ボットネットに見る脅威の変化と今後の対応

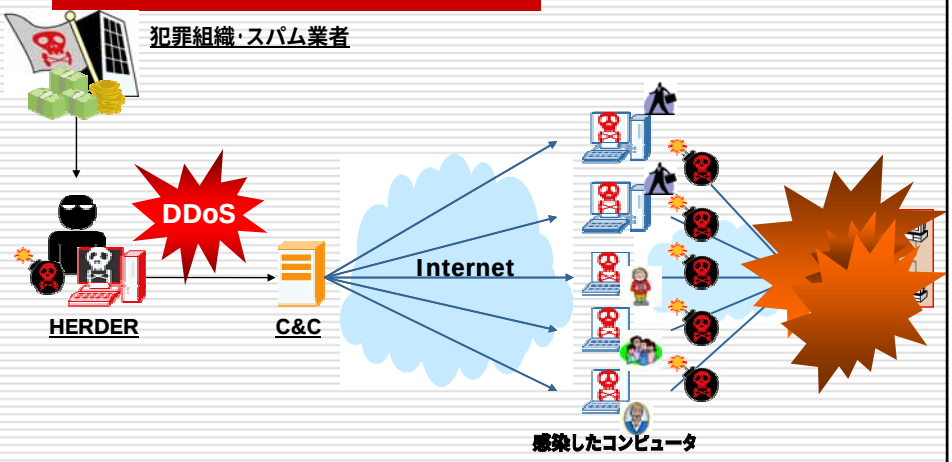
有限責任中間法人
JPCERT コーディネーションセンター

理事　真鍋　敬士
MANABE　Takashi

本日のトピック

- ボットネットのおさらい
- 脅威の変化
- JPCERT/CCの取り組み
- ユーザの対策

ボットネットのおさらい



- ボットネットのおさらい -

ボットとは…

- マルウェア(広義のウィルス)の一形態
  - Malicious Software
  - Robot
- 複数の機能をあわせもつ
  - 感染(脆弱性, 便乗, ソーシャルエンジニアリング, …)
  - 情報収集(アカウント情報, 脆弱なシステムの情報, …)
  - 攻撃(DDoS, スパム, …)
  - 自己防衛(暗号化, 難読化, "Anti-"技術, …)
  - 遠隔制御･管理(IRC/P2P, バージョンアップ, …)

- ボットネットのおさらい -

ボットネットとは…

- ボットで構成されたネットワーク
  - 指令者によって運用される
    - ハーダー(HERDER)/マスター(MASTER)
    - C&C(Command and Control)
  - 堅牢な分散システム
    - 暗号化・難読化による安全(?)性
    - 冗長化による高可用性
- カスタマイズや管理・運用が容易

- ボットネットのおさらい -

注目すべき点は?

- OSS的な開発手法
  - 無数の亜種が発生
  - 標的型攻撃(Targeted Attack)の温床
- ビジネス化
  - 成果だけでなく機能として売買される
  - 「潜む」ことで安定的に継続稼動

マルウェアは本格的な実用段階に

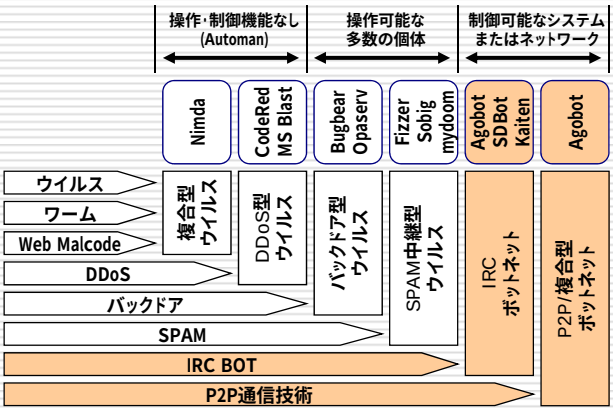
脅威の変化

- 背景
  - 価値の高まり
    - インフラとしてのインターネットの価値
    - インターネット上の資産の価値
      - 電子取引
      - 個人情報・機密情報
      - 著作物
  - 利用者層の広がり

現実社会が標的に

- 脅威の変化 -

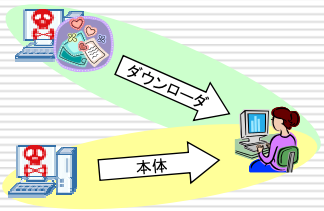
マルウェアの進化



- 脅威の変化 -

侵入・感染に使われる技術

- ソフトウェアの脆弱性
- アカウントへの辞書攻撃
- 他のマルウェアに便乗
- ソーシャルエンジニアリング的手法
  - 個人情報や組織内情報の漏洩が温床に



- 脅威の変化 -

自己防衛に使われる技術(1)

- パッキング
  - 自己解凍実行形式
  - ほとんどのマルウェアが何らかの形でパッキング
  - 複数のパッキングを使っているマルウェアも
- 暗号化・難読化
  - API呼び出しの変造
    APIを直接呼ばずに専用の関数を実装
  - 文字列のエンコード
    URL等のハードコードされる文字列

- 脅威の変化 -

自己防衛に使われる技術(2)

- “Anti-”技術
  - デバッガ・仮想化環境
    ～デバッガや仮想化環境を検知して挙動を変える～
    - IsDebuggerPresent(), 割り込み, …
    - デバイス名, ホスト・ゲスト間の通信インターフェイス, …
  - アンチウイルス
    - アンチウイルスソフトのプロセスを停止
    - アンチウイルスベンダのサーバへのアクセスを妨害

- 脅威の変化 -

最近の傾向

- 技術の複合化
  - 「より大きな脆弱性」=「人」への流れ
    - 一般利用者に近い場面での脆弱性
    - 標的型攻撃(Targeted Attack)
  - 攻撃技術は「短時間化」と「多様化」
- ビジネスとしての確立
  - 自己顕示から金銭目的へ
  - 現実社会における犯罪との関連
  - 流行を避けて潜む

JPCERT/CCの取り組み

- インシデントレスポンス
  - CSIRTの構築
  - 業種・地域・管轄・分野を越えた連携
- 脆弱性情報取り扱い
  - 情報の適切なコントロール
  - 設計開発・品質管理へのフィードバック
- 脅威分析・研究
  - ボットを始めとするマルウェアの分析
  - 短期と中長期の両方の視点から対策を検討

- 取り組み -

マルウェア分析

- 捕獲
  - インシデント報告
  - ハニーポット・ダウンロード
- 解析
  - 動的解析
  - 静的解析
- 成果
  - 捕獲・解析手法の改善と共有
  - 傾向・統計

- 取り組み -

解析手法

	Blackbox	Whitebox
静的	Surface分析	(狭義の)静的解析 ～リバースコードエンジニアリング～
動的	(狭義の)動的解析	デバッギング

- 取り組み -

分析におけるリスク

- 捕獲･分析手法
  - 法律への抵触
  - 手法の進歩がマルウェアの進化を促す
    - “Anti-”技術はダマシ合い
    - 暗号化･難読化には無数の選択肢
- 検体や分析結果の取り扱い
  - インシデント情報の混入
  - 漏出による二次被害

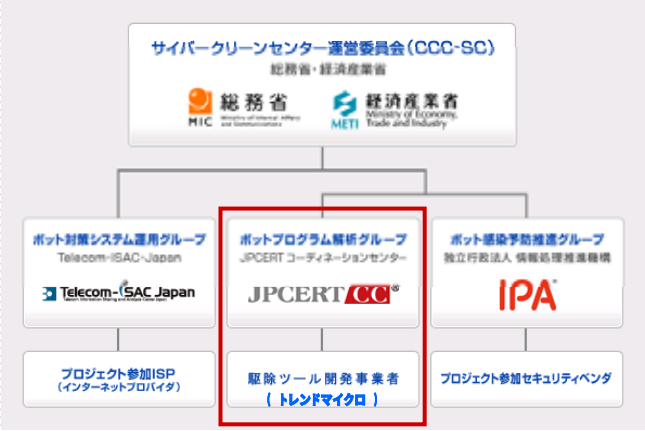
- 取り組み -

調査/研究資料

- http://www.jpcert.or.jp/
  Home>公開情報>調査/研究
- 2006年7月20日公開
  - ボットネット概要
- 2007年6月21日公開
  - マルウェアの最近の傾向とウェブアプリケーションの脆弱性を狙うボットの実態
  - P2P型ボット分析レポート

- 取り組み -

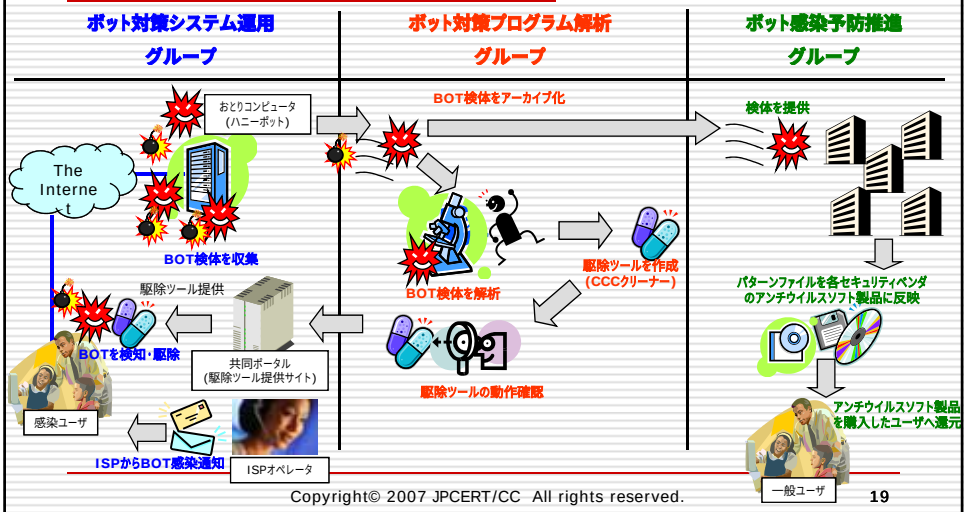
CCC(サイバークリーンセンター)



サイバークリーンセンター
(https://www.ccc.go.jp/)

- 取り組み -

各グループの役割



- 取り組み -

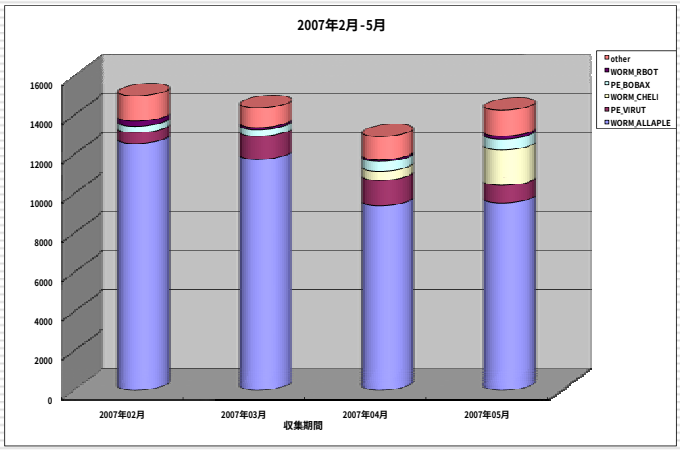
活動状況(2007年5月末時点)

収集検体総数	1,089,280
同定検体数	58,083
未知検体数	3,840

更新回数	18
確認検体数	45,462
作成検体数	3,032

- 取り組み -

収集検体トップ5(2007年2～5月)



ユーザの対策

- ウイルスの一種として
  - ウイルスと同じ対策から始める
- ボットとして
  - ボットに弱点はないか?
  - ボットの特徴を活かせないか?

2007年7月10日現在、ボットの特効薬はありません

- 対策 -

体調管理

- セキュリティのための習慣
  - Webサイトへのアクセス
  - メールの添付ファイル･HTMLメール
- セキュリティアップデート
  - 脆弱性を利用するものは少なくない
    - ボット詳細解析(20検体)
      - 脆弱性を利用する可能性があるものが8検体
      - それぞれが複数(3～12種類)の脆弱性を利用
        MS02-039, MS02-061, MS03-007, MS03-026, MS03-049,
        MS04-007, MS04-011, MS04-012, MS05-039, …

    → 未知の脆弱性は防げない

- 対策 -

免疫力の維持

- ファイアウォール
  - ワーム型ウイルスに有効
  - ブロードバンドルータのNAT/NAPT機能でも有効
    → UPnPや簡易DMZのような機能に注意
- セキュリティ対策ソフトウェア
  - アンチウイルス
    → 必ずしもすべてのボットに対応できるわけではない
  - スパム･フィッシング対策

- 対策 -

ボット対策の問題点

- 潜行化
  - ボット化したら見た目では発見不可能
  - 通信プロトコルとしてHTTPを使うものも
- 組織化

ひとりひとりの意識を高めて総合的な対策力を向上させる

お問い合わせ先

- JPCERTコーディネーションセンター
  - Email：office@jpcert.or.jp
  - Tel：03-3518-4600
  - http://www.jpcert.or.jp/
- インシデント報告
  - Email：info@jpcert.or.jp
    PGP Fingerprint：BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8
  - 報告様式
    http://www.jpcert.or.jp/form/

JPCERT CC®

ご清聴ありがとうございました