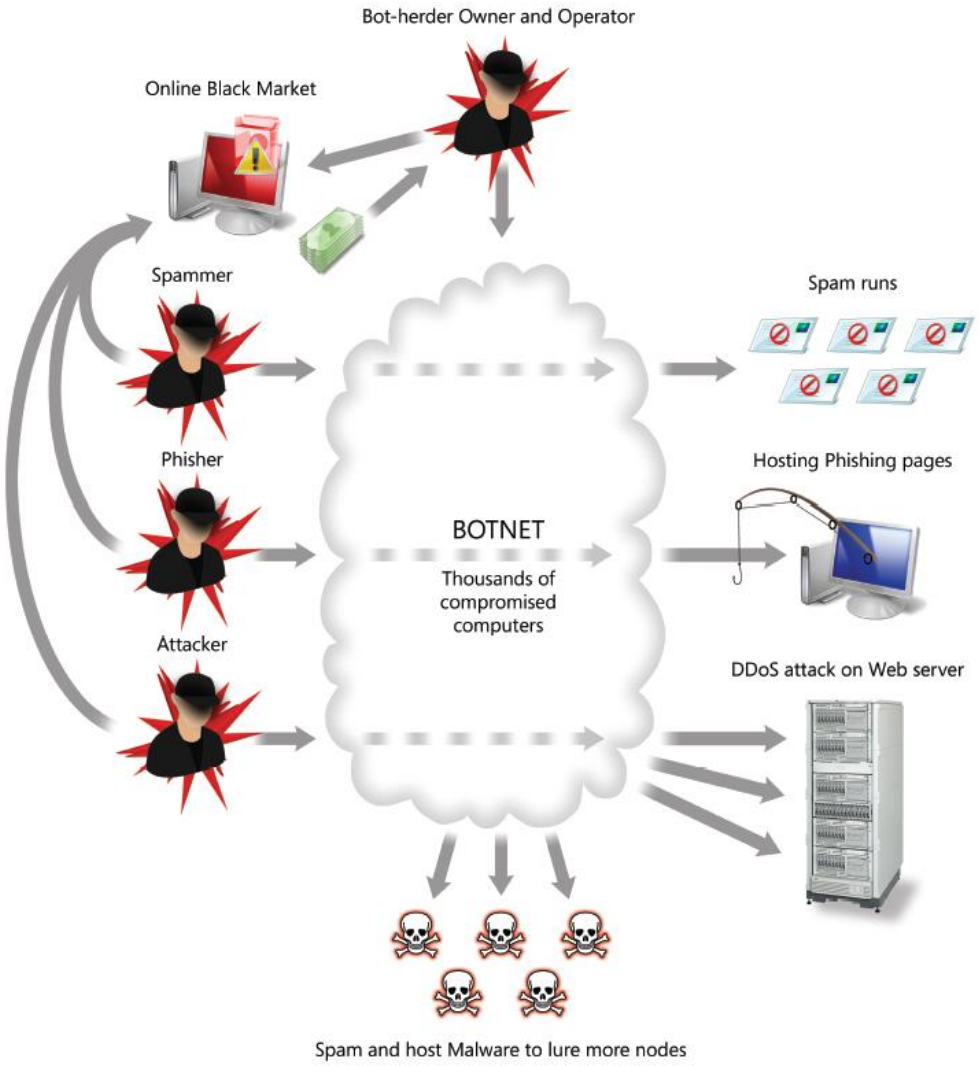
Botnet Takedown事例

日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋　正和

Microsoft

犯罪基盤としてのボットネット



- ボットネットは、様々なサイバー犯罪の基盤として利用されている
  - 電子メール
    - メールアカウントの詐取
    - フィッシングメールの送信
    - SPAMメールの送信
  - 認証情報の詐取
    - オンラインバンキングから現金を盗む
    - 電子商取引を通じて、損害を与える
  - DDoS
    - DDoS攻撃への利用
  - 他のコンピューターへの感染

ボットネットのTakedown事例

日時	ボット名	推定台数	概要
2010/2/22	**Waledac**	数十万台	Operation b49 1日当たり15億通以上のスパム・メール送信に悪用
2010/10/25	**Bredolab**	3千万台	オランダ当局ハイテク犯罪チーム主導。ボットネットの停止の他、追加コマンドを送信し、コンピュータが感染していることを表示するプログラムをダウンロードさせてユーザーに通知
2011/4/11	**Coreflood**	2百万台	FBI 主導。感染したPCに対してマルウェアの停止コマンドを送信
2011/3/17	**Rustock**	2百万台	Operation b107 1日当たり300億通以上のスパム・メール送信に悪用。全スパム流通量の47.5%はRustock経由で送信
2011/9/27	**Kelihos**	4万台	Operation b79 スパムの大量送信、個人情報の窃盗、DDoS 攻撃など。Waledac との類似性から Waledac 2.0 とも呼ばれている。
2012/3/19	**Zeus**	800ドメイン 1300万	Operation B71 5億ドルに上る被害をもたらしている Zeus, SpyEye, Ice-IXをTakedown
2012/9/13	**Nitol**	7万ドメイン 500種	市場で販売されているコンピューターから検出されたNitolボットネットをTakedown

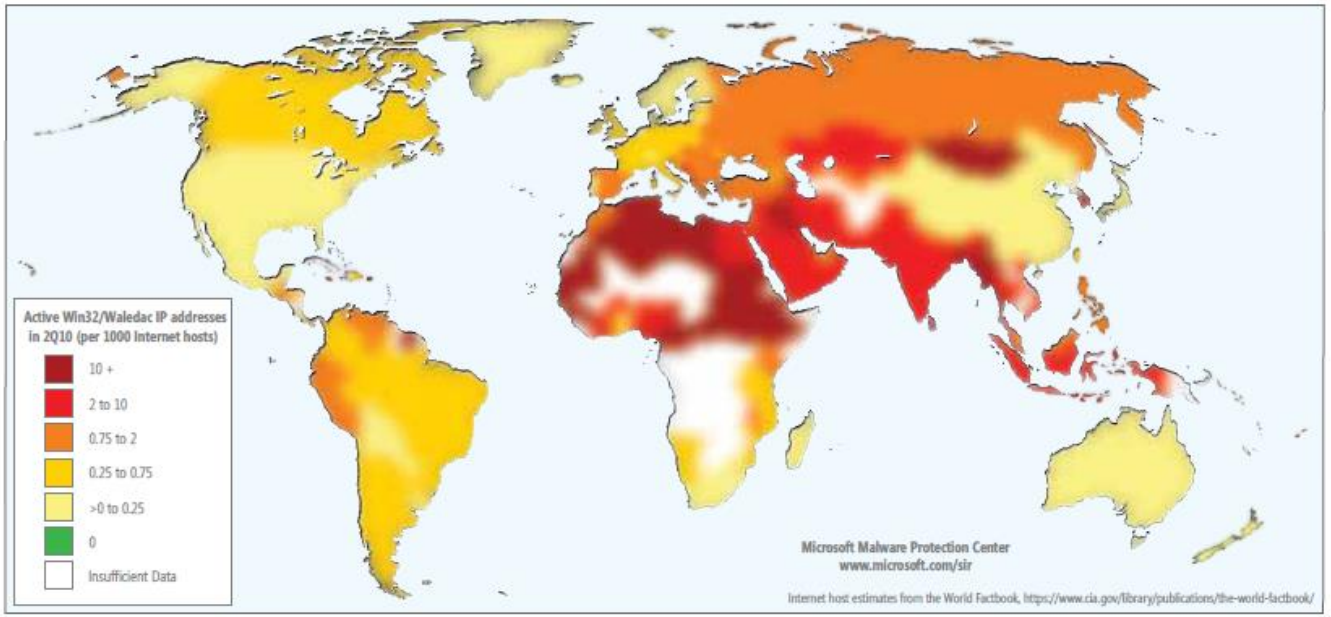
WALEDAC TAKE DOWN

Win32/Waledac and Law / Fighting Botnets in Court

- 2009年10月に開催されたDCC(Digital Crimes Consortium)において、マイクロソフトのデジタル犯罪部門（DCU: Digital Crimes Unit)は、業界、法執行機関、政府機関、研究者に、能動的なアクションを提案した
- Waledacは、技術的に複雑で、対処が困難なボットネット考えられていたことから、Waledacのテークダウンが具体的なアクションとした。
- DCUは、まず、TrendMicro, iDEFENSE, MMPC(Microsoft Malware Protection Center)等、他の組織や研究者が行っている調査・研究結果の分析を行った。

2010年10月の国別のWaledacの感染状況

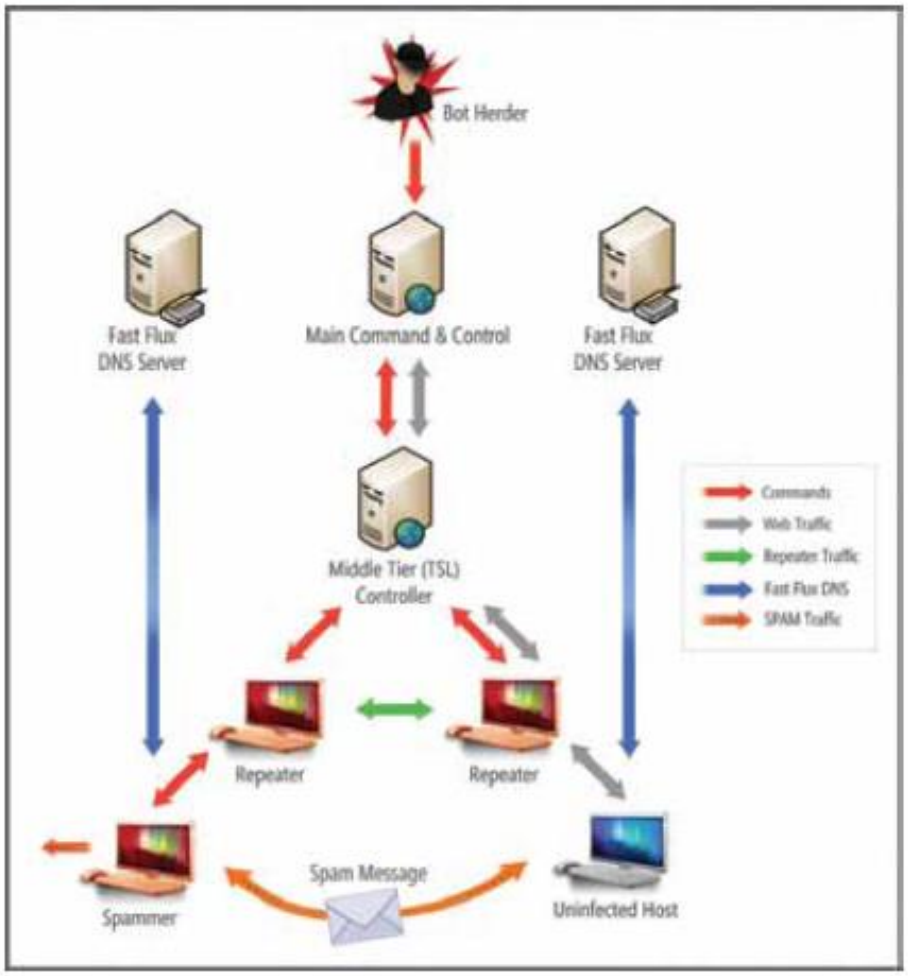
FIGURE 17. Active IP addresses in the Win32/Waledac botnet in 2Q10, per 1000 Internet hosts



- DCUは、ワシントン大学、シャドーサーバー、ウィーン技術大学、ボン技術大学、MMPCと共に、アクションプランの策定を始め、最終的には、マイクロソフト、ウィーン技術大学、iDEFENSEによって、Waledacボットネット停止のための技術的な計画が立案された
- 計画は、以下の3つのアプローチで構成される。
    - P2Pによる指揮命令系統の破壊
    - DNS/HTTPによる指揮命令系統の破壊
    - 指揮命令を行う上位2層の破壊

Waledacボットネットの概要

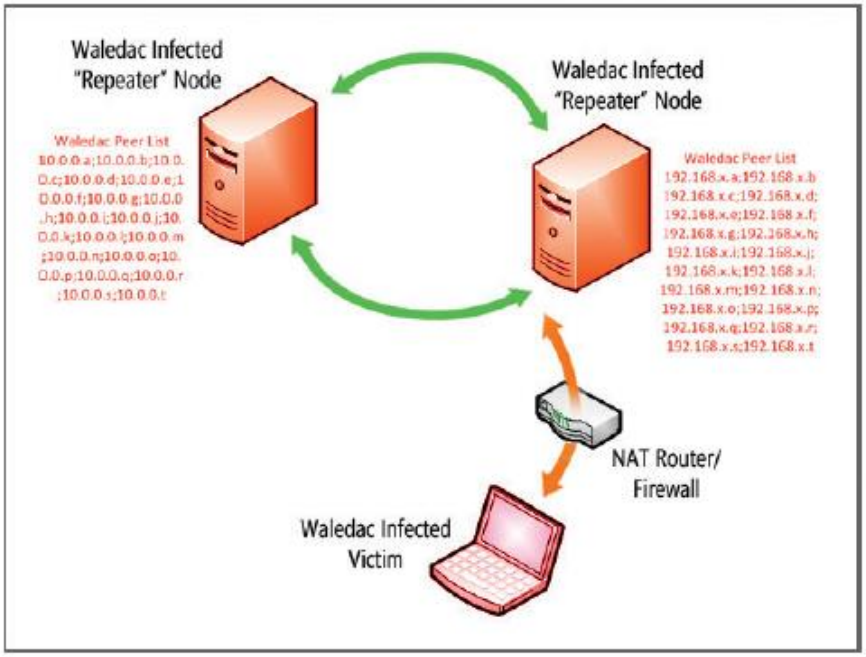
FIGURE 18. The Win32/Waledac tier infrastructure



- Waledacボットネットの概要は、左図のようになっている。
  - スパマー・ノード
    - スパムを送信するためのノード
    - リピーター・ノードと接続し、指揮命令を受ける
  - リピーター・ノード
    - P2Pのアドレスリストを維持し、上位層からの指揮命令を受ける。
    - Fast Flux　DNSに登録される
  - 中間コントローラー
    - リピーター・ノードに対して、指揮命令を行うための中間コントローラー
  - メイン　コマンド・アンド・コントロールサーバー
    - ボットハーダーが、直截操作するC&C。
  - Fast Flux DNSサーバー
    - P2Pによるアドアレスが取得できない場合に問い合せ先を登録するDNSサーバー。
    - Fast Flux: 頻繁にIPアドレスを書き換えて、追跡を困難にしている。

P2Pネットワーク

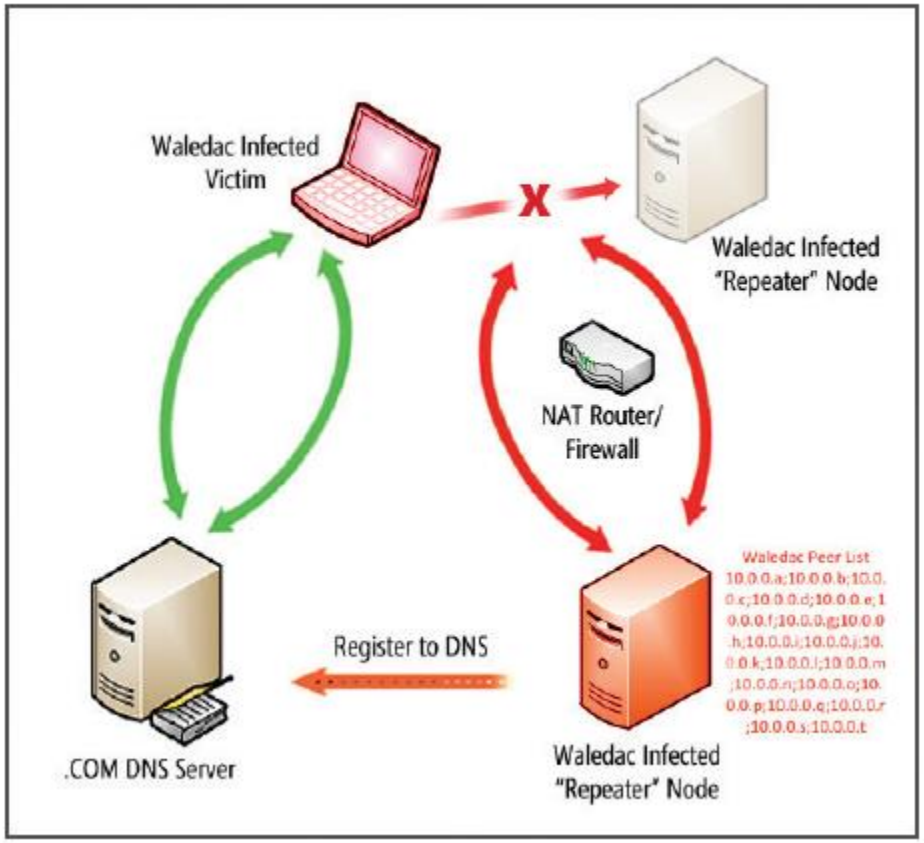
FIGURE 19. Win32/Waledac peering list exchange between infected spammer node and repeater node



- PCがWaledacに感染すると、スパマー・ノードか、リピーターノードに分類される。
  - PCが、プライベートIPを使っている場合は、WaledacのHTTPを使った指揮命令が利用できないと判断し、スパマー・ノードに割り当てられる。
  - グローバルIPを利用し、TCP/80を使ってアクセスができる場合は、リピーター・ノードとして割り当てられ、Fast Flux DNSに組み込まれる。
- リピーターノードは、有効なP2Pノードのアドレスを維持する
  - リピーターノードは、他のリピーターノードと、有効なP2Pノードのアドアレスを交換し、最新の状態を維持する。
  - 保持するリストは、すべてのノードではなく、100程度のリピーター・ノード
- スパマー・ノードは、リピーター・ノードからP2Pアドレスリストを取得する

P2Pが機能しない際の対応

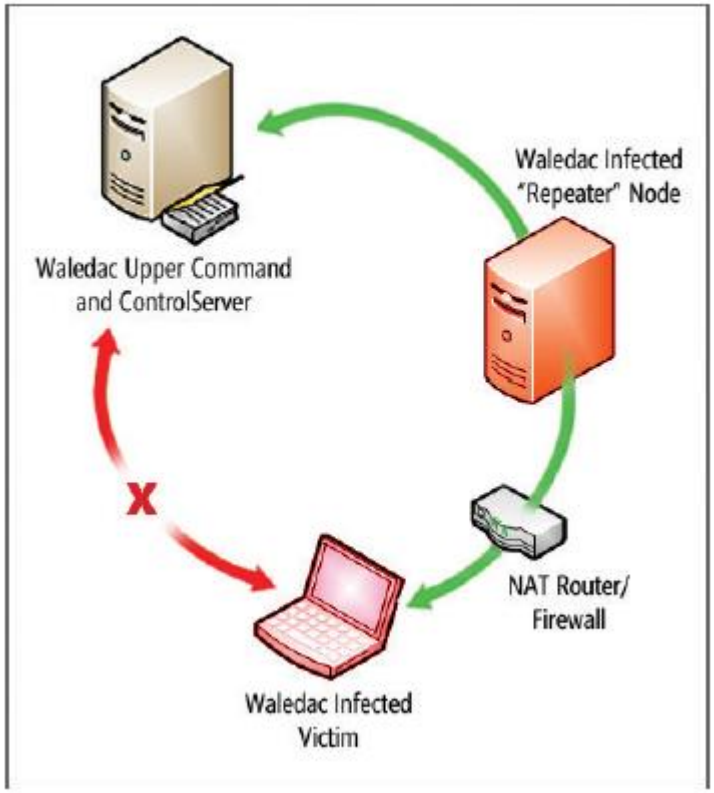
FIGURE 20. Win32/Waledac peering list exchange using fast flux DNS



- リピーターノードの Fast Flux DNSへの登録
  - リピーター・ノードが一定期間オンランだと、信頼できるノードとして、DNSに登録され、Waledacボットネットの制御に利用される。
- P2Pが機能しない場合のバックアップ
  - 保持しているリストでP2Pとの接続ができない場合、あらかじめ組み込まれたアドレス（ホスト名）に問い合わせを行う。
  - このアドレスは、Fast Flux DNSに登録されており、上記条件で登録された、リピーター・ノードのIPアドレスが割り当てられる。

上位層へのPROXYとしての機能

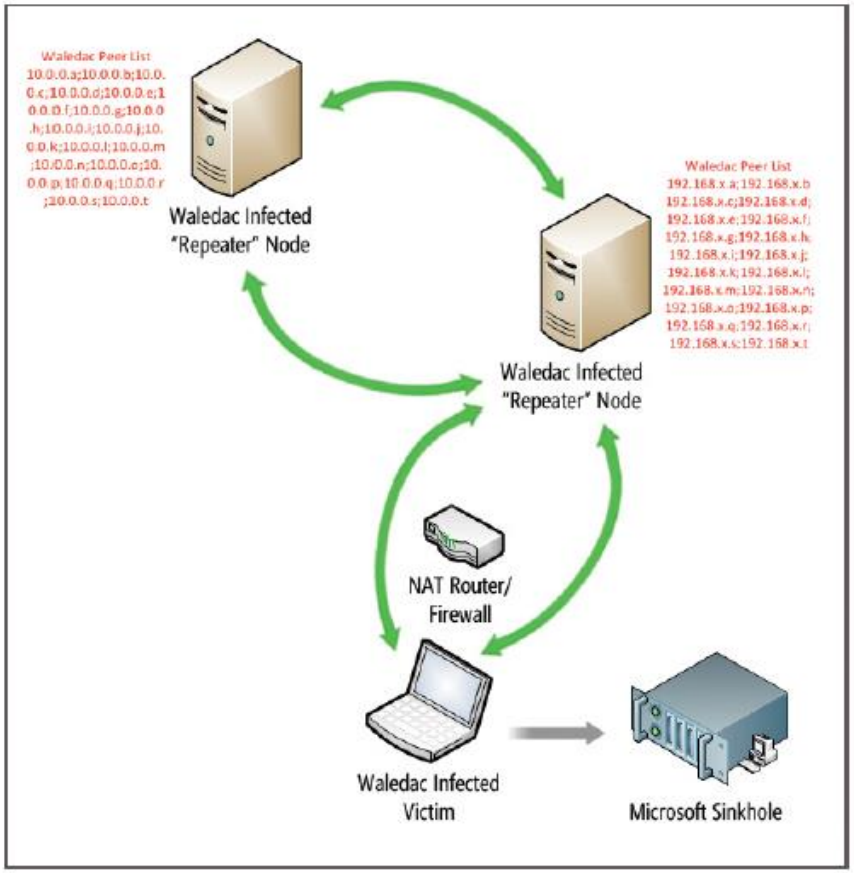
FIGURE 21. Win32/Waledac proxy function through the repeater tier



- リピーター・ノードは、上位層へのPROXYとして機能する
  - 上位層は、感染したPCではなく、ハーダーによって設置されたサーバーで構成される。
  - 上位層のサーバーは、固定的であることから、リピーター・ノードを経由しないとアクセスできないなど、意図しないアクセスを極力排除する仕組みになっている。
  - リピーター・ノードは、ある種のファイアウォール機能を果たしている。

Waledac P2Pネットワークの破壊

FIGURE 22. Poisoning the Win32/Waledac botnet with Microsoft sinkhole IP addresses



- P2Pネットワークを崩壊させることから始めた
- リピーター・ノードは、グローバルIPを持ち、80/TCPが接続できるPCで構成される。
- Waledacに感染すると、あらかじめ設定されたIPアドレスに接続し、リピーター・ノードとなると、アクティブなリピーターノードのリストをダウンロードする。
  - このリストは、必ずしも適切に機能しておらず、ハニーポット上で感染したPCの、フォールバックアドレスへのアクセスが頻繁に観測された。
- この仕組みを利用し、アクティブ・ノードリストに、シンクホール（なにも返さないアドレス）をポイゾニングすることで、P2Pネットワークを崩壊させることができた。

- しかし、Waledacは、DNSを利用したバックアップシステムがあるため、あわせて、DNS問題にも取り組む必要があった。

DNSの対策：ホスト名の削除

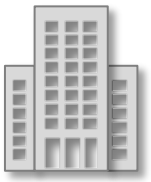
ICANNの紛争解決方針

ハーダーに動きを知られ、対応の時間を与える

犯人逮捕

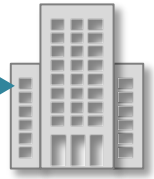
犯人不明のため、法的対策が取れない

ハーダー



ICAN

統括

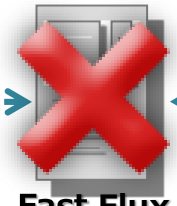


レジストラ

連邦裁判所

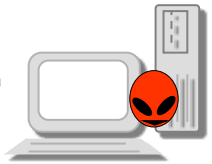
xxTLD

登録



Fast Flux DNS Server

名前解決



Waledac

一方的な仮処分（ex parte TRO）

48時間以内のドメイン名の停止を、当事者に知らせることなく強制できる

停止依頼（非公式なレター）

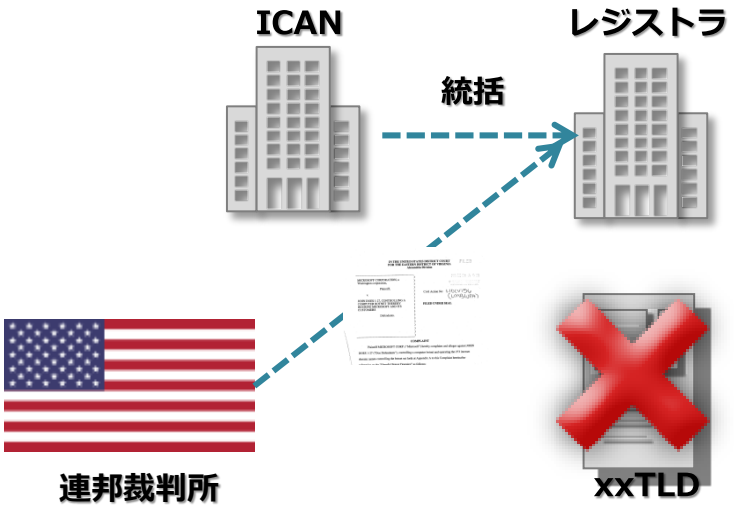
強制力がないため、必ずしも実施されない

DNS サーバーの Take Down

DNSサーバーは、ハーダーのものではない

このページは、Security Intelligence Report Vol.9（SIR9)に基づいて発表者が資料化したものであり、内容を保証するものではありません。正確な情報については、SIR9をご確認ください

DNSの対策：ホスト名の削除



一方的な仮処分
(ex parte TRO)

紛争相手への事前通知なしに、一時的（14-28日間）な対処を行うための特別な救済策、証拠隠滅や回避策の実施を阻止するために適用される。
一般に”一方的なTRO“の発行は困難で、連邦原則ルール 65 に基づき、**「これを行わない場合に即座に解決できない危害が継続すること」**、**「相手方への通知を行い、それができない場合にはその理由を明確にすること」**を求めている。

連邦裁判所に対する一方的なTRO発行の必要性の訴求

連邦裁判所は、通知を行った場合、訴訟を避け、不法行為を続ける機会があると判断し、“一方的なTRO”を発行した。
（30年以上前に偽ブランド品に対して実施）

ドメインが乗っ取られているケースの対処

ドメイン登録者を被告とせず、27のドメイン登録者に対して被告人不詳として訴訟（John Does訴訟）。

中国のレジストラを通じて登録されたドメインの対処

起訴手続きの連邦原則、米国憲法、中国の法律を満たすことを確認し、ハーグ条約に基づいて、中国法務省に依頼

ドメイン登録者に通知

適法手続権利の維持を保証するため、ドメイン登録者に、訴状を送ると共に、電子メール、FAX、書簡による通知を行い、加えて、サイトを作成し、訴訟に関する書面をすべて掲載の上、これをメディアなどを通じて周知
www.noticeofpleadings.com

停止命令が実施されない場合の対処

停止命令が実行されない場合に、ドメインの所有権がマイクロソフトに移行するように申請し、認められる。

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

FILED

2010 FEB 22 A 9:03

CLERK US DISTRICT COURT
ALEXANDRIA VIRGINIA

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

v.

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

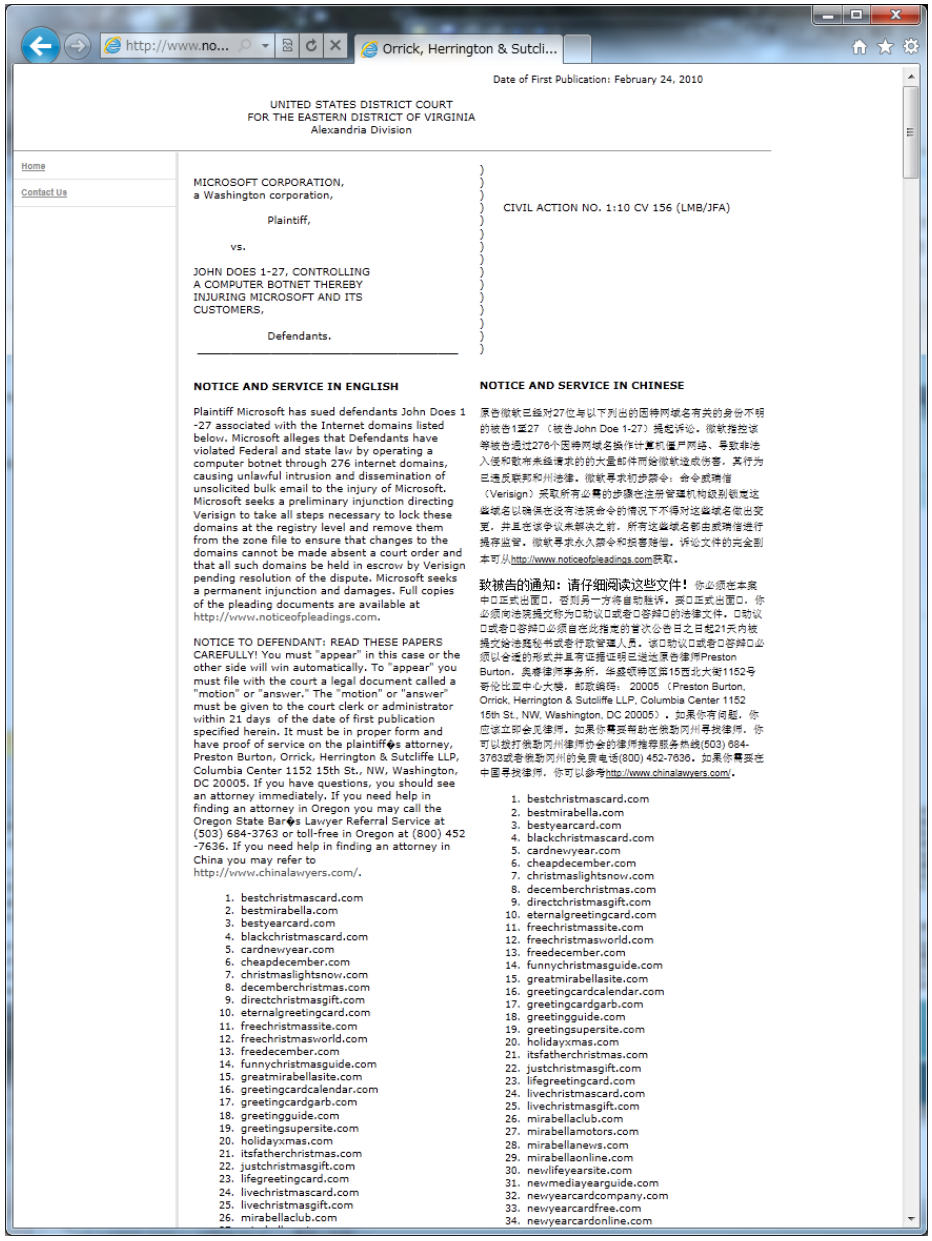
Defendants.

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 referred to as the "Harmful Botnet Domains" as follows:

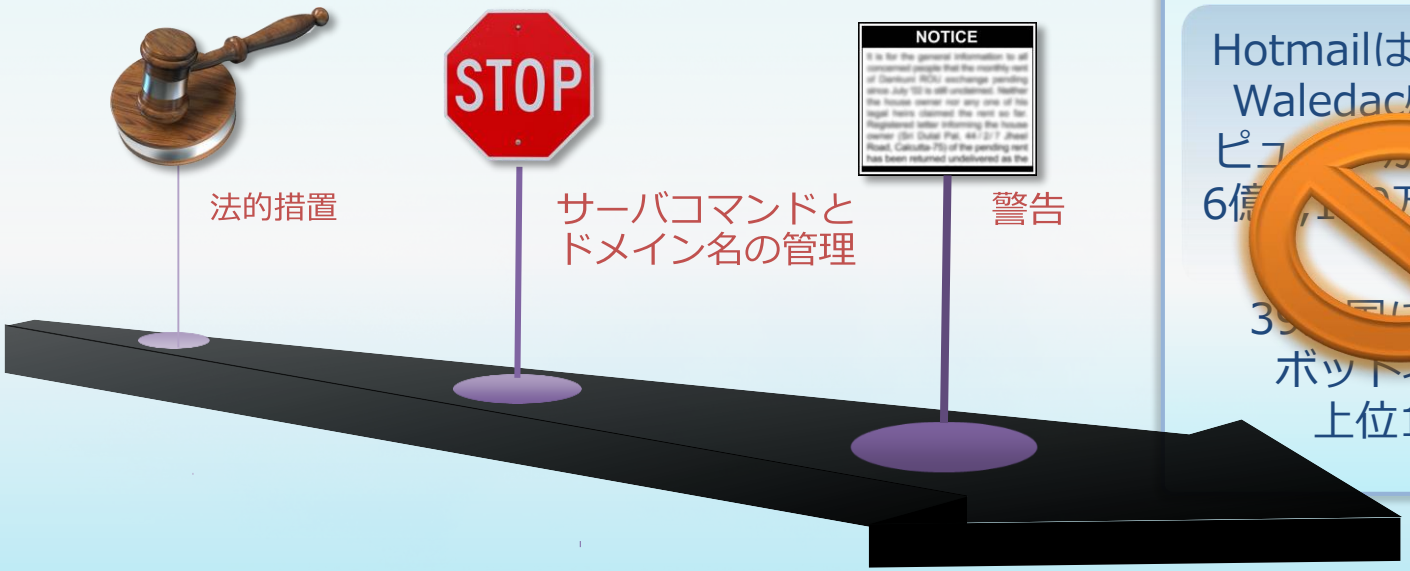


http://www.noticeofpleadings.com/

ボットネット

WALEDACボットネット「遮断」アプローチ

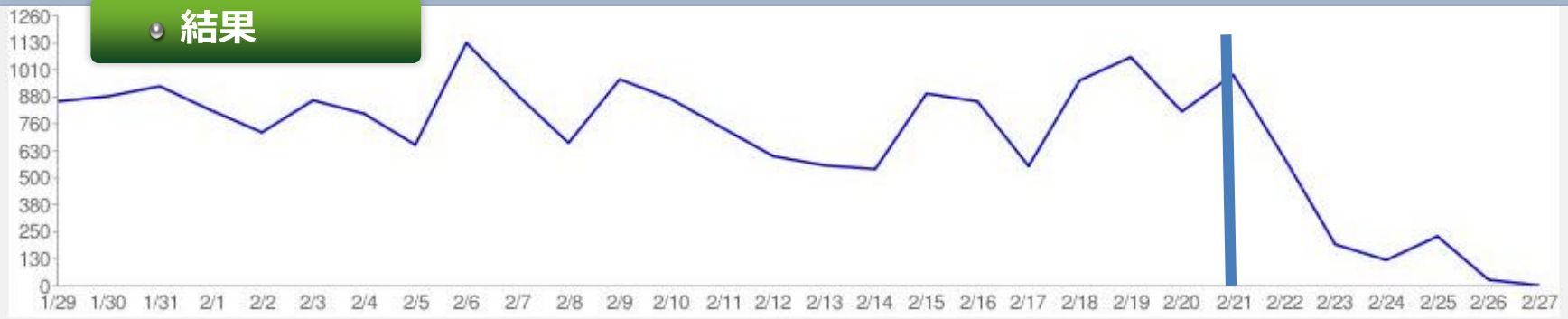
短期的 – 先例を作る



Hotmailは18日間で
Waledac感染コン
ピュ　　接続
6億　　万件を　　遮断

3　　る
ボットネット
上位10位

結果

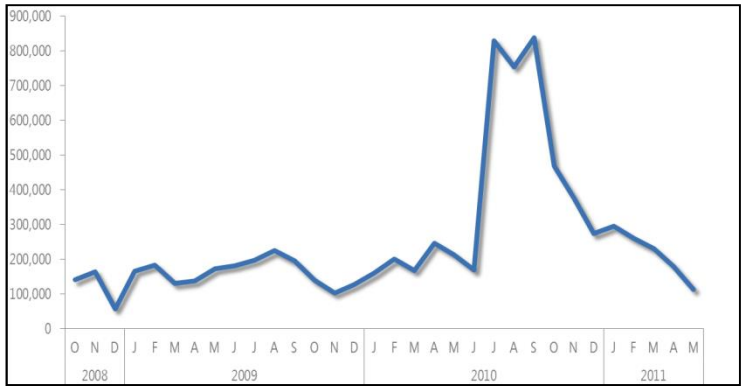


Microsoft

Rustock Takedown

プロジェクト MARS (Microsoft Active Response for Security)
Operation b107

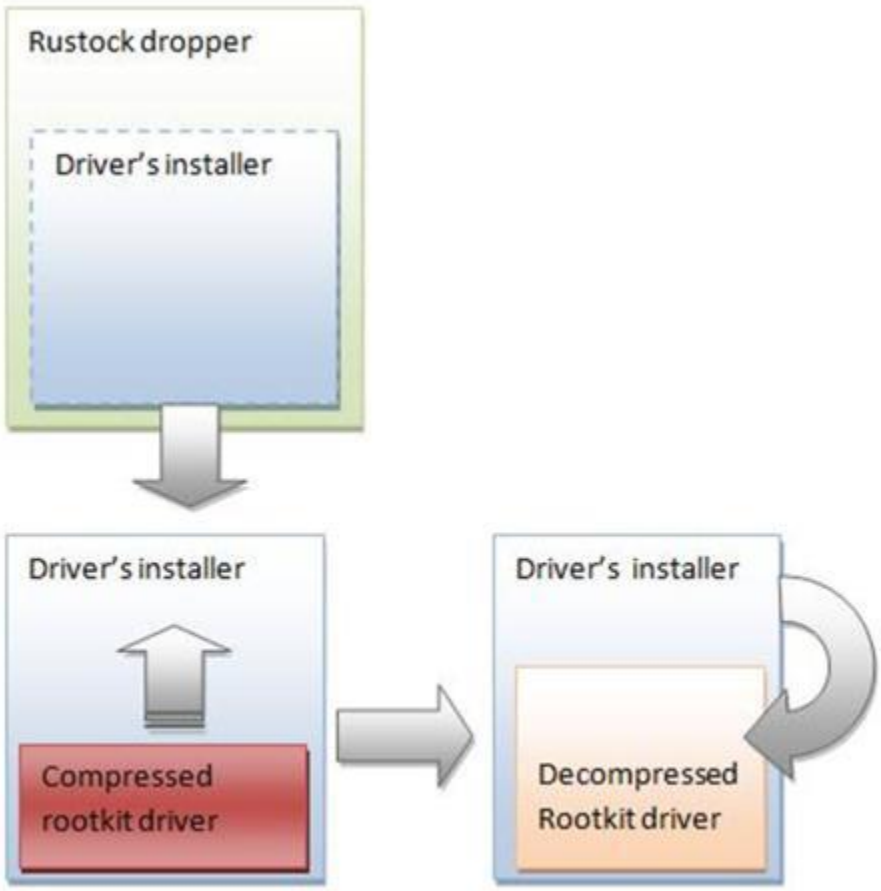
- Rustock
  - 約100万台で構成されるボットネット
  - 主にスパムの送信に利用される
    - 毎日数十億通の送信が可能
    - マイクロソフトの宝くじ、
    - 虚偽の処方薬など
- Operation b107（2011/3/16に実施）
  - Microsoft Active Response for Securityの一環として実施（Waledacに次ぐ2例目）
    - Microsoft Digital Crimes Unit (DCU)
    - Microsoft Malware Protection Center (MMPC)
    - Microsoft Trustworthy Computing
  - 協力・共同
    - Pfizer：製薬会社
    - FireEye：ネットワーク セキュリティ プロバイダー
    - ワシントン大学のセキュリティ専門家
    - オランダ警察当局の内部組織 Dutch High Tech Crime Unit
      - 米国以外の国で稼動しているボットネットのコマンド構造の破壊することを支援



マイクロソフトのマルウェア対策ソリューションによる Win32/Rustock の検出数 (2008 年 10 月～ 2011 年 5 月)

Rustockの構成

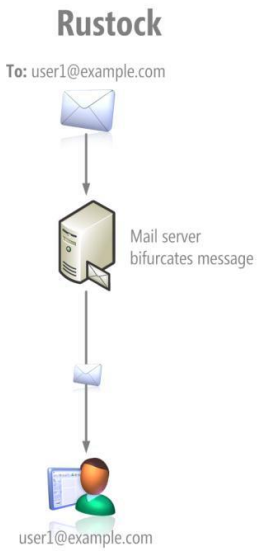
- ドロッパー
  - ユーザーモードで実行
  - C&Cから、ルートキットドライバーの複合化とドロップ
  - ポリモーフィック型、
  - 静的な文字列は使わない
  - RC4で暗号化しaPLibで圧縮
- ドライバーインストーラー
  - システムドライバーに成りすまし、カーネルモードで実行
  - Beep.sys, null.sys等の置き換え
  - ハードコード化されたファイル名とランダムなファイル名
- ルートキットドライバー
  - カーネルモードで実行
  - INT 2eh割り込みを賜与してユーザーモードボットクライアントと通信
  - SSDT*をフックし、自身を除外
  - ntoskrnl.dll , ntdll.dll, tcpip.sys, wanarp.sys などもフックし、ディスク操作とネットワーク操作も隠蔽

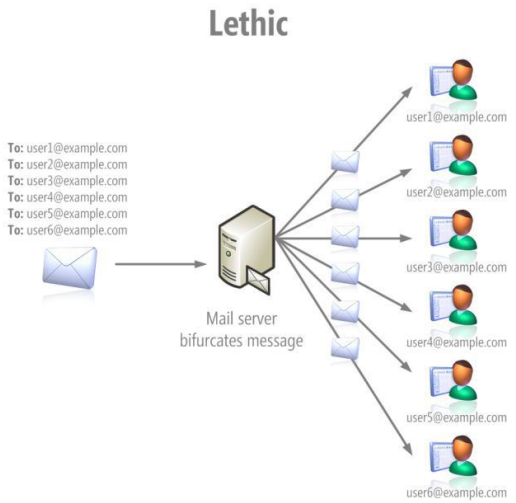


*SSDT: System Service Dispatch Table

スパム

- 古いバージョンのRustock
  - Botdll.dll　SMTPクライアントエンジン
- 2008年以降のRustock
  - Hotmailを経由したスパムの送信
    - C&Cから資格情報を取得
    - 送信元PCのIPアドレスを隠ぺいする効果がある
    - SSLを利用することにより、送信トラフィックを暗号化
  - 最大100スレッド
  - 1メール＝1送信アドレス





展開とペイロード

脅威名	MD5
Adware:Win32/Zugo	5a77b40c7e9de96a4183f82da0836a19
Backdoor:Win32/Kelihos.A	1454b22c36f1427820b24b564efb2e39
TrojanDownloader:Win32/Stasky.A	19616154d6d63a279d77ae11f7b998e9
TrojanDownloader:Win32/Bubnix.A	8e159ff1bbd5a470f903d0e32979811c
Rogue:Win32/FakeSpypro	76f4c35d23b7363fcf6d1870f0169efe
Trojan:Win32/Malagent	7d6ead50862311242902df065c908840
Trojan:Win32/Harnig.gen!D	D0556114e53bae781a5870ef4220e4fc
Trojan:Win32/Hiloti.gen!D	1c8cb08d2841f6c14f69d90e6c340370
Trojan:Win32/Hiloti.gen!D	444bcb3a3fcf8389296c49467f27e1d6
TrojanDownloader:Win32/Renos.MJ	5571a3959b3bd4ecc7ae7c21d500165f
TrojanDownloader:Win32/Renos.MJ	89f987bdf3358e896a56159c1341f518
TrojanDownloader:Win32/Small.SL	Ccd08d114242f75a8f033031ceeafb88
Trojan:Win32/Meredrop	23472a09a1d42dc109644b250db0ca1e
TrojanDownloader:Win32/Waledac.C	B7030bdf24d6828c6a1547dc2eece47d
TrojanDownloader:Win32/Waledac.C	De5bd40cb5414a5d03ffd64f015ffacc
Backdoor:Win32/Cycbot.B	86d308e7a03e9619dbf423e47ac39c50
TrojanDownloader:Win32/Small.SL	2664b0abf4578d0079e3ad59ab697554
Worm:Win32/Skopvel	331fe9a906208ce29ba88501d525356b
Rogue:Win32/Winwebsec	e4a9504875c975b8053568120c56743b

- McColo, Russian Business Networkとの関連
- 偽の医薬品販売サイト
- 偽ウイルスソフト

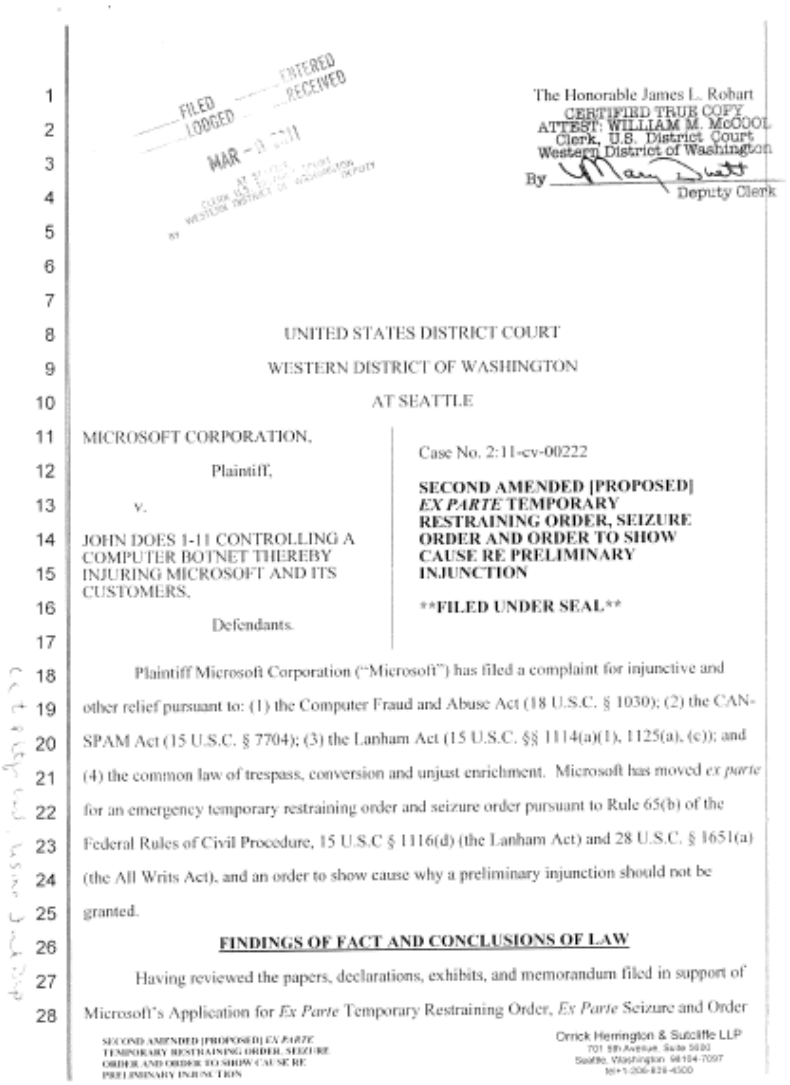
- マルウエアの追加インストール
  - 既知のRustock ドロッパー（Win32/Harnig）に感染させる
  - 対話的な操作を行わずに5分間で左表のマルウエアをダウンロード・インストール
  - これらのマルウエアは、さらに別のマルウエア等をダウンロード（多層構造のダウンローダー）

バックアップ

- C&Cサーバーにアクセスできない場合のバックアップ
  - 毎日16個の新しいドメイン名を生成し、接続を試みる
    - jvwyqarglgwqvt.info 、hy38la8rwpaqlpiy.com 等の無意味な文字列
  - 6種類の生成アルゴリズム
    - 毎日96個のドメイン

- ボットネットの制御にはIPアドレスを使用

裁判における Rustock の対処



FILED LODGED ENTERED RECEIVED
MAR – 9 2011
AT SEATTLE CLERK U.S. DISTRICT COURT WESTERN DISTRICT OF WASHINGTON DEPUTY

The Honorable James L. Robart
CERTIFIED TRUE COPY
ATTEST: WILLIAM M. McCOOL
Clerk, U.S. District Court
Western District of Washington
By _____ Deputy Clerk

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

MICROSOFT CORPORATION,

Plaintiff,

v.

JOHN DOES 1-11 CONTROLLING A COMPUTER BOTNET THEREBY INJURING MICROSOFT AND ITS CUSTOMERS,

Defendants.

Case No. 2:11-cv-00222

SECOND AMENDED [PROPOSED] *EX PARTE* TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

****FILED UNDER SEAL****

Plaintiff Microsoft Corporation ("Microsoft") has filed a complaint for injunctive and other relief pursuant to: (1) the Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) the CAN-SPAM Act (15 U.S.C. § 7704); (3) the Lanham Act (15 U.S.C. §§ 1114(a)(1), 1125(a), (c)); and (4) the common law of trespass, conversion and unjust enrichment. Microsoft has moved *ex parte* for an emergency temporary restraining order and seizure order pursuant to Rule 65(b) of the Federal Rules of Civil Procedure, 15 U.S.C § 1116(d) (the Lanham Act) and 28 U.S.C. § 1651(a) (the All Writs Act), and an order to show cause why a preliminary injunction should not be granted.

FINDINGS OF FACT AND CONCLUSIONS OF LAW

Having reviewed the papers, declarations, exhibits, and memorandum filed in support of Microsoft's Application for *Ex Parte* Temporary Restraining Order, *Ex Parte* Seizure and Order

SECOND AMENDED [PROPOSED] EX PARTE TEMPORARY RESTRAINING ORDER, SEIZURE ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

Orrick Herrington & Sutcliffe LLP
701 5th Avenue, Suite 5600
Seattle, Washington 98104-7097
tel+1-206-839-4300

- マイクロソフトは、商標が不正に使用されたことに基づき、被告人名不詳として起訴
- C&CのIPアドレスに基づき、裁判所の差し押さえ命令を請求し、2011年3月9日に発令
- 連邦保安官の警護の下、現場から証拠を収集し、サーバーをホスティングプロバイダーから押収
  - 本件に関係する法的文書は、www.noticeofpleadings.com に掲載されています

Rustock ボットネットのオペレーターに対して発令された一時禁止命令

解析結果

- 2011年3月16日、米国の7都市に拠点を置くホスティングプロバイダー5社からサーバーを押収
- プロバイダーの支援を受け、ボットネットを制御しているIPアドレスを分断

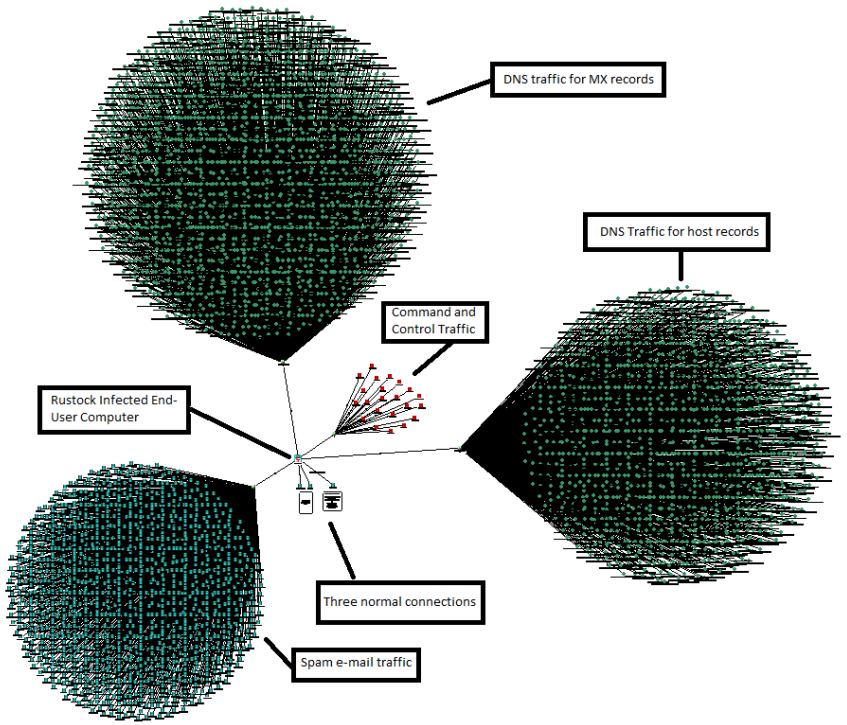
- ハードディスク20台の解析結果
  - スパムを送信するためのソフトウェアとデータ
    - 数千個の、メールアドレス、ID/パスワードの組み合わせを含んだテキストファイル
    - 42万個以上の電子メールアドレス
    - マイクロソフトや製薬会社の商標を不正に利用したテンプレート
  - ロシアのIPアドレスに対するサイバー攻撃に利用されていたことを示すデータ
  - 匿名インターネットアクセスを提供するノードとして使用
    - 電子メールテンプレート、商標、電子メールアドレスなどを保存する Rustockシステムへの匿名アクセスを提供するために使用したとみられる
- サーバーのホスティング契約を調査
  - オンライン決済サービスを利用
  - アカウントはモスクワ付近の住所が登録
  - C&Cサーバの多くは“Cosma2k”という個人によって設定
  - このニックネームは多数の異なる名前と関連
  - 法的な措置を取るために、これらの名前、電子メールアドレス、その他の証拠に対する調査を継続している

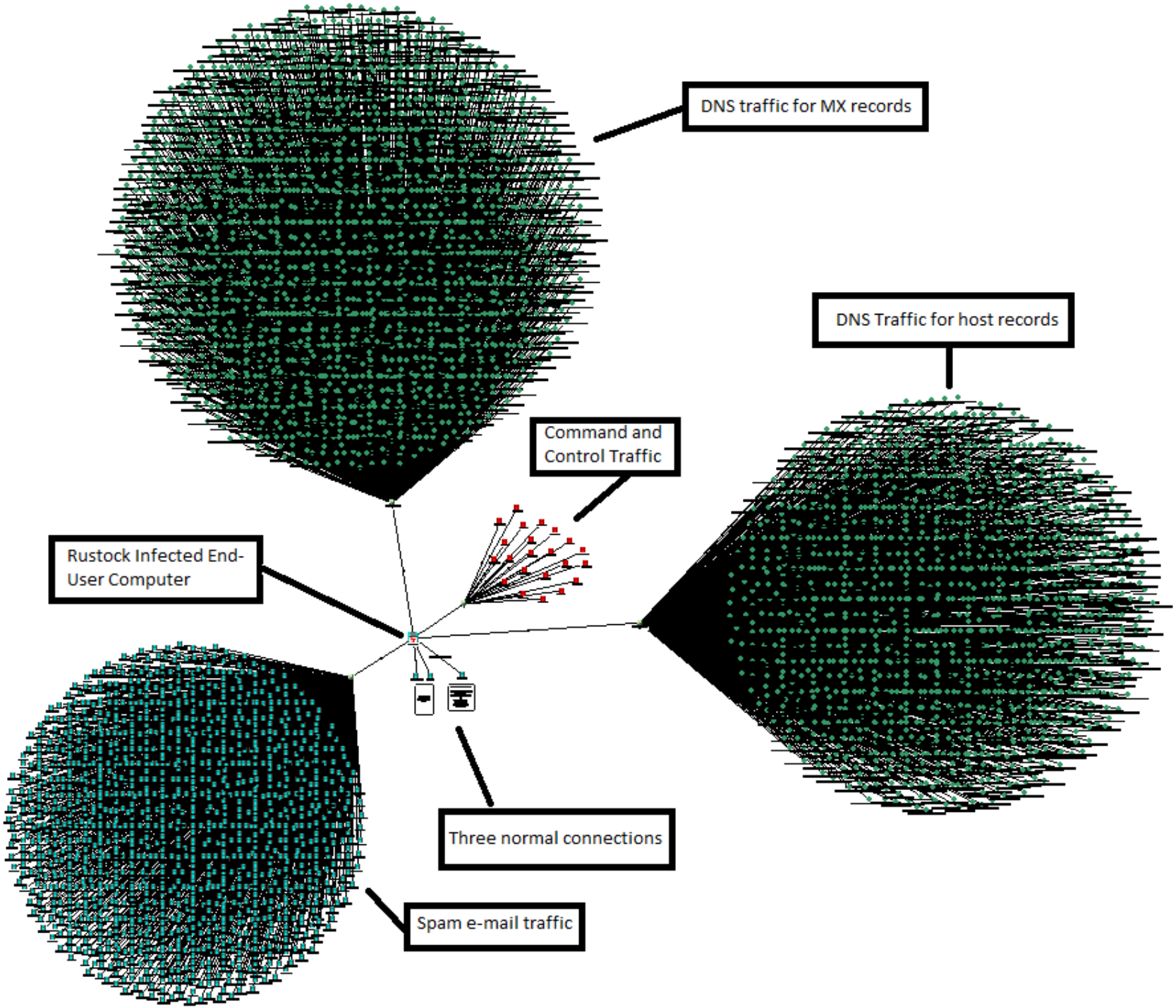
Rustock に関する統計

- 130万を超えるIPからRustockを検出
  - 2011/1/22　～　2011/2/4

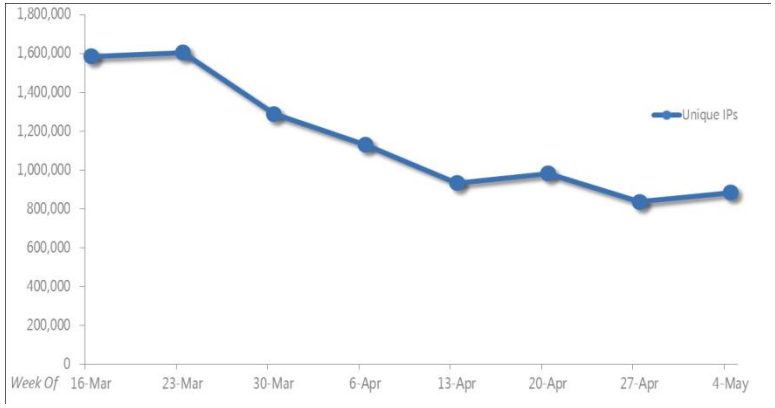
- Rustockのネットワーク活動

  1台のRustockに感染したPCの24分間の動き
  - 3つの通常通信
  - DNS　Aレコード　　1,406回
  - MXレコード　　2,238回
  - 送信したメールサーバ　1,376台
  - C&C等との通信　　22回

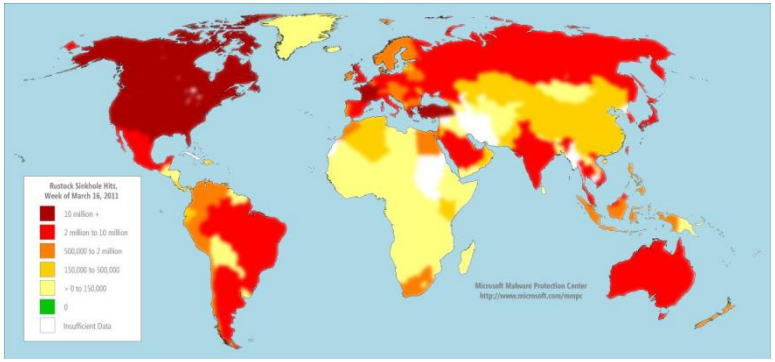


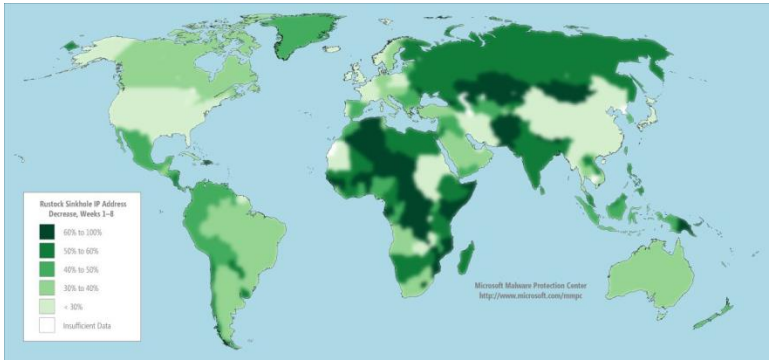

DNS traffic for MX records
DNS Traffic for host records
Command and Control Traffic
Rustock Infected End-User Computer
Three normal connections
Spam e-mail traffic

オペレーションの結果



シンクホールに接続した IP アドレス数の推移 (1 週間ごと)





- Rustockが利用するフェールオーバー用ドメイン名を使った観測
  - アルゴリズムを解析し、該当するドメイン名をマイクロソフトが取得
  - このドメインへの通信は、シンクホールへ向けられる

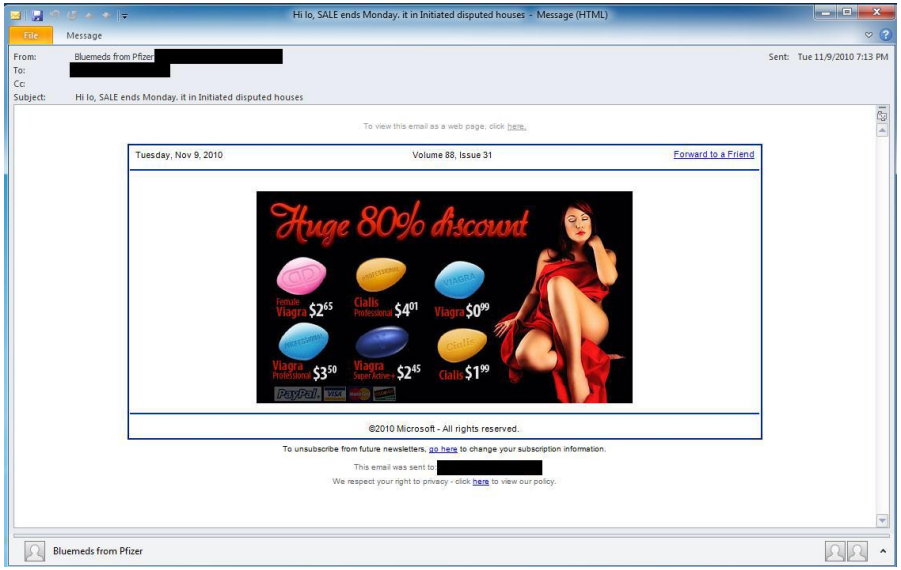
- 地理的な分析

第1週(トラフィックの多い国)	
米国	5,580万
フランス	1,370万
トルコ	1,340万
カナダ	1,140万
インド	730万
ブラジル	710万

第1週(トラフィックの少ない国)	
中国	42万
チリ	50万
デンマーク	53万
ノルウエー	58万

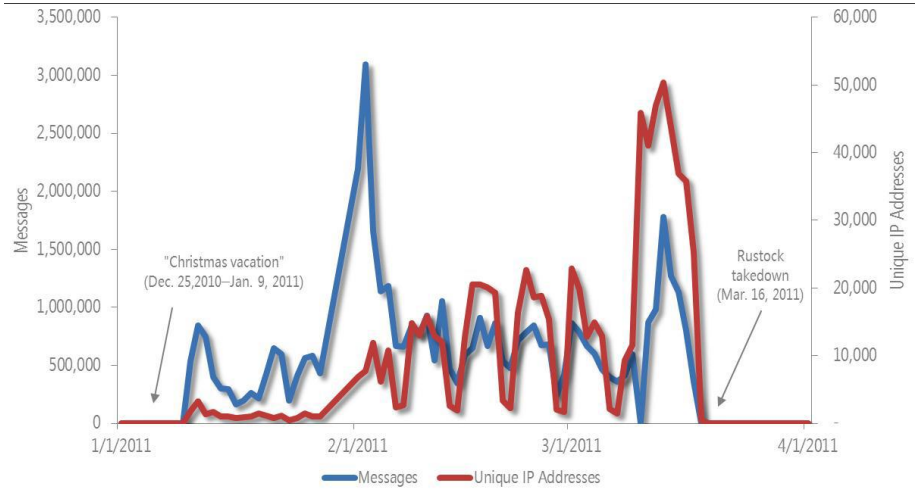
スパムに関する統計

- スパムメールの送信量
  - 一日で300億通の発信を記録
  - 1台の感染PC（DCU）
    - 45分間で7,500通のスパムを送信
    - 24万通/日に相当



- Pfizerからの裁判での参考人としての供述
  - Rustockによって宣伝されている医薬品を購入し分析し、その結果を供述
    - 製造環境条件が安全ではない
    - 不適切な有効線分を含む
    - 間違った投薬量を表示
    - 殺虫剤、鉛を含んだ路面標示用塗装、床用ワックスなどによる汚染

マイクロソフト製品によって検出された Rustock スパム活動



2011 年第 1 四半期に FOPE によって検出された Rustock ボットネットの活動 (受信したメッセージの数と使用された IP アドレスの数)

- Rustock から発信される大量のスパムは、Microsoft® Forefront® Online Protection for Exchange (FOPE) を使用して検出
- 2010年12月25日から2011年1月9日の間、Rustockボットネットは完全に非アクティブ
  - クリスマス休暇と、休息期間がぶつかったことの影響？
- 休暇期間後は、通常通りの活動を再開
- 2月初旬までは典型的な安定した活動パターン
- 遮断後の3月中旬には活動量が、ほぼゼロまで急減

むすび

- Rustock ボットネットは、かつては世界最大のスパムボットの 1 つとして報告され、1 日に 300 億通のスパム メッセージを発信したこともあります。
- マイクロソフト、司法制度、そして業界が力を合わせた結果、Rustock を 2011 年 3 月 16 日に遮断することに成功しました。
- Waledac や Rustock などの大規模ボットネットに対して取られた対応は、この種の対応としては前例のないものですが、これが最後ではないことは確かです。
- サイバー犯罪集団がサイバー犯罪活動の基幹としてボットネットを利用し続ける限り、マイクロソフトと世界中の業界パートナー、学術機関、法執行機関は犯罪集団との闘いに継続的に尽力していきます。
- 私たちが力を合わせれば、犯罪集団によってボットネットが利用されるのを阻止し、誰にとっても安全で信頼できるインターネットを作成することが可能となります

Operation B71
Zeus ボットネットのTakedown

Operation B71/Zeus ボットネットの Takedown

- 概要
  - 2012/3/12 最も危険視されるZeusボットネットの主要なC&Cを押収し、Takedownを行った。
  - 押収したC&Cのモニターと収集した情報に基づき、Zeusに感染したPCの特定と回復、犯罪者の追跡を進めている。
  - 今回の、オペレーションでは、Zeusボットネットを完全に停止させるには至らないが、サイバー犯罪組織に対して、長期的なインパクトを与えたものと考えられる
- オペレーション参加組織
  - Microsoft Digital Crime Unit(+MMPR, Support, TwC)
  - Information Sharing and Analysis Center (FS-ISAC)
  - NACHA – The Electronic Payments Association
  - Kyrus Tech Inc.
  - 他に、F-Secure等のサポートを受ける
- Zeusボットネットによる被害（Microsoft 調べ）
  - 被害額は5億ドル（≒　350億円）に上ると推定
  - 世界では1300万以上の感染が疑われ、米国内でも300万以上

ZEUS / ZBOTの概要

Zeus / Zbot

- Zeusについて
  - Zbotとも呼ばれるボットで、ジェネレーターとC&Cを構築するツールキットとして流通している
    - バージョンや機能により　$700-$15,000程度
  - 多数の亜種が存在し、数百におよぶZeusボットネットが構築されている。
  - Zeusは、キーロガー等を使い、認証情報を盗み出すことで、金銭的な利益を得ることを主要な目的としている。
  - 被害額は、5億ドルにのぼり、感染数は 1300万台に上ると推定されている

Figure 2
Countries where Zeus has been found, for the month of October 2009

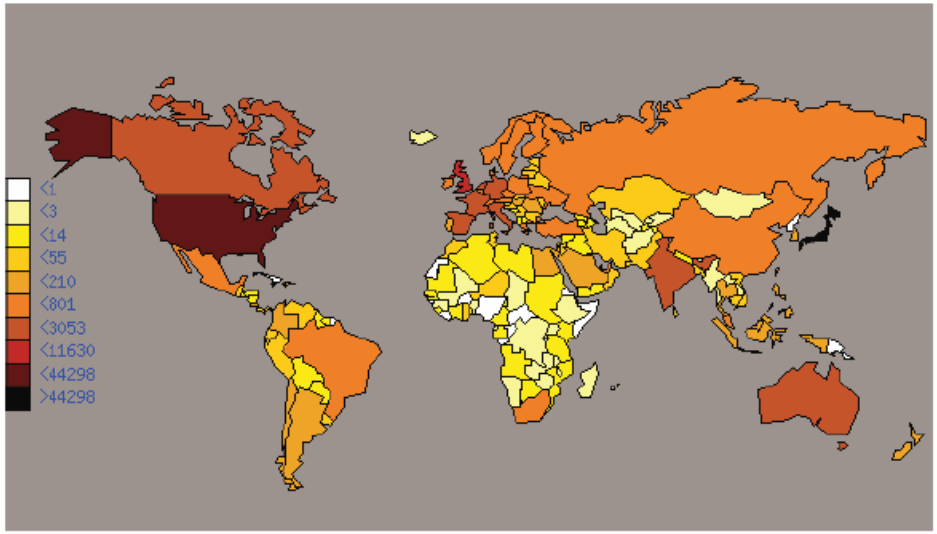
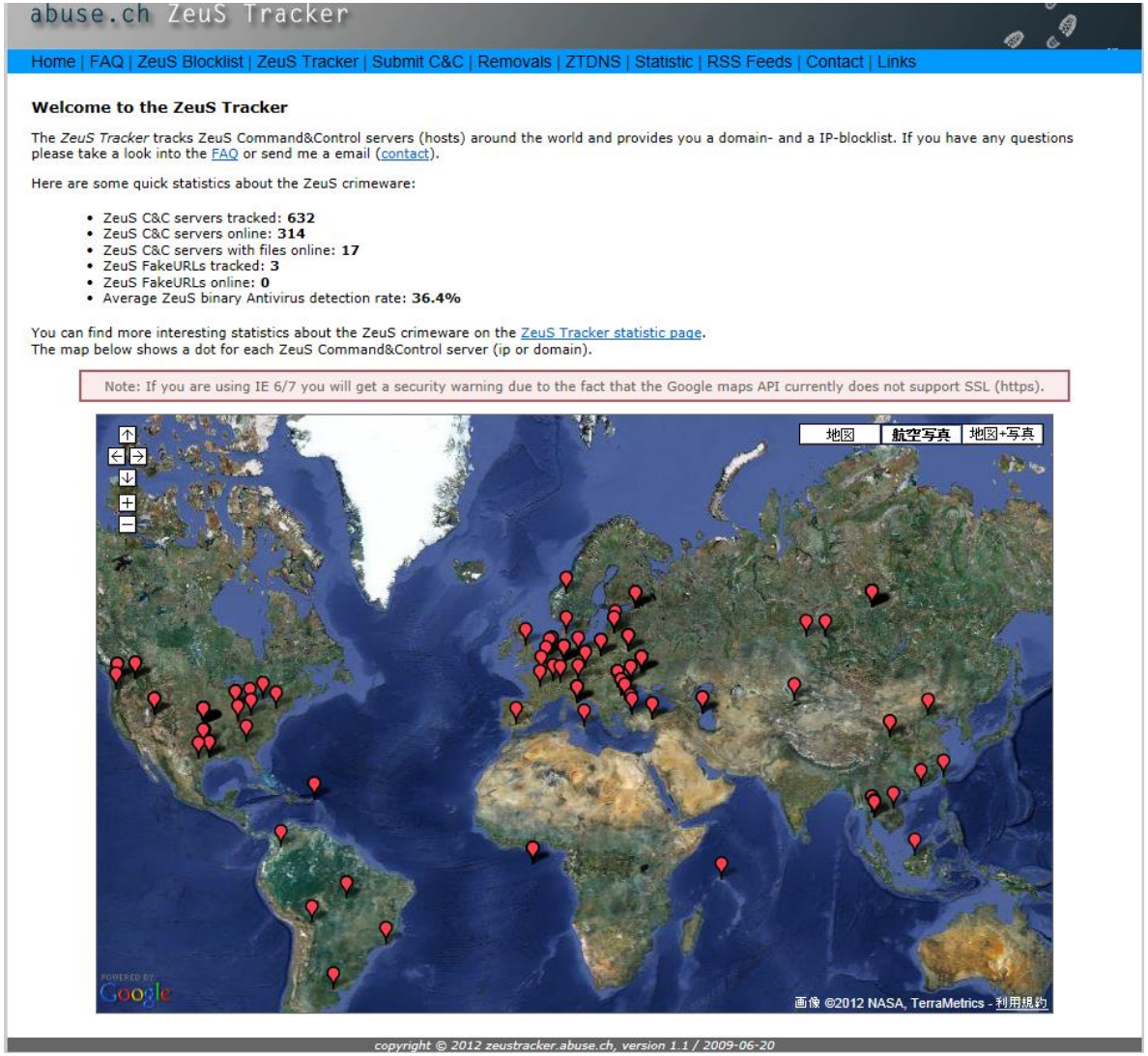


Figure 4
Web page before injection

Figure 5
Web page after injection

図およびグラフの出典：Symantec Zeus: King of the Bots
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

ZeuS Tracker



What is abuse.ch ZeuS Tracker?

The *abuse.ch ZeuS Tracker* provides you the possiblity to track ZeuS Command&Control servers (C&C) and malicious hosts which are hosting ZeuS files. The tracker captures and track the ZeuS hosts aswell as the associated config files, binaries and dropezones. The main focus is to provide system administrators the possiblity to block well-known ZeuS hosts and avoid ZeuS infections in their networks. Therefore you can download a ZeuS domain blocklist and the ZeuS IP blocklist (see ZeuS blocklist). Additionally the ZeuS Tracker should help CERTs, ISPs and LEs (law enforcement) to track malicious ZeuS hosts in their network / countries. For this purpose there are some RSS feeds available (see section *"Is there a RSS feed available?*").

https://zeustracker.abuse.ch/faq.php

FS-ISACからのアラート
（Secret Service, FBI, IC3, FS-ISA）

Fraud Advisory for **Businesses**: Corporate Account Take Over

This product was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Problem:
Cyber criminals are targeting the financial accounts of owners and employees of small and medium sized businesses, resulting in significant business disruption and substantial monetary losses due to fraudulent transfers from these accounts. Often these funds may not be recovered[1].

N.Y. Firm Faces Bankruptcy from $164,000 E-Banking Loss

European Cyber-Gangs Target Small U.S. Firms, Group Says

e-Banking Bandits Stole $465,000 From Calif. Escrow Firm

La. firm sues [bank] after losing thousands in online bank fraud

Cyber attackers empty business accounts in minutes

Zeus hackers could steal corporate secrets too

TEXAS FIRM BLAMES BANK FOR $50,000 CYBER HEIST

Computer Crooks Steal $100,000 from Ill. Town

FBI Investigating Theft of $500,000 from NY School District

Zeus Botnet Thriving Despite Arrests in the US, UK

Figure 1: Recent news headlines from *The New York Times*, *The Washington Post*, *Computer World*, and *Krebs on Security*.

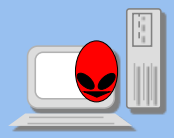
- サイバー犯罪組織は、中小規模企業の経営者と従業員の口座情報をターゲットとしている。
- これにより、重大なビジネス上の混乱と、相当額の金銭的な損失が発生している

  - ＮＹの企業が$16.4万の損失で破産
  - E-Bank強盗が、$46.5万をカリフォルニアの金融機関から盗んだ
  - ロサンゼルスの企業が、数千ドルのオンライン詐欺をうけ、銀行に対して訴訟を起こした
  - サイバー攻撃は、ビジネス講座を、数分で空にする
  - Zeusハッカーは、企業の機密情報を盗むこともできる
  - テキサスの企業が、$5万のサイバー強盗に対して、銀行を非難している
  - コンピューター詐欺が、イリノイ州の町から、$10万を盗んだ
  - FBIは、ニューヨークの学校区から、$50万が盗まれた件を捜査している
  - 米国・英国での逮捕にも関わらず、Zeusボットネットは生き残っている

http://www.fsisac.com/files/public/db/p265.pdf

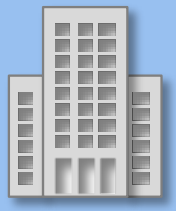
二要素認証の回避（Zeus）

PCから口座情報を詐取



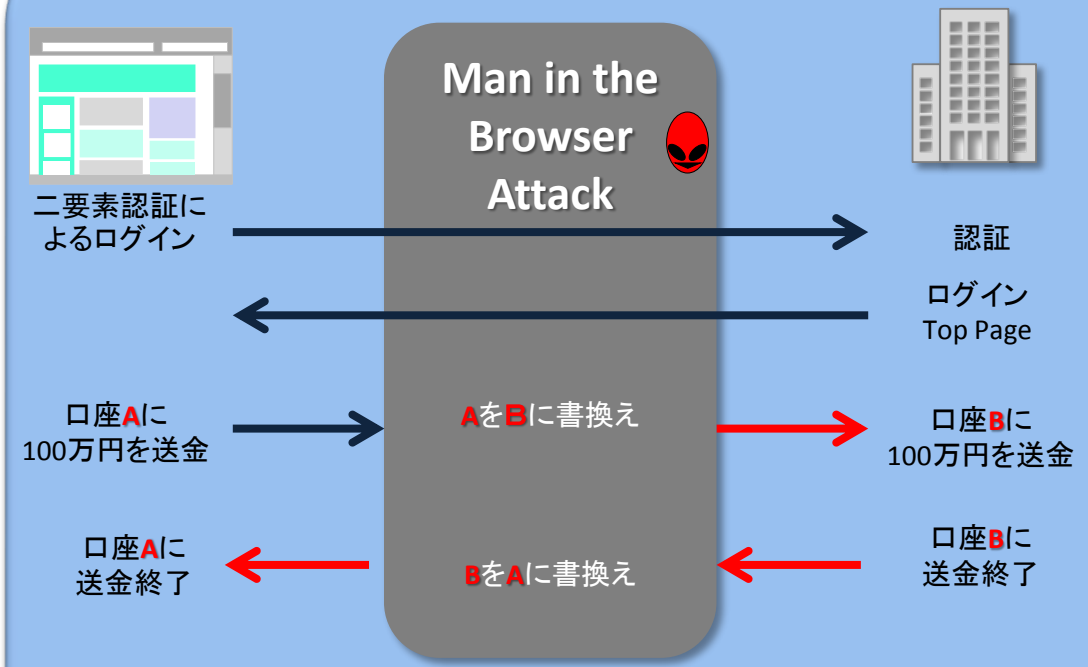
・ファイル等からの詐取
・Key loggerによる詐取

銀行などの
ID盗難の対策



・二要素認証
乱数表
ワンタイムパスワード

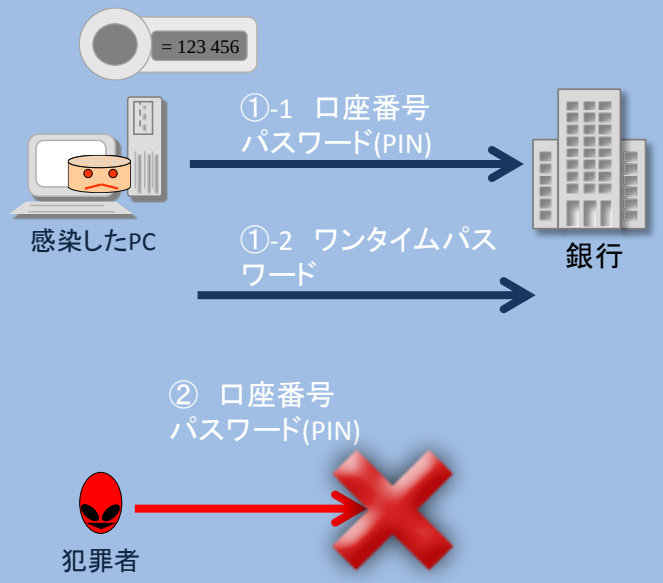
二要素認証を使うオンラインバンクからの金銭を詐取



認証の確立したセッションを利用して、トランザクションを改ざんするため、二要素認証でも攻撃を防ぐことができない。また、銀行から表示されるデータも改ざんされているため、この行為に気づくことは困難。
一般に、送金先は、Money Muleと呼ばれる運び屋の口座が利用される。
Zeus/Zbot, URLZone/Bebloh 等

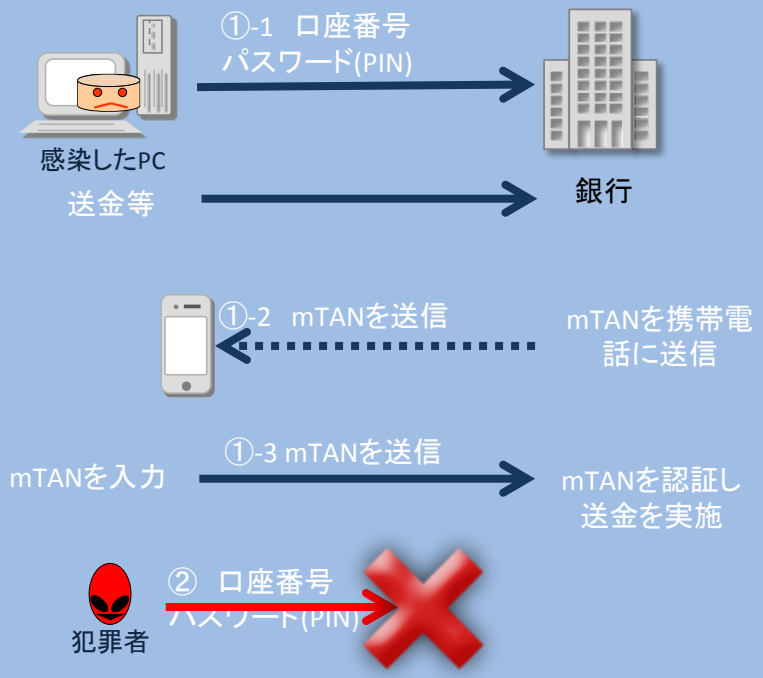
mTANに対する攻撃（SpyEye）

ワンタイムパスワードによる対策



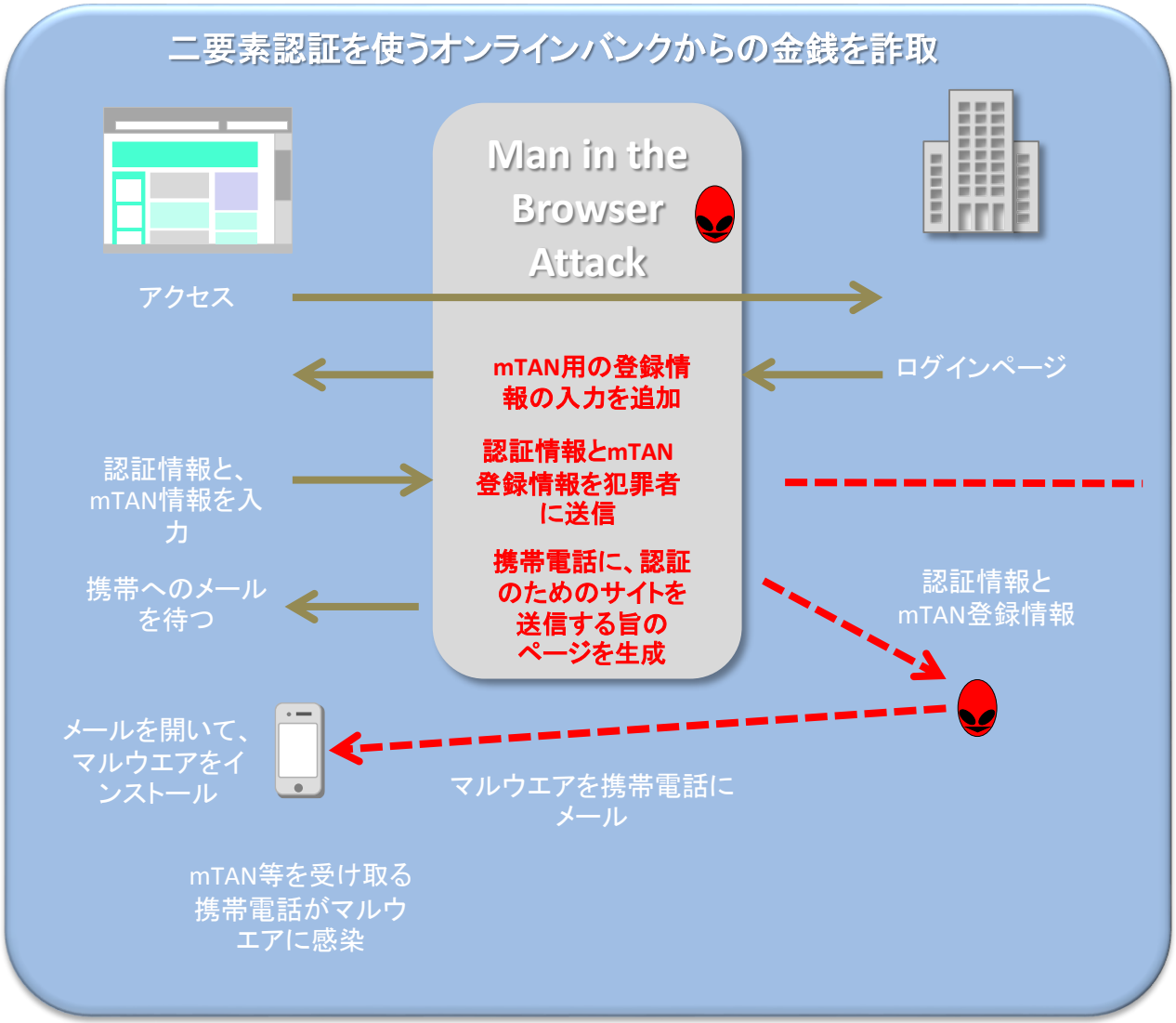
乱数表による対策
① 利用者がオンラインバンクにログインする
ワンタイムパスワードで認証する
② キーロガーがこれを詐取し、外部の犯罪者に送信する
③ 犯罪者は、認証情報を利用して、銀行から現金を引き出そうとするが、ワンタイムパスワードが取得できないため、ログインができない

mTANによる対策



乱数表による対策
① 利用者がオンラインバンクにログインする
重要な取引は、mTANを通じて携帯電話に送信される認証コードを使って確認が行われる
② キーロガーがこれを詐取し、外部の犯罪者に送信する
③ 犯罪者は、認証情報を利用して、銀行から現金を引き出そうとするが、mTANに送信された認証コードが手に入らないため、取引ができない。

MIBによるインジェクション　1



Mobile TAN (mTAN)

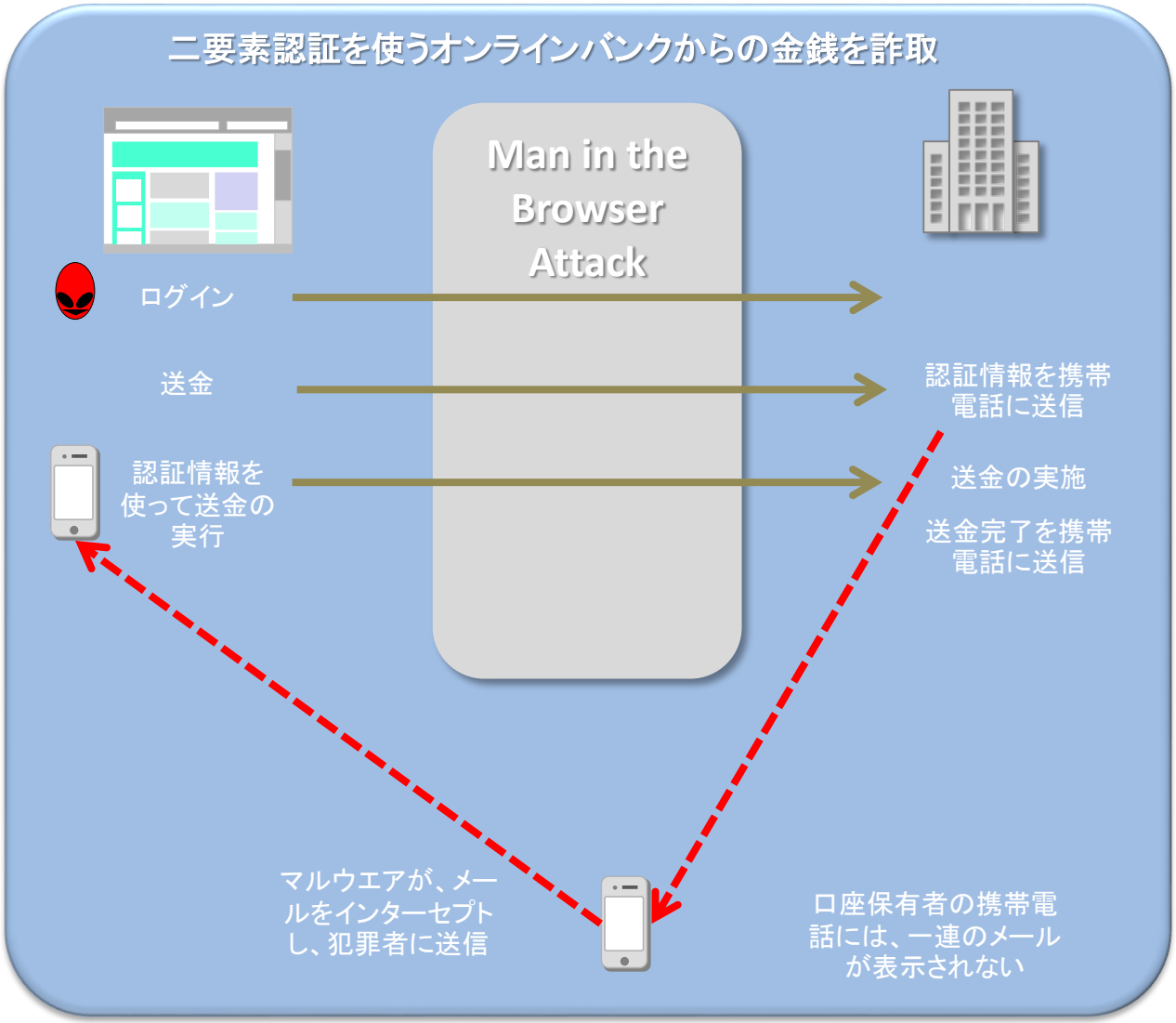
Mobile Transaction authentication number

mTANs are used by banks in Germany, Spain, Switzerland, Austria, Bulgaria, Poland, the Netherlands, Hungary, Russia and South Africa. When the user initiates a transaction, a TAN is generated by the bank and sent to the user's mobile phone by SMS. The SMS may also include transaction data, allowing the user to verify that the transaction has not been modified in transmission to the bank.

However, the security of this scheme depends on the security of the mobile phone system. In South Africa, where SMS-delivered TAN codes are common, a new attack has appeared: SIM Swap Fraud. A common attack vector is for the attacker to impersonate the victim, and obtain a replacement SIM card for the victim's phone from the mobile network operator. The victim's user name and password are obtained by other means (such as keylogging or phishing). In-between obtaining the cloned/replacement SIM and the victim noticing their phone no longer works, the attacker can transfer/extract the victim's funds from their accounts.[3]

出典：Wikipedia

MIBによるインジェクション　2



UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MICROSOFT CORP., FS-ISAC, INC., and NATIONAL AUTOMATED CLEARING HOUSE ASSOCIATION, Plaintiffs v. JOHN DOES 1-39 D/B/A Slavik, Monstr, IOO, Nu11, nvidiag, zebra7753, lexa_Mef, gss, iceIX, Harderman, Gribodemon, Aqua, aquaSecond, it, percent, cp01, hct, xman, Pepsi, miami, miamibc, petr0vich, Mr. ICQ, Tank, tankist, Kusunagi, Noname, Lucky, Bashorg, Indep, Mask, Enx, Benny, Bentley, Denis Lubimov, MaDaGaSka, Vkontake, rfcid, parik, reronic, Daniel, bx1, Daniel Hamza, Danielbx1, jah, Jonni, jtk, Veggi Roma, D frank, duo, Admin2010, h4x0rdz, Donsft, mary.J555, susanneon, kainehabe, virus_e_2003, spaishp, sere.bro, muddem, mechan1zm, vlad.dimitrov, jheto2002, sector.exploits AND JabberZeus Crew CONTROLLING COMPUTER BOTNETS THEREBY INJURING PLAINTIFFS, AND THEIR CUSTOMERS AND MEMBERS, Defendants.	Case No. CV 12-1335 (CBA)

Plaintiffs Microsoft Corporation, National Automated Clearing House Association and FS-ISAC, Inc. (Financial Services – Information Sharing and Analysis Center) have sued defendants John Does 1-39 associated with the Internet Domains and Internet IP Addresses listed in the documents below. Plaintiffs allege that Defendants have violated Federal and state law by operating a computer botnet through these Internet domains and Internet IP addresses, causing unlawful intrusion, intellectual property violations and dissemination of unsolicited bulk email to the injury of Microsoft and the public. Plaintiffs seek a preliminary injunction and seizure order directing the registries and web hosting companies associated with these Internet domains and IP addresses to take all steps necessary to disable access to and operation of these Internet domains and IP addresses, ensure that changes or access to the Internet domains and IP addresses by Defendants cannot be made absent a court order and that all content and material associated with these Internet domains and IP addresses is to be isolated and preserved pending resolution of the dispute. Plaintiffs seek a permanent injunction, other


Scranton, PA

Operation b70
販売されているPCに組み込まれた NitolボットネットのTakedown

Operation b70 の概要

- 2012/9/13　マイクロソフト デジタルクライムユニットから、市場で販売されているPCからWindowsの海賊版にNitolと呼ばれるボットの組み込みが確認されたこと、このボットがC&Cなどに利用して3322.orgへの法的措置により、Nitolボットネットのtakedownを実施したことを発表
  - **Microsoft Disrupts the Emerging Nitol Botnet Being Spread through an Unsecure Supply Chain**
    - http://blogs.technet.com/b/microsoft_blog/archive/2012/09/13/microsoft-disrupts-the-emerging-nitol-botnet-being-spread-through-an-unsecure-supply-chain.aspx
  - 販売されている PC に組み込まれた Nitol ボットネットのTakedown（オペレーション b70）
    - http://blogs.technet.com/b/jpsecurity/archive/2012/10/02/3523720.aspx
- 2012/10/3 3322.orgの所有者との和解によりマイクロソフトは訴訟を取下げ、CN-CERTが、3322.orgの所有者と共に対応が行われることとなった
  - **Microsoft Reaches Settlement with Defendants in Nitol Case**
  - http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx
- 今回の事案のような、マルウエアが埋め込まれた安全ではないPCやソフトウェアを避け、安心してPCを利用するためには
  - コンピューター、ソフトウェアともに、信頼できる販売元から購入する
  - 不自然に安価で売られているPC、ソフトウェア、パーツなどに注意する
  - 利用するPCはソフトウェアを常に最新にアップデートを行う
  - より詳しい対策はHow to Tellを参照ください
    - http://www.microsoft.com/ja-jp/howtotell/default.aspx

Nitolボットネット発見の経緯

- DCUの研究者が購入したコンピューターからマルウエアを検出
  - 訝しい(unsecured)PCモールから購入した20台のコンピューターのうち、4台からマルウエアを検出
- Nitolボットへの着目
  - この内、1台のPCから検出したNitolボットが検出され、サイバー犯罪者により、コンピューターやソフトウェア製品を通じて構築されるC&Cに接続すること、さらにUSBメモリなどを通じて感染を広げることを確認
  - 他のPCで検出されたマルウエアは、ボットではなく、DDoSツール、バックドア、キーロガーであった

- NitolボットネットのC&C: 3322.orgドメイン
  - NitolのC&Cサーバーとして3322.orgのサブドメインが利用されていた
  - これらのドメインは、評判の悪く不穏な活動と関係があった
  - これらの70,000を超えるサブドメインでは、NitolボットネットのC&Cに他に、500以上のマルウエアをホストしていた
    - Webカメラをリモートから利用するものも確認された

NitolボットネットのTakedown

- 3322.orgのDNSをマイクロソフトに移管する ex parte TRO（2012/9/10)
  - 3322.orgの所有者と彼の会社、その他のJohn Doesに対する訴訟
  - 3322.orgと70,000のサブドメインのアドレスは、マイクロソフトが新たに構築したネームサーバーの管理下とした
  - C&Cやマルウエアを配布するサブドメインのIPアドレスは、シンクホールへと変更され、証拠収集とNitolと500以上のマルウエアに感染した利用者が、これをクリーンアップするために利用する
  - 正常なサブドメインは、本来のIPアドレスで利用される

- ISPおよびCERTとの連携
  - 感染した利用者をマルウエアから守るため、世界中のISPとCERTとの連携を開始した

和解の成立と訴訟の取下

- 3322.org所有者と和解（2012/10/3)
  - 和解条件に従い、3322.orgの権威ネームサーバーを再開する
  - ブロックリストにあるすべてのサブドメインを、CN-CERTが指定し管理するシンクホールに向けることによりブロックする
  - MicrosoftおよびCN-CERTによりマルウエアと関係するサブドメインが特定された場合、これをブロックリストに追加する
  - 可能な限り、合理的で適切なステップを講じ、中国で感染したコンピューターの所有者を特定し、マルウエアを削除することを助ける

- 今後の対応
  - すべての成果物はCN-CERTに引き継がれる
  - CN-CERTは、被告と共に中国の法律に準じて、サブドメインの背後にいる人物を特定する

Operation B71の概要

- Zeusとその変種である SpyEye, Ice-IXによって構成されるボットネットに対するオペレーション
- 2012/3/19 に、 Microsoftはパートナーと共に、Waledac, Rustock, Kelihos のケースと同様に、ZeusボットネットのC&Cを切断を行うためのJohn Does 1-39訴訟を行った
  - パートナー
    - Microsoft Digital Crime Unit(+MMPR, Support, TwC)
    - Information Sharing and Analysis Center (FS-ISAC)
    - NACHA – The Electronic Payments Association
    - Kyrus Tech Inc.,
- これまでの訴訟と同様に、連邦商標法等違反等により、ホスティングプロバイダーに設置されたサーバーを差し押さえ、証拠保全を行う事を目的としている

- 加えて、Zeusが犯罪者ネットワークに係わることから、RICO法の適用も行ったRICO法を適用することで、Zeusの犯罪的なオペレーションに係わった全ての関係者に対して、民事訴訟を起こすことが出来るようになった。
  - リコ（ＲＩＣＯ）法とは http://plus.yomiuri.co.jp/article/words/%EF%BC%B2%EF%BC%A9%EF%BC%A3%EF%BC%AF%E6%B3%95
  - 組織犯罪を取り締まるための米国の法律。１９７０年に制定された。組織犯罪そのものを禁じて重い刑を適用するほか、犯罪組織が不法に得た財産などの没収を規定している。犯罪組織が支配する企業や団体などの解散を求めることもできる。

- Microsoft, FS-ISAC, NACHAは、執行官と共にペンシルバニア州　Scrantonとイリノイ州　Lombardの2ヶ所でホストされているC&Cサーバーを差し押さえ、重要なデータと仮想的な証拠を押収
  - Zeusに係わる二つのIPアドレスを無効化
  - C&Cを押収で判明した800ドメインをモニターし、数千に上るZeusに感染したコンピューターの特定を進めている

Microsoft Names Defendants in Zeus Botnets Case; Provides New Evidence to FBI

The Official Microsoft® Blog

NEWS & PERSPECTIVE FROM MICROSOFT

MICROSOFT NEWS CENTER →

TechNet Blogs > The Official Microsoft Blog – News and Perspectives from Microsoft > Microsoft Names Defendants in Zeus Botnets Case; Provides New Evidence to FBI

Microsoft Names Defendants in Zeus Botnets Case; Provides New Evidence to FBI

2012/7/3 1:00 AM

MICROSOFT DIGITAL CRIMES UNIT

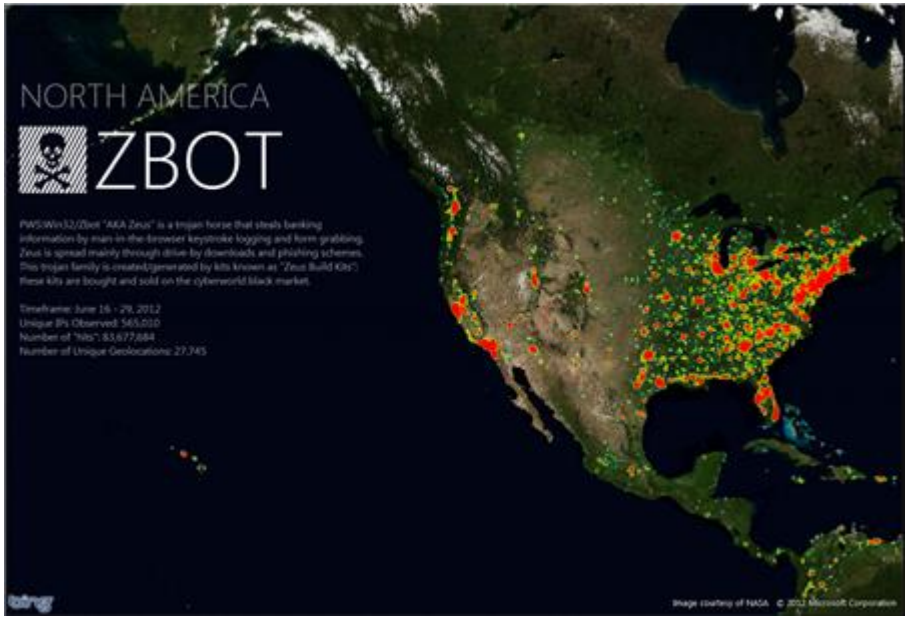
A little over three months ago, I wrote here about how Microsoft's Digital Crimes Unit, along with its financial industry partners and Kyrus Tech, took action to disrupt the dangerous Zeus botnets, known for fueling half a billion dollars in online fraud and identity left. We are pleased to announce that we have identified and named two defendants as members behind the Zeus botnet family, and that we will also be referring the case to the FBI for criminal review, turning over all of the evidence gathered so far, including evidence of a broader group of perpetrators beyond the named defendants.

- Zeus Botnetの二人の関係者Yevhen KulibabaとYuriy Konovalenko 2人を特定し、被告人として訴えた
- 犯罪捜査はFBIに委ねており、特定した2名の情報を含む、グループに関する全ての情報を提供し、犯罪として立件することを目指している
- Yevhen KulibabaとYuriy Konovalenkoは、他のZeus事件で、イギリスで服役中である事を掴み、イギリス政府に対し、FBIへの被疑者照会を勧めた

http://blogs.technet.com/b/microsoft_blog/archive/2012/07/02/microsoft-names-defendants-in-zeus-botnets-case-provides-new-evidence-to-fbi.aspx

オペレーションの成果

- The Electronic Payments Associationは、NACHAを装ったフィッシングメールが、90%減少したと報告している
- Zeus Botnetも 3月末時点の 43%　に低下した



2012/3/25-31	2012/6/17-23
779,816	336,393

サイバー犯罪のコストを上げ、サイバー犯罪を抑止する

補足

Kelihos作成者との和解

TechNet Blogs > The Official Microsoft Blog > Microsoft Reaches Settlement with Second Kelihos Defendant

Microsoft Reaches Settlement with Second Kelihos Defendant

19 Oct 2012 9:00 AM

Last September, I shared that Microsoft, Kaspersky and Kyrus Inc. took action against the Kelihos botnet, the first case in which Microsoft named a defendant in one of its civil cases involving a botnet. In January, based on new evidence in the case, Microsoft amended its original complaint and named Andrey N. Sabelnikov, a Russian software programmer, as a new defendant in the lawsuit. Today, I am pleased to say we have reached an agreement with Mr. Sabelnikov, and have officially settled and closed the Kelihos botnet case.

Late last week, Microsoft and Andrey Sabelnikov agreed to the following joint statement, which closed the case:

"Microsoft and St. Petersburg software programmer Andrey Sabelnikov have entered into a Settlement Agreement in the matter of Microsoft v. Sabelnikov. During the negotiations, after reviewing the evidence provided by Microsoft and engaging in discussions, the parties have come to an understanding that Mr. Sabelnikov wrote code that was used in the Kelihos botnet code, but the

セキュリティインテリジェンスレポート

http://www.microsoft.com/ja-jp/security/resources/sir.aspx

http://www.microsoft.com/security/sir/default.aspx

今回ご紹介した内容は、セキュリティインテリジェンスレポート内、
もしくは特別エディションで紹介しています

Microsoft Digital Crimes Unit

Sign c

News Center

Mobile Subscribe Follow

Our Company | Our Products | Blogs & Communities | Press Tools

Microsoft Digital Crimes Unit Newsroom

Home | Press Materials | Video Gallery | Image Gallery | News Archives

The Microsoft Digital Crimes Unit is a worldwide team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer and more secure through strong enforcement, global partnerships, policy and technology solutions that help:

- Promote a secure Internet
- Defend against fraud and other threats to online safety
- Protect children from technology-facilitated crimes
- Champion a healthy Internet marketplace for advertisers and businesses

Microsoft Reaches Settlement with Second Kelihos Defendant

Oct. 19, 2012
Microsoft reached an agreement with the second

Press Contact

Rapid Response Team
Waggener Edstrom Worldwide
(503) 443-7070

Related Links

DCU on YouTube
DCU on Facebook

http://www.microsoft.com/en-us/news/presskits/dcu/