Infection Network内での仮想インターネットの構築

Symantec Security Response
Takayoshi Nakayama

プレゼンテーション内容

- 定義ファイルができるまでに行われる解析作業
- Infection Network 内での仮想インターネットの構築
- 最近の動向

定義ファイルができるまでに行われる解析作業

ユーザーからサンプルが提出されてから定義ファイルができるまでに行われる作業の解説

- 自動解析システム
- Black box での解析
- White box での解析
- シグネチャの作成
- QA, Liveupdate の配信

自動解析システム

- ユーザーから提出されたサンプルをある程度自動的に解析する。
- 提出されるサンプルの形態は多種多様。zip や rar などで圧縮されている場合は、ファイルの展開を行う必要がある。
- サンプルが電子メールの場合は、添付ファイルを切り離す。
- 既知のサンプルは、自動的にユーザーにそのファイルがウィルスかどうか回答をする。

Black Box での解析(1)

- エンジニアによって手作業で行われる作業。
- 実際にウィルスを動かして、その動作を観察する。
- レジストリやファイルの変更をトレースするツール、アセンブラレベルのデバッガー、またネットワークアナライザなどのツールを利用する。

Black Box での解析(2)

- Black boxは手軽だがウィルスの正確な特性が分からないことが多い。
- 実行環境に依存する場合もある。
- 日付が設定されている場合もある。
- インターネットアクセスが必要な場合もある。
(解析作業は、隔離されたネットワークで行われる)
- アンチデバッキングや root kit のテクニックが施されている場合もある。

Topic: Root Kit のテクニック

- Root kit のテクニックを使い、Windows API を横取りする。
- これによりファイルやプロセスが隠匿される。
- Root Kit のテクニックが使われているとウィルスの発見が困難になる。

White box での解析

- エンジニアによって手作業で行われる作業。
- 逆アセンブルなどを行いコードを直接解析する。
- White box での解析は、ウィルスの挙動を正確に調べられるが、Black Box での解析に比べ時間が掛かる。
- 限られた時間内に解析を終える必要があるため、時間との戦いとなる。

シグネチャの作成

- ウィルスを検知するためのシグネチャ(ワクチン)を作成する。
- ウィルスの特徴的な部分をシグネチャとして定義する。
- バイナリのどこにウィルスの特徴的な部分が配置されているか探し出す必要がある。

QA, Liveupdate の配信

- QA(Quality Assurance)のテストが行われ、Intelligent Update や Liveupdate が作成される。
- 緊急度の高いウィルスが発生した場合は、QAの作業が終了後、即座に Liveupdate が配信される。(弊社基準で危険度 3以上のウィルスが発生した場合など。)

Infection Network内での仮想インターネットの構築

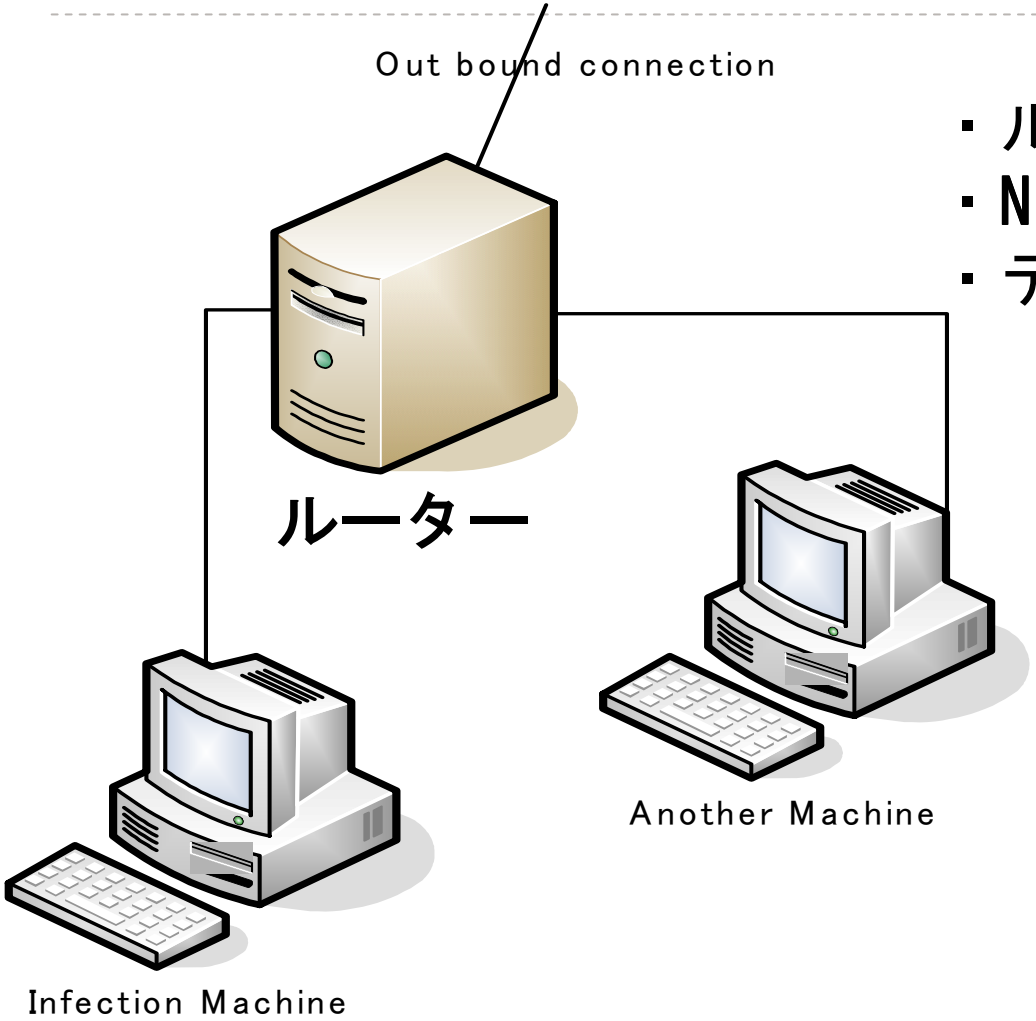
- Infection Network について
- 仮想インターネットのネットワーク
- ウィルスのタイプ別、必要となるネットワーク機能
  - Downloader の場合
  - Mass Mailer の場合
  - Network Worm の場合(Sasser や Bot系ワーム)
  - その他のネットワークサービス
- 今後の発展について

Infection Network について

- 完全に外のネットワークから隔離されたネットワーク
(ウィルスの拡散防止のため)
- 実際のインターネットとは、ほど遠いとても貧弱なネットワーク
- ウィルスを動かしても、まともに動かない。
接続先がないため、connect さえも確認できない。

それでは、Infection Network内でウィルスを動作される場合、どのようなインターネットサービスを仮想的に構築すれば、ウィルスの解析に役立つか、ウィルスのタイプ別に解説する。

仮想インターネットのネットワーク



・ルーター(Linux)
・NIC は３個用意
・テスト用のPCは２台

Downloader の場合(1)

- Downloader とは、インターネットからウィルスをダウンロードし、実行するウィルス。
- ネットワーク的な挙動としては、DNS query と HTTP アクセス。
- 隔離されたネットワークで動かす場合、まず DNS の query を解決する必要がある。
- また、IP address で直接アクセスされる場合も…。

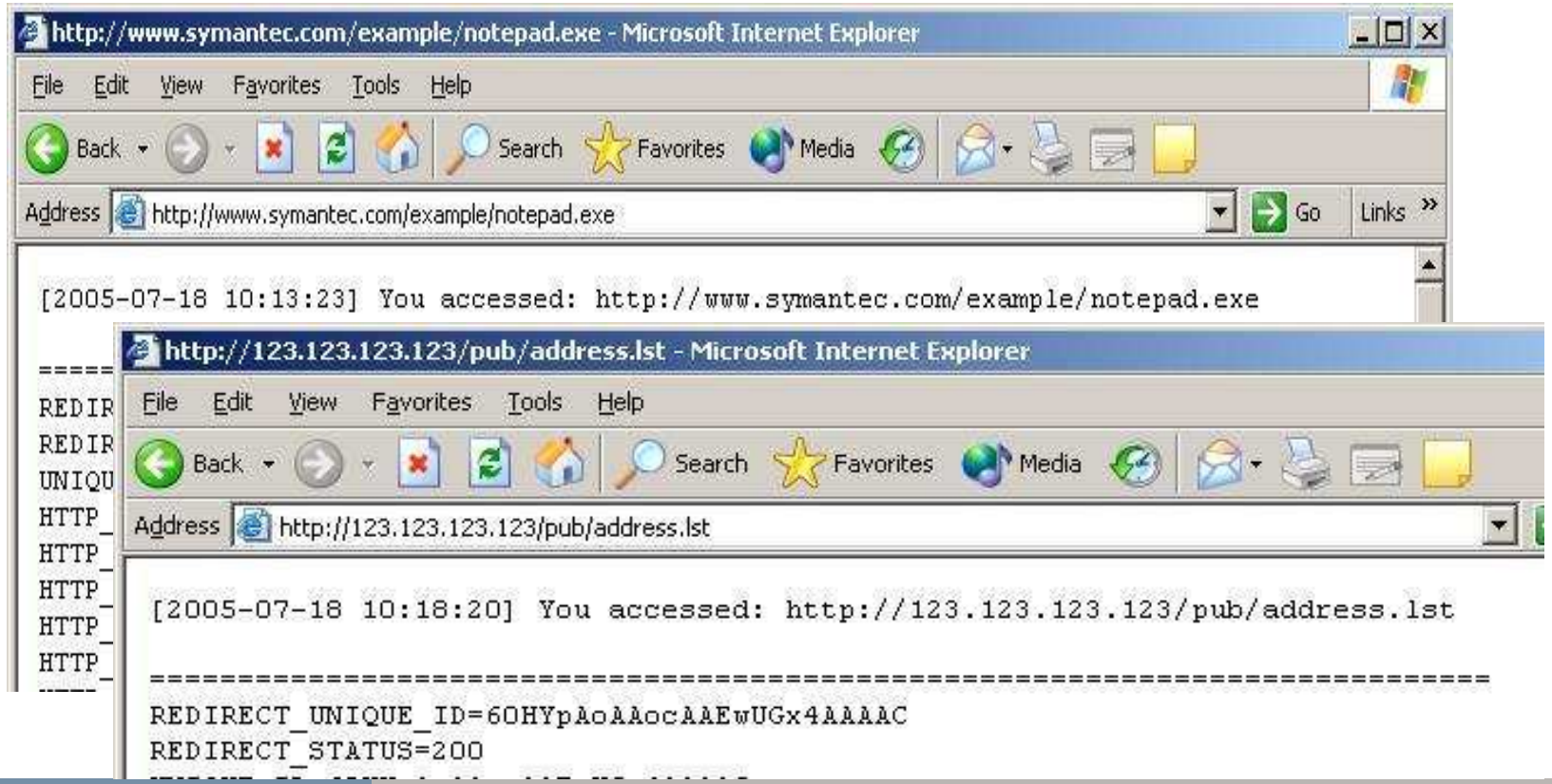
これらの問題を解決するには…。

Downloader の場合(2)

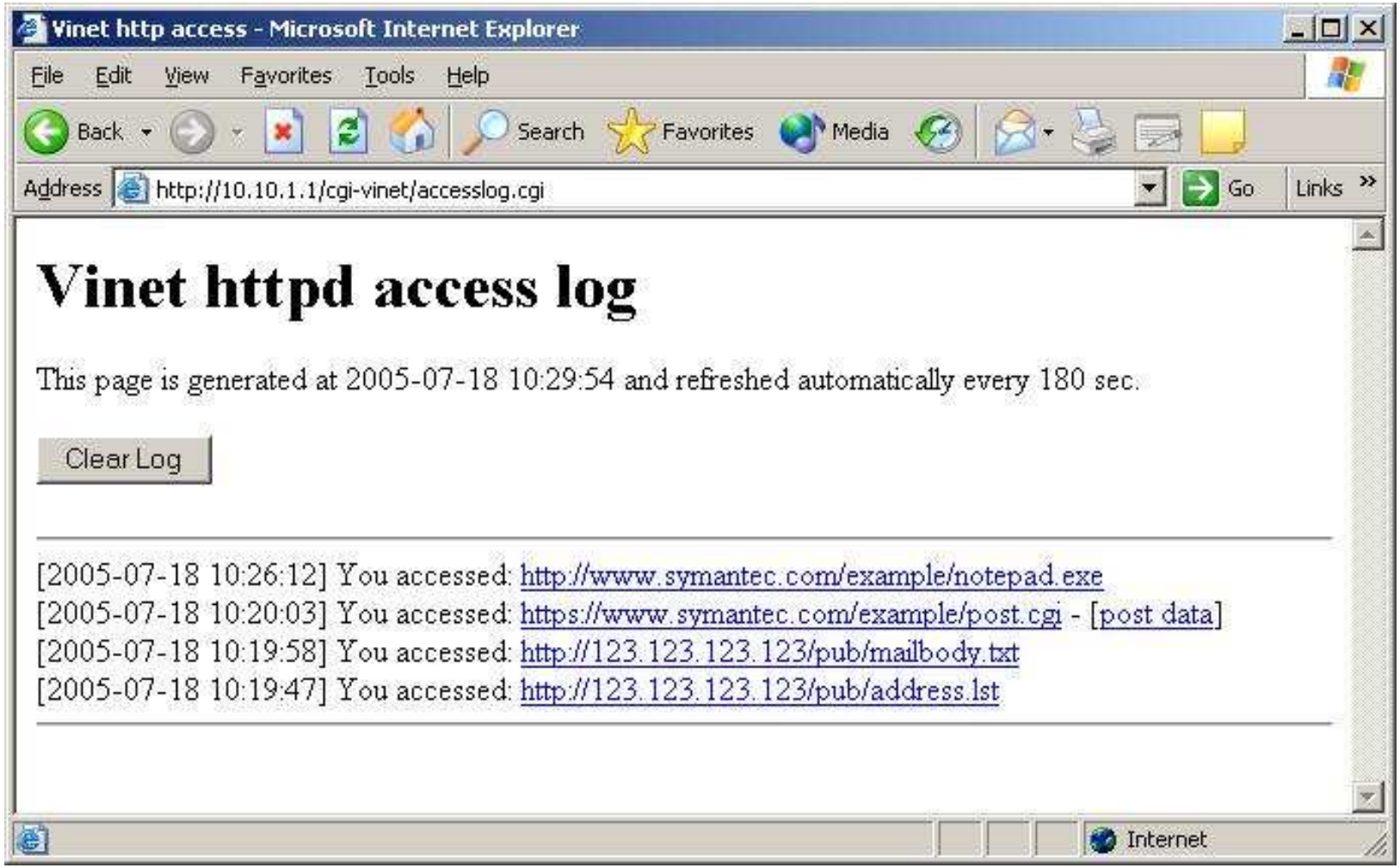
- 全ての DNS query に対してルーターのIPアドレスを返すように DNS を構築。(BIND のワイルドカードを利用)
- NAT を使い全てのパケットをルーターに転送する。これにより、直接 IP address でアクセスされた場合も接続先を確保できる。
- ルーター上で HTTP サーバを起動する。これにより、どこにアクセスされても HTTPの Connect を確立できる。
- また、HTTP でどのフォルダの、どのファイルにアクセスされてもエラーを返さないように HTTP サーバーを構築。
- 加えて、アクセス先の URL を含んだテキストを Reply するようにカスタマイズすると解析作業が容易になる。

Downloader の場合(3)

- これらの機能をルーター上に実装することで、Downloader が正常に動作し、その挙動を観察できる。



Downloader の場合(4)

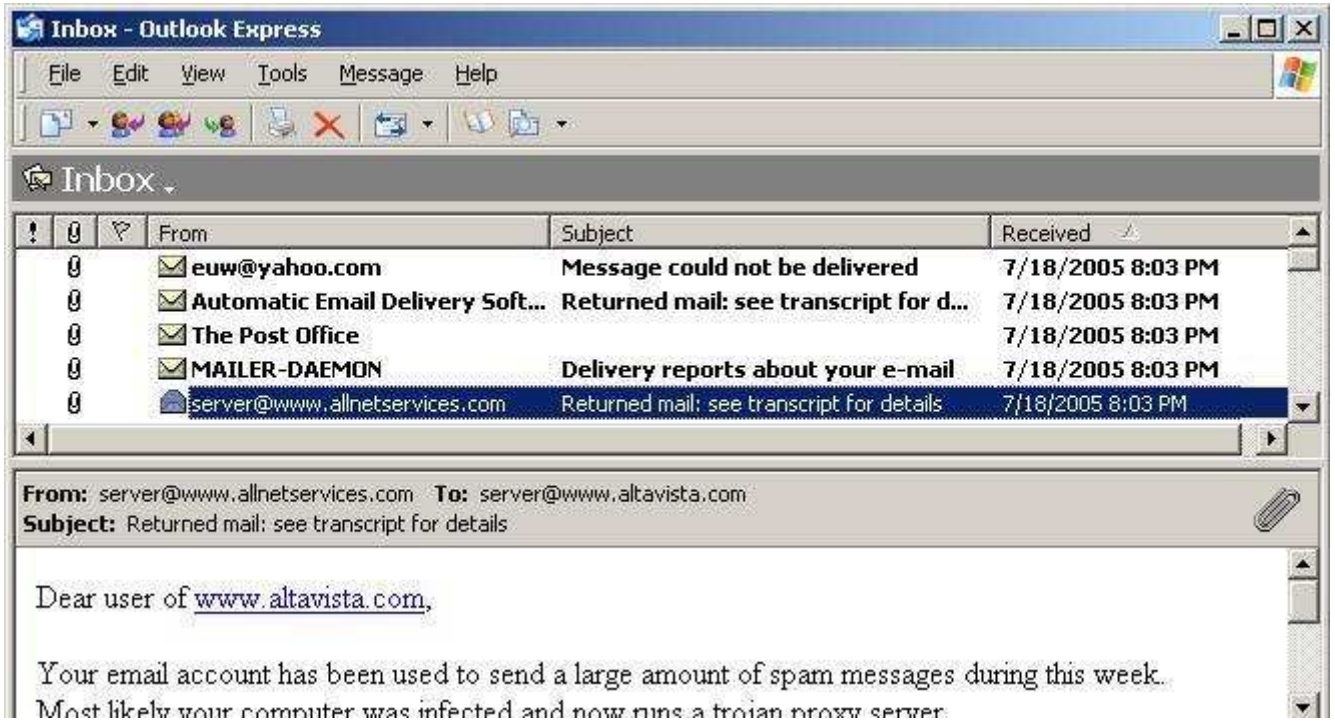


Mass Mailer の場合(1)

- Mass Mailer とは電子メールを媒体として感染を広げるウィルス。
- ネットワーク的な挙動は、DNS query と SMTP アクセス。
- DNS の解決については Downloader の場合と同じ。ただし、MX も解決する必要がある。MX もルーターのアドレスを返すように設定する。
- ルーターで SMTP サーバを動かす。
- また、全ての電子メールを受け取るため、ルーターの SMTP サーバ上で、RCPT TO をある 1つのメールアカウントに書き換える。

Mass Mailer の場合(2)

- これにより、全ての電子メールを受け取ることができる。
- 実際に Mass Mailer を動作させると一分間に何十通もの電子メールが送信されることが確認できる。

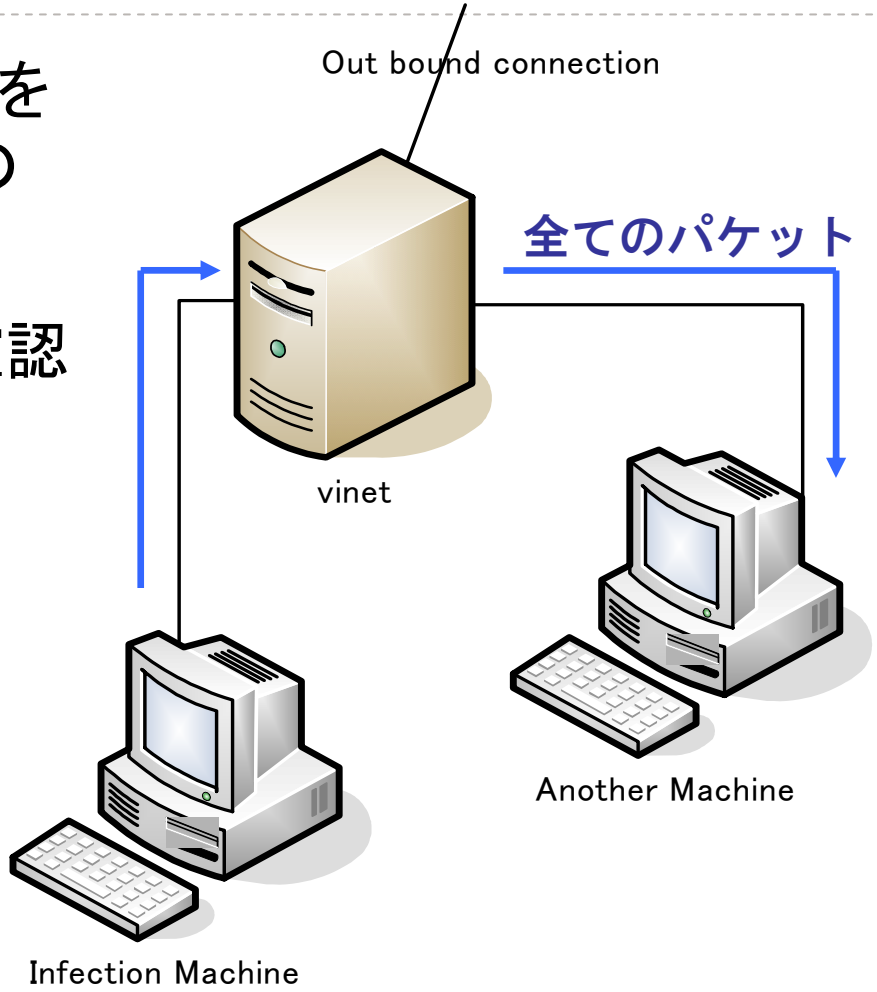


Network Worm の場合(Sasser や Bot系ワーム)

- Network Wormとは、ネットワーク経由で直接感染を広げるウィルス。
- ネットワーク的な挙動としては、ランダムに生成した IP アドレスへ exploit パケットが送信される。
- 通常のネットワークで感染活動を観察するには、とても時間が掛かる。
- また、いつ感染するか分からないのでは確実な検証が難しくなる。

Network Worm の場合(2)

- NATを使い Exploit パケットを含む全てのパケットを特定の PC にフォワードする。
- これにより、即座に感染を確認できる。



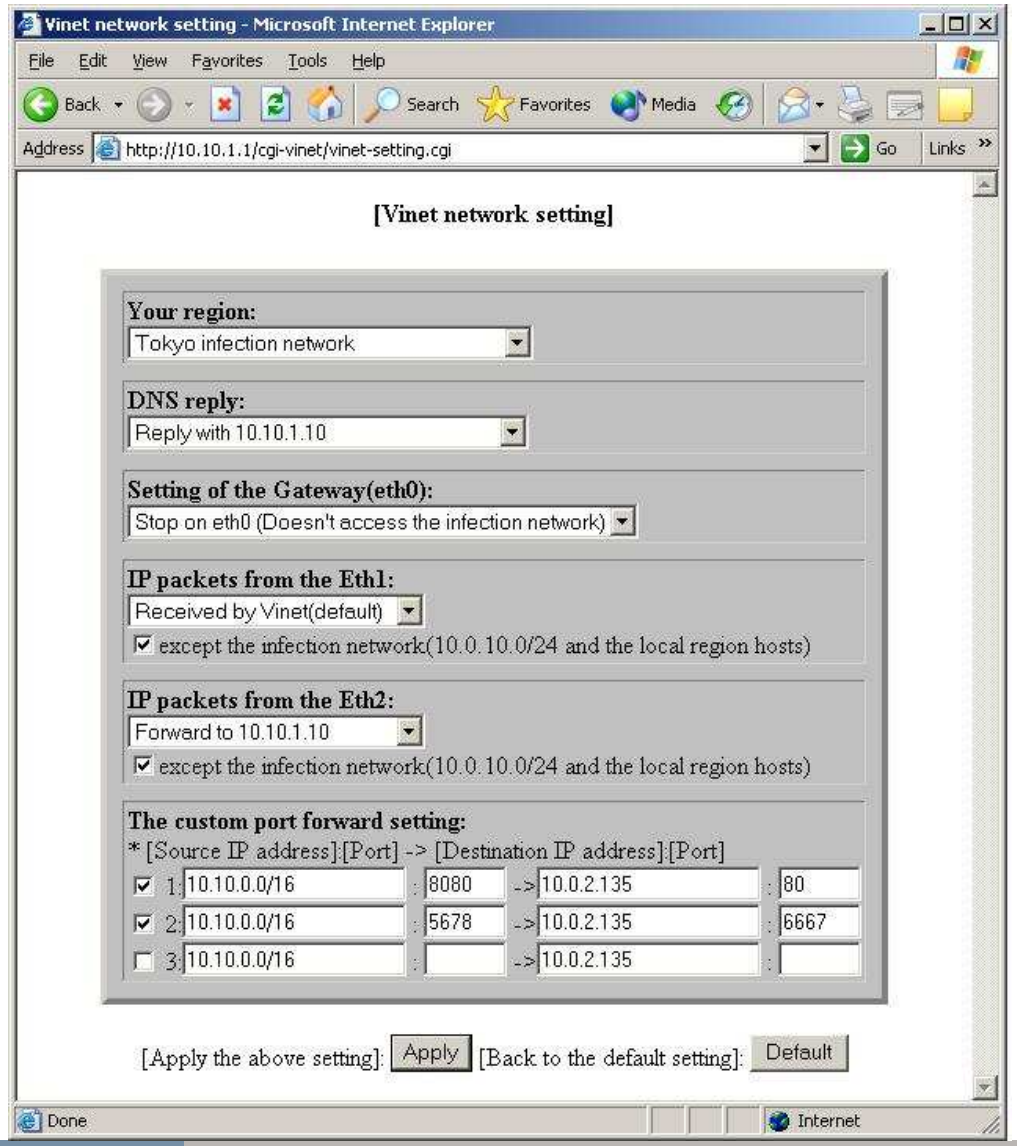
その他のネットワークサービス

- その他にも、ルーターに多くのサービスを実装。
- IRC Backdoor の観察のために IRC サーバを実装。
- NTP も実装。(Sober ワームは、NTPで時間を調べて動作する日付を特定している。)
- MSN Messenger や AOL Messenger を経由するウィルスもいるため、これらのサーバも社内で開発し実装。
- 上記のサービスを活用するためにも、前述 DNS や NAT が役立つ。
- またルーターに Snort やネットワークアナライザなどを導入することで全てのネットワークアクセスを観測できる。

今後の発展について

- ルーター上で動作させるサービスの拡充。
- FTP を使う Downloader への対応。
- アクセスログの集中的な管理。
- 自動解析システムへの組み込み。

参考: ルーターの設定画面



参考: ルーターの設定画面(拡大)

Your region:
Tokyo infection network

DNS reply:
Reply with 10.10.1.10

Setting of the Gateway(eth0):
Stop on eth0 (Doesn't access the infection network)

IP packets from the Eth1:
Received by Vinet(default)
☑ except the infection network(10.0.10.0/24 and the local region hosts)

IP packets from the Eth2:
Forward to 10.10.1.10
☑ except the infection network(10.0.10.0/24 and the local region hosts)

The custom port forward setting:
* [Source IP address]:[Port] -> [Destination IP address]:[Port]

☑ 1:	10.10.0.0/16	: 8080	->	10.0.2.135	:	80
☑ 2:	10.10.0.0/16	: 5678	->	10.0.2.135	:	6667
☐ 3:	10.10.0.0/16	:	->	10.0.2.135	:	

最近の動向(1)

- 一日平均3500件以上のサンプルがユーザーから提出されている。
- また、一日平均80件以上、新たに見つかったウィルスや Security Risk に対してシグネチャが追加されている。
- 昨年と比べると、およそ1.8倍以上に増えている。

最近の動向(2)

- Bot系ワームが更に増えている。
- Mass Mailer は相変わらず脅威。
- Mydoom に Bot機能が追加された W32.Mytob@mm の亜種が増加中。
- IMで感染するウィルスが増えてきている。
- 愉快犯的なウィルスよりも、金銭の詐取、バックドア、DoSやスパムの踏み台など実利を目的としたウィルスが多くを占める。

Infection Network内での仮想インターネットの構築

Takayoshi Nakayama
Symantec Security Response