻撃に関する調査研究

調査報告書

ニアリング)などを用いてバックドアを実行させる、あるいは、web ブラウザや e-mail クライアントなどの脆弱性を利用してバックドアをインストールするなどの手法が用いられてきた。

表 1 に、代表的な標的型攻撃で利用された脆弱性の例を示す。また、表 2 に、表 1 で利用された脆弱性の概要を示す。

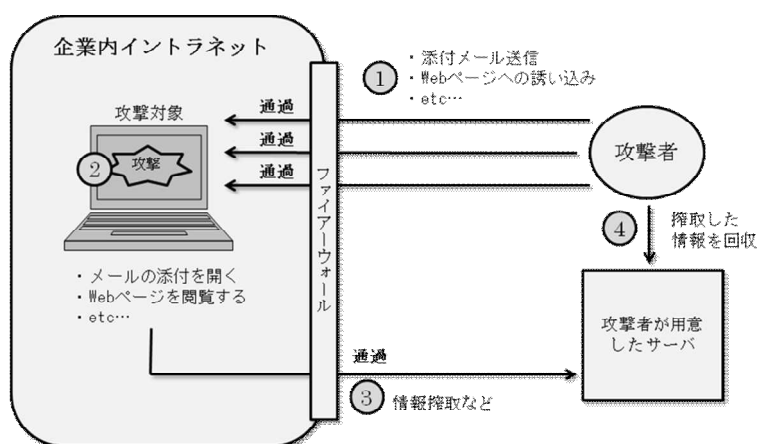


図2. 標的型攻撃に利用される受動的攻撃

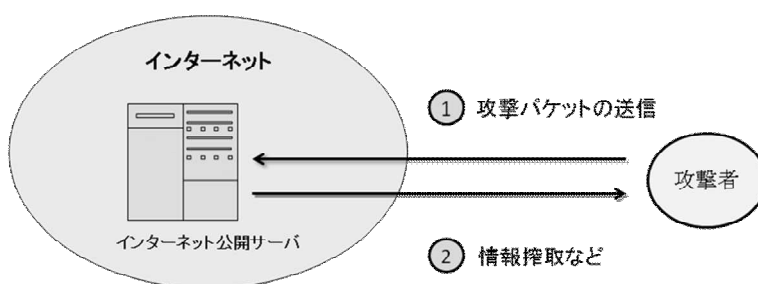


図 3. ネットワークサービスを攻撃する能動的攻撃

近年の標的型攻撃に関する調査研究

調査報告書

表 1. 代表的な標的型攻撃で利用された脆弱性

系列	名称	脆弱性	
MDropper 系	Trojan.Mdropper.A Trojan.Mdropper.B Trojan.Mdropper.D	Microsoft Word (MS03-050)	
	Trojan.Mdropper.C Trojan.Mdropper.F Trojan.Mdropper.G	Microsoft Office 製品 (MS03-037)	
	Trojan.Mdropper.J	Microsoft Office 製品 (MS06-037)	
	Trojan.Mdropper.H Trojan.Mdropper.I Trojan.Mdropper.K Trojan.Mdropper.Q Trojan.Mdropper.T Trojan.Mdropper.U Trojan.Mdropper.W Trojan.Mdropper.X	Microsoft Office (0-day、もしくは不明)	
	Trojan.Mdropper.L Trojan.Mdropper.P Trojan.Mdropper.S	Microsoft Word (MS06-027)	
	Trojan.Mdropper.N Trojan.Mdropper.R	Microsoft Office (MS06-047)	
	Trojan.Mdropper.Z	Microsoft Word (MS07-015)	
	Acdropper 系	Trojan.Acdropper Trojan.Acdropper.B	Microsoft Jet Database Engine (0-day、もしくは不明)
		PPDropper 系	Trojan.PPDropper Trojan.PPDropper.D Trojan.PPDropper.E
	Trojan.PPDropper.B Trojan.PPDropper.C		Microsoft Power Point (0-day、もしくは不明)
Trojan.PPDropper.F	Microsoft Office 製品 (MS06-058)		
Trojan.PPDropper.G	Microsoft Office 製品 (MS07-015)		
Tarodrop 系	Troj_Tarodrop	一太郎 (0-day 詳細不明)	
解凍ソフト系	Exploit-LHAZ.a	Lhaz の脆弱性	
	Trojan.Radropper	WinRAR の脆弱性	

近年の標的型攻撃に関する調査研究

調査報告書

表2. 標的型攻撃で利用された脆弱性の概要

脆弱性	概要
MS03-037	VBA(Visual Basic for Applications)の脆弱性の脆弱性により、任意のコードが実行される
MS03-050	Microsoft Word および Microsoft Excel の脆弱性により、任意のコードが実行される
MS06-012	Microsoft Office の脆弱性により、任意のコードが実行される
MS06-027	Microsoft Word の脆弱性により、任意のコードが実行される
MS06-047	VBA の脆弱性の脆弱性により、任意のコードが実行される
MS06-058	Microsoft PowerPoint の脆弱性により、任意のコードが実行される
MS07-015	Microsoft Office の脆弱性により、任意のコードが実行される
Lhaz の脆弱性	ZIP ファイル処理における脆弱性により、任意のコードが実行される
WinRAR の脆弱性	LZH ファイル処理における脆弱性により、任意のコードが実行される

4.2 標的型攻撃に利用された脆弱性を持つソフトウェアやコンポーネントの傾向

4.2.1. ファイル処理における脆弱性と標的型攻撃

攻撃手法としては、標的型攻撃の場合は e-mail の添付ファイル、あるいは外部 web サーバへのハイパーリンク(他の文書などの位置情報)であるケースが大半であり、標的型攻撃を成立させるための第1ステップとなっている。ただし、web ブラウザや e-mail クライアントそのものは、第三者やベンダーによる安全性確認と脆弱性対応が進み、簡単に悪用できる致命的な脆弱性が少なくなってきた。このため、近年は文

近年の標的型攻撃に関する調査研究

調査報告書

書処理ソフトウェアや圧縮ファイル解凍ソフトウェアなど、アプリケーションの脆弱性が利用されるケースが多くなっている。標的型攻撃に利用された脆弱性は、web ブラウザや e-mail クライアントそのものに存在しているものではなく、web ブラウザや e-mail クライアントを経由し、対象システム内に取り込まれたファイルを開くことで発動するアプリケーションの脆弱性が主流である。

これらファイルは、通常、対応するアプリケーション経由で開いても、開くだけであればセキュリティ上脅威とならないという事が前提となっている。例えば、Microsoft Word の文書は通常危険性は無いとされている。仕様上危険性が認められるマクロを含む文書は、開く前に Microsoft Word が警告を発する。このため、通常は、警告さえ無視しなければセキュリティ上の問題は発生しない。また、Microsoft Office 文書(Office XP 以前)や PDF (Acrobat Reader など) 文書、一太郎文書などは、web ブラウザのプラグインや ActiveX コントロールにより web ブラウザ経由で自動的に開かせることが可能であるため、これら文書ファイルは開いても安全なファイルであるという事が前提となっている。しかし、文書ファイル进行处理するアプリケーションにはしばしば脆弱性が報告されており、4.1 に示したように、これら脆弱性は標的型攻撃において非常に狙われやすい。また、ベンダーからの対策が情報公開されていない 0-day 脆弱性も多数悪用されている。開いても安全であるという事が前提となっている文書ファイルは、実行ファイルなどと比較すると開かれる可能性が高い。また、ソーシャルエンジニアリングにより言葉巧みに文書ファイルを開かせるような工夫がなされているケースも存在しており、もともと開いても安全であるという事が前提となっている文書ファイルは、ソーシャルエンジニアリングを組み合わせることで非常に開かれやすい対象となる。また、LZH などのアーカイブファイルは、解凍後にアーカイブ中に含まれる実行ファイルを意図的に実行しない限り危険性は無いという事が前提となっている。このため、実行ファイルなどと比較すると安易に開かれる(解凍される)事が多い。しかし、解凍ソフトウェアのファイル解凍処理に脆弱性があり、それが利用されると、アーカイブファイルを解凍するだけでアーカイブファイル中に含まれるコードが実行されてしまう。

このように、多くのユーザーの間で「開いても安全である」という認識が高いファイル进行处理するアプリケーションの脆弱性が、標的型攻撃においてはよく利用されている。

近年の標的型攻撃に関する調査研究

調査報告書

4.2.2. ソフトウェアの知名度と標的型攻撃の関連性

4.1 に示したように、比較的著名なソフトウェアの脆弱性が標的型攻撃においてよく利用されている。これは、能動的攻撃が成立する脆弱性を利用したサーバシステムに対する攻撃とは異なり、対象のシステムで利用されているアプリケーションの推測が困難であるというのが大きな理由であると考えられる。対象システムで利用されている Web ブラウザや e-mail クライアントなどは把握できるケースもあるが、対象システムでどのようなアーカイバが使われているのかを把握するためには、ソーシャルエンジニアリングを駆使するなど様々な工夫、あるいは予期しない偶然が必要となる。しかし、各分野で著名なアプリケーションであれば、攻撃対象システム上で利用されている可能性が高い。このため、比較的著名なソフトウェアの脆弱性が必然的に狙われやすくなると考えられる。

しかし、アプリケーションの著名さは国ごとに異なるケースがある。例えば、日本国内においては、アーカイブファイルの展開は「Lhaplus」や「Lhaca」、「Lhaz」などが広く利用されている。また、文書作成ソフトウェアの分野では「一太郎」のシェアも高い。標的型攻撃においては、不特定多数を対象とした無差別攻撃と比較すると対象が限定的である。このため、特定の地域や組織においてのみよく利用されているソフトウェアの脆弱性も、標的型攻撃に悪用されるケースがある。4.1 に示した「Lhaz」や「一太郎」の脆弱性は、その典型例であるといえる。

5. 標的型攻撃に利用されていたセキュリティ脆弱性

5.1 標的型攻撃に利用された脆弱性

TROJ_MDROPPEE 系および PPDROP 系で利用された脆弱性2例について、アタックベクタ、脆弱性の性質、攻撃安定性、環境依存性などの観点から分析した。

(1) アタックベクタ

両者とも Microsoft Office ファイルである。e-mail に添付されたファイルを開くことにより、Microsoft Office 製品の脆弱性が攻略され、マルウェアに感染する。

(2) 脆弱性の性質

両者ともバッファオーバーフロー脆弱性が利用されている。Microsoft Office 製品では、過去発見された脆弱性の大半がバッファオーバーフロー脆弱性であり、それを狙うものが大半である。バッファオーバーフローとは、アプリケーションが確保したメモリエリアが溢れる現象であり、大半のケースでアプリケーションの誤動作を引き起こす。攻撃者が攻撃対象のシステムで動作するアプリケーションに対して意図的にバッファオーバーフローを引き起こすことができれば、状況によっては攻撃者が作成したコードを実行することができる。標的型攻撃で利用された Microsoft Office の脆弱性では、Office の文書ファイルに細工し、Office アプリケーションでその文書ファイルを読み込むと、Office アプリケーション内でバッファオーバーフローを発生させる事ができるというものである。これにより、Office 文書ファイルに

近年の標的型攻撃に関する調査研究

調査報告書

記述されている攻撃コードが実行される。

(3) 攻撃安定性

両者とも、非常に安定して攻撃できる脆弱性のみが利用されている。例えば、同じバッファオーバーフロー脆弱性であっても、メモリコピーの際に常にページバウンダリにヒットしてしまうようなヒープオーバーフロー(ヒープ領域で発生するバッファオーバーフロー)脆弱性は攻撃安定性が低く、このような脆弱性が利用されている標的型攻撃は確認されなかった。

(4) 環境依存性

TROJ_MDROPPER 系の一部に実装されている 攻撃コードと、そのコードを実行するための一連の手続き(以下、Exploit)は、環境依存性が高く発動しなかった。このため、本調査研究では、発動しない Exploit を書き換え、発動させて解析した。今回解析を行った標的型攻撃の攻撃シーケンスは全体的に高度に設計・実装されているが、攻撃シーケンスにおいて最も重要な要素の一つである Exploiting(攻撃コードを実行するための一連の手続き)が非常に稚拙な作りとなっている。本来、非常に攻撃安定性の高いスタックベースのバッファオーバーフロー脆弱性を利用しているにもかかわらず、十分にその安定性が生かしきれていない。

5.2 標的型攻撃に利用される可能性が高いソフトウェアの傾向

4 に示したように、近年の標的型攻撃に利用されている脆弱性は、受動的攻撃を成立させるものが大半である。その中で、多くのユーザーの間で「開いても安全である」という認識が高いファイル処理するアプリケーションの脆弱性がよく利用されている。また、比較的著名なアプリケーションに存在している脆弱性が良く利用されている。

近年の標的型攻撃に関する調査研究

調査報告書

また、5.1 で示したように、標的型攻撃に利用されている脆弱性はバッファオーバーフロー脆弱性が多く、また、比較的安定して攻撃可能なものに限定されている。脆弱性は、たとえニュースなどで話題になった脆弱性であっても、攻撃安定性が低い脆弱性は標的型攻撃に用いられていない。例えば、Windows GDI (Graphic Device Interface) のバッファオーバーフロー脆弱性(MS07-046)は、Microsoft Office 製品をはじめ様々なアプリケーションに影響することで話題になったが、この脆弱性はメモリコピーの際に常にページバウンダリにヒットすることを避けられないタイプのヒープオーバーフロー脆弱性であるため攻撃安定性が低い。このような、攻撃安定性の低い脆弱性が標的型攻撃に利用された例は確認できない。

これらを考慮すると、標的型攻撃に利用される可能性が高いソフトウェアは、以下のような特徴があると見られる。

- A) 受動的攻撃を成立させる脆弱性
- B) 多くのユーザーの間で「開いても安全である」という認識が高いファイル进行处理するアプリケーションの脆弱性
- C) 比較的著名な脆弱性
- D) バッファオーバーフロー脆弱性
- E) 比較的安定して攻撃可能な脆弱性

さらに、過去に発表された脆弱性の経緯から、深刻な影響を及ぼすソフトウェアは、第三者やベンダーにおける検査や対応が進み、将来的には安全になっていく可能性がある。しかし、これによって攻撃対象となるソフトウェアの範囲が広がる可能性がある。以前は、攻撃の多くが Windows システムや Internet Explorer など、OS 標準の機能やアプリケーションの脆弱性を狙ったものが大半であった。しかし近年では、4 に示したように様々なベンダーの様々なアプリケーションが対象となりつつある。また、国産のアーカイバである Lhaz などが対象となっており、対象となるアプリケーションの範囲が広がりつつあるものと推測される。今後は、より広範なソフトウェアに対し、適切なリスク管理が必要となる可能性がある。

6. 標的型攻撃用マルウェアの実態調査・傾向分析

近年の標的型攻撃に利用されたマルウェアを解析した。解析マルウェアは TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDROP 系である。また、一般に対して無差別に配布されている検体との比較を行うため、PEACOMM.D (Storm Worm 検体)の詳細な解析を行った

7. 近年の標的型攻撃で用いられるマルウェアの分析

近年は、脆弱性を利用してマルウェアを設置する例が多くなっており、また、マルウェアも従来のように単体で動作するのではなく、ダウンローダを介して設置されるシーケンシャルマルウェアとなっている事が多い。図 4 に、その代表的なモデルを示す。

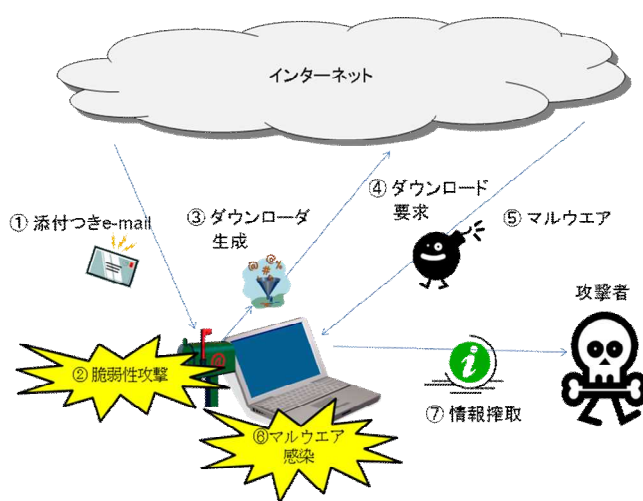


図 4. 近年の標的型攻撃のモデル

7.1 マルウェアの解析と攻撃シーケンスの分析

7-1-1. TROJ_MDROPPER 系の攻撃シーケンス

TROJ_MDROPPER 系の攻撃シーケンスの概要を図5に示す。

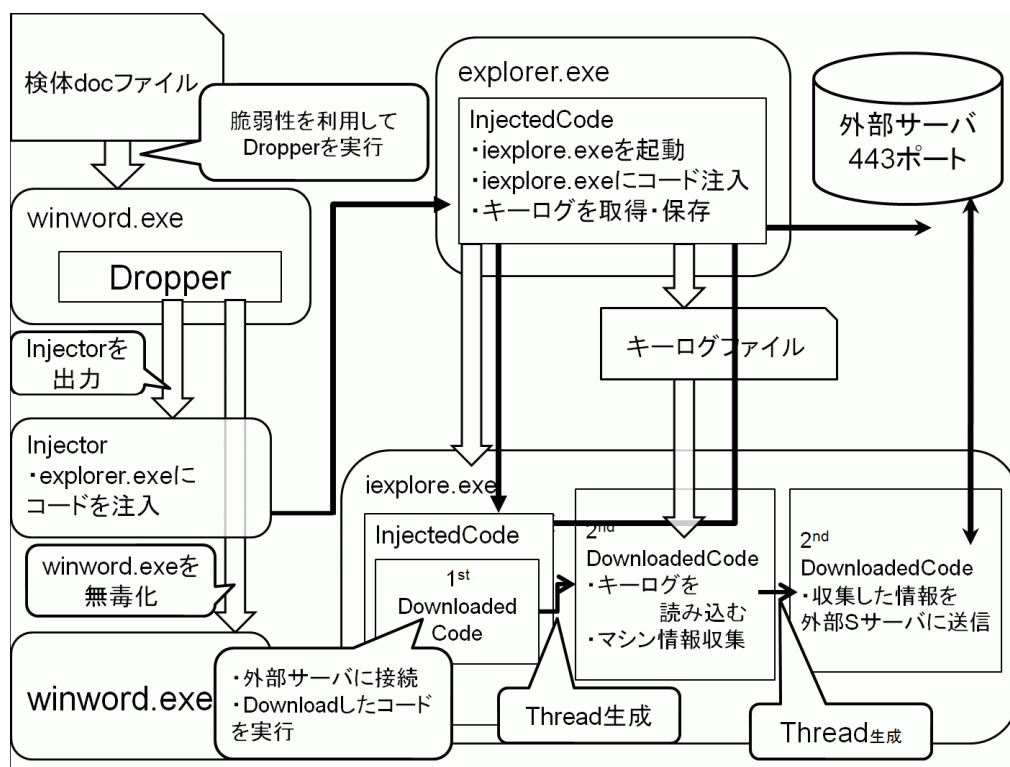


図5. TROJ_MDROPPER 系攻撃シーケンス概要

近年の標的型攻撃に関する調査研究

調査報告書

検体 doc ファイルは、脆弱性を利用して機械語で記述された攻撃コード(以下、Shellcode)を実行する。他のプロセスに対して、機械語で記述された更なる攻撃コードを挿入するためのプログラム(以下、Injector)を検体 doc ファイルから抽出し、ファイルシステム上に作成する。

このように、新たなプログラムをファイルシステムに生成するためのプログラムや Shellcode は Dropper と呼ばれる。図 5 に示す TROJ_MDROPPEER 系の Dropper は、2 つの Shellcode(以下、1st Shellcode、および 2nd Shellcode とする)から構成される。1st Shellcode は、単純に 2nd Shellcode を生成するためのものであり、Dropper の実質的な機能は 2nd Shellcode に実装されている。TROJ_MDROPPEER 系の Dropper の動作は以下の通りである。

- (a) 脆弱性 MS06-027 を利用して Shellcode 実行
- (b) 1st Shellcode をデコードし実行
- (c) 2nd Shellcode の難読化をデコードし実行

難読化とは、機械語コードの解析を困難にするための技術の一つである。機械語コードやデータに対してビットシフトや排他的論理和などを施し、ディスアセンブラツールやバイナリエディタなどによる解析を防ぐものが一般的である。ビットシフトや排他的論理和が施された機械語コードは直接実行できないため、対象となる機械語コードを実行する前に、機械語コードやデータを元に戻す処理が実行される。

1st Shellcode は、2nd Shellcode の難読化をデコードし、実行する。動作概要は以下の通りである。

- (a) 必要な API のエントリアドレスを取得
- (b) 2nd Shellcode を展開するためのメモリを確保

近年の標的型攻撃に関する調査研究

調査報告書

- (c) 確保したメモリ上に 2nd Shellcode を展開
- (d) 2nd Shellcode の難読化をデコード
- (e) 2nd Shellcode を実行

2nd Shellcode は、検体 doc ファイルから Injector コードを読み込みファイルに書き込む。動作概要は以下の通りである。

- (a) 検体 doc ファイルのファイルハンドルを取得
- (b) Injector 実行ファイルの生成
- (c) Injector コードイメージの読み込み
- (d) Injector コードイメージの複合
- (e) Injector コードイメージの書き出し
- (f) Injector コードの実行
- (g) 検体 doc ファイルの無毒化
- (h) 無毒化された doc ファイルの表示

2nd Shellcode は検体 doc ファイルを上書きすることで exploit 部を削除する。これにより、検体 doc ファイルは無毒化され、以降この検体 doc ファイルを開いても exploit は発動しなくなる。その後無毒化された検体 doc ファイルを表示することで、ユーザーに攻撃を察知されにくくしている。

TROJ_PCCLIE 系は TROJ_MDROPPER 系と同じ動作をするが、シーケンスが一部異なる。

近年の標的型攻撃に関する調査研究

調査報告書

TROJ_PCCLIE 系 Dropper は TROJ_MDROPPER 系 Dropper と異なり、Dropper 自身が実行可能ファイルとなっている。Microsoft Word の文書ファイルに似たアイコンとなっており、ユーザーの実行を促す。

Dropper はローカルファイルシステム内に 2 種類の実行ファイルと、ドキュメントファイルを生成する。実行ファイルの内一つは、コード注入用実行ファイル(Injector)、もう一つは Dropper 自身のコピーとなっている。

図 6 に TROJ_PCCLIE 系に特化した部分のシーケンス概要を示す。

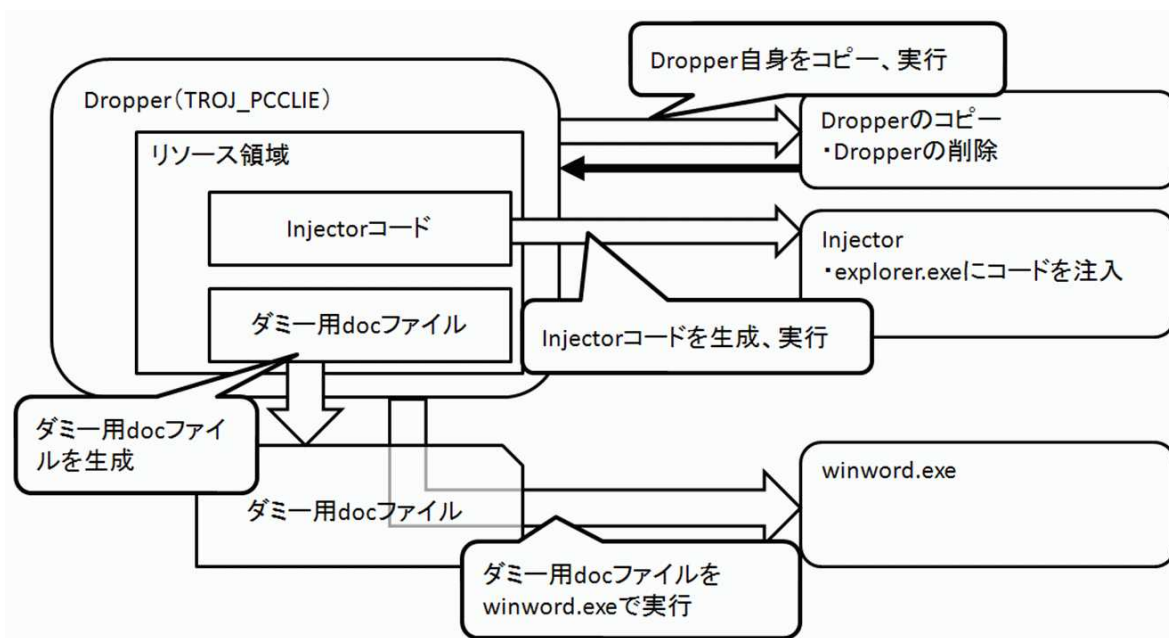


図 6. TROJ_PCCLIE 系攻撃シーケンス概要

Injector は、explorer.exe のプロセス空間内に、メモリを確保しコードをインジェクトする。動作概要は以下の通りである。

- (a) 難読化デコード
- (b) コマンドライン引数のチェック

近年の標的型攻撃に関する調査研究

調査報告書

- (c) デバッガチェック
- (d) ライブラリのロード
- (e) 二重起動防止
- (f) API のエントリアドレス取得
- (g) 権限チェック
- (h) explorer.exe を検索しコードをインジェクト
- (i) explorer.exe 内でインジェクトしたコードを実行

explorer.exe 上の Injected Code は、iexplore.exe にコードを Inject し、キーログを採取・保存する。動作概要は以下の通りである。

- (a) API エントリアドレスの取得
- (b) システムディレクトリ配下に自分自身をコピー
- (c) システム起動時に自動起動させるようにレジストリに書き込む
- (d) 標準のブラウザ(iexplore.exe)プロセスを起動し、コードをインジェクトする
- (e) 標準のブラウザ(iexplore.exe)プロセス内のインジェクトしたコードを実行する
- (f) キーストロークをロギングする

iexplore.exe 上の Injected Code は、攻撃者が用意したサーバに接続し、実行可能コードをダウンロードする。本報告書作成時点では、外部サーバから2つのコードがダウンロードされた。それぞれを、1st

近年の標的型攻撃に関する調査研究

調査報告書

Downloaded Code、2nd Downloaded Code とする。なお、1st Downloaded Code、および 2nd Downloaded Code は、状況やタイミングに応じて変化する可能性がある。本報告書では、動作検証時にダウンロードされた攻撃コードの分析結果を示す。

Injected Code の動作概要は以下の通りである。

- (a) API のエントリアドレスの取得
- (b) 接続先 IP アドレスとポート番号の生成
- (c) ソケットを生成し、攻撃者が用意したサーバに接続
- (d) 認証用データを送受信
- (e) クライアント、サーバの認証を行う
- (f) 実行可能コード受信
- (g) 受信コードの実行(1st Downloaded Code)

1st Downloaded Code は、外部サーバから更に実行可能コードを受信し、実行する。動作概要は以下の通りである。

- (a) API のエントリアドレスの取得
- (b) エラーモード設定
- (c) データ受信、デコード
- (d) クリティカルセクション初期化
- (e) データ受信、デコード(2nd Downloaded Code)

近年の標的型攻撃に関する調査研究

調査報告書

(f) スレッドを生成し、2nd Downloaded Code 実行

2nd Downloaded Code は、ロギングしたキーストローク情報やマシンの情報を、外部サーバに送信する。動作概要は以下の通りである。

(a) 必要な DLL (Dynamic Link Library) のロード

(b) API のエントリアドレスの取得

(c) データ送受信を行うスレッドを生成

(d) キーログファイルをオープンし、ファイル内容をチェック

(e) コンピュータ名取得

(f) ユーザー名取得

(g) バージョン情報を取得

(h) キーログ結果を含むデータを圧縮

(i) データ送受信スレッドが、圧縮されたキーログ結果を含むデータを送信

送信されているキーログ結果を含むデータの例を図 7 に示す。

近年の標的型攻撃に関する調査研究

調査報告書

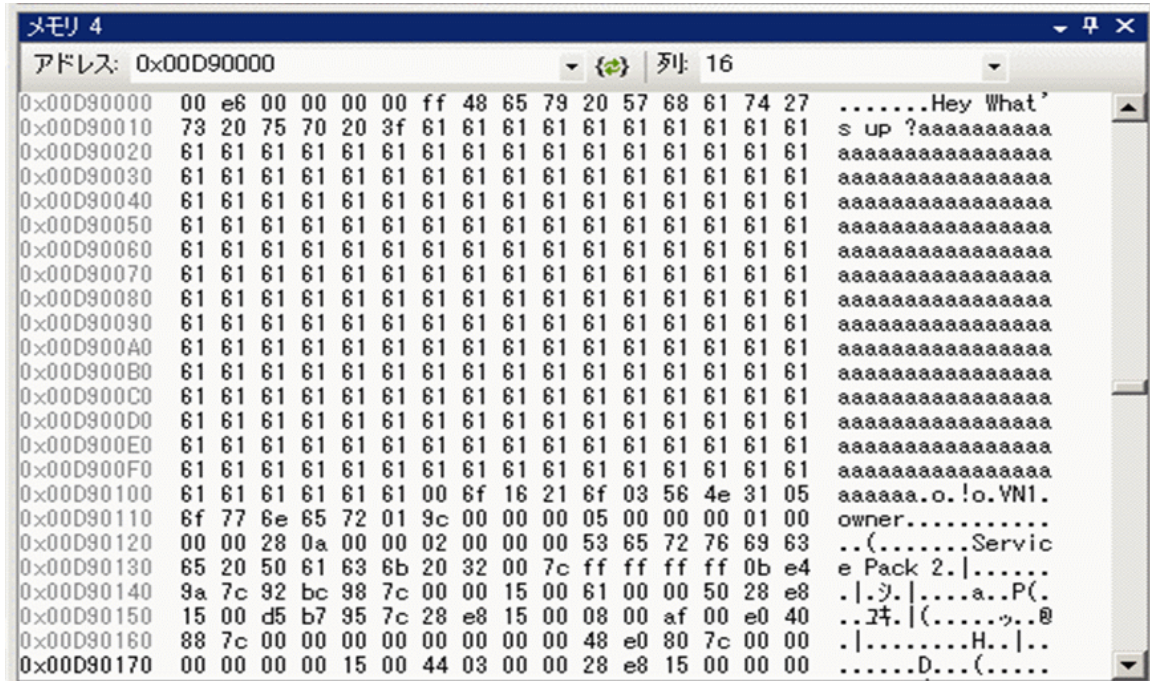


図 7. 送信されているキーログ結果を含むデータの例

7-1-2. TROJ_PPDRP 系の攻撃シーケンス

TROJ_PPDRP 系の攻撃シーケンスの概要を図 8 に示す。

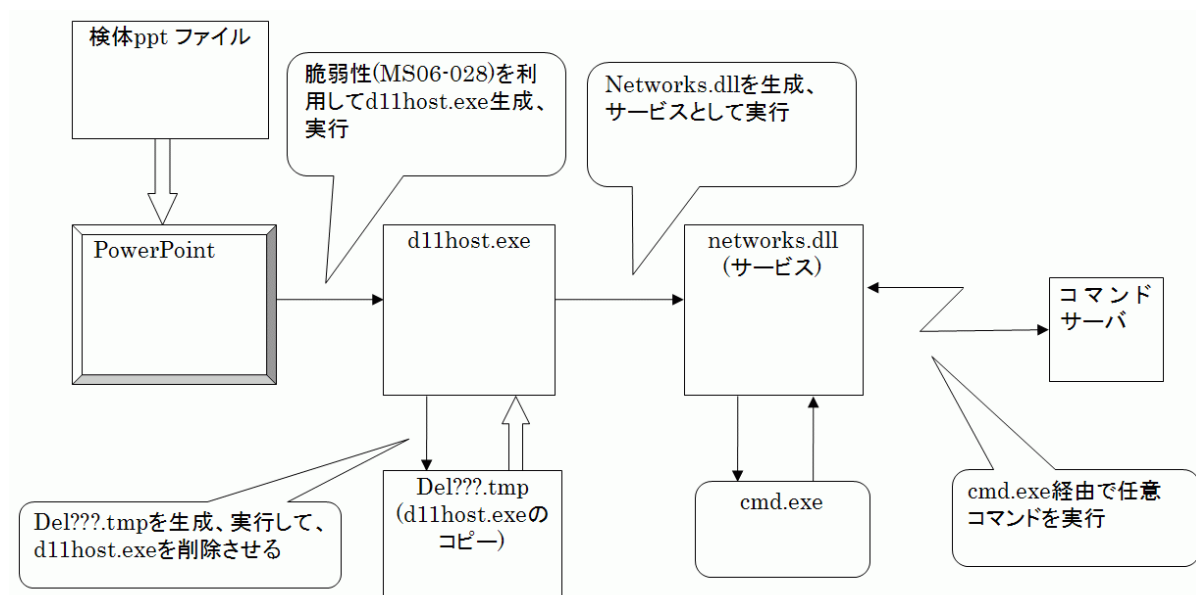


図 8. TROJ_PPDRP 系攻撃シーケンス概要

検体 ppt ファイル内の Shellcode は、以下のように動作する。

- (a) 難読化を解除する。
- (b) API のエントリアドレスを取得する。
- (c) Networks.dll を生成する d11host.exe を生成。
- (d) 自分自身の ppt ファイルから Shellcode を削除し、通常の ppt ファイルへと変換する。この変換は、

近年の標的型攻撃に関する調査研究

調査報告書

メモリ上にマップされているファイルイメージを変更することで実装している。

- (e) 同じファイルをテンポラリフォルダにも生成。
- (f) 最後に、テンポラリフォルダに生成した ppt ファイルを別プロセスで開き、今のプロセスを終了させる。

d11host.exe は、以下のように動作する。

- (a) networks.dll の生成
- (b) svchost.exe 経由で networks.dll をサービスとして設定
- (c) 自分自身の削除

networks.dll は、以下のように動作する。

- (a) 難読化を解除する。
- (b) nett.j2ee.us の名前を引いて、コマンドサーバとして登録する。
- (c) 名前が引けなかったり 127.0.0.1 に向いていたりした場合は 61.97.129.7 を使用する。
- (d) サーバポート 80 と 443 に順番に接続する。
- (e) クライアントからコマンド 2 番を送信する。
- (f) サーバからの応答が「(特定のマジックキー)」であった場合、次のステップへ進む。そうでなかった場合は再度サーバへ接続する。
- (g) サーバからの応答が「(特定のマジックキー)」であった場合、cmd.exe を起動する。

近年の標的型攻撃に関する調査研究

調査報告書

- (h) 以後、コマンド 1 番で送られて来たデータは、`cmd.exe` の標準入力へパイプされる。
- (i) `cmd.exe` の出力は、コマンド 1 としてサーバへと返信される。
- (j) サーバ、クライアントがお互いにコマンド 1 を送信しあうことで、サーバからクライアント上で任意のシェルコマンドを実行可能である。

7.2 攻撃サイトの特徴

TCP (Transmission Control Protocol) のポート 80 番、および、443 番を利用しているこれらマルウェアは HTTP (Hyper Text Transfer Protocol)、および HTTPS (Hyper Text Transfer Protocol over SSL) のポートを利用しているにも関わらずそれらプロトコルに則った通信を行っておらず、全て独自のプロトコルである。このため、サーバシステムは攻撃者が用意した専用のコントロールサーバがセットアップされており、攻撃者により完全にコントロールされているものと推測される。

また、TROJ_MDROPPER 系および PCCLIE 系においては、サーバ側、およびクライアント側の両方で認証が行われており、マルウェアにとって不正な接続を全て遮断している。

なお、TROJ_MDROPPER の動作解説として、あるアンチウイルスベンダーの web サイトにて以下のように解説されている。

- (a) `explorer.exe` プロセスのメモリに書き込む
- (b) `iexplorer.exe` を起動してバックドアを開く
- (c) コマンドを受信し盗み出した情報を送信する

近年の標的型攻撃に関する調査研究

調査報告書

この解説では、攻撃シーケンスの関連性が不明である。また、コマンドを受信するとあるが、実際に受信するのはコマンドではなくコードそのものであり、そのコード自体は状況に応じて変化する可能性がある。情報を攻撃者に送信するのは新たにダウンロードしてきたコードであるため、MDropper から生成されたトロイの木馬そのものにこの情報送信機能は存在しない。また、仮に MDropper がシステムに感染しており、それがアンチウイルスシステムで検知された場合、「コマンドを受信し、盗み出した情報が送信」されただけに留まっているという保証は無い。「コマンド」の場合は、マルウェアに実装されている事以外には行わないが、「コード」の場合は何が発生するのかは状況次第であり、MDropper の上記解説を前提としたインシデント対応は場合によっては誤りである可能性がある。攻撃者が用意したサーバと通信した時点で、攻撃者がサーバ上に用意した任意のコードが実行される。コードは常に変更可能であるため、つぎつぎに不正なコードが実行されている可能性は否定できない。ネットワークを流れるパケットは、近年のマルウェアでは通常暗号化が施されているため、自動的解析によるアプローチでは、このように「コマンドを受信して情報を送信する」のか、あるいは、「新たなコードを受け取ってそれが実行されているのか」を区別する事は難しい。図 9 に、コマンドを受信してキーログデータを送信するマルウェアと、コードを受信してキーログデータを送信するマルウェアの構造的な違いを示す。

このように、自動解析の結果に基づいて発表されている分析では正確な脅威判断を行うことが難しい。表面的に見える挙動のトレースのみで分析を行っているため、脅威の本質的な分析が不正確となってしまうケースがある。

近年の標的型攻撃に関する調査研究

調査報告書

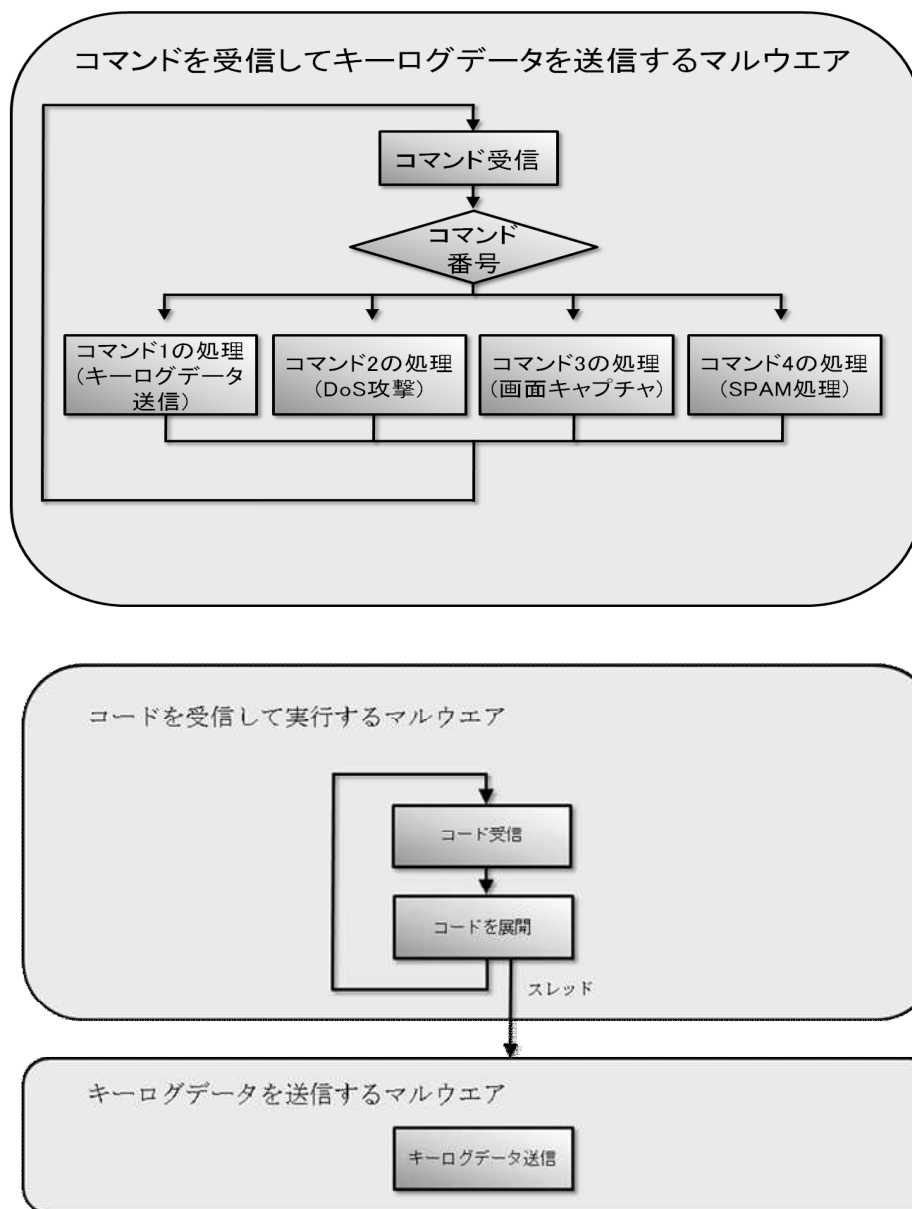


図 9. コード受信とコマンド受信の違い

7.3 ボット型マルウェアと標的型攻撃マルウェアの共通仕様分析

不特定多数を対象とした無差別攻撃型マルウェアであるボット型マルウェアとの比較を行うため、Peacomm(通称 Storm Worm)の解析を行った。Storm Wormとは、2007年1月に実際に起きた欧州の暴風雨の際に猛威をふるったマルウェアで、「欧州を襲った暴風雨で〇〇人が死亡」などのタイトルで注意をひき、ユーザーにトロイの木馬をダウンロードさせるものである。上記を発端にたびたび手口を変えた亜種の出現が知られている。今回は、「Happy New Year 2008」版(Peacomm.D)の解析を行った。

本節では、無差別攻撃型マルウェアの Peacomm.D の動作概要を解説する。また、標的型攻撃で利用されたマルウェアの TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDROP 系との比較を行う。

Peacomm の攻撃シーケンスの概要を図 10 に示す。

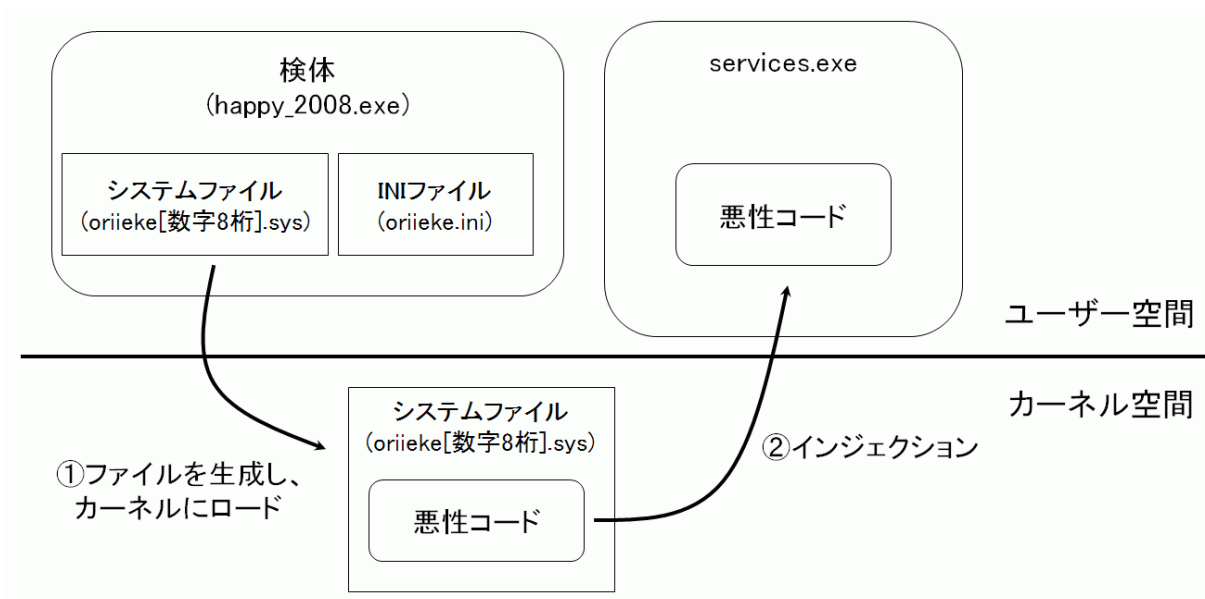


図 10. Peacomm 攻撃シーケンス概要

近年の標的型攻撃に関する調査研究

調査報告書

検体(happy_2008.exe)のプログラムは、難読化されておらず容易に処理を把握することができる。まず、システムファイルと ini ファイル(初期設定記述ファイル)をシステムディレクトリに生成する。つぎに、システムファイルをサービスに登録し、起動する。これによりシステムファイルがカーネルにロードされる。

システムファイル(oriieke[数字 8 桁].sys)は、主にコードインジェクション機能およびルートキット機能の二つの機能を備えている。生成されたシステムファイル自体は難読化されていないが、コードインジェクション機能によってインジェクトされるコードは簡単なエンコード処理が施されている。

コードインジェクション機能では、まず、プロセス一覧から、インジェクト対象プロセスのプロセスエントリを取得する。今回のケースでは、services.exe である。つぎに、システムファイル内の悪性コードをデコードする。インジェクト対象プロセス中にメモリを確保し、デコードしたコードをコピーする。最後に、APC (Asynchronous Procedure Call) を利用して、コピーしたコードをインジェクト対象プロセスのコンテキストで実行させる。

ルートキット機能では、まず複数の API をフックし、"oriieke"が含まれるファイル、レジストリをユーザーから見えないように隠蔽する。ルートキットは、Windows 2000/XP/Server 2003 にそれぞれ対応しており、OS 毎の上記 API のオフセットテーブルを用意している。つぎに、TCP のディスパッチルーチンをフックし、netstat コマンド(通信の状況を把握するコマンド)等による接続情報を隠蔽する。具体的には、プロセス ID に基づいて services.exe の通信情報エントリを特定し、当該接続情報エントリの先頭バイトをゼロクリアする。

Storm Worm の本体部分(services.exe にインジェクトされた悪性コード)には、P2P(Peer to Peer)通信機能、SPAM 送信機能、FTP (File Transfer Protocol)通信機能(downloader 機能)、IFRAME インジェクション機能などが存在している。Storm Worm が動作を開始すると、まず、必要な API のアドレスを取得し、独自の IAT (Import Address Table) を作成する。次に、本体コード実行用スレッドを生成する。そして P2P 通信を開始する。

標的型攻撃で利用されたマルウェアの TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDRUP 系と比較を行った結果、コードインジェクションなど基本的な技術については類似性が多数見受けられた。ま

近年の標的型攻撃に関する調査研究

調査報告書

た、両者とも、感染の事実を極力隠蔽するためのさまざまな工夫が施されており、一般のユーザーにとっては攻撃が非常に見えにくくなっている。また、アンチフォレンジックやアンチデバッグなどさまざまな解析対策が施されており、セキュリティベンダーによる対策を遅らせるためと思われるさまざまな工夫がほどこされている。

また、TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDRAP 系標的型攻撃マルウェア、および、これらによりダウンロードされた攻撃コードは、その目的が情報搾取に特化しており、「小規模特定機能型」であると言える。それに対し、Storm Worm など大量無差別型のマルウェアは、SPAM など様々な用途に利用される事が前提となっている「大規模多機能型」である事を確認した。

7.4 標的型攻撃用マルウェアの検知手法

TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDRAP 系では、攻撃者が用意した外部サーバとの通信さえ遮断できれば、脅威は発生しない事が分かった。このため、以下のような対策を全て施すことで脅威を未然に防ぐことができる。

- (a) 不必要な外向きの TCP ポートを全て閉じる。
- (b) TCP 80 番、443 番において、それぞれ HTTP、および HTTPS 以外の通信を検知したら通信を遮断する。あるいは、HTTP(TCP 80 番)、および HTTPS(TCP 443 番)においては、プロキシサーバ経由でのみ外部との接続を許可する。

しかし、TROJ_MDROPPER 系、PCCLIE 系、および TROJ_PPDRAP 系以外の標的型攻撃で利用された

近年の標的型攻撃に関する調査研究

調査報告書

マルウェア検体を解析していないため、上記対策が全てのケースで有効であるとは言えない。このため、他の標的型攻撃用マルウェア検体解析を行っていく必要があると考えられる。また、今後はこれら対策を迂回するような仕組みが実装される可能性があるため、標的型攻撃用マルウェア検体の解析を今後も継続していく必要があると考えられる。

7.5 効率の良い脅威分析手法に関する検討

今回解析した標的型攻撃用マルウェア、および大量無差別型マルウェアは、両者とも、ファイルシステム内にさまざまなファイルを生成している。このため、ファイルシステムをモニタすれば生成されるファイルを捕獲できることが分かった。また、新たなコードを実行ファイルとしてダウンロードし、ファイルシステムに展開するような攻撃が行われた場合も、ファイルシステムをモニタすれば捕獲できる事が分かった。

ただし、インジェクトされたコード、あるいは、TROJ_MDROPPER 系や PCCLIE 系にてダウンロードされたオンメモリで動作するコードについては、ファイルシステムモニタリングでは捕獲できない。また、API トレースやパケットモニタリングなど自動解析手法を用いた場合でも、攻撃者からコマンドを受信して処理しているのか、あるいは、オンメモリで動作する新たなコードをダウンロードしてそれが実行されているのかを区別する事が難しく、脅威分析が不正確になってしまうケースがある事が分かった。

このため、API トレースなどを用いて、外部サーバからのパケット受信が行われた時点で切り分けを行い、それ以前を動的解析、それ以降を静的解析するというアプローチを取れば、効率のかつ正確な脅威分析を行うことができると考えられる。

また、今回解析した標的型攻撃用マルウェア、および大量無差別型マルウェアは、さまざまな解析対策、および解析を困難にする要素があった。具体的には、多重難読化、独自 API テーブル、多数の無駄コード挿入、アンチデバッギング、アンチリバースエンジニアリング、マルチスレッド、圧縮されたコードの展開、他プロセスへのインジェクト、リモートホストからの部分コード受信と実行、などが挙げられる。

近年の標的型攻撃に関する調査研究

調査報告書

コードサイズも大きく、シーケンスの大半で IDA(HexRay 社の高機能ディスアセンブラ)が利用できなかった。このため、デバッガのみで大量のコードをトレースする必要があった。また、上記のような特徴があるため、コードも通常のアプリケーションと比較すると非常に解析困難である。迅速な解析を行うためには、熟練した解析技術が必要となる。このため、解析エンジニアの育成が重要な課題であると考えられる。

8.まとめ

(1) 標的型攻撃で利用されている脆弱性は受動的攻撃を成立させるものが主流

標的型攻撃用マルウェアで利用された脆弱性は受動的攻撃を成立させるものが主流であった。また、多くのユーザーの間で「開いても安全である」という認識が高いファイル进行处理するアプリケーションの脆弱性がよく利用されている事が分かった。

(2) 攻撃シーケンスは複数のパートに分かれている

攻撃のシーケンスは複数のパートに分かれていることを確認した。一部は非常に洗練されたコードであるが、一部は非常に稚拙であるなど、各パートによって技術レベルが一定していない事が分かった。また、マルウェアコードのライブラリ化や、ツールキットにより生成されたと思われる箇所が多数存在する事を確認した。

(3) アンチフォレンジックが実装されている

一度検体ドキュメントファイルを開くと Exploit 部が上書きされて消えるなど、他さまざまなアンチフォレンジックテクニックが実装されていた。

(4) 標的型攻撃は「小規模特定機能型」

今回解析した標的型攻撃用マルウェア検体やダウンロードコードは目的が情報搾取に特化しており、「小規模特定機能型」である事が分かった。それに対し、Storm Worm など大量無差別型のマルウェアは、様々な用途に利用される事が前提となっている「大規模多機能型」である事を確認した。

近年の標的型攻撃に関する調査研究

調査報告書

(5) 通信は独自プロトコル

今回解析した標的型攻撃用マルウェアの通信は、TCP ポート 80 番、443 番を利用しているが、全て独自のプロトコルであった。マルウェアによっては、サーバ側、およびクライアント側の両方で認証が行われている事が確認できた。

(6) 自動解析に基づいた情報では的確な対応ができないケースがある

近年の標的型攻撃用マルウェアにおいて、API トレースなどの自動解析に基づいた情報を前提としたインシデント対応を行った場合、的確な対応ができない可能性がある事が分かった。ダウンロードされるコードは状況に応じて変化する可能性があるため、あるタイミングで確認された脅威が前後のタイミングで同じであるという保証が無い事を確認した。

(7) 外部サーバとの通信を遮断すれば脅威は発生しない

今回解析した標的型攻撃用マルウェアでは、攻撃者が用意した外部サーバとの通信さえ遮断できれば、脅威は発生しない事が分かった。しかし、今回解析対象となった以外のマルウェアを解析していないため、この対策が全てのケースで有効であるとは言えない。また、今後はこれら対策を迂回するような仕組みが実装される可能性がある。このため、標的型攻撃用マルウェアの解析を今後も継続していく必要があると考えられる。

(8) さまざまな解析対策が施されている

今回解析した標的型攻撃用マルウェア、および大量無差別型マルウェアは、様々な解析対策、および解析を困難にする要素を確認した。迅速な解析を行うためには、熟練した解析技術を持つエンジニアの育成と解析効率化ツール環境の整備が重要な課題であると考えられる。