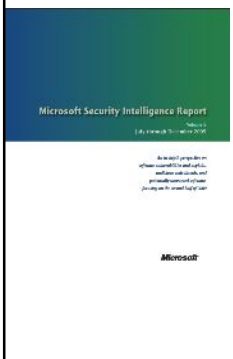
マルウェアの動向と事業者としての対策

マイクロソフト株式会社
2010年11月

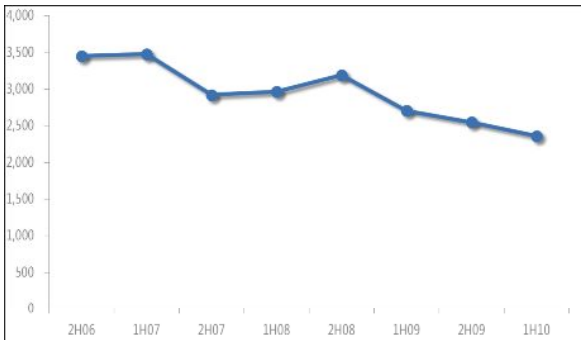
Microsoft Security Intelligence Report Volume9
2010年 1月～6月



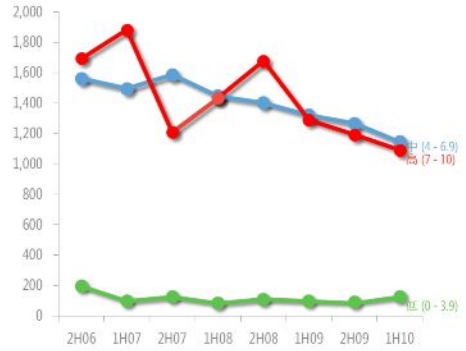
- マイクロソフトが半期に一度公表している分析レポート
  - 情報ソース（MMPC, MSEC, MSRC）
    - Forefrontなどのマイクロソフトのセキュリティ製品
    - MSRT, Defender, MSEなどの無償で提供しているセキュリティ製品

http://www.microsoft.com/japan/security/contents/sir.mspx

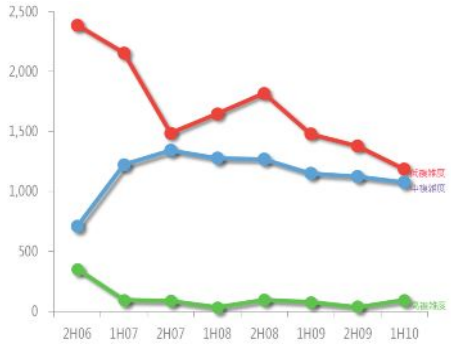
脆弱性の公開件数（総数）



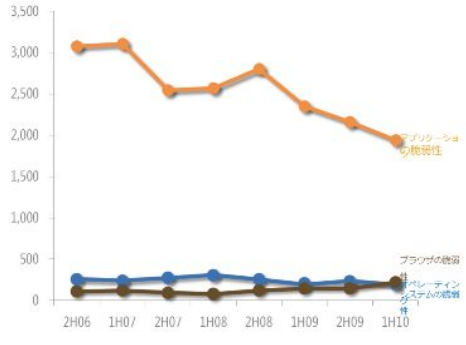
脆弱性の公開件数（深刻度別）



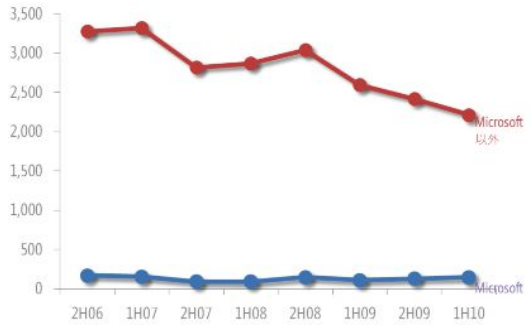
脆弱性の公開件数（複雑性別）



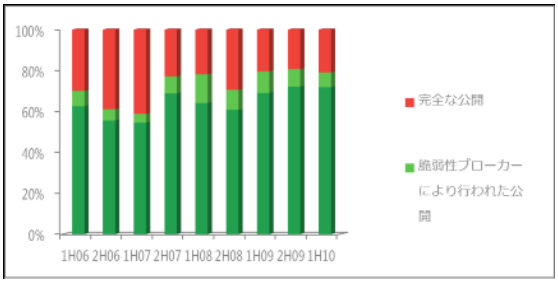
脆弱性の公開件数（種類別）



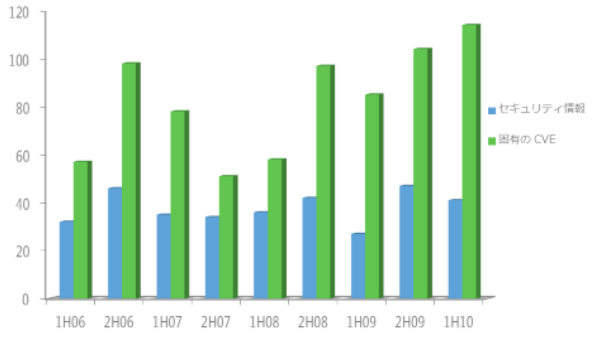
脆弱性の公開件数（MS・他）



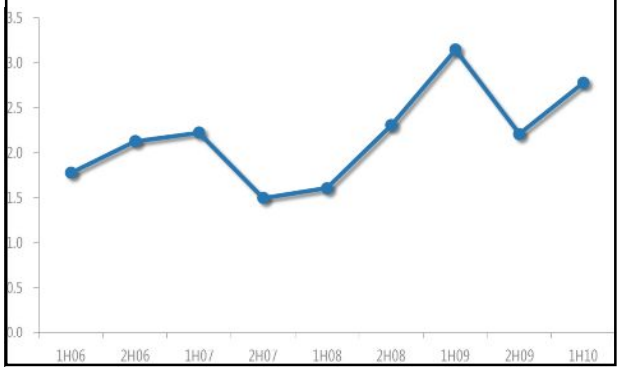
脆弱性公開の経緯



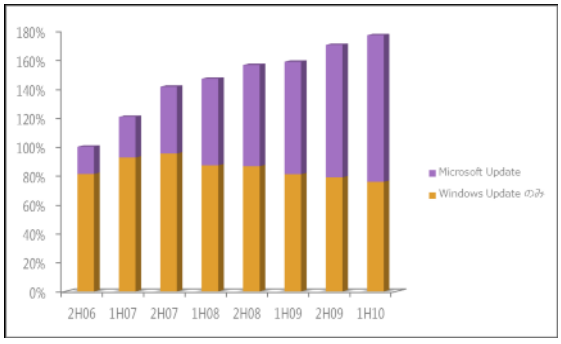
セキュリティ情報とCVE件数



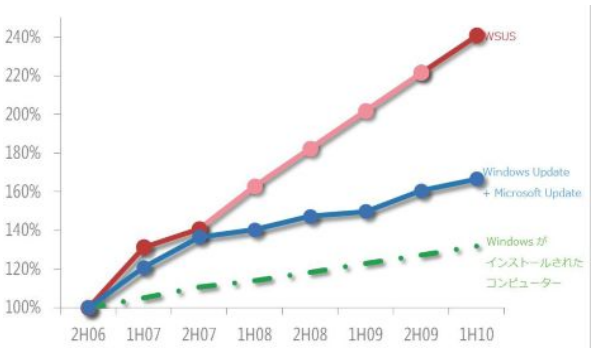
Security情報毎の平均CVE件数



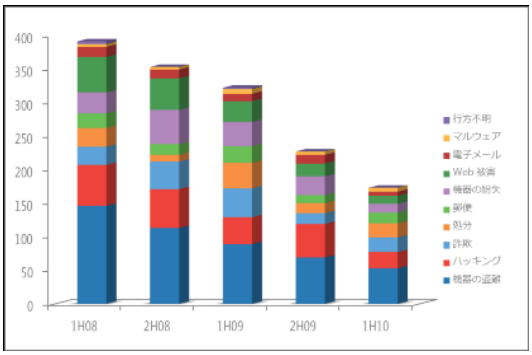
セキュリティ更新の普及



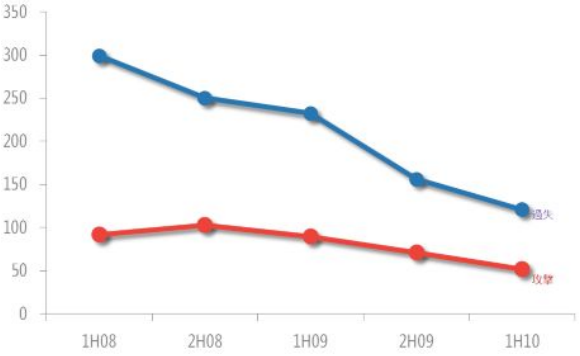
セキュリティ更新の普及



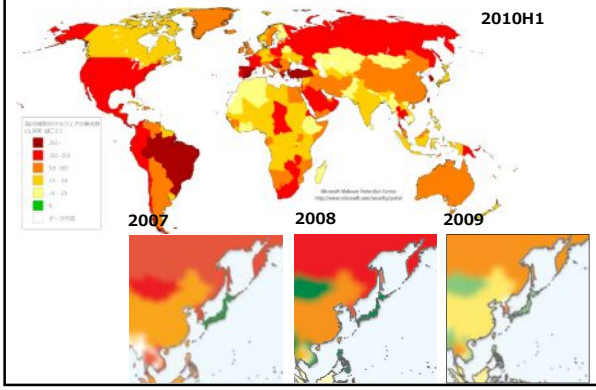
種類別インシデント数



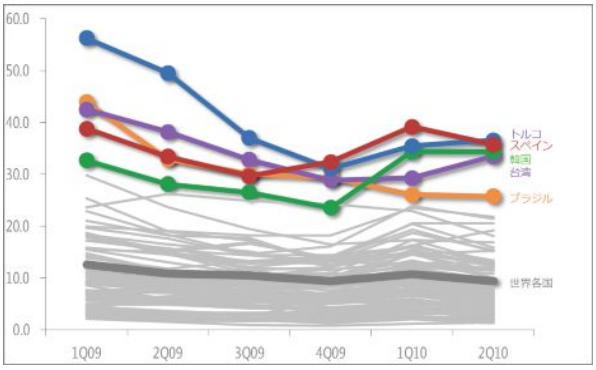
攻撃・過失の事件数



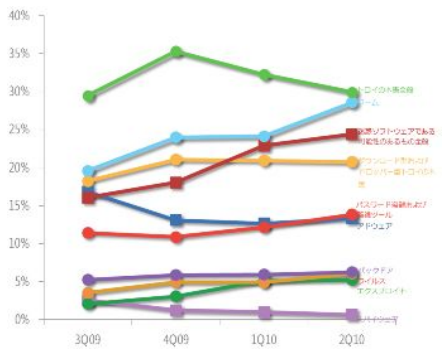
国・地域毎のマルウェア感染率



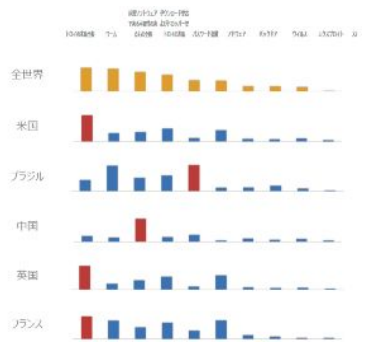
高感染率地域の動向



脅威の種類別駆除率

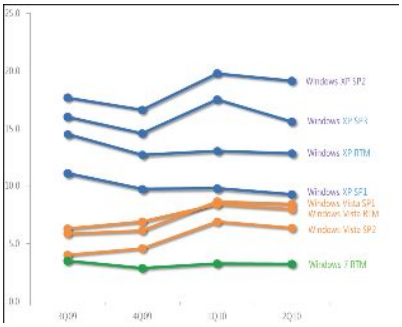


感染上位5地域でみた脅威の傾向

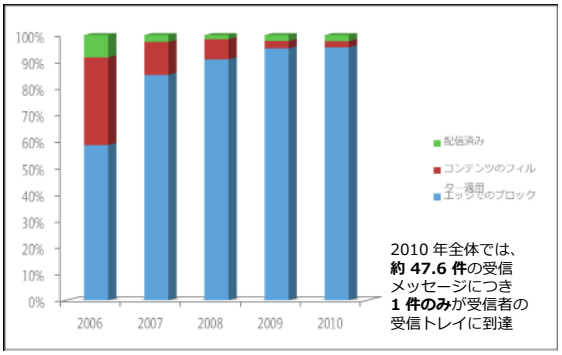


OS別でみたマルウェア感染率

OS別でみたCCM傾向

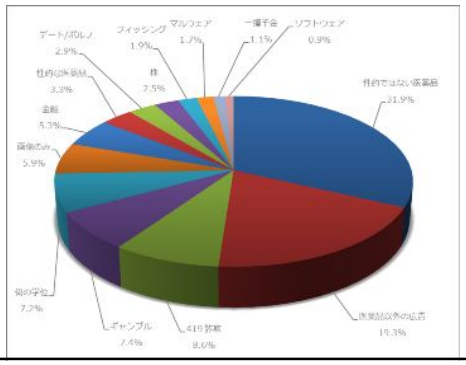


迷惑メールの遮断状況



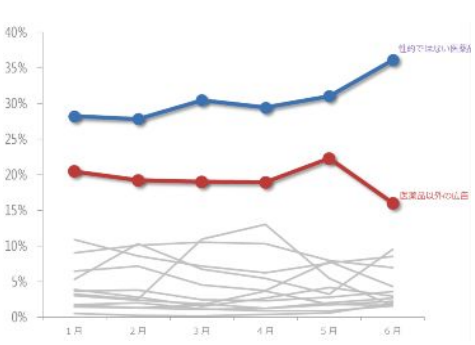
2010 年全体では、**約 47.6 件**の受信メッセージにつき **1 件のみ**が受信者の受信トレイに到達

迷惑メールの種別

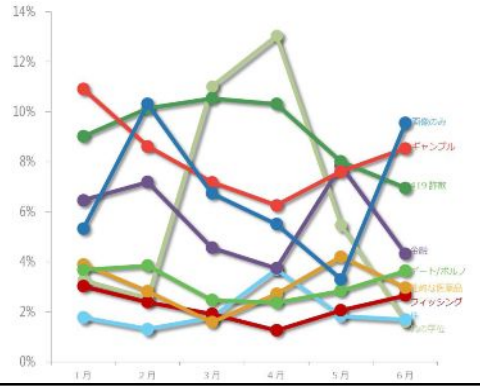


画像のみの迷惑メール（例）

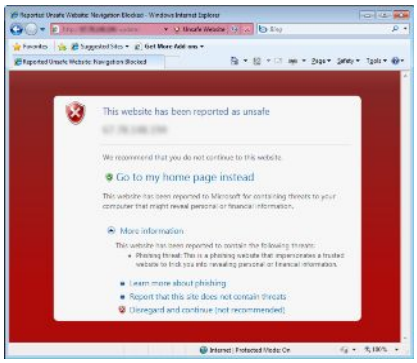
迷惑メール種別の推移



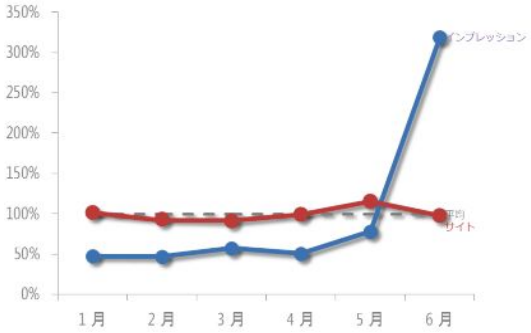
迷惑メール種別の推移



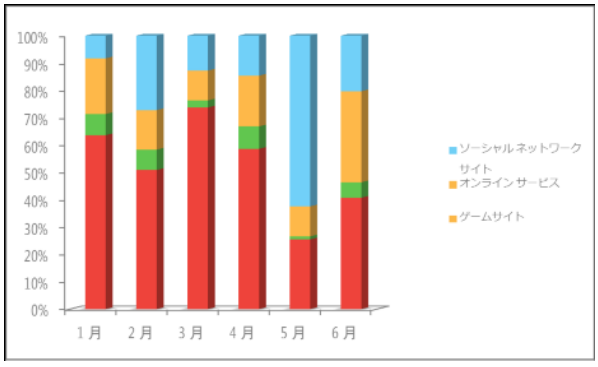
フィッシング詐欺からの保護



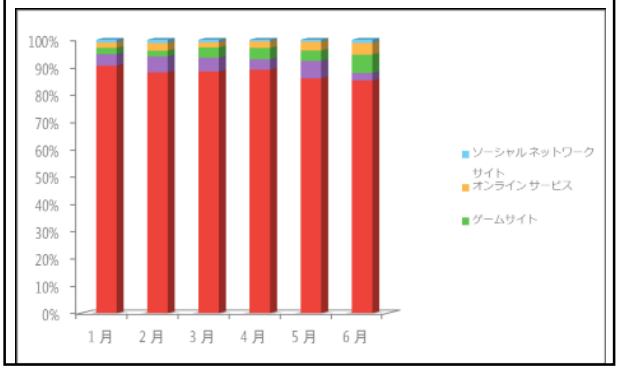
詐欺サイトの推移



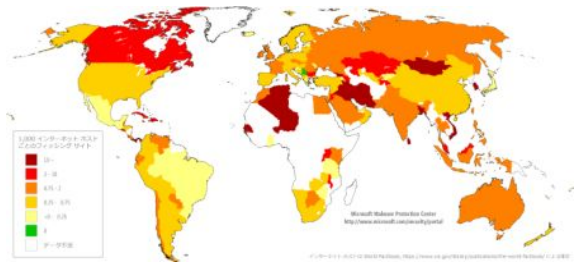
詐欺サイトのインプレッション



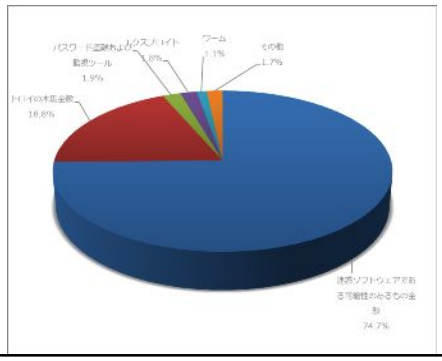
詐欺サイト改竄標的の種別



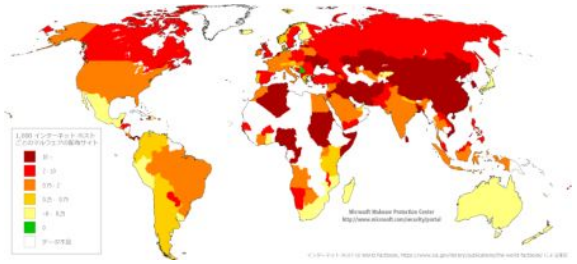
詐欺サイトの地理分布



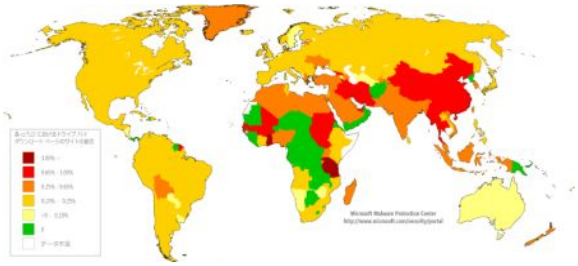
遮断された脅威の種別



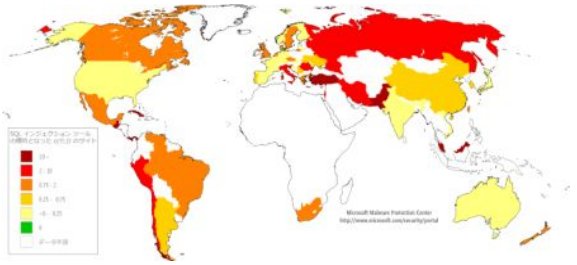
マルウェア配布サイトの地理分布



マルウェア配布サイトの比率

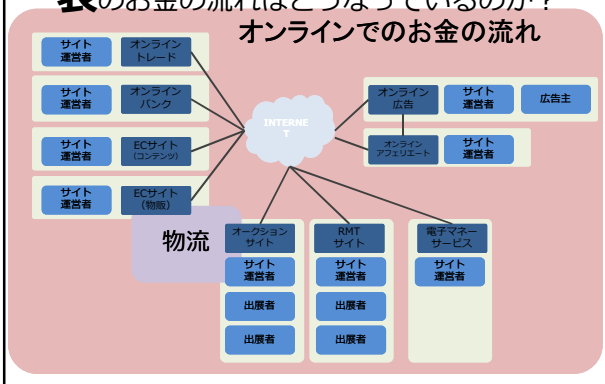


SQLインジェクションの標的

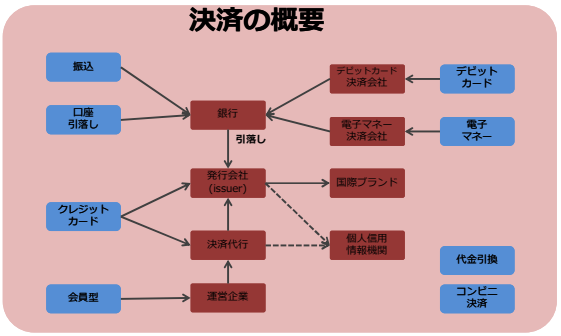


マルウエアの経済化

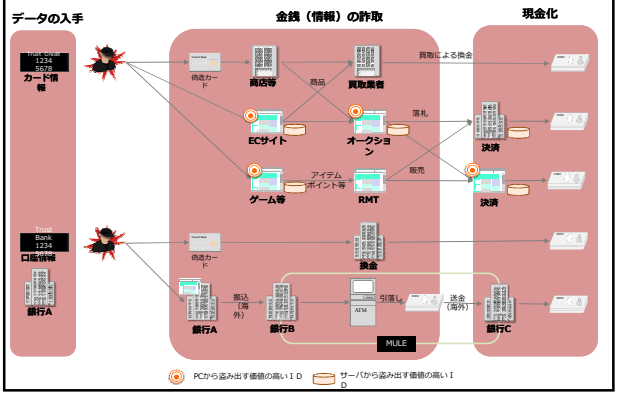
表のお金の流れはどうなっているのか？



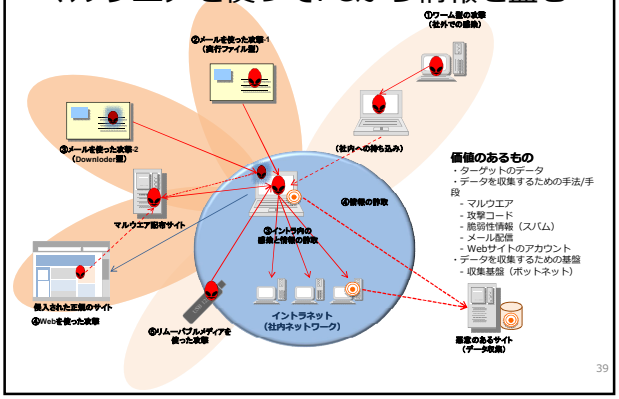
表のお金の流れはどうなっているのか？



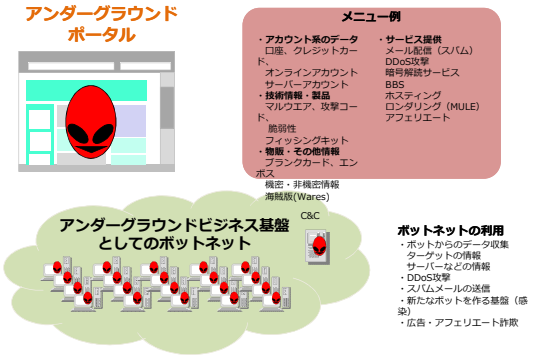
口座・クレジットカード情報を現金化



マルウエアを使ってPCから情報を盗む



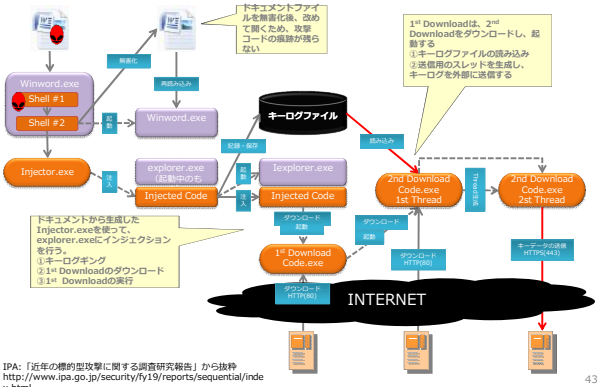
アンダーグラウンド　ポータルとボットネット



ボットネットの世界的な展開

国際的な金銭の流れ

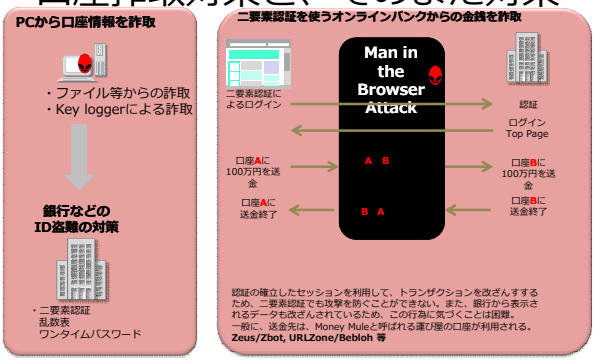
マルウエアによる口座情報などの詐取



IPA:「近年の標的型攻撃に関する調査研究報告」から抜粋
http://www.ipa.go.jp/security/fy19/reports/sequential/index.html

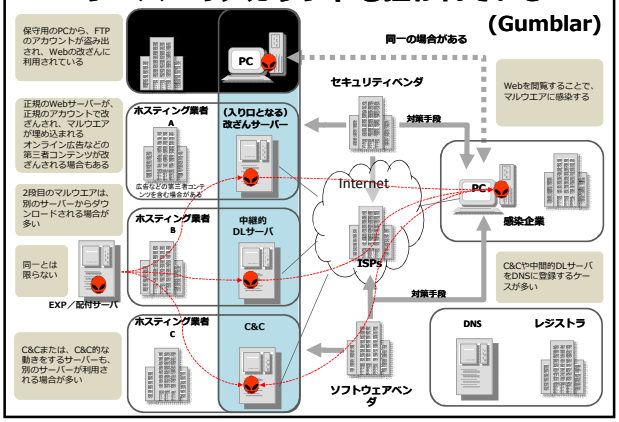
43

口座搾取対策と、そのまた対策



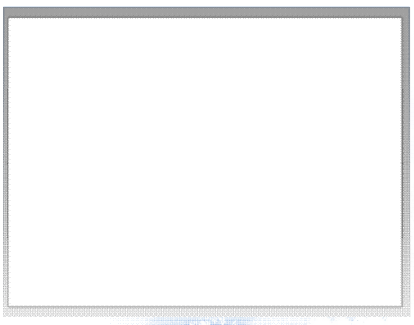
Man in the Browser http://blog.fireeye.com/research/2010/02/man-in-the-browser.html
Malware Analysis - Trojan Banker URLZone/Bebloh http://www.finjan.com/Content.aspx?id=2345

サーバーのアカウントも狙われている (Gumblar)



犯罪基盤としてのボットネットと対策の事例

ボットネット



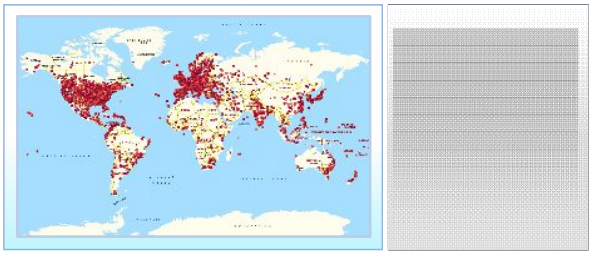
未承諾電子メールの87%はボットネットが原因でおこる。

ボットネットに感染したコンピュータは380万台以上 – 米国のみで100万台

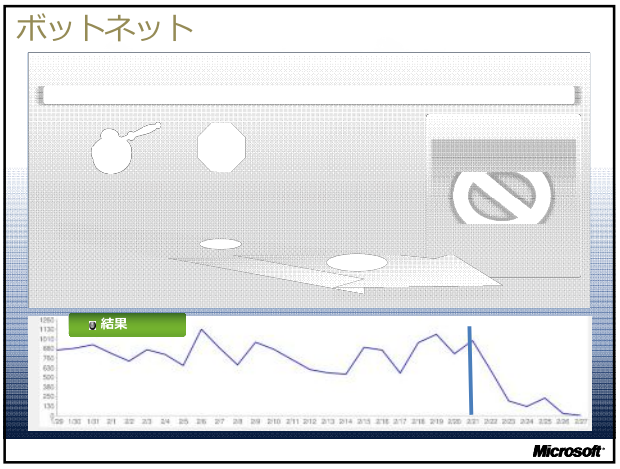
DDoS攻撃– 2008年中の攻撃190,000件

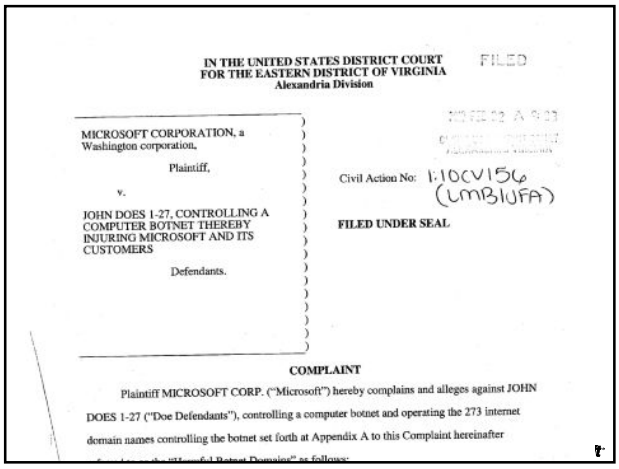
Microsoft

Waledac：2009年7月～12月



Microsoft





IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

FILED

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

JOHN DOES 1-27, CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS

Defendants.

Civil Action No: 1:10CV156 (LMB/IDFA)

FILED UNDER SEAL

COMPLAINT

Plaintiff MICROSOFT CORP. ("Microsoft") hereby complains and alleges against JOHN DOES 1-27 ("Doe Defendants"), controlling a computer botnet and operating the 273 internet domain names controlling the botnet set forth at Appendix A to this Complaint hereinafter