特集

サイバー攻撃の現状と防止策

サイバー攻撃は政府機関や企業だけではない。これまで、大学は個人情報を含め様々な情報の漏洩、あるいは流失防止に努めてきた。しかしながら、サイバー攻撃による情報の盗み出し、システム破壊等の被害が発生している中で、高度な研究成果を保有する大学の対策は企業などに比べ対策が十分でない場合もあり、サイバー攻撃の対象となったり、あるいは攻撃の拠点として悪用される危険性が現実のものとなっている。

そのような現状を踏まえ、本特集では、高度化するサイバー攻撃の仕組みや脅威、さらには具体的な防御システムを紹介し、大学においても喫緊の課題である情報セキュリティの危機管理能力の向上、強化に向けて理解を深めたい。

巧妙化する標的型攻撃とその対策

名古屋大学情報基盤センター
情報基盤ネットワーク研究部門教授　**高倉　弘喜**

1．はじめに

標的型攻撃により、中央官庁や大手企業から漏れるはずのない重要な情報が外部に持ち出される事案が増加しています。

この種の攻撃が蔓延するとは考えにくいのですが、各種ハッキング・マルウェア作成ツールが容易に入手できるようになった現在、ある程度、一般化するのは時間の問題と言えます。

本稿では、標的型攻撃の概要について説明し、その対策案について提案します。

2．従来のセキュリティ対策

これまでの組織に対するサイバー攻撃では、攻撃者が組織内LANに直接侵入し、機密や機微な情報（保護対象情報）を持ち出していました。これに対するセキュリティ対策の典型的な例を図１に示します。ここでは、

- 対外接続点に設置したファイアウォールやIDSなどにより、組織内ネットワークへの侵入や攻撃を阻止
- DMZに設置したメールサーバやproxyサーバなどの中継サーバにより、組織内のコンピュータと外部との通信を仲介し、その際にマルウェア検査や保護対象情報の漏洩検査を実施
- 組織内LANから外部への通信では、DMZの中継サーバの利用を必須化し、各PCにセキュリティソフトを搭載
- 保護対象情報は、組織内からのアクセスを制限したネットワーク、あるいは、隔離したネットワークで管理

という多段の対策により、組織の外に居る攻撃者が、保護対象情報に到達するのを防いできました。

3．標的型攻撃の仕組み

標的型攻撃は以下のような手順を踏むことで従来の対策を無力化します。

（1）偵察

一般に、保護対象情報にアクセスできる人は情報セキュリティの意識が高く、発信者に覚えがな

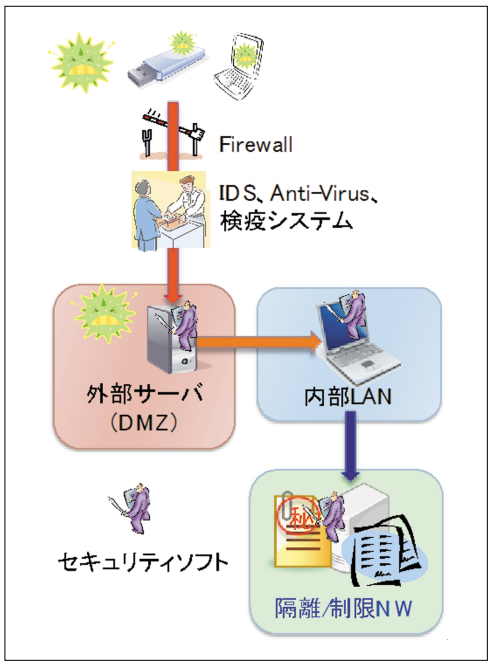

図１　従来のセキュリティ対策

い添付ファイルを開かせることは期待できません。そこで、同じ組織の中で、不特定多数との情報交換を行う人物を捜します。例えば、ホームページに掲載された問い合わせ先を調査します。

場合によっては、まず関連先に侵入し、そこから本命の組織に標的型攻撃を仕掛けることもあります。例えば、「社内報で先生の研究を特集させていただくことになり・・・」といったメールが共同研究先から来ることが考えられます。

（2）侵入

偵察で狙いを定めた人物に、マルウェアを送りつけます。送付手段としては、電子メールがよく用いられますが、USBメモリやCD/DVDを送りつけることもあります。このときのマルウェアは、本攻撃だけのために作成され、アンチウィルスでは検知できないものが用いられます。

図２は2011年7月に発生した標的型攻撃で、メールに添付されていたマルウェアをhttp://www.virustotal.comで検査した結果を示します。このWebサイトでは43社のアンチウィルスを使って、検知パターンでマルウェアを検出できるかを評価するのですが、この場合で検知できたものは皆無でした。

通常、送りつけられるマルウェアは、実行ファイル（exe等）ではなく、ワープロソフトや表計算ソフト用のファイルです。これらのソフトの未確認の脆弱性を突いて、PCへの感染に成功します。

最初に感染するこのマルウェアは、大抵の場合、外部サイトから新たなマルウェアを持ち込むダウンローダ機能のみを備えています。

これにより新たに持ち込まれるマルウェアも、さらに別の外部サイトからマルウェアを持ち込もうとするダウンローダです。このように、ダウンローダの持ち込みを複数回繰り返し、最終的に偵察機能を備えたマルウェアを持ち込みます。

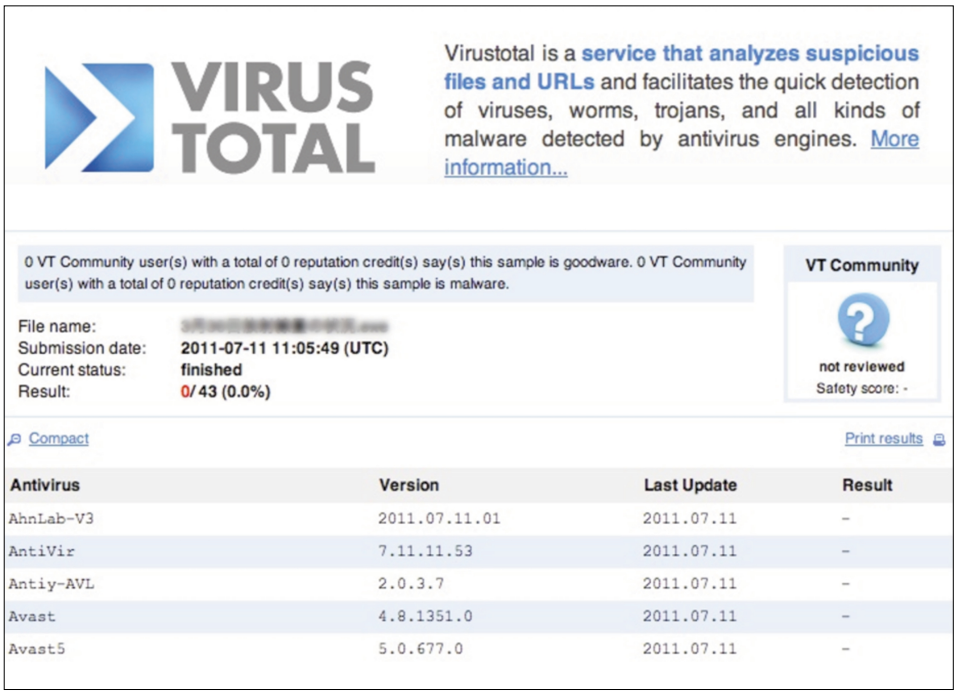

図２　検知できないマルウェア

（3）検証対策

その後、攻撃者は最初に送りつけたマルウェアを多くの組織にばらまくことがあります。これにより、このマルウェアはアンチウィルスで検知できるようになります。

多くの場合、マルウェアを開いてしまった人物は、そのことに気付きます。数日後にアンチウィルスがこれを検知し、駆除成功を報告すれば、上記の偵察マルウェアを持ち込まれる経緯を予想で

きる人は稀ですので、自分のPCは安全だと思い込ませることができ、隠密な活動を継続しやすくなります。

ダウンロードされるファイルは先着１名様限りで、多くの場合、ダウンロードを確認したら直ちに削除されます。さらに先述のダウンロードの繰り返しを組み合わせることで、マルウェア感染の事後検証を妨害しようとします。

（４）前線基地構築

１）情報収集

偵察マルウェアは、初期の段階では組織内を攻撃することは滅多になく、前線基地として主に以下の情報を集めます。

- 感染PCの設定情報
- 感染PCから見えるネットワーク構成
- 感染PCの所有者情報
- 感染PCやファイルサーバに保存された文書やメール

２）外部通信手段の確保

収集した情報を攻撃者に伝える手段を確保します。一般に、組織外に設置されたWebサーバやメールサーバに情報を送ります。前記２．で述べた通り、DMZにある中継サーバの利用が必須である場合、それに必要な情報をPCの設定情報から得ます。また、中継サーバで通信内容の検査が想定されますので、収集した情報は暗号化を施します。

攻撃者は得られた情報をもとに、組織内の次の標的者を定め、攻撃に必要なマルウェアを感染PCに送ります。

さらに、アンチウィルス対策として、感染したマルウェアを定期的に最新のものへ更新します。

（５）組織内部への展開

感染PCでは、前記（４）の１）で得た情報をもとに、組織内部への浸食を開始します。

まず、認証サーバ（LDAPやActive Directory等）を攻撃し、組織ユーザ全員の認証情報の奪取を試みます。通常、認証サーバは外部からアクセスできないネットワークに設置されますが、その用途のため組織内のPCすべてからアクセス可能になっています。また、５．（２）で後述する理由により、OSやアプリケーションを最新のものに維持できない場合が多く、攻撃対象の第一候補となりやすいです。

次に、攻撃メールを作成します。まず、同じく（４）の１）で集めた文書ファイルに、持ち込まれたマルウェアを組込みます。これを図３のように、議事録のメール送信の直後、再送を装ったメールに添付して送ります。送り先は、（４）の１）で得たメールや認証サーバで得た情報をもとに選びます。

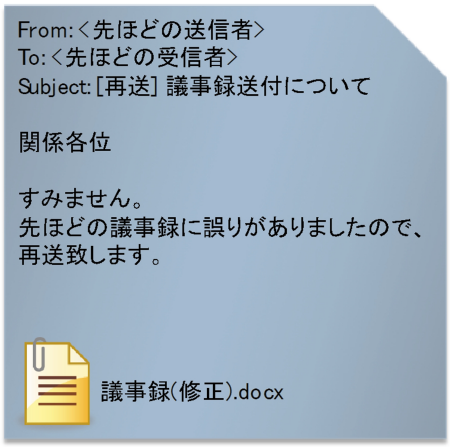

図３　攻撃メールの例

このように巧みに偽装された攻撃メールを疑うことは難しく、次の標的者にかなりの確率で添付ファイルを開かせることができます。

次の標的者のPCでも３．（４）で述べた前線基地の構築が行われ、偵察活動が始まります。最終的には、以下の人物へのPCまで攻撃が繰り返されることになります。

- システム・ネットワーク管理者
- 保護対象情報にアクセス権限を持つ者

（６）情報搬出手段の構築

組織内部への浸食が進み、最終的な標的PCに到達したとしても、これらのPCは外部とのアクセスが厳しく制限されており、中継サーバすら利用できない場合がよくあります。このため、これまでに構築した前線基地を中継基地として活用し、保護対象情報を持ち出せる経路を確保します。

さらには、システム・ネットワーク管理者のPCを乗っ取り、組織内に裏ネットワークを構築

した事例もあります。例えば、最近のOSやモバイルディバイスはIPv6に最初から対応しています。IPv6ではStateless Address Autoconfiguration機能により自動的にアドレス設定が完了すること、かつ、容易にトンネリングが構築できることから、図４に示すように、ネットワーク管理者に気付かれることなく、アクセス制限ネットワークのコンピュータをIPv6としてはインターネット直結にしてしまうことも起こり得ます。

一般に、情報セキュリティシステムのIPv6対応は遅れており、また、多くの組織において、情報セキュリティシステムの監視対象を、自組織が使用するIPv4アドレスの範囲内に限定しています。このため、IPv6網を組織内に構築されても気付けないことになります。

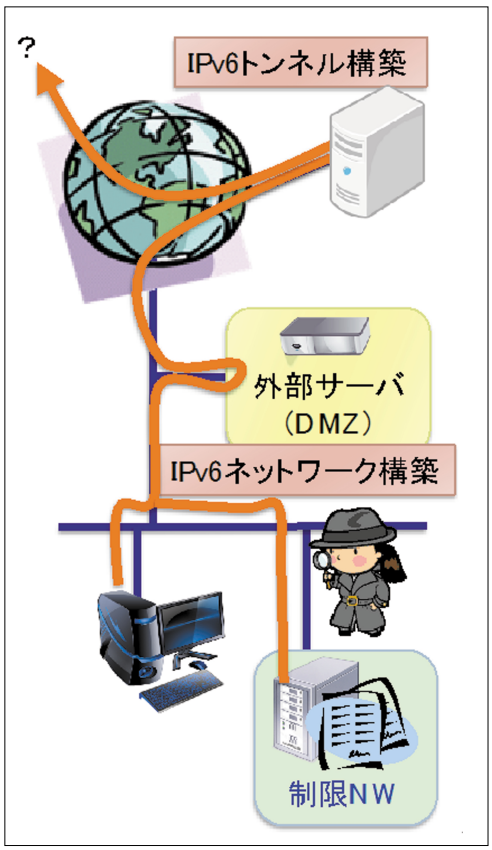

図４　IPv6による裏口ネットワーク

（７）痕跡改竄

保護対象情報の持出しに成功した攻撃者はログの消去や改竄を試みます。すべてのログはログ収集サーバで一元管理されるようになっており、すべてのログの辻褄を合わせた消去は難しくなっています。このため、偽のログを大量に生成したり、ログを改竄することで、攻撃発覚後の解析を妨害します。

４．検知が困難な理由

（１）検知パターンの限界

一般に、アンチウィルスがマルウェアを検知するためには、検知パターンが予め定義されている必要があります。検知漏れとなるマルウェアに対する検知パターンを作成するためには、まず、そのサンプルを入手しなければなりません。

マルウェアが生成されるペースは極めて早く[1]、手作業による解析は不可能なため、ほとんどのアンチウィルスベンダーでは、自動解析システムによって検知パターンを作成しています。

しかし、前述の通り、標的型攻撃で使用されるマルウェアはすべて標的となった組織専用です。このため、当該組織で感染PCを検査し、サンプルをアンチウィルスベンダーに送付しない限り、検知できるようになるのは稀です。

さらに、攻撃者は標的組織が使用するアンチウィルスを事前に把握しており、同じ製品を容易に入手できます。従って、マルウェアを送りつける前やマルウェアを最新版に更新する前に、アンチウィルスで検知できないことを検証することもできます。

他の情報セキュリティシステムも、基本的には検知パターンに依存しており、その裏をかく攻撃は比較的容易なのです。

自動解析システムによる弊害も生じています。自動解析システムの目的は、未知のマルウェアを解析し、その悪性を確認するだけではなく、既知のマルウェアのどれに近いか（どのファミリー）まで分類します。自動解析システムは各社ごとに異なるため、新種のマルウェアの場合は、それぞれ異なるファミリーに分類されることがあります（後日、名前の統一が行われます）。

また、新種のマルウェアに関する速報で説明される挙動は、自動解析の結果や分類されたファミリーの典型的なものに基づいていることが多く、すべての挙動を正しく記述されている訳ではありません。

このため、新種のマルウェアをアンチウィルスが検知した場合、説明には無い活動をする可能性に注意する必要があります。

（2）中継サーバと暗号の利用

3．で述べた通り、収集した情報や奪取した保護対象情報は暗号化され、中継サーバを介して外部に持ち出されます。情報を受け取るサーバとしては、Webサーバかメールサーバがよく使われます。

組織内の構成員が行う通常のWebアクセスやメール送受信との違いはほとんどなく、暗号化された情報が解読できない限り情報の持出しに気付くことはできません。

昔は、攻撃者が頻繁に使うサーバというのが知られていましたが、標的型攻撃で使用されるサーバは、乗っ取った企業や学校のもの、Amazon EC2やGmail等の一般に広く利用されているものとなっており、接続先で察知することも難しくなっています。

5．標的型攻撃への備え

これまでに述べてきた通り、最近の標的型攻撃はその手法が巧妙化しており、完璧な防御はほぼ不可能です。そのため、いくつかの手法を組み合わせ、早期発見と対処が可能となる体制作りが必要となります。

（1）増加するネットワーク対応機器の把握

現在のネットワークには、PCやサーバだけでなく、プリンタ等のOA機器、プロジェクタやテレビといった情報家電、温度計などの各種センサーや空調照明といった建物設備、変わり種としてはSDメモリ[2]までもがネットワークに繋がるようになっています。

その多くで、PC用OSの組込み版（embedded OS）が使用されており、また、クライアント・サーバプログラムもPC用のものがベースとなっていることがあります。一方で、これら組込みシステムはハードウェア資源の制約が厳しく、PC並みのセキュリティ対策を講じることは不可能です。

これらの機器のセキュリティ対策は別途講じる必要があり、必要に応じて別ネットワークに隔離する、重点的な監視体制を備える必要があります。

（2）重要機器の更新問題

クライアントPCであれば、新しいパッチが公開されれば、直ちに適用すべきです。しかし、一方で、一瞬たりとも止められない機器、あるいは、OSの更新に際してアプリケーションの念入りな動作検証が求められる機器での対応は異なってきます。

例えば、3．（5）で述べた認証サーバは、教職員の業務、学生の教育への影響を考慮すると、月に1回程度の停止も気軽には実施しにくいものです。また、アプリケーションによっては、OSの更新に対して、動作保証が得られるまでに数ヶ月を要するものもあります。

これは、機器の重要性が増せば増す程、強固な情報セキュリティ対策が求められる一方で、速やかな更新が行えないというジレンマを抱えることになります。

さらに、

1）OSの更新（特にメジャーバージョン）

2）最新OSに対応するため、アプリケーションの更新

3）OSとアプリケーションの更新による、ハードウェアのスペック不足

が連鎖的に発生することがあります。しかし、ハードウェアを入れ換えようとすると、

4）新ハードウェアは現行OS非対応

という事態に陥ってしまい、結局、すべてを新規に構築し直さねばならないことも珍しくありません。

このような事態を回避するためには、重要機器について、以下の点を注意する必要があります。

- 導入時に使用期限を設定
- 使用期限内の保守が保証され、更新による動作も保証されたOSやアプリを選択
- 使用期限前の更新計画の立案

逆に言えば、保守や動作の保証がないfreewareやshareware を用いてシステムを構築するのであれば、それらのサポート終了や更新の際に速やかな対応が可能か検討する必要があります。

（3）組織内ネットワークのアクセス制御

標的型攻撃が組織内に浸食していく速度を抑えるためには、ネットワークを細分化し、その間のアクセス制御をする必要があります。

例えば、図5に示すように、用途別にVLANを

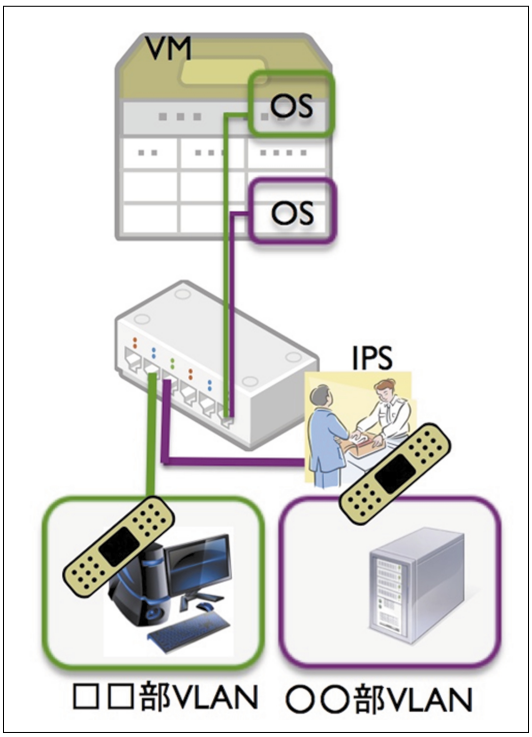

図５　VLAN化と仮想パッチ

分割し、VLAN間のアクセスを制限します。最近は、VLAN対応のネットワークスイッチも廉価になり、かつ、VLANの設定をGUIで行うツールも登場していますので、比較的、容易に実現できます。

また、最近のサーバの高性能化により、一つの筐体に複数の仮想マシンを搭載し、VLANごとに接続先を制限することも簡単になりました。

このように、VLAN間のアクセス制限により、マルウェアによる組織ネットワークへの侵食を遅らせることができます。さらに、標的型攻撃発生の疑いがある場合、ネットワークの監視を強化する必要がありますが、アクセス制限により、監視対象のトラフィックを少なめに抑えることができ、監視装置やそのオペレーションのコスト削減が期待できます。

さらに、あるVLANの機器で、最新のパッチを適用できない場合、そのVLANが繋がる回線上にIPSをインラインモードで設置し、未対応の脆弱性を狙った攻撃を遮断することで仮想的にパッチ適用を実現する方法も考えられます。

これにより、完全ではないものの、ある程度の安全性を確保した状態で、業務を継続することが可能となります。

（４）ネットワークフォレンジックス

標的型攻撃を早期に察知するために最も重要なものはネットワークトラフィックやログの解析です。偵察活動では攻撃はしませんが、ネットワーク構成を把握するための探索は行います。このとき５．（３）で述べたアクセス制御なされていれば、これを乗り越えようとする挙動が不審なものとして検知できます。また、中継サーバのログを解析すれば、他に比べて長時間のセッション、規則性のある挙動など不自然な点を見つけられる可能性があります。

ただし、そのためには、従来、対外接続点でのみ行われていたネットワーク監視を、組織内ネットワークの各所で行う必要があります。これは、ログの量が爆発的に増大することを意味しますので、闇雲に記録をとればよい訳ではありません。

早期察知のためには、１時間間隔のような短周期の解析が必要となります。また、不審な活動を見つけたときでも、解析に数日もかかるようでは役に立ちません。さらに、膨大なログを解析する機器のコストも常識的な範囲内に収める必要があります。

すなわち、各自の解析能力に応じて、どこでどのような記録を取るかを検討する必要があります。

６．まとめ

以上、標的型攻撃がなぜ察知されにくいのかについて解説し、そのための対策案について提案をしました。この主の攻撃を完璧に防ぐことは困難で、早期発見・早期対応が重要となります。

関連ＵＲＬ

[1] http://caislab.kaist.ac.kr/77ddos/DDoS%20Monitoring%20System%20using%20Cloud%20AV.pdf
[2]http://linux.slashdot.jp/story/12/04/11/0954236/telnet
でログインできるSDメモリーカード