サイエンティフィック・システム研究会　　2010 年 9 月 6 日
2010 年度教育環境分科会 第 1 回会合

高等教育機関におけるセキュリティ脅威の最新動向とその対策
ーウィルス感染からみえてくるアンチウィルスの限界と今後ー

名古屋大学情報基盤センター
高倉弘喜

[アブストラクト]
マルウェア(ウィルス)の挙動は大きく変化し、無差別に大量感染を試みるよりも、限られた台数の PC に長期間潜伏し、自身の感染拡大、DDoS 攻撃参加、spam メール送信といった活動を散発的に行うようになってきた。また、潜伏期間中に、感染 PC での盗聴を行い、ID とパスワードのような機密情報を抜き出す。本稿では、このようなマルウェアの感染実例を挙げ、一旦感染を受けると完全な駆除が困難であることを解説する。さらに、このような状況下で、情報システムを構築する際に考慮すべき事項についても述べる。
[キーワード]
マルウェア、ゼロデイ、アンチウィルス、bot プログラム、情報漏洩

1. はじめに

従来のマルウェア感染では、インターネット越しに攻撃を受け、マルウェアに感染した PC は直ちに感染拡大のための攻撃を始める、あるいは、ある一つの機能に特化したものが一般的であった。しかし、最近は、ID やパスワードといった機密情報の奪取、DDoS 攻撃参加や spam メール送信などの多機能なマルウェアが増加している。いずれも、ハッカー側に経済的な利益をもたらすものであり、安定した長期間の感染を好むようになった。

このため、感染後に一定の潜伏期間を設け、PC の所有者が感染に気付いていないかを調査し、活動開始後も、PC やネットワークリソースを浪費しないように心がけるなどの挙動が観測されるようになった。また、感染ファイルも従来のような実行ファイル(exe)ではなく、ライブラリ(dll)を選ぶようになり、マルウェアの発見や挙動解析が難しくなりつつある。

このような新たな脅威に対し、firewall や IDS などを用いた従来型のセキュリティ対策では万全と言えなくなっており、新たなネットワーク設計が求められるようになった。

本稿では、2 節において、マルウェアの挙動が従来とどのように変わったかを述べる。次に、3 節で、実際のゼロデイ攻撃によって PC 内でのマルウェア感染がどのように進むかを解説し、マルウェアの完全駆除が難しさについて説明する。4 節では、このような新たな脅威の元での安全なネットワーク構築手法について述べる。

2. マルウェアの挙動変化

2.1 マルウェア感染の経路

従来のマルウェア感染では、インターネット越しに攻撃を受け、マルウェアに感染した PC は直ちに感染拡大のための攻撃を始めるものが一般的であった。しかし、最近の感染経路として、電子メールの添付ファイル、外部記憶ディバイスを介した感染事例が急増している。また、感染後の活動も、感染拡大、DDoS 攻撃参加、spam メール送信と多岐に渡るだけでなく、散発的に活動することで、感染していることを PC の所有者に悟らせないよう用心深くなっている。

また、Conficker ワーム等により、外部ディバイスとして USB メモリが問題となっているが、OS からすると同種のディバイス(Interface Descriptor の bInterfaceClass が Mass-Strage のもの[4])であれば、デジタルカメラ、携帯電話、音楽プレーヤも全て USB メモリと同等に扱われる。デジタルカメラ(のメモリ)の取扱についても USB メモリ同様の規程が必要となる。

この他にも、知人や宛先間違いを装って、興味を引くメールを送りつけ、添付ファイルをクリックさせる手法も相変わらず使われている。

2.2 Web アクセスによる指令受信

最近のマルウェアは bot のような通信機能を備えたものが一般的となっている。通信プロトコルも HTTP プロトコルに準拠しており、一見すると通常の Web アクセスにみえてしまうことが多い。この Web アクセスを通じて以下に示すような指令を受信している。

・悪意ある活動の開始/停止
　盗聴、感染拡大、DDoS 攻撃参加、spam メール送信など
・最新版の入手
　最新のマルウェアの入手先を通知
・活動報告の提出
　悪意ある活動の成果について報告

これらの指令と報告は全て暗号化されており、マルウェアを解析し暗号アルゴリズムを解読しない限り、その内容を把握することはできない。

また、マルウェアは 5 分から数時間間隔で更新されている。Web アクセスによる指令に従い、マルウェアは頻繁に自己を更新し続けている。この更新頻度は、一般的なアンチウィルスの更新頻度である 1 時間から 1 週間よりも遥かに高く、結果として検知パターンの提供が追い付けない原因となっている。

多くの機関において、firewall 等により厳重に保護されている PC でも、Web アクセスを許可している。Proxy を強制している場合でも、マルウェアは OS の設定を調べることで Web アクセスを行うことができる。従って、Web アクセスさえ出来れば、マルウェアは十分に活動できる。もし、Web アクセスすら許されていない環境であれば、そもそもそのような環境下の PC は有効活用できないため、感染を継続する必要性が無い。

2.3 散発的な活動

マルウェアの活動も、従来であれば、PC やネットワークが使用不能になるまでリソースを消費し尽くすものが多かったが、最近は、1 日に数時間の活動に留め、かつ、各種リソースの消費を抑えるようになってきている。このため、PC の所有者だけでなく、ネットワーク管理者でさえ、マルウェア感染に気付かないことが多くなった。

2.4 多段ダウンロードによる追跡妨害

最近では、一気にマルウェア感染を起こすのではなく、複数のダウンロードサイトを介してマルウェアを感染させる攻撃が増えている。例えば、図 1 に示すように、メールへの添付ファイルそのものは、単なるダウンローダであり、指定された Web サイトからファイルをダウンロードするだけの機能しか持たない。その Web サイトから入手したファイルも、単なるダウンローダである。これを数回(1～n-1 回)繰り返し、最終的(n 回目)に盗聴機能等の悪意を持ったプログラムを入手させる。

特に、標的型攻撃などでは、ダウンローダの取得を確認すると、Web サイトから直ちに当該ファイルを消去することが多い。これにより、通信ログに基づいた追跡調査を妨害しようと試みている。

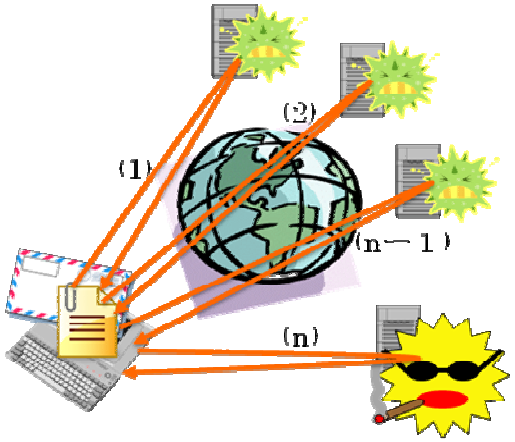


図 1：多段ダウンロードによるマルウェア感染

さらに、最初の添付ファイルのみをアンチウィルスベンダに採取させ、検知パターンを作らせるよう試みる事例も確認されている。多段ダウンロードの実態を理解していない PC ユーザであれば、添付ファイルがマルウェアであり、かつ、安全に駆除されたとの報告で安心してしまうことを期待していると考えられる。

2.5 救援要請をするマルウェア

一般に、マルウェア感染が疑われる場合にまず行うべきことはアンチウィルスによる調査であるとされている。ハッカー側もこの原則は承知しており、以下のような対策を講じている。

(i) スケジュール外のスキャンを検知
(ii) 指令サイトにスキャン開始を報告
(iii) 指令サイトより囮マルウェア取得の指示
(iv) 囮マルウェアダウンロードおよびインストール

この時インストールされるマルウェアは、任意のアンチウィルスで検知できるようにするため、有名な数年前のものを用いることが多い。これは、何らかのマルウェアが検知でき、かつ、安全に駆除できたとの報告を見れば安心する PC ユーザの心理を狙った手法である。冷静に考えれば、手動によるスキャンで、数年前のマルウェアが突然見つかるのは極めて不自然なことであり、アンチウィルスが検知できない「何かが」存在している間接的な証拠と言える。

2.6 感染後のパッチ適用

ハッカーにすれば、一旦乗っ取った PC は経済的利益を生む大切な資産となる。脆弱性が放置されたままでは、別のハッカーによる更なる乗っ取りを許してしまうことになり、資産を失う危険性がある。PC の所有者によるパッチ適用が最も望ましいのであるが、脆弱な PC の場合、所有者がパッチ適用を怠っていることが多い。このため、暫く様子を見た後、所有者によるパッチ適用が期待できないと判断すると、ハッカーがパッチ適用を行ってしまう事例も多数観測されている。

3. 感染対象ファイル

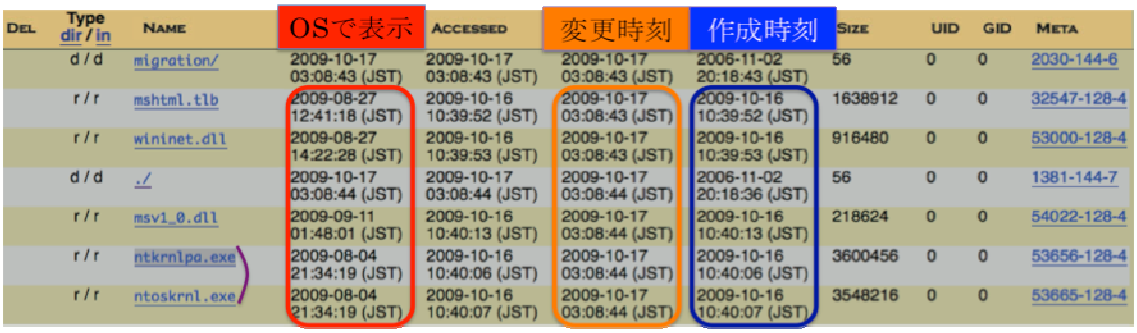
3.1 実行ファイルからライブラリファイルへ

これまで、マルウェアは実行ファイル(exe)であるものが多かった。しかし、最近では、ライブラリファイル(dll)に悪意あるプログラムコードを埋め込む事例が増えている。Exe ファイルの調査では、単に exe ファイルを実行するだけで挙動が分かるし、難読化されていたとしても、プログラムの解析は比較的容易である。一方、dll ファイルの場合、疑わしいプログラムコードの存在は確認できるが、それがどの exe ファイルにより、何時呼び出されるのかを特定するのは難しい。

また、Windows に搭載されているユーザアカウント制御(UAC)では、マイクロソフト社が認定していない exe ファイルを実行しようとすると警告するようになっている。しかし、dll は UAC の保護対象とはならない。

3.2 感染の実例

図 2 に、2009 年 10 月 10 日に MS09-050[2]を狙ったゼロデイ攻撃を受け、その後の潜伏期間を経て、様々なマルウェアに感染したシステムの実例を示す。この例では、autopsy[3]を用いて解析を行った。二つの dll ファイルと二つの exe ファイルにマルウェアが仕掛けられている。図 2 中の「作成時刻」は、実際にファイルが生成された時刻を表している。これらのファイルは、ハッカーが実行した WindowsUpdate により 2009 年 10 月 16 日 10 時台に生成された。その後、「変更時刻」の 10 月 17 日 3 時台に何らかの変更が施されていることが分かる。この時点で、何らかの悪意あるプログラムが仕掛けられている。さらに、「OS で表示」の時刻は 8 月 4 日や 8 月 27 日といった過去の時刻に改竄されたことが分かる。



DEL	Type dir / in	NAME	ACCESSED		SIZE	UID	GID	META
	d / d	migration/	2009-10-17 03:08:43 (JST)	2009-10-17 03:08:43 (JST)	2009-10-17 03:08:43 (JST)	2006-11-02 20:18:43 (JST)	56	0	0	2030-144-6
	r / r	mshtml.tlb	2009-08-27 12:41:18 (JST)	2009-10-16 10:39:52 (JST)	2009-10-17 03:08:43 (JST)	2009-10-16 10:39:52 (JST)	1638912	0	0	32547-128-4
	r / r	wininet.dll	2009-08-27 14:22:28 (JST)	2009-10-16 10:39:53 (JST)	2009-10-17 03:08:43 (JST)	2009-10-16 10:39:53 (JST)	916480	0	0	53000-128-4
	d / d	./	2009-10-17 03:08:44 (JST)	2009-10-17 03:08:44 (JST)	2009-10-17 03:08:44 (JST)	2006-11-02 20:18:36 (JST)	56	0	0	1381-144-7
	r / r	msv1_0.dll	2009-09-11 01:48:01 (JST)	2009-10-16 10:40:13 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:13 (JST)	218624	0	0	54022-128-4
	r / r	ntkrnlpa.exe	2009-08-04 21:34:19 (JST)	2009-10-16 10:40:06 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:06 (JST)	3600456	0	0	53656-128-4
	r / r	ntoskrnl.exe	2009-08-04 21:34:19 (JST)	2009-10-16 10:40:07 (JST)	2009-10-17 03:08:44 (JST)	2009-10-16 10:40:07 (JST)	3548216	0	0	53665-128-4

図 2：dll ファイルやカーネルファイルへの感染例

通常、OS でファイル一覧を見ると「OS で表示」で設定された日時が表示される。WindowsUpdate は PC ユーザではなくハッカーが行っているため、更新後の日時を表示してしまっては、感染を疑われる可能性が高くなる。そこで、このタイムスタンプの改竄を行っていると考えられる。

また、二つの exe ファイル ntkrnlpa.exe と ntsokrnl.exe は OS のカーネルそのものである。これらのファイルがマルウェアに感染した後、各種のマルウェアファイルやマルウェアの作業フォルダが OS からは表示できなくなるように rootkit が仕掛けられたと考えられる。

次に、ゼロデイ攻撃を受けた 10 月 10 日から 10 月 17 日までの間に設置または改竄されたファイルを、10 月 23 日に Virus Total[5]で検証した。Virus Total では、市販されている 41 種類のアンチウィルスを用いて検知を行う。その結果、手動による解析で、キーロガー(盗聴機能)が仕掛けられていた dll ファイルを確認したにも関わらず、ゼロデイ攻撃から 14 日が経過した段階で、41 種類中、マルウェアを検知できたものは皆無であった。

このことから分かるように、一度感染を許すと、どのファイルにマルウェアが感染したのか、そのマルウェアがどのような活動を行うのかを調べることは容易ではない。

4. 次世代のネットワーク構築

4.1 新たなマルウェア感染を想定した構築

従来用いられてきた firewall や IDS による防御手法は、このようなマルウェアの挙動変化には対応できなくなっている。特に、感染経路に Web アクセスが多用されるため、Web アクセスが可能な PC は全て、ゼロデイ攻撃によるマルウェア感染のリスクに曝されていると考えなければならない。

4.2 業務システムの機種更新

一方で、2000 年頃に導入された各種業務システムの入れ替えも始まりつつある。このとき問題となるのが、既存ソフトウェアが新システムに追従できないことである。例えば、ハードウェアの更新を行おうとすると、連鎖的に以下の問題に直面することになる。

(i) OS が新ハードウェアに非対応
(ii) サーバアプリが新 OS に非対応
(iii) クライアントソフトも更新
(iv) クライアント OS が非対応
(v) クライアントハードウェアが非対応

結果的に、サーバのハードウェア更新を切っ掛けに全システムの更新が求められることとなる。

4.3 サーバ仮想化による解決

上記の問題を解決する一つの手法として、サーバの仮想化が挙げられる。幸運なことに大抵の仮想システムでは、既存 OS が稼働可能なものが多く、かつ、ハードウェアの性能向上分を考慮すると、既存システムよりも高い処理能力が期待できる。しかし、この手法では、セキュリティ対策が見落とされやすい。仮想システムで稼働させる既存 OS は、メーカのサポートが終了している場合もある。そのため、新たなセキュリティ対策の枠組みが必要となる。

4.4 VLAN によるネットワーク分離

一つの手法として、図 3 のように、部課あるいは掛単位で VLAN に分けることが考えられる。

VLAN で分離することにより、例えば総務 VLAN でマルウェア感染が発生しても、他の部課には影響が及ばないようにできる。

また、仮想化と VLAN の親和性は非常に高く、1 筐体のサーバで複数の VLAN を収容することができる。既存 OS が tag-VLAN に対応できない場合でも、仮想システムで VLAN を受けることもできる。このことにより、ある VLAN でマルウェア感染が発生しても、他の VLAN 用のサーバへの影響も回避可能となる。

さらに、VLAN により影響範囲を絞り込むことができれば、感染 PC の特定、IPS(Intrusion Prevention System)による悪意ある通信のブロックなどの作業負荷も軽減させることが可能となる。

ただし、このためには、全ての PC について所属部課を特定し、スイッチングハブと PC の間を正しい VLAN ネットワークで配線する必要があり、そのためのコストが生じることになる。

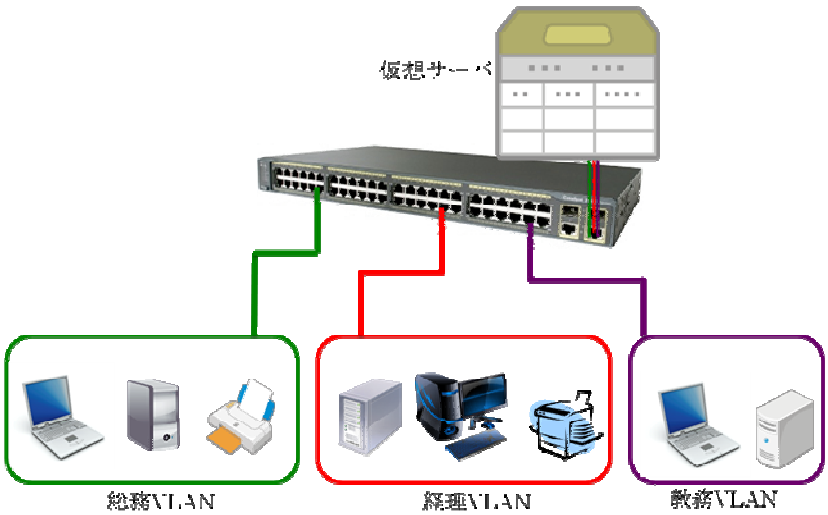


図 3：仮想サーバと VLAN によるネットワーク分離

4.5 バックアップの重要性

災害対策として、重要データのバックアップは一般的に行われている。しかし、バックアップデータの保管場所については考慮されていない場合が多い。その一因として、情報セキュリティポリシにより、重要データの保管場所の物理セキュリティレベルを厳格に定めていることが逆効果になっていることがある。大抵の場合、基準を満たす場所は、オリジナルデータが存在するサーバ室しか無い、または、バックアップデータが保管可能な場所が確保できたとしても、移送時のセキュリティが確保できないため、やむを得ずサーバの近辺にバックアップデータが保管されてしまう。

5. まとめ

本稿では、最近のマルウェア感染の実情について解説し、感染後の完全駆除の難しさについて述べた。また、新たな脅威の出現に対し、今後のネットワーク構築の際に考慮すべき課題について述べた。

当面の間はハッカー側が有利な情勢が継続すると懸念されるため、重要データのバックアップは最終手段としては重要であると考える。また、マルウェア感染によるデータ破壊だけでなく、自然災害も想定したバックアップ手法についても、今後の議論が必要になると考えている。

謝辞

本研究の成果の一部は、総務省戦略的情報通信研究開発推進制度（SCOPE、受付番号091603006）の支援を受けている。

参考文献

[1] J.Song, H.Takakura, Y.Okabe, Cooperation of Intelligent Honeypots to Detect Unknown Malicious Codes, WOMBAT Workshop on Information Security Threat Data Exchange (WISTDE 2008), pp.21-22, 2008.
[2] http://www.microsoft.com/japan/technet/security/bulletin/ms09-050.mspx
[3] http://www.sleuthkit.org/autopsy/
[4] USB Mass Storage Class – Bulk only Transport, http://www.usb.org/developers/devclass_docs/usbmassbulk_10.pdf
[5] http://www.virustotal.com/