

本格的 P2P アプリケーション時代のための (基礎知識と) ネットワーク運用技術

奈良先端科学技術大学院大学
情報科学センター
油谷 暁 (yuta@itc.naist.jp)

もくじ

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - **P2P アプリケーションのいろいろ**
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

P2P アプリケーションのいろいろ

- そもそも P2P とは？
 - 従来のサーバ・クライアント型
 - 召使い vs. ご主人
 - 新しい Peer to Peer 型
 - 対等な、お友達同士
- P2P にすると？
 - 耐故障性
 - 資源の分散
 - スケーラビリティ
 - 中心がなく全体がわからない
 - 自由な参加、離脱

P2P アプリケーションのいろいろ

- 第一世代 (ハイブリッド型)
 - Napster (MP3 専用、サーバーにインデックス)
 - WinMX (OpenNap, Napster のプロトコルを継承)
- 第二世代 (ピュア型)
 - Gnutella (センターサーバが無い)
- 第三世代
 - Winny (本来の P2P, 高い匿名性)
- 成功した? P2P
 - BitTorrent (合法的な大容量ファイル配布に最適)
 - Skype
 - Napster 復活 ?

P2P アプリケーションのいろいろ

- P2P ファイル分散共有
 - 第一世代
 - Index とデータの分離
 - 第二世代
 - データと帯域の分離
 - 第三世代
 - データと場所を分離
 - キャッシュ、転送 (中継)
 - ファイルの保有、送信、受信の匿名性を実現

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - **オーバーレイネットワーク**
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

オーバーレイネットワーク

- IP ネットワーク
 - 組織毎のネットワークの相互接続
- オーバレイネットワーク
 - アプリケーションの目的に応じて構成
 - サービスオリエンテッド
 - もちろん IP ネットワーク上に論理的に構成
 - 例：skype, メッセンジャー

オーバーレイネットワーク

□ P2P システムの基本要素

- 共通要素
 - ピアの発見
 - ピアグループへの参加
 - データの検索、広告
 - ピア同士の通信
 - ピアの監視
- サービス毎に異なる機能

オーバーレイネットワーク

□ 一般的に言えること

- トランスペアレンシー
 - 物理的ネットワークはほとんど気にしなくて良い
- ある目的を達成しやすい
- 管理が楽
 - ゲートウェイモデルは苦勞する
 - 自由なネットワークポロジ

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - **成功例 ? BitTorrent**
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線: では、実際に見てみましょう
- まとめ

成功例 ? BitTorrent

- BitTorrent の新しい取り組み
 - 違法データからの脱却
 - 検索できない
 - 欲しいデータのみ、決めうちダウンロード
 - 配布方法は Web に .torrent ファイル
 - 基本は Web サーバから始まる
 - データは torrent 網に自ら泳がせる
 - 匿名保持の機構がない
 - キラーコンテンツが見えたら負け ?
 - 著作権物、アダルト ...

成功例 ? BitTorrent

□ BitTorrent の仲間

■ クライアントソフト

- BitTorrent
 - 元祖、シンプルです
- BitComet
 - 一番のはやり
- Azureus
 - Linux, OSX 等で動作 (java)
- などなど、多数存在

成功例 ? BitTorrent

□ BitTorrent 対応ブラウザ

■ やっぱりブラウザで

- Opera (Ver. 9)
- Firefox (MozTorrent PlugIn 開発中)

成功例 ? BitTorrent

□ BitTorrent の仕組み

■ おきて

- ファイルの一部を受け取るには自分もファイルの一部を渡さなければいけない
 - 誰でも必ずファイル配布に協力する
 - 人気のあるファイルほどたくさんの人が協力する

- ポートの開放 (6881 番)

■ 大量のピアと少量のデータを扱う

- 結果、超高速の転送速度
- ルーターへの負担大 ?

成功例 ? BitTorrent

□ BitTorrent の仕組み (cont'd)

■ ダウンロードの仕組み

- まずは .torrent ファイル
 - ファイル情報やトラッカーのアドレスが明記
- トラッカー
 - ファイルの持ち主 (ピア) の情報 (IP) を教えてくれる
- ピア
 - ファイル共有に参加しているコンピュータのこと
 - ピアは定期的にトラッカーと情報交換
- シェアレシオ
 - Up/Down 量の比率、基本的に 1:1 に達するまで共有すべきとされる

成功例？ BitTorrent

□ BitTorrent の仕組み (cont'd)

- アップロードの仕組み
 - まずは .torrent ファイル
 - ツールを使用して作成
 - あるトラッカーに情報を登録
 - シーダーの開始
 - 全てのデータをもっている
 - ダウンロードが 100% のクライアントはシーダーに昇格
 - Web サーバ等に .torrent ファイルを公開
 - ダウンロードが繰り返されると torrent 網がどんどん形成される

成功例？ BitTorrent

□ BitTorrent は最近の流行

- こんなことに使ってます
 - 著作権のない大容量ファイル
 - OS (Linux 等) の配布
 - FedoraCore, CentOS
 - ソフトウェアの配布
 - Mozilla, OpenOffice.org
 - そろそろ「違法データ交換ソフト」から卒業させよう
 - 合法、違法データの混在が問題
 - 検索機能が悪

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - **情報漏洩対策**
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

情報漏洩対策

- そもそも情報漏洩とは
 - Winny の使用時に紛れているウイルスが問題
 - Antinny, 山田オルタナティブ、亜種
 - 暴露ウイルス感染が原因
 - Winny の使用そのものには問題は無い
 - 著作権が存在する物のやり取りはやはり違法
 - 実際は、ほとんどのファイルが違法かもしれません

情報漏洩対策

- 漏洩対策の基本
 - Winny を使うな、持ち込むな !!
- とは言っても。
 - ウイルス、スパイウェア対策ソフトの導入
 - 組織内での Winny 使用禁止
 - 無許可のアプリケーションの起動禁止 (強制もあり)
 - 私用 PC の接続禁止
 - 最低でもセキュリティポリシーをクリアしているかを確認
 - データのコピー禁止 (USB メモリ、その他記憶媒体)
 - 通信経路の常時モニタリング

情報漏洩対策

- 実は、Winny 以外にも ...
 - Share (シェア) に注意
 - 日本製
 - シェアとは読まない (今は読んでみたいです)
 - Winny 同様の ファイル交換ソフト
 - Share にも感染する Antinny の亜種が出現中
 - 同様の情報流出の危険あり
 - ウイルス検出ソフトで検出可能

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？BitTorrent
 - 情報漏洩対策
- 運用技術
 - **運用ポリシーについて**
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

運用ポリシーについて

- 組織（企業や学校）のネットワーク
 - 組織特有の様々なルールが存在
- 守らねばならないもの
 - 情報 → 信用
- もし、守れなければ
 - 情報漏えい等、一回の失態で確実に信用を失う
 - イメージダウン
 - 信用回復には相当の時間とお金がかかる
 - 企業や学校の存続が難しくなるかも

運用ポリシーについて (cont'd)

- 組織の運用ポリシー
 - 外側と内側が存在
 - 守るべきものが存在
 - 守りすぎても使いにくい
 - 運用ポリシーで組織のルールを決定
 - 住人の住み心地を決定
- 組織の管理者のスキル
 - 管理者のスキルでも住み心地は変わる

運用ポリシーについて (cont'd)

- 例えば大学という組織
 - 自由な研究の場を提供
 - 研究と言う名を借りてさまざまなリクエストが存在
 - ファイアウォールが存在しない大学もある(らしい)
 - 研究の中には 危ない研究 ? も存在
 - P2P の研究
 - Full HD 動画の転送実験
 - 特殊な研究 (番外編)
 - 大量な遺伝子情報
 - 分子解析

運用ポリシーについて (cont'd)

□ ある大学のポリシー

■ 学内ポリシー

- どんなことでも出来る、が目標
 - 出来るべきことは出来ます
- でも、守るべき情報はしっかり守る
- どこからどこを守るべきか

■ 最近の気持ち

- 以前は、学内に悪いやつはいない！
- 最近は、学内にも相当悪いやつがいる？

運用ポリシーについて (cont'd)

□ ある大学のポリシー (cont'd)

■ 具体的には

- ファイアウォールを設置
 - 学内はファイアウォールで確実に守る
 - 学外からのアクセスが必要なサーバは外側に設置
 - 踏み台防止のため、一定期間で脆弱性のチェック
- 個別の穴あけは基本的には行なわない
- 学外サテライトオフィスは VPN で学内を延長

運用ポリシーについて (cont'd)

□ ある大学のポリシー (cont'd)

■ P2P に関して

- skype はとりあえず使用可
- Winny は全面禁止
- その他のファイル交換系ソフト
 - 基本的に使用可能
 - ただし ...
 - 交換したファイルの著作権等が大問題
 - 実際、ほとんどソフトはほとんど NG な感じ
 - skype を除き使用には申請が必要になる予定

運用ポリシーについて (cont'd)

□ ある大学のポリシー (cont'd)

■ P2P 発見時の対応

- 違法性の判断
 - パケット等の分析 (何処から何処にどの位)
 - 著作権等に引っかかっているかチェック
 - 実際に PC を検閲
 - 指導教官に説明の上、立ち会っていただき実施
- 場合によりアカウント剥奪等の処分あり
 - 初犯は誓約書、二回目は剥奪の可能性
- 経験的には
 - BitTorrent のみ グレー、その他は ...

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - **通信状態の把握**
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

通信状態の把握

- 既存の技術
 - MRTG (Multi Router Traffic Grapher)
 - SNMP でネットワークの負荷を監視するツール
 - tcpdump
 - パケットをダンプするツール
 - NetFlow
 - 主に Cisco ルータに実装されている
 - ヘッダ情報の一部を提供
 - sFlow
 - サンプリングしてそのままのデータを提供

通信状態の把握 (cont'd)

□ sFlow データを利用した検出

- 10ヶ所以上の所から大量のダウンロードを行なっている

Daily Report of Suspected p2p traffic 2005/12/08 00:00:00 - 2005/12/09 00:00:00
THIS REPORT MAY CONTAIN FALSE POSITIVES!

--- down traffic(top or udp, except well-known ports, num_of_uniq_srcaddrs > 10) ---

dst_addr	fqdn_dst_addr	first_time	last_time	num_of_captured_flows	total_bytes	num_of_uniq_srcaddrs
163.221.156.XXX		2005-12-08 00:16:54	2005-12-08 23:59:08	944	1570404	26
163.221.170.XX		2005-12-08 00:02:54	2005-12-08 23:59:08	217	386790	12
163.221.146.XX		2005-12-08 12:57:02	2005-12-08 20:32:06	127	270591	18
163.221.183.XX		2005-12-08 06:11:58	2005-12-08 23:59:08	112	260062	12
163.221.130.XXX		2005-12-08 00:41:54	2005-12-08 12:11:01	410	103424	21
163.221.250.XX		2005-12-08 14:09:03	2005-12-08 22:37:08	40	58972	28
163.221.238.XX		2005-12-08 00:01:54	2005-12-08 23:19:08	62	56994	18
163.221.157.XX		2005-12-08 01:08:55	2005-12-08 17:05:04	311	26405	86
163.221.157.XXX		2005-12-08 00:58:55	2005-12-08 20:25:06	15	20196	14
163.221.139.XX		2005-12-08 00:37:54	2005-12-08 22:14:07	38	17321	18
163.221.52.XXX		2005-12-08 19:53:06	2005-12-08 22:02:07	96	11418	11
163.221.130.XXX		2005-12-08 19:45:06	2005-12-08 22:33:08	108	9625	15
163.221.130.XXX		2005-12-08 00:08:54	2005-12-08 22:08:07	14	2256	11
163.221.170.XX		2005-12-08 00:15:54	2005-12-08 23:54:08	17	1049	17
163.221.52.XXX		2005-12-08 01:51:55	2005-12-08 23:48:08	14	1013	12
163.221.246.XX		2005-12-08 11:05:01	2005-12-08 23:40:08	22	1010	22

通信状態の把握 (cont'd)

□ sFlow データを利用した検出 (cont'd)

- BitTorrent のポートを使用

--- down traffic(BitTorrent(6881-6889/top)) ---

dst_addr	fqdn_dst_addr	first_time	last_time	num_of_captured_flows	total_bytes	num_of_uniq_srcaddrs
163.221.158.XXX		2005-12-08 20:14:06	2005-12-08 20:14:06	3	1982	3

- 1日に1GB以上のダウンロード

--- mass downloading hosts (>1GB/day) ---

dst_addr	fqdn_dst_addr	first_time	last_time	num_of_captured_flows	total_bytes	num_of_uniq_srcaddrs
163.221.44.XX		2005-12-08 02:28:55	2005-12-08 23:59:08	2834	21181308	2
163.221.157.XXX		2005-12-08 00:00:54	2005-12-08 23:59:08	2794	15342698	13
163.221.139.XX		2005-12-08 00:00:54	2005-12-08 23:45:08	1665	4155397	14
163.221.156.XX		2005-12-08 00:00:54	2005-12-08 23:59:08	1501	3933945	31
163.221.158.XX		2005-12-08 00:59:55	2005-12-08 22:04:07	1316	3143420	2
163.221.157.XX		2005-12-08 00:59:55	2005-12-08 07:25:59	239	2631520	38
163.221.157.XX		2005-12-08 00:48:54	2005-12-08 23:21:08	80	2174655	18
163.221.126.XXX		2005-12-08 00:00:54	2005-12-08 23:59:08	640	1988602	17
163.221.247.XXX		2005-12-08 12:00:01	2005-12-08 15:05:03	171	1846124	15
163.221.156.XXX		2005-12-08 00:01:54	2005-12-08 23:59:08	1046	1806954	50
163.221.157.XXX		2005-12-08 00:11:54	2005-12-08 23:52:08	740	1769744	45
163.221.38.XX		2005-12-08 00:03:54	2005-12-08 23:59:08	1182	1322428	126
163.221.157.XXX		2005-12-08 00:01:54	2005-12-08 23:59:08	226	1154441	79

通信状態の把握 (cont'd)

□ 侵入検知場所

■ IDS (Intrusion Detection System)

- 侵入検知
- 不正行為を検出し、通知するためのシステム
 - 検出後、メール等で通知

■ IPS (Intrusion Prevention System)

- 侵入防御
- 不正行為を検出し、防御するためのシステム
 - 不正な通信を止める

通信状態の把握 (cont'd)

□ 侵入検知手法

- 全てのパケットをモニタリング
 - サンプリングより高精度
- リアルタイムでパケットを分析
- 必要に応じて積極的に行動を起こす
 - TCP Reset (IDS)
 - Block Attack (Drop Packets) (IPS)

通信状態の把握 (cont'd)

□ パケットの分析方法

■ シグネチャ型

- パケットの特徴を記述、マッチングを行なう
- 実際に照らし合わせて検出

■ アノマリ型

- 管理者が正常状態 (閾値) を定義
- 定義した閾値を超えると警告
 - たとえば、通信量などを定義

通信状態の把握 (cont'd)

□ 検出場所

- ファイアウォールルータの横で IDS
 - フィルタ後の全てのトラフィックを計測

□ 実際のパケットの流れ

- ルータのスパンポートから全てのパケットをゲット
- 実際には application switch (L7) で制御
 - 付加分散、検出したいパケットの選別
- 実は、もうすぐ溢れそうです ...

通信状態の把握 (cont'd)

- 現在、運用管理コストがとても大きい
 - Manual から Automatic にしたい
 - 最低でも Semi-Automatic に
- Automatic の方法案
 - IPS の運用体制の確立
 - IDS とファイアウォールの連携
 - 通信のリセット、ブロック
 - ルータにコンフィグの自動流し込み
- 学内では啓蒙活動が一番効果があるかも
 - 最近、P2P の使用はほとんどなくなりました
 - skype については、トラフィック量の測定が課題に

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - **Winny 対策**
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

Winny 対策

- 検出対象
 - Winny 本体
 - 暴露ウイルス
- 検出方法
 1. PC 内でチェック
 - 検出が確実、手間と時間がかかる
 2. ネットワーク越しに PC をチェック
 - 使用中、発症中でないと検出できない
 3. トラフィックを監視して PC を検出
 - 比較的、簡単に検出

Winny 対策 (cont'd)

1. PC 内でチェック
 - 一般的なウイルス対策ソフトで暴露ウイルスをチェック
 - 各社、Winny 対策用のバージョンが出揃う
 - Winny 検索専用ソフトを利用
 - Symantec
 - Winny 検索ツール
 - W32.Antinny 駆除ツール
 - アンラボ (ahnlab)
 - ウィニーワクチン
 - ウィニーシールド

Winny 対策 (cont'd)

2. ネットワーク越しに PC をチェック

- 脆弱性チェックの付加機能
- 基本はポートスキャン
- 専用ツール
 - symantec
 - セキュリティチェック
 - 住商情報システム (株)
 - eEye Winny Scanner
 - eEye Digital Security Products 社製
- ウイルス対策ソフトに邪魔される可能性が大

Winny 対策 (cont'd)

3. トラフィックを監視して PC を検出

- IDS, IPS 製品
 - 各社、対応始まる
 - McAfee
 - IntruShield
- 専用ツール
 - 住商情報システム (株)
 - eEye Winny Monitor
 - eEye Digital Security Products 社製

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - **IDS 達を少し紹介**
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう
- まとめ

IDS 達を少し御紹介

- 本学で現在採用中の IDS 達
 - McAfee IntruShield (有償)
 - eEye Winny Monitor (無償、住商情報システムより配布)
 - Snort + SnortSnarf (無償)
 - sFlow (無償、現在休止中)

McAfee IntruShield (Console)

□ 数ヶ月前まで ...

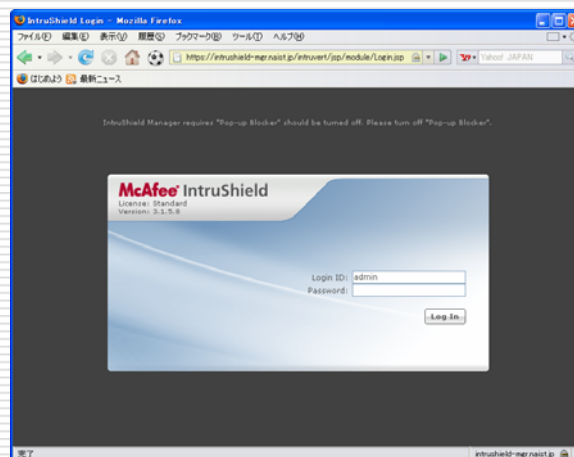


Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

47

McAfee IntruShield (Login)

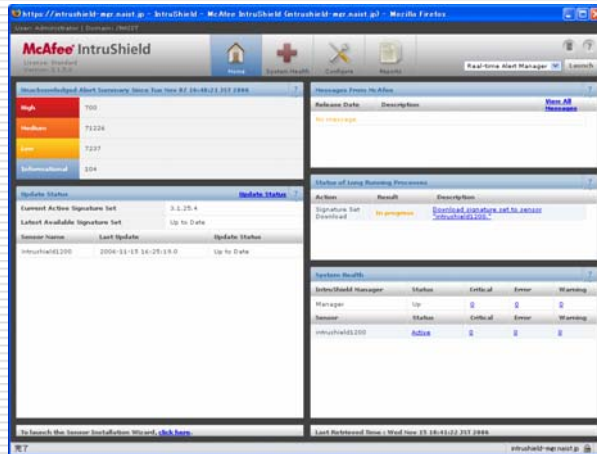


Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

48

McAfee IntruShield (Console)



Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

49

McAfee IntruShield (Alert Manager)



Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

50

McAfee IntruShield (P2P Policy)

Configure Attack Detail for Attack Gateway: p2p

View Option	View Edit	Enable Attack	Disable Attack	Full Edit						
Atta...	Alert...	Attack Name	Attack ID	Severity	Cust...	Pac...	Sen...	Block	# of ...	Noti...
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ISS_FAM_JCO Module Buffer Overflow	0x40015700	5 (High)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Appear Traffic Detected	0x42033000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_BearShare Alive	0x42007000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_BitTorrent File Transfer HandShaking	0x40e06000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_BitTorrent Meta-Info Retrieving	0x42020000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Onutelus Alive	0x42005000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Onutelus Connected to Server	0x40e01000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Onutelus File Transferring	0x42004000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Onutelus Alive	0x42006000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Orzone Virtual Office Orzone Net Age...	0x42027000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_KaZaA Client Connected to Server	0x42002000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_KaZaA Client Connecting to Server	0x40015100	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_KaZaA File Transferring	0x42003000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_LimeWire Alive	0x42008000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_MOE File Transferring	0x42034000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Marcillo Protocol File Search Detected	0x42003200	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Morphous Alive	0x42006600	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Mudita Alive	0x42028000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Phex Alive	0x42000000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Slope Login Process Detected	0x42026000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Slope Version Check Detected	0x4202a000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_SolRiser Alive	0x4201e000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_SoulSeek Alive	0x42025000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Swapper Alive	0x42009000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_WinMX File Transferring	0x42014000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_Winny Traffic Detected	0x42025000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_XosRo Alive	0x4200a000	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_eDonkey Client Connecting to Server	0x40015300	5 (Medium)					0	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	P2P_eDonkey File Transferring	0x42013000	5 (Medium)					0	

Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

51

McAfee IntruShield (Winny)

Alert Viewer - Intrushield-mgr.nast.jp | Monitored Domain: /NAST

All Alerts - All Alerts/Attack-P2P: Winny Traffic Detected

Time	Attack	Source IP	Src. Port	Destin. IP	Da. Port	Sen. ID	Applic.	Attac.
2006-04-20 15:39	P2P Winny Traffic Detected	163.221.16	182243	244.15	28491	ANAIST	intrush.1B	----
2006-04-20 15:37	P2P Winny Traffic Detected	163.221.16	1793220	217.7	21287	ANAIST	intrush.1B	----
2006-04-20 15:36	P2P Winny Traffic Detected	163.221.16	177461	210.77	6699	ANAIST	intrush.1B	----
2006-04-20 15:35	P2P Winny Traffic Detected	163.221.16	1763220	210.1	11569	ANAIST	intrush.1A	----
2006-04-20 15:34	P2P Winny Traffic Detected	163.221.16	1752	80.42.51	2424	ANAIST	intrush.1A	----
2006-04-20 15:34	P2P Winny Traffic Detected	163.221.16	1748219	86.20	3410	ANAIST	intrush.1B	----
2006-04-20 15:33	P2P Winny Traffic Detected	163.221.16	1737221	90.38	19942	ANAIST	intrush.1A	----
2006-04-20 15:30	P2P Winny Traffic Detected	163.221.16	1702219	126.1	16750	ANAIST	intrush.1B	----
2006-04-20 15:28	P2P Winny Traffic Detected	163.221.16	168480	238.16	27887	ANAIST	intrush.1B	----
2006-04-20 15:29	P2P Winny Traffic Detected	163.221.16	16880	66.167	7743	ANAIST	intrush.1A	----
2006-04-20 15:28	P2P Winny Traffic Detected	163.221.16	1681219	61.30	6219	ANAIST	intrush.1B	----
2006-04-20 15:29	P2P Winny Traffic Detected	163.221.16	1678220	48.70	51298	ANAIST	intrush.1A	----
2006-04-20 15:28	P2P Winny Traffic Detected	163.221.16	1668	21.8.97	29180	ANAIST	intrush.1B	----
2006-04-20 15:27	P2P Winny Traffic Detected	163.221.16	1649219	127.2	6549	ANAIST	intrush.1B	----
2006-04-20 15:27	P2P Winny Traffic Detected	163.221.16	1638219	124.1	32088	ANAIST	intrush.1A	----
2006-04-20 15:26	P2P Winny Traffic Detected	163.221.16	163158	190.44	8948	ANAIST	intrush.1B	----
2006-04-20 15:26	P2P Winny Traffic Detected	163.221.16	1627222	15.15	19208	ANAIST	intrush.1B	----
2006-04-20 15:26	P2P Winny Traffic Detected	163.221.16	1620210	139.2	13148	ANAIST	intrush.1A	----
2006-04-20 15:24	P2P Winny Traffic Detected	163.221.16	1617	50.70.38	9102	ANAIST	intrush.1A	----
2006-04-20 15:24	P2P Winny Traffic Detected	163.221.16	1615	124.84.1	30206	ANAIST	intrush.1A	----
2006-04-20 15:23	P2P Winny Traffic Detected	163.221.16	1608125	192.6	13621	ANAIST	intrush.1A	----
2006-04-20 15:21	P2P Winny Traffic Detected	163.221.16	1593124	18.14	24368	ANAIST	intrush.1B	----
2006-04-20 15:20	P2P Winny Traffic Detected	163.221.16	1584221	188.1	14057	ANAIST	intrush.1B	----
2006-04-20 15:18	P2P Winny Traffic Detected	163.221.16	157858	92.241	28800	ANAIST	intrush.1B	----
2006-04-20 15:18	P2P Winny Traffic Detected	163.221.16	1576	50.70.2	22058	ANAIST	intrush.1A	----
2006-04-20 15:17	P2P Winny Traffic Detected	163.221.16	1571210	191.1	7742	ANAIST	intrush.1B	----
2006-04-20 15:17	P2P Winny Traffic Detected	163.221.16	1565222	225.1	8843	ANAIST	intrush.1A	----

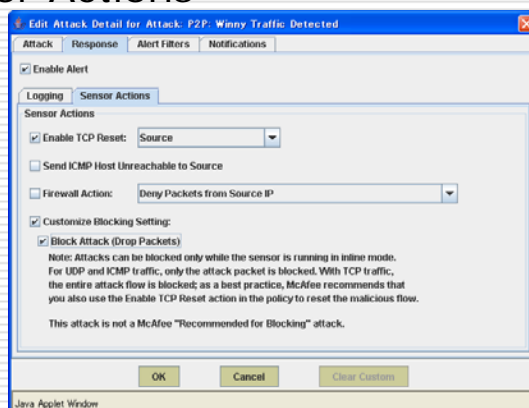
Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

52

McAfee IntruShield (Response)

□ Sensor Actions



Internet Week 2006

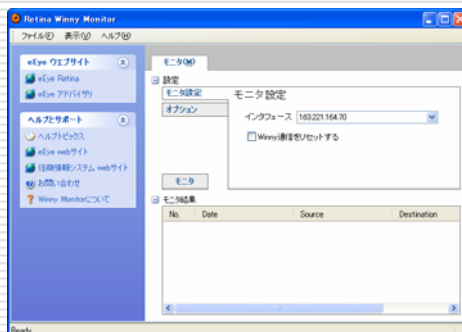
本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

53

eEye Winny Monitor

□ 住商情報システム (株) より提供

■ eEye Digital Security 社 開発

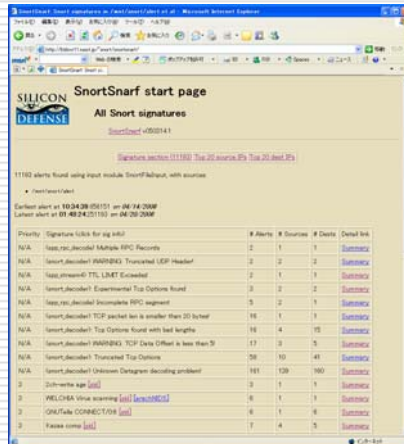


Internet Week 2006

本格的P2Pアプリケーション時代のための
基礎知識とネットワーク運用技術

54

Snort + SnortSnarf



P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - **IDS で行なっていること**
 - 脱線：では、実際に見てみましょう
- まとめ

IDS で行なっていること

- 様々なアタックの検出
 - Worm Virus
 - Bagle, LovGate, MyDoom, NetSky, Sober ...
 - BOT (← RoBOT)
 - SDBot, SpyBot ...
 - BackDoor
 - Back Orifice Trojan ...
 - PUP (Potentially Unwanted Programs)
 - Adware-gain, Adware-MySearch, Hotbar ...

IDS で行なっていること (cont'd)

- 怪しい HTTP, SMTP 等のデータを利用
 - ここで言う怪しいデータとは
 - 80 番ポートに HTTP 以外を喋る
 - 25 番ポートに SMTP 以外を喋る
 - 一瞬で数十台のマシンの 80 or 25 番ポートと喋る
 - ずっと、喋り続ける
 - PUP の行動パターンにも似ている

IDS で行なっていること (cont'd)

- 怪しい HTTP, SMTP 等のデータを利用
 - こんな風にデータを加工をすると
 - Src IP で sort
 - Dest port で sort
 - Dest port 80 (8000, 8080) & 25 付近に注目

IDS で行なっていること (cont'd)

- 怪しい HTTP, SMTP 等のデータを利用
 - こんなことが見えてきます
 - 特定 IP からの異常な HTTP or SMTP 接続
 - 何らかの個人情報が送られている可能性大
 - アクセスした Web ページの履歴 ...
 - PC でのキーストローク等、個人情報 ...
 - HTTP の場合: 検出できなかった P2P の可能性大
 - SMTP の場合: SPAM の発信元になっている可能性大
 - たぶん P2P 中か Virus 感染中の模様です

IDS で行なっていること (cont'd)

□ 最近厄介な BOT

- 用意されているシグネチャに引っかからない時
 - IRC activity アラートをチェック
 - チャットサーバから命令を受けている
 - やらかすこと
 - 大量の SPAM メール
 - hostsweep (あな探し)
 - 同じチャットサーバに接続しているものを一網打尽

IDS で行なっていること (cont'd)

□ こんなものも見えます

- skype (LogonProcess, VersionCheck)
- 検索エンジンからの Robots.txt
 - かなりの勢いで飛んできます
- HTTP ポートを使用した MediaTunnel
 - 接続先は Real, MSN, Asahi ...
- メッセンジャの alive (MSN, Yahoo!, AOL)
- hostsweep, portscan
- IPv6 over IPv4 tunneling

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - **脱線：では、実際に見てみましょう**
- まとめ

脱線：では、実際に見てみましょう

- McAfee IntruShield
 - 環境
 - ある大学の現在の状況
 - 接続
 - VPN (OpenVPN or L2TP) 経由で接続
 - デモ内容
 - 状況を見ながら考えます
 - 得られた情報
 - 部屋を退出したと同時に忘れてください !!

P2P アプリケーション時代のための運用技術

- P2P アプリケーションの現状
 - P2P アプリケーションのいろいろ
 - オーバレイネットワーク
 - 成功例？ BitTorrent
 - 情報漏洩対策
- 運用技術
 - 運用ポリシーについて
 - 通信状態の把握
 - Winny 対策
- IDS
 - IDS 達を少し紹介
 - IDS で行なっていること
 - 脱線：では、実際に見てみましょう

□ まとめ

まとめ

- いろいろ言いましたが ...
 - P2P アプリケーションは悪くない
 - Winny だけが特に悪いわけではない (はず)
 - P2P で交換するファイルは怪しいものが多い
 - P2P はファイル交換が全てじゃない !!
 - ほんとに良い技術は正しくドンドン使おう !!
- 普及!! or 不朽!!! or 腐朽!?
 - 後世まで残ってほしいです !!!!!