マイクロソフトのサイバー犯罪対策の取り組み

セキュリティ問題 – サーバールームから役員室へ

“ネットセキュリティはCEOレベルで対処すべき事項”

McKinsey & Co.
高度ネットワーク社会で出来ることとそのリスク: 企業への示唆
2014年1月

CEOの61%

ネット攻撃が増加することを心配
PwC
グローバル CEO 調査 2015年1月

内部監査担当者の65%

「ここ1～2年のネットセキュリティーリスクについて、役員の見方はどう変わりましたか？」との問いに対し65%以上の内部監査担当はリスクに対する認識が高い、あるいは高まっていると回答した
内部監査担当者
2014年 動向調査より

APAC CIO 調査: 新しいテクノロジ採用に際しての最大の障壁

1

予算
81%

新しいテクノロジに対する
投資の不足

2

信頼
79%

新しいテクノロジに対する
セキュリティ、プライバシーや
コンプライアンスの懸念

3

採用に伴う影響
72%

ITに関する決定をする際に、
多くの利害関係者が生まれ、意思決定が遅延

デジタルクライムユニット

マルウェアとの戦い
~ ネットの危険性の減少 ~

ネット上の弱者の保護

デジタルクライムユニット

ビッグデータ

調査

法的対応

マイクロソフト サイバークライムセンター

DCU ボットネットのテイクダウンとマルウェアの駆除

OPERATION Conficker

2010年2月

マイクロソフト主導モデル

業界広域での取組

ボットネットワーム

65% ⬇

OPERATION Waledac

2010年2月

業界主導での取組モデルの証明

70,000-90,000の感染デバイスをボットネットから断絶

スパム

30% ⬇

OPERATION Rustock

2011年3月

業界全体の利害関係者によるサポート

米国とオランダの法執行機関とCN-CERT参加

スパム

99% ⬇

OPERATION Zeus

2012年3月

金融サービスとの業界間協力

複雑な技術のため根絶に注力

個人情報盗難/金融詐欺

95% ⬇

OPERATION Nitol

2012年9月

中国で信頼されるサプライチェーンで広まったNitol

問題発生のドメイン管理者と話し合い解決

ボットネットを広めているマルウェア、分散型サービス拒否攻撃

OPERATION Bamital

2013年2月

検索結果を乗っ取り、被害者を危険サイトに誘導

Symantec社と協力し、プロアクティブな通知とクリーンアッププロセスを実施

広告ワンクリック詐欺

93% ⬇

OPERATION Citadel

2013年6月

オンラインバンク詐欺で5億ドル以上の損失発生

ネット犯罪を防止する官民プログラムとの協力で解決

個人情報盗難/金融詐欺

76% ⬇

OPERATION ZeroAccess

2013年12月

検索結果を乗っ取り、被害者を危険サイトに誘導

毎月270万ドル以上の費用がオンライン広告主に発生

広告ワンクリック詐欺

78% ⬇

OPERATION Game over Zeus

2014年6月

ネットバンキングのトロイの木馬

法執行機関と協力

個人情報盗難/金融詐欺

98% ⬇

OPERATION Bladabindi & Jenxcus

2014年6月

ダイナミックDNS を用いたマルウェア

パスワード、個人情報の窃盗、およびWEBカメラの乗っ取り

200以上の異なる種類のマルウェアが影響を及ぼしました

個人情報盗難/金融詐欺/プライバシー侵害

47% ⬆

OPERATION Caphaw

2014年7月

オンラインバンク詐欺で2億500万ドル以上の損失発生

官民協力による解決

個人情報盗難/金融詐欺

84% ⬇

スパム:Exchange Online のデータから

Figure 14. Messages blocked by Exchange Online Protection each half-year period, 2H09–1H13

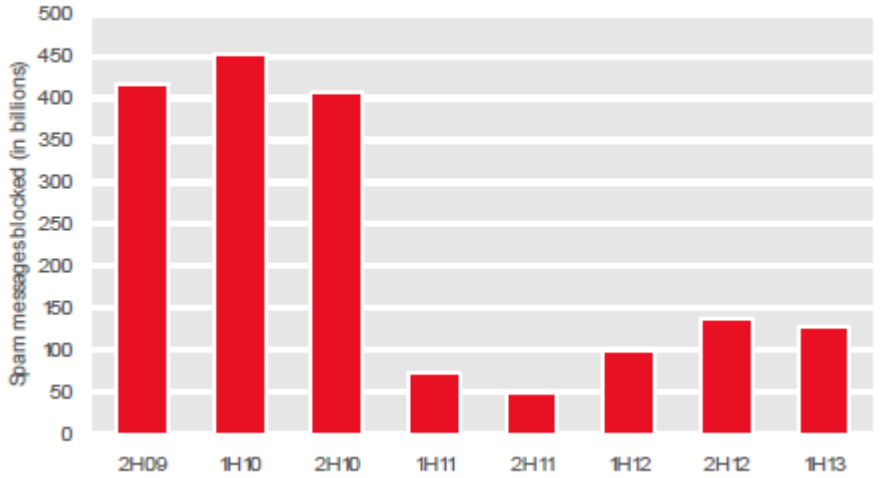
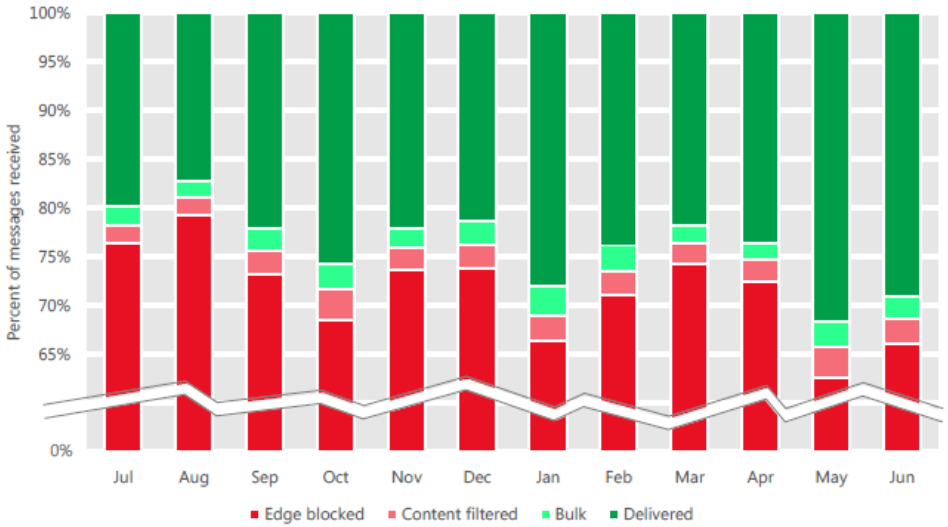
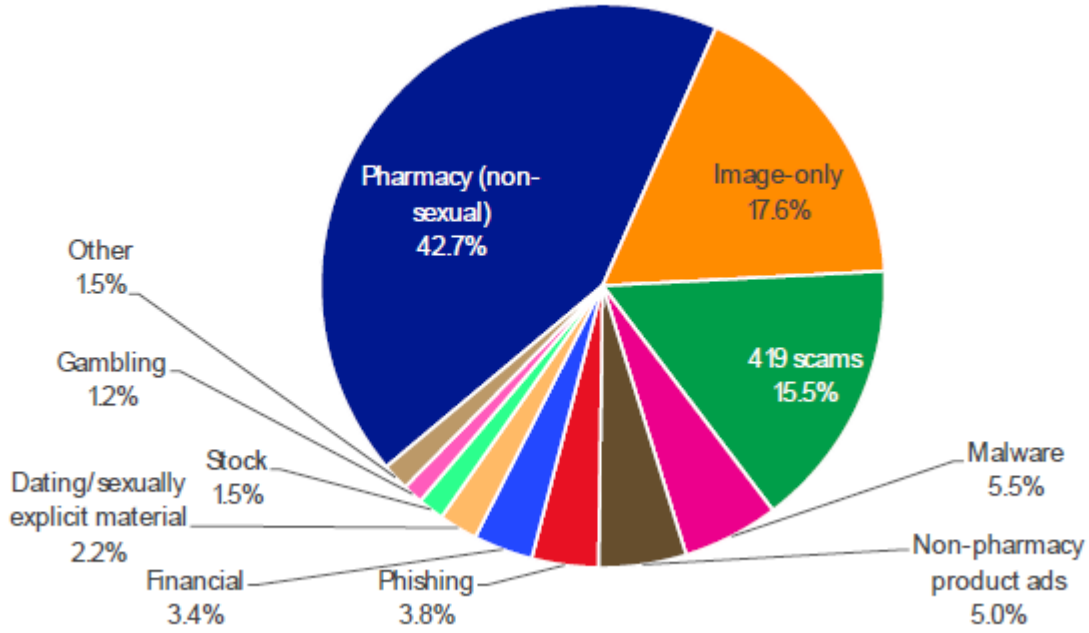


Figure 57. Percentages of incoming messages blocked, categorized as bulk email, and delivered, July 2012–June 2013



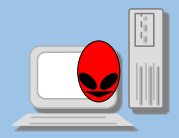
- Exchange Online Protectionのデータに見るスパム
  - スパムの送信量は、2010年に実施されたCutwailと RustockTakedownにより大きく減少し、2010年には1:33(スパム)から、2013年上半期には1:4(スパム)となっている
  - 62.7 - 74.2%のメールは、ネットワークエッジ（Reputation等）でブロック
  - 25.8 - 37.3%のメールだけが、よりリソースを必要とするコンテンツフィルタリングの対象となり、そのうちの7.6 -10.0%（全体の1.7 - 2.7%)がスパムとしてフィルターされる。

Figure 15. Inbound messages blocked by Exchange Online Protection filters in 1H13, by category



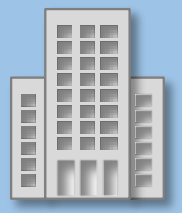
二要素認証の回避（Zeus）

PCから口座情報を詐取



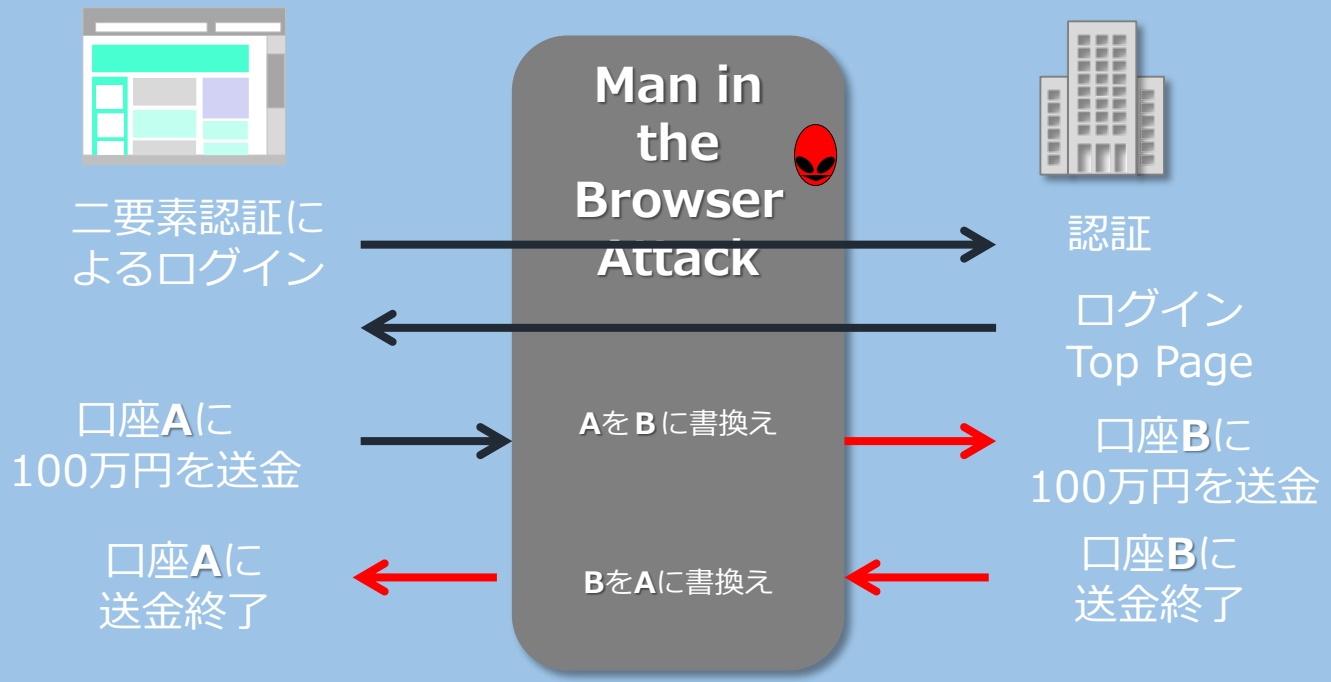
・ファイル等からの詐取
・Key loggerによる詐取

銀行などの
ID盗難の対策



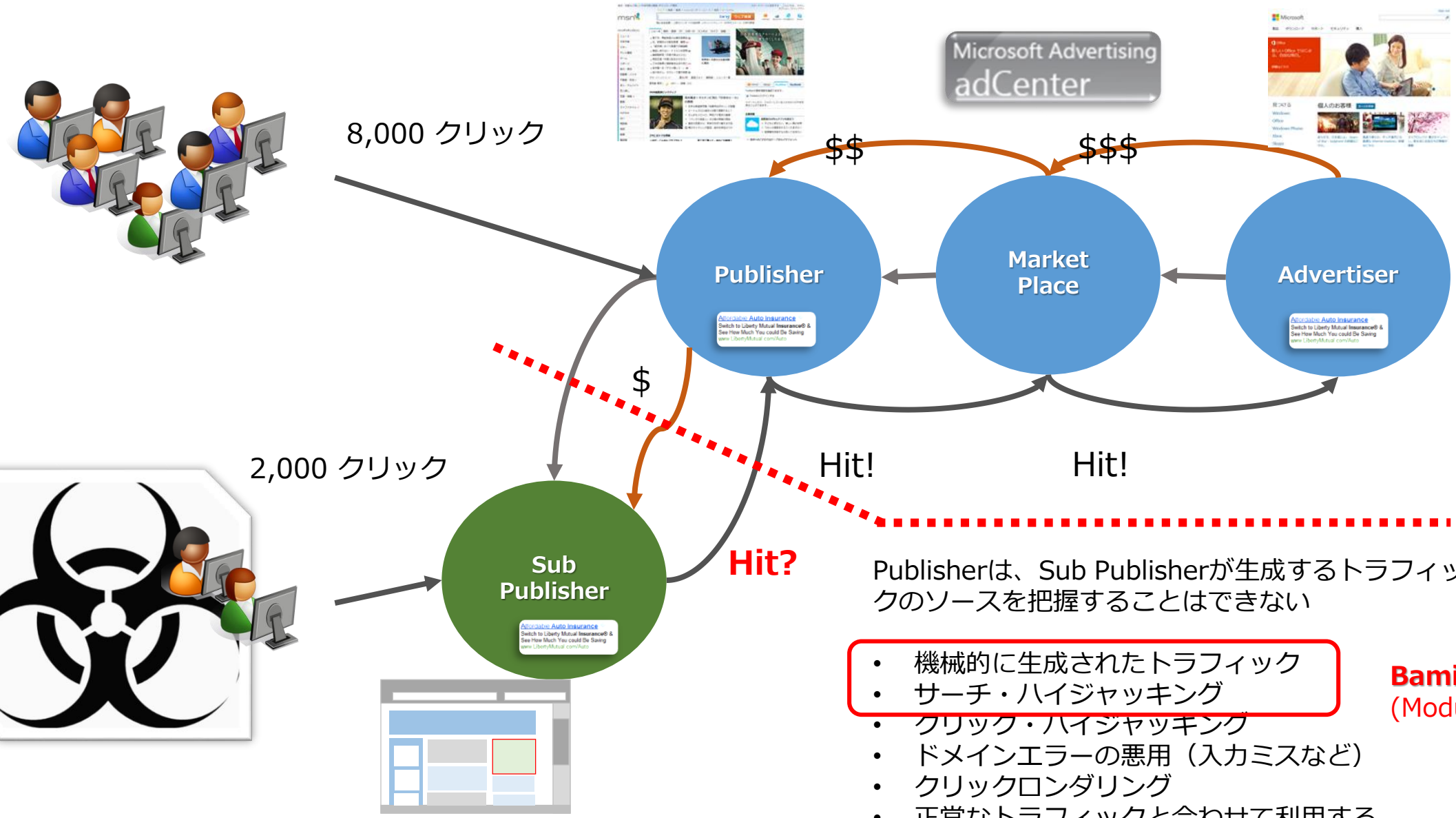
・二要素認証
乱数表
ワンタイムパスワード

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

Sub-Syndicationの問題と悪用



例：BLOG向けのアフェリエートプログラム

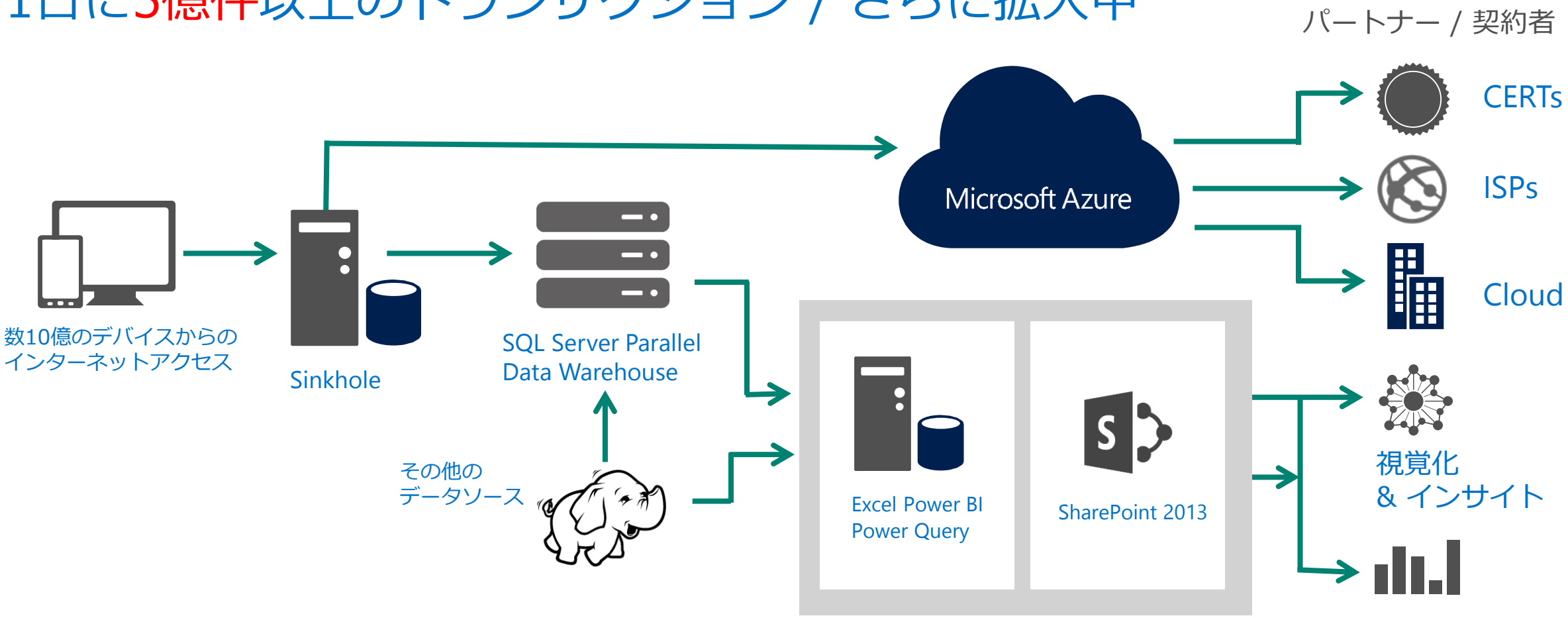
Publisherは、Sub Publisherが生成するトラフィックのソースを把握することはできない

- 機械的に生成されたトラフィック
- サーチ・ハイジャッキング
- クリック・ハイジャッキング
- ドメインエラーの悪用（入力ミスなど）
- クリックロンダリング
- 正常なトラフィックと合わせて利用する

Bamital
(Module C)

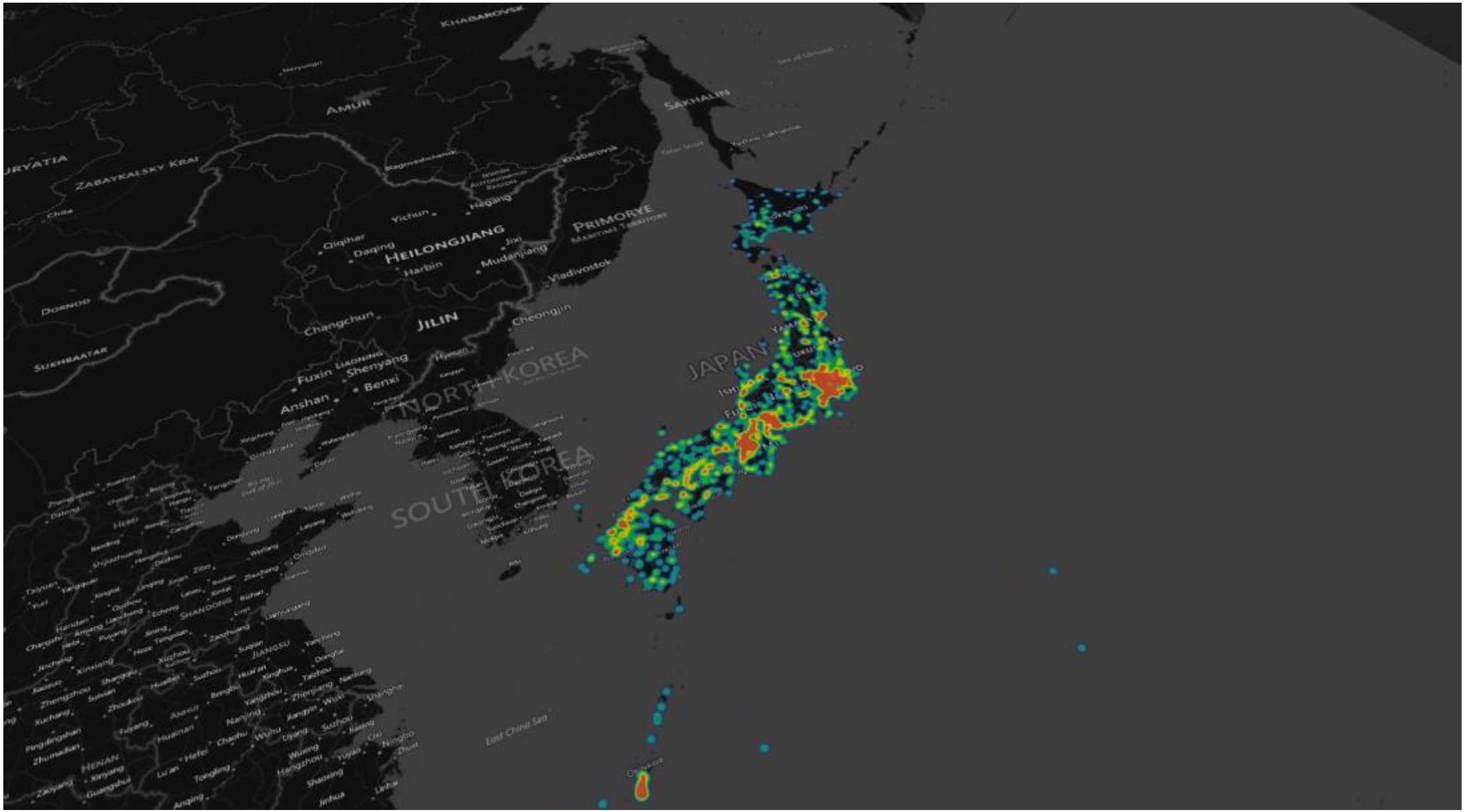
Microsoft Cyber Threat Intelligence Program (CTIP)

1日に5億件以上のトランザクション / さらに拡大中



Microsoft Cybercrime Center BI is powered by:

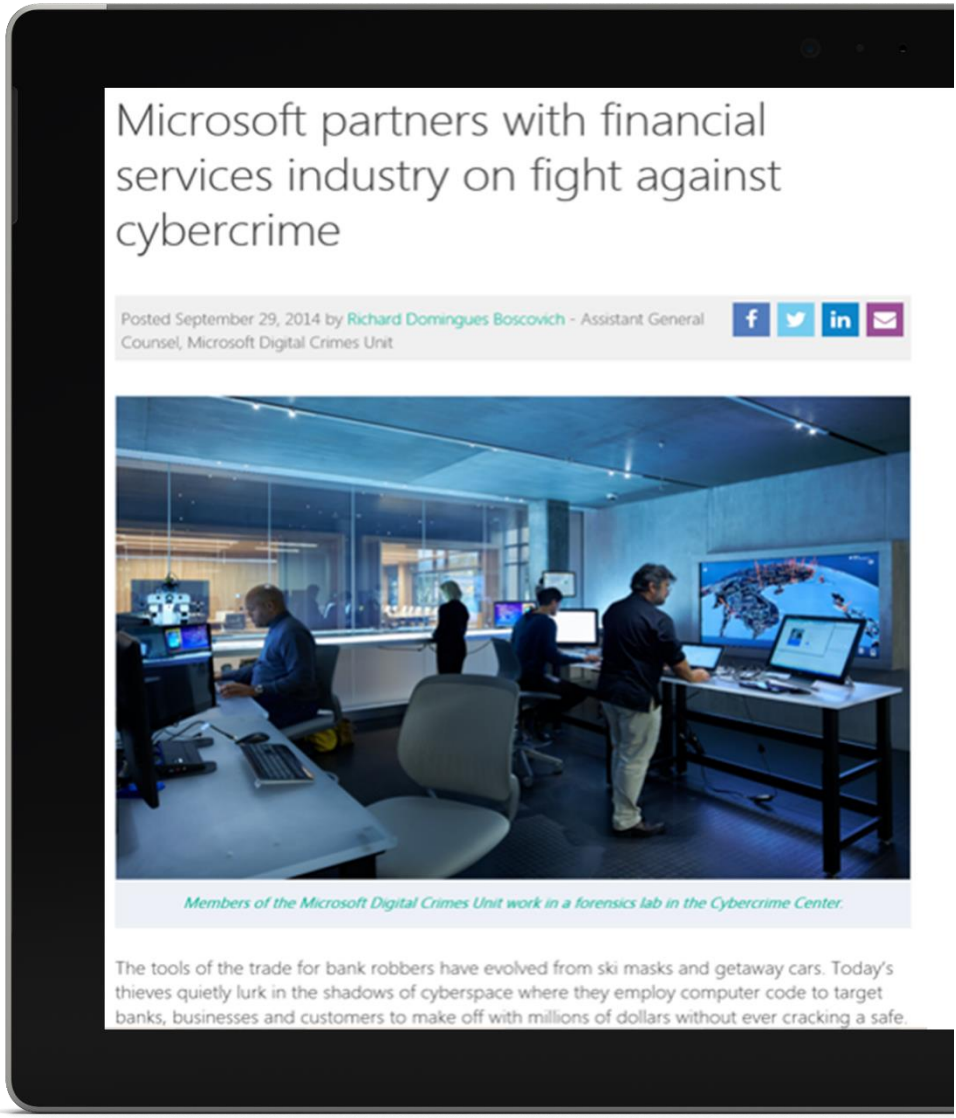
Office 365 Microsoft SQL Server Microsoft Azure Office SharePoint Windows


Khabarovsk
Amur
Sakhalin
Zabaykalsky Krai
Yichun
Hegang
Primorye
Heilongjiang
Qiqihar
Daqing
Harbin
Jixi
Mudanjiang
Vladivostok
Dornod
Changchun
Jilin
Cheongjin
Sukhbaatar
Fuxin
Liaoning
Shenyang
Benxi
Anshan
North Korea
Japan
South Korea
Shandong
Jiangsu
Henan
East China Sea

産業界とのパートナーシップ

2014年9月29日、
マイクロソフト デジタルクライムユニットは
Financial Services Information Sharing
and Analysis Center との協力を発表

FINANCIAL SERVICES | Information Sharing and Analysis Center







被害者となりやすい人々の保護

オンライン上での児童保護 | 人身取引 | 高齢者への詐欺





- 世界中の50以上の組織に無料でライセンス
- 業界標準 – Facebook, Twitter, Google が使用
- マイクロソフト製品の環境で実行
- マイクロソフトからNCMECへの通知により、2014年は**58件の犯罪者を検挙**

Outlook.com bing OneDrive

マルウェアとの戦いとデジタルリスクの減少

被害者となりやすい人々の保護

マイクロソフト サイバークライムセンター 日本サテライト

サイバー犯罪の脅威についての情報発信基地

最新データから日本のマルウェアの情報/状況を解析

サイバー攻撃の傾向等の情報をセキュリティ関連団体などを通じて公表

お客様・パートナー企業へ、「信頼できるクラウド」とセキュリティのベストプラクティスを周知

クラウド上で提供されるPhotoDNA等のツールによりオンライン上の児童ポルノなどの犯罪を防止

デジタルクライムユニットとの連携でサイバー犯罪抑止に貢献

Microsoft

サイバークライムセンター
サテライト

ワシントン

ベルリン

北京

シンガポール

東京

Microsoft

www.youtube.com - Microsoft Digital Crimes Unit

www.facebook.com/MicrosoftDCU

www.twitter.com/MicrosoftDCU

日本サテライトの機能と支援サービス

サイバークライムセンター 日本サテライト

サイバー脅威の最新情報から日本の情報/状況を解析し、情報発信

オンラインサービス事業者や捜査機関に「PhotoDNA」等サイバー犯罪対策の最新技術情報を提供

政府機関へのソースコードの開示などの技術支援・情報提供

標的型攻撃体験ワークショップの開催

本社デジタルクライムユニットと連携

政府機関・企業向け 支援サービスの提供

日本マイクロソフトからのサービス

- 組織内のセキュリティ対策を評価し、改善点を提示するリスクアセスメント
- 攻撃パターンを分析、ゼロデイ攻撃や標的型攻撃などの脅威を検知・監視する脅威検知サービス

パートナー企業と連携したサービス

- 問題の検知 + 駆除

日本マイクロソフトのコミット

日本の経済成長・イノベーションには
サイバー空間が不可欠

より安心・安全な
クラウドサービスを
提供

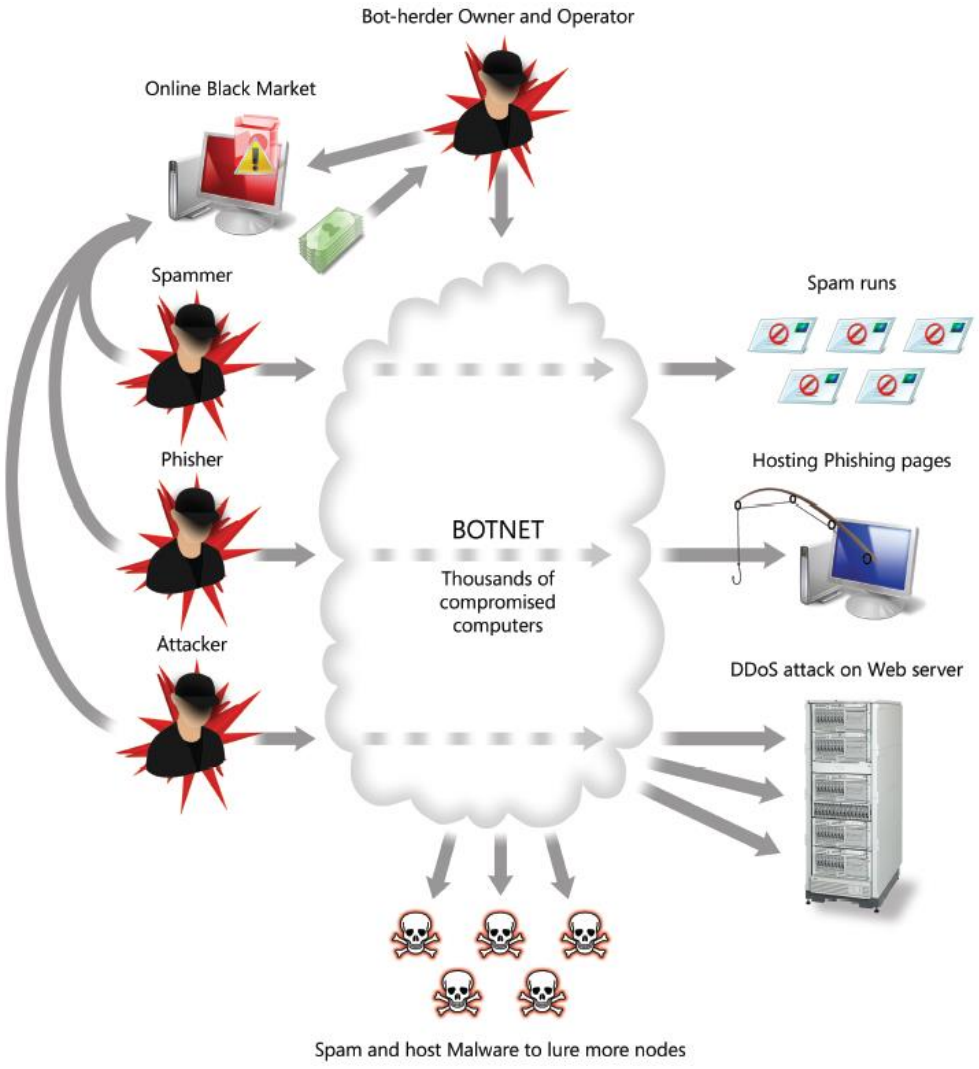
＋

日本のサイバー
セキュリティの確保
への貢献

ボットネットにかかわる技術的な推移と、Takedown事例について

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

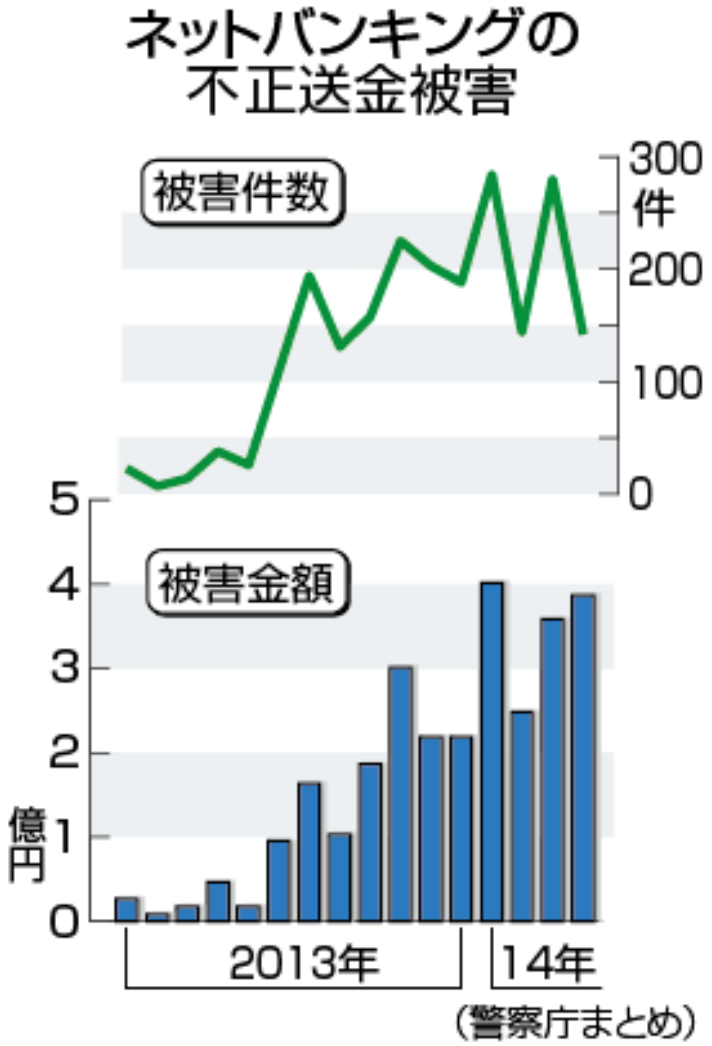
犯罪基盤としてのボットネット



ボットネットとは、感染した数百~数百万台のPCを操作する手法で、様々なサイバー犯罪の基盤として悪用されている

- スパムメール等の送信
  - メールアカウントの詐取
  - フィッシングメールの送信
  - スパムメールの送信
- 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

ボットネット被害の例（Citadel）



◎不正送金、既に最悪被害＝ネット銀58行で14億円－法人口座急増、標的拡大

※記事などの内容は2014年5月15日掲載時のものです

インターネットバンキング利用者の口座から預貯金が勝手に別口座へ送金される被害が、今年は9日までの4カ月余りで約14億1700万円となり、年間で過去最悪だった昨年（14億600万円）を既に上回ったことが15日、警察庁のまとめで分かった。被害に遭った金融機関は32行から58行に拡大。地方銀行と信用金庫・信用組合が増えている上、法人口座の被害も急増している。

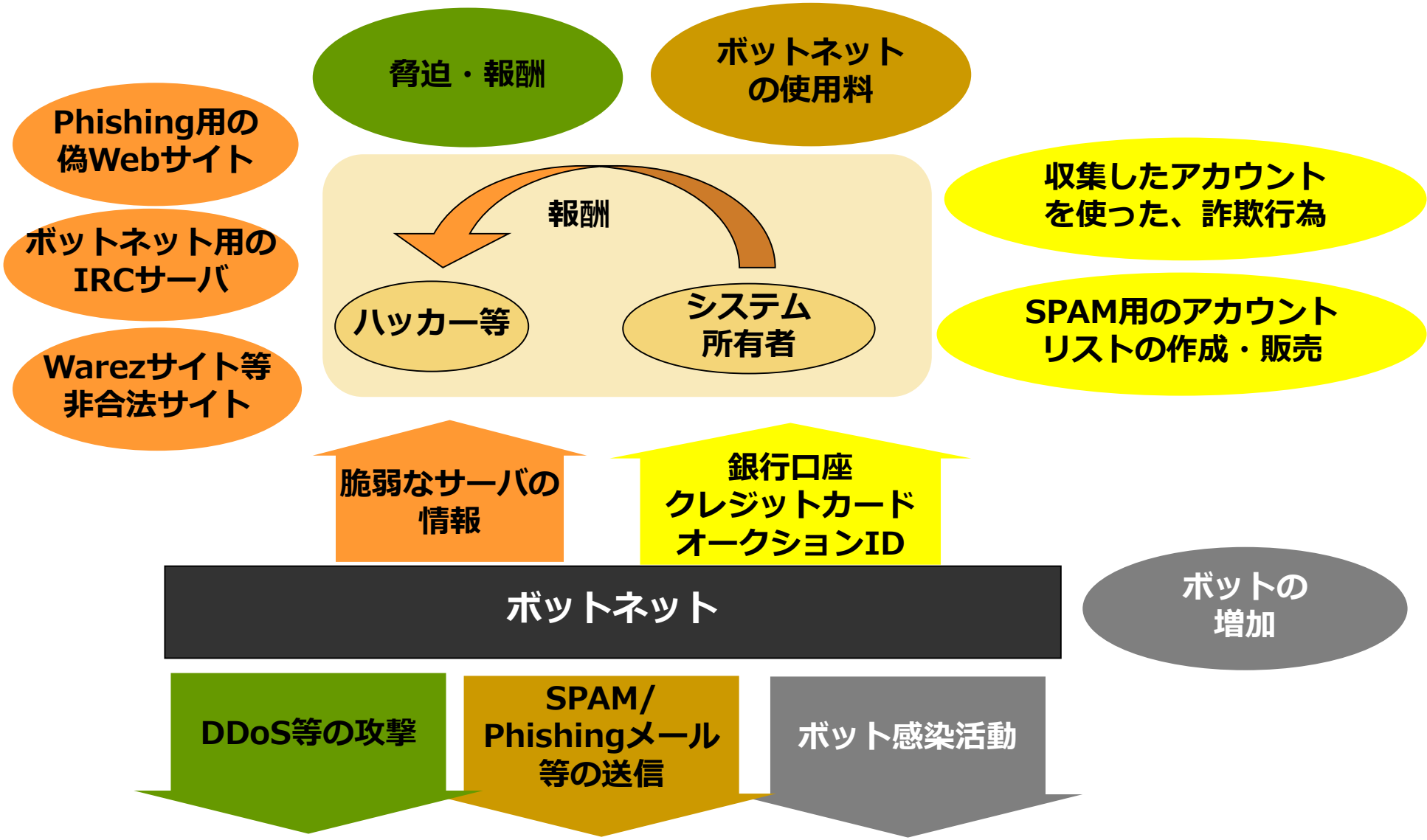
警察庁は「犯人が標的を広げており、被害はさらに膨らむ恐れがある」と警戒。全国銀行協会など金融関係の9団体に同日、対策強化を要請した。

9日までに確認された不正送金は873件あり、利用者の居住地は鳥取を除く46都道府県に及ぶ。1件当たりの平均被害額は約162万円で、昨年より52%増えている。

これは送金額の上限が大きい法人口座が狙われているためで、法人の被害は昨年1年間に54件と全体の4%だったが、今年は既に109件発生し、割合も12%に上昇。被害額は9800万円（7%）から4億8000万円（34%）に増えている。

時事ドットコム
http://www.jiji.com/jc/graphics?p=ve_soc_network-bankfuseisoukin

ボットネットの代表的な機能

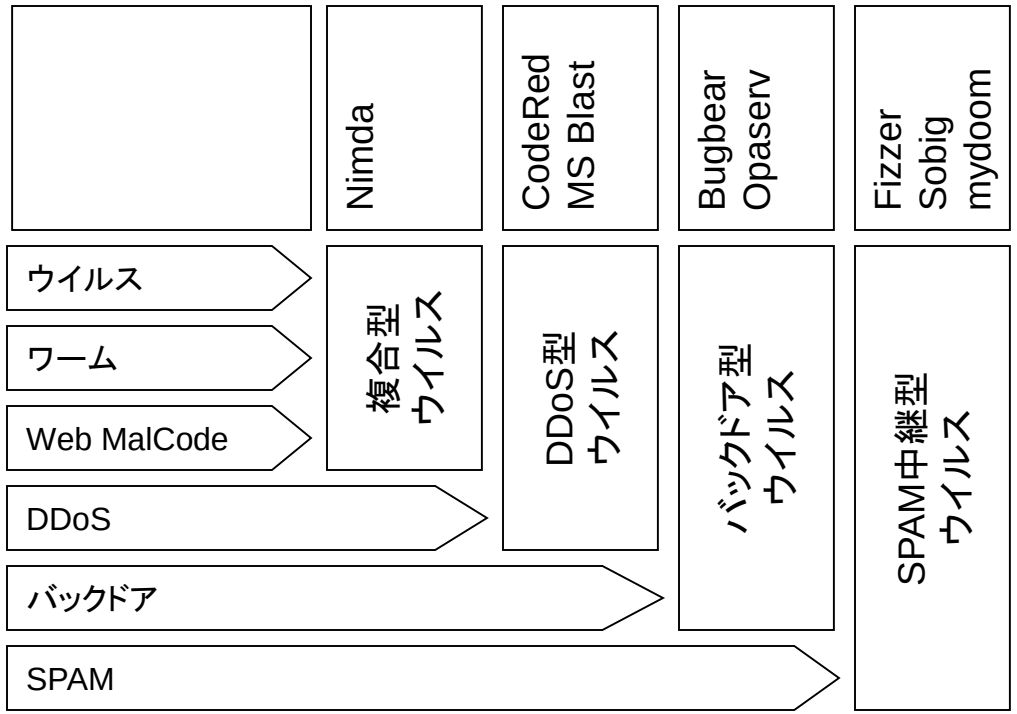


機能面から見た、Malicious Codeの推移

Malicious Programs（有害プログラム）

感染形態に対する呼び方	**ウイルス**	狭義：電子メールを媒体として感染するプログラム 広義：ウイルス・ワームなどを全部ひっくるめて、ウイルス 最近は、Malware(マルウェア)という用語が使われることが増えてきた ペストとか、有害プログラムとよぶ場合もある
	ネットワーク・ワーム	メール型ウィルスが、人間のアクション(メールを開く、添付ファイルを開く等）で感染するのに対して、ワームはPCをネットにつないだだけで感染するもの Nimdaに代表されるように、電子メールでも、ネットワークでも感染するものも少なくない
	マリシャスコード（Web感染）	WEBへのアクセスで感染するもの。 ブラウザ(Internet Explorer）の脆弱性や、脆弱な設定（ActiveX、Java Script、Zone)を利用して感染する。 Nimdaが、msnのホームページに感染したケースや、カカクコムのケースがこれ
	トロイの木馬	ウイルスや、ワームのような自動感染の機能は無いが、ソーシャル的なテクニックで、プログラムを実行させることで、感染（実行）するプログラム
動作に対する呼び方	**スパイウェア**	PCに入っている情報や、PCを操作した内容などを、勝手にどこかに送るプログラム。口座情報や、パスワードなんかが、もって行かれる。キーロガーなども、スパイウェアの一種。
	アドウェア	もともとは、プログラムの料金を**”ただ”**にすることの代償として、広告の表示機能を入れたもの。（Advertising　Ware) しかし、上記スパイウェアと分類されるものが多いなど色々と問題がある場合が少なくない
	バックドア	利用者が意図しない操作を行うための仕掛けを全て、バックドアと呼ぶ。 スパイウェアも、バックドア。他に、ポートを開けて待っているようなバックドアも多い。フィッシングのサーバは、実はバックドア（？）として動いていることが多い

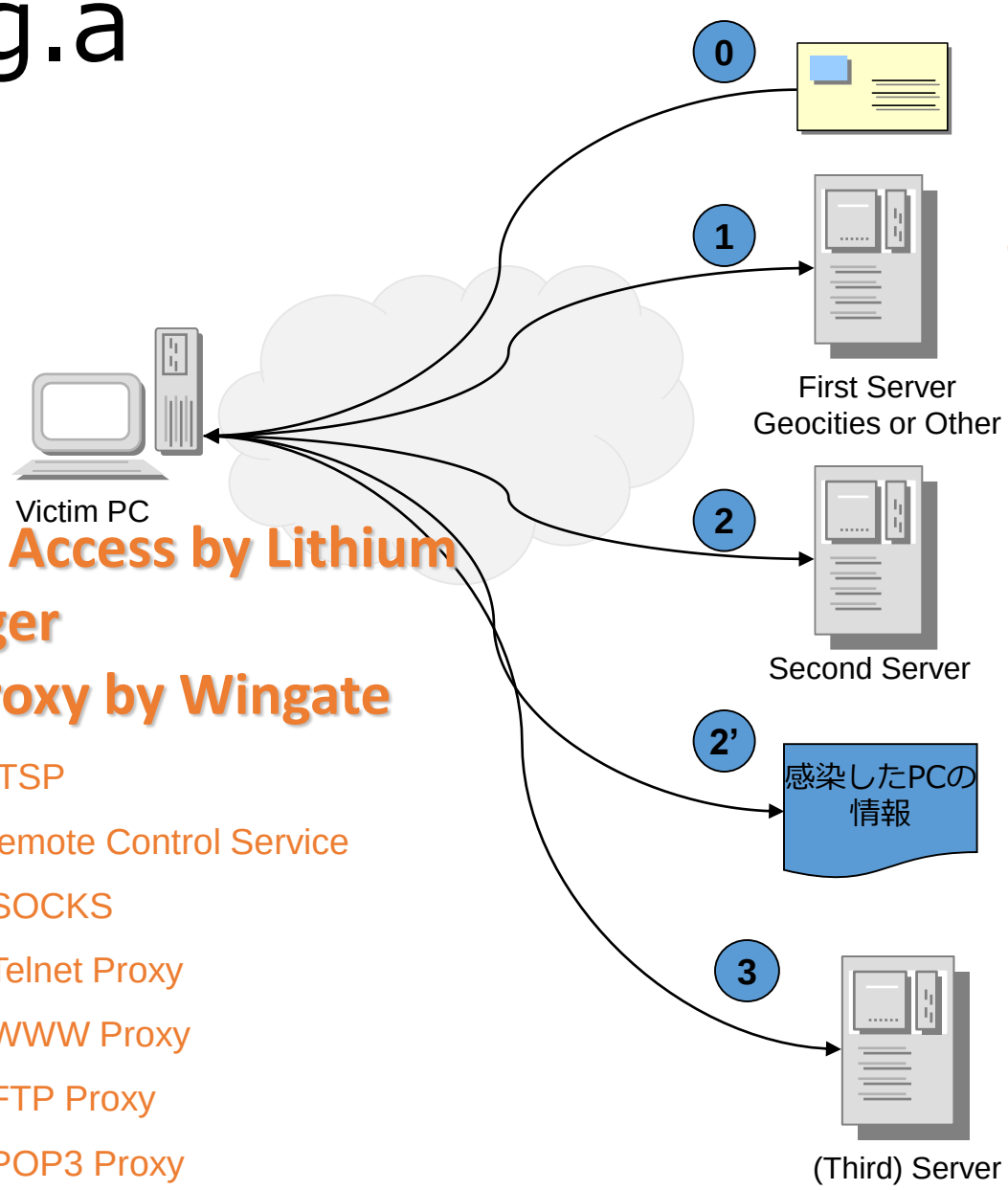
ウイルスの変化（CCSA基本要素 ）



- 複合型ウィルス
  - 2001/9/18　Nimda
- DDoS型ウィルス
  - 2001/7/18　CodeRed
  - 2003/8/11 MS Blaster
  - 2004/2/16　Netsky
  - 2003/1/9 Sobig
- バックドア型ウィルス
  - 2002/9/30　Bugbear
  - 2002/9/30　OPaserv
- SPAM中継型ウィルス
  - 2003/1/9 Sobig
  - 2003/5/9 Fizzer
  - 2004/1/26 mydoom

CCSA：Cyber Crimes and Suspicious Activities

Sobig.a



4 **Remote Access by Lithium**

Key logger

Open Proxy by Wingate

555/TCP - RTSP

608/TCP - Remote Control Service

1180/TCP - SOCKS

1181/TCP - Telnet Proxy

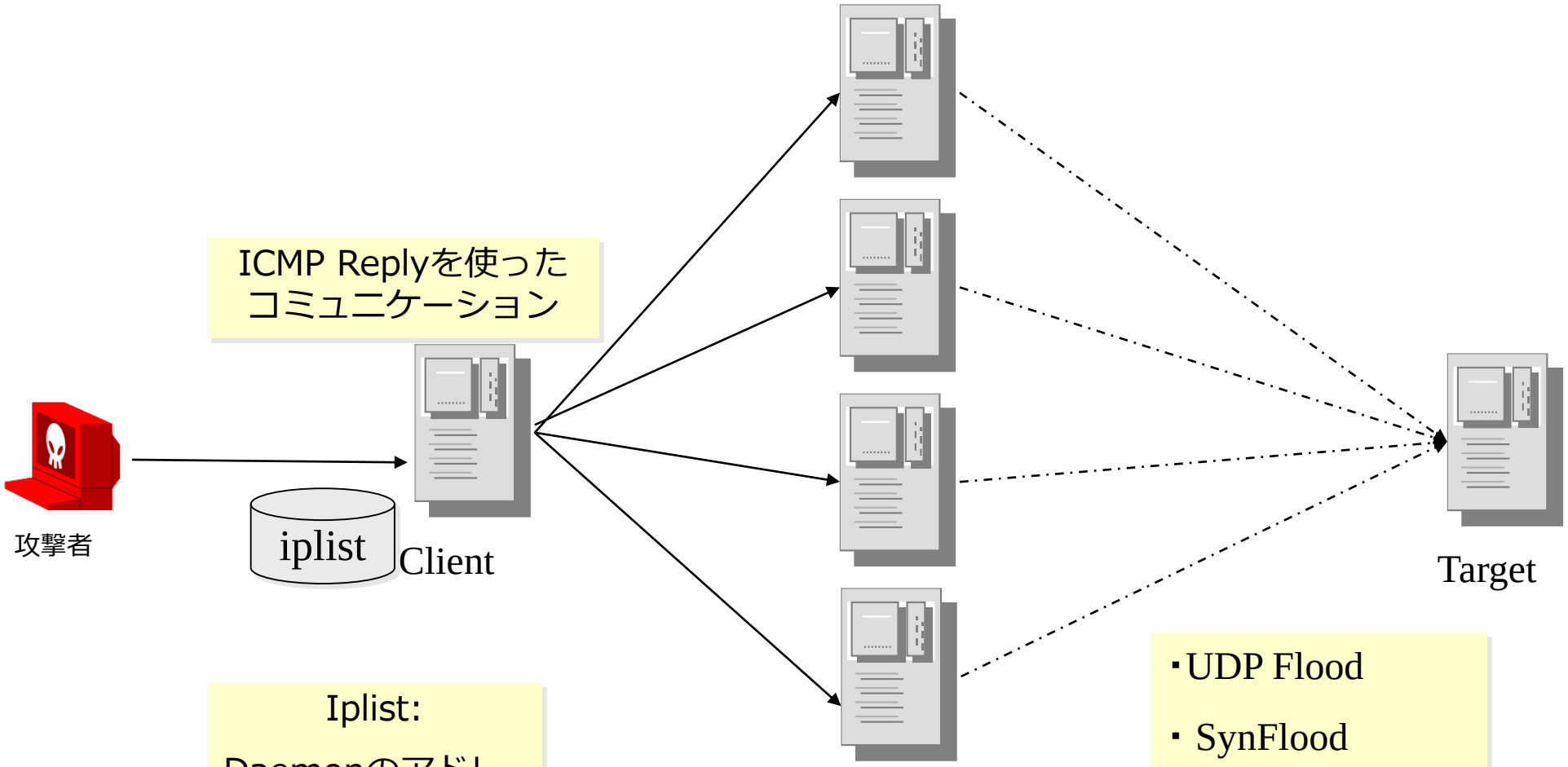
1182/TCP - WWW Proxy

1183/TCP - FTP Proxy

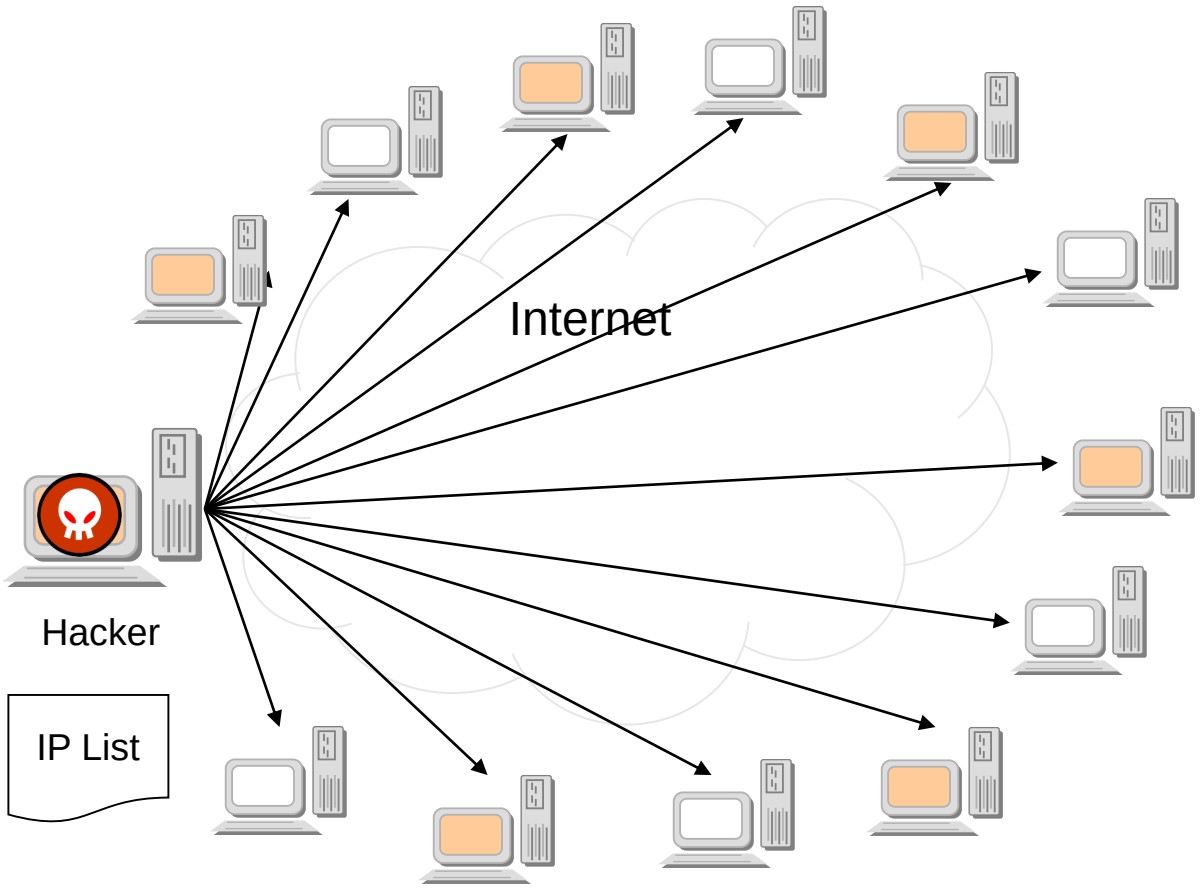
1184/TCP - POP3 Proxy

1185/TCP - SMTP Server

TFN（DDoSツール）


ICMP Replyを使った
コミュニケーション
攻撃者
iplist
Client
Target
Daemon
(Zombie)
Iplist:
Daemonのアドレスを記録したもの
・UDP Flood
・ SynFlood
・icmp Flood
・smurf

点在する感染PCを利用する方法 -1



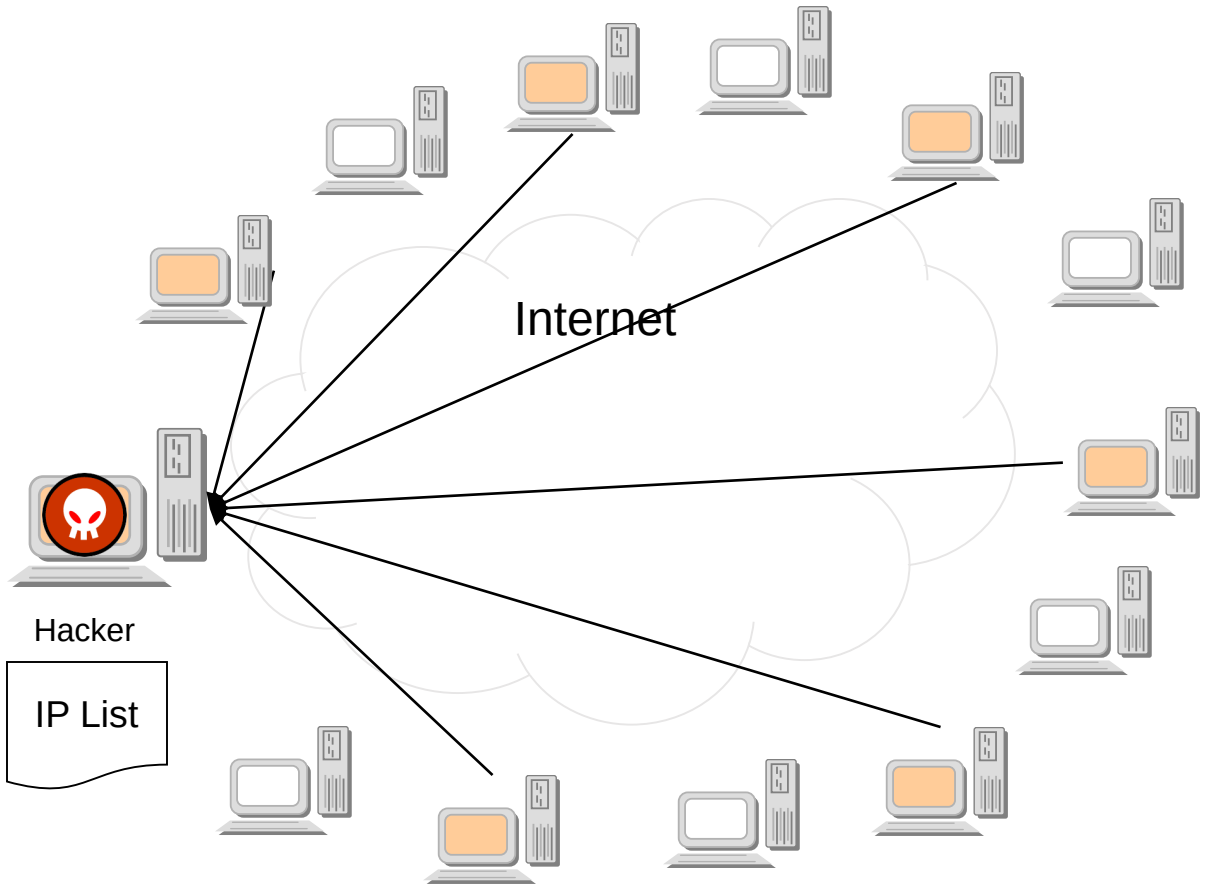
感染PCサーチ（mydoomなど）

ポートスキャンなどを使って、感染したPCを探査する

問題点

- 感染後に幅広いIPレンジを探す必要がある。
- 新たな感染を検知できない
- IPリストが陳腐化する
- FWを乗り越えられない

点在する感染PCを利用する方法 -2



IP報告型（Sobigなど）

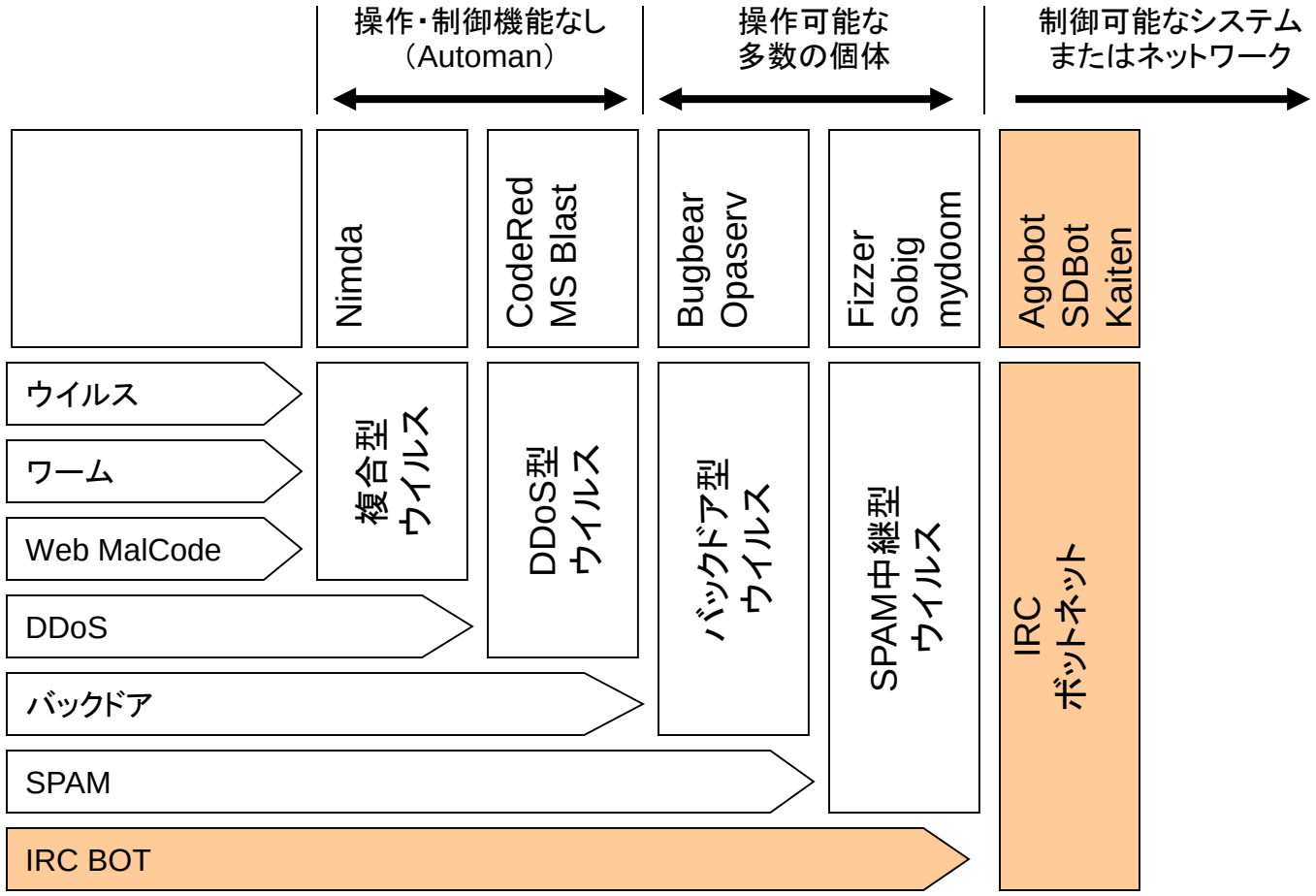
ウィルスが感染すると、特定のIPまたは、
FQDNに接続に行く

問題点

- IPリストが陳腐化する
- サーバを維持する必要がある
- メンテナンスが困難

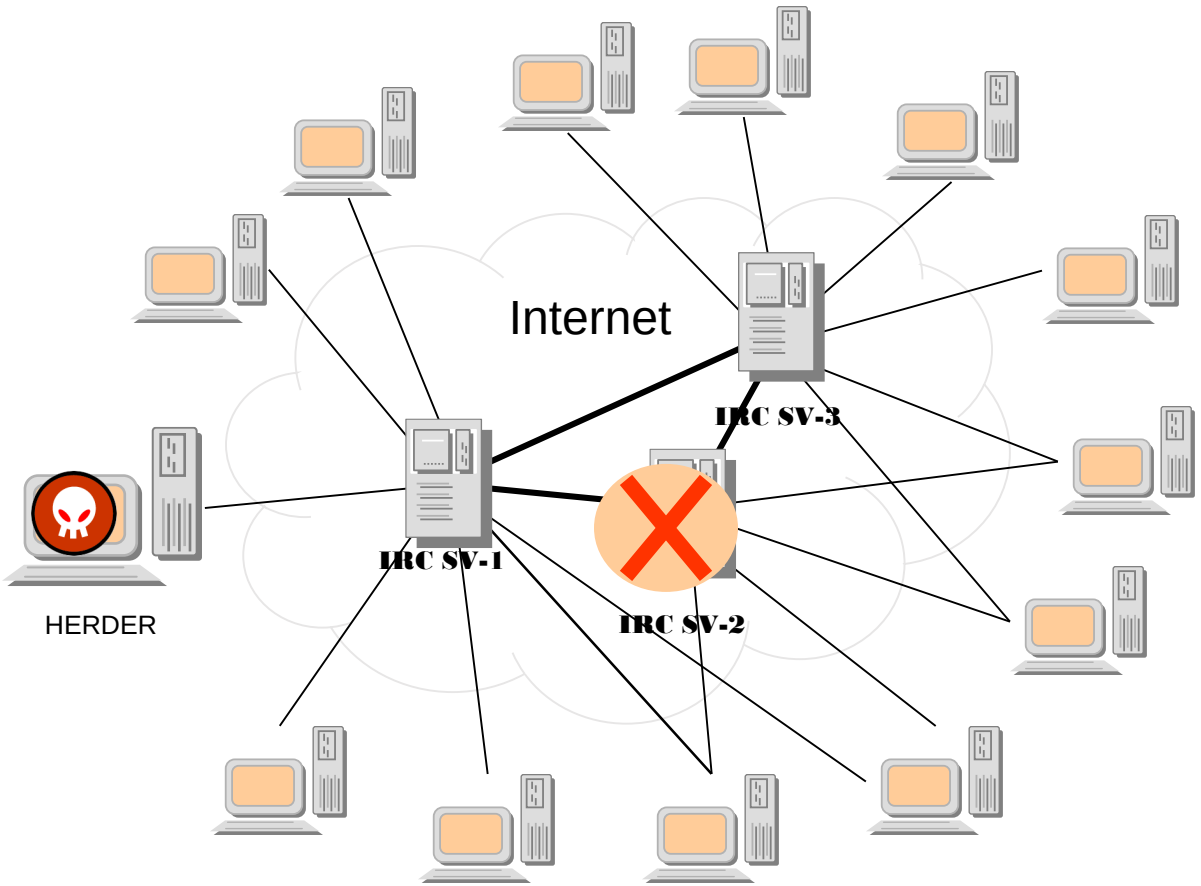
分散システムとしてのボットネット

ボットによる解決（分散システム）

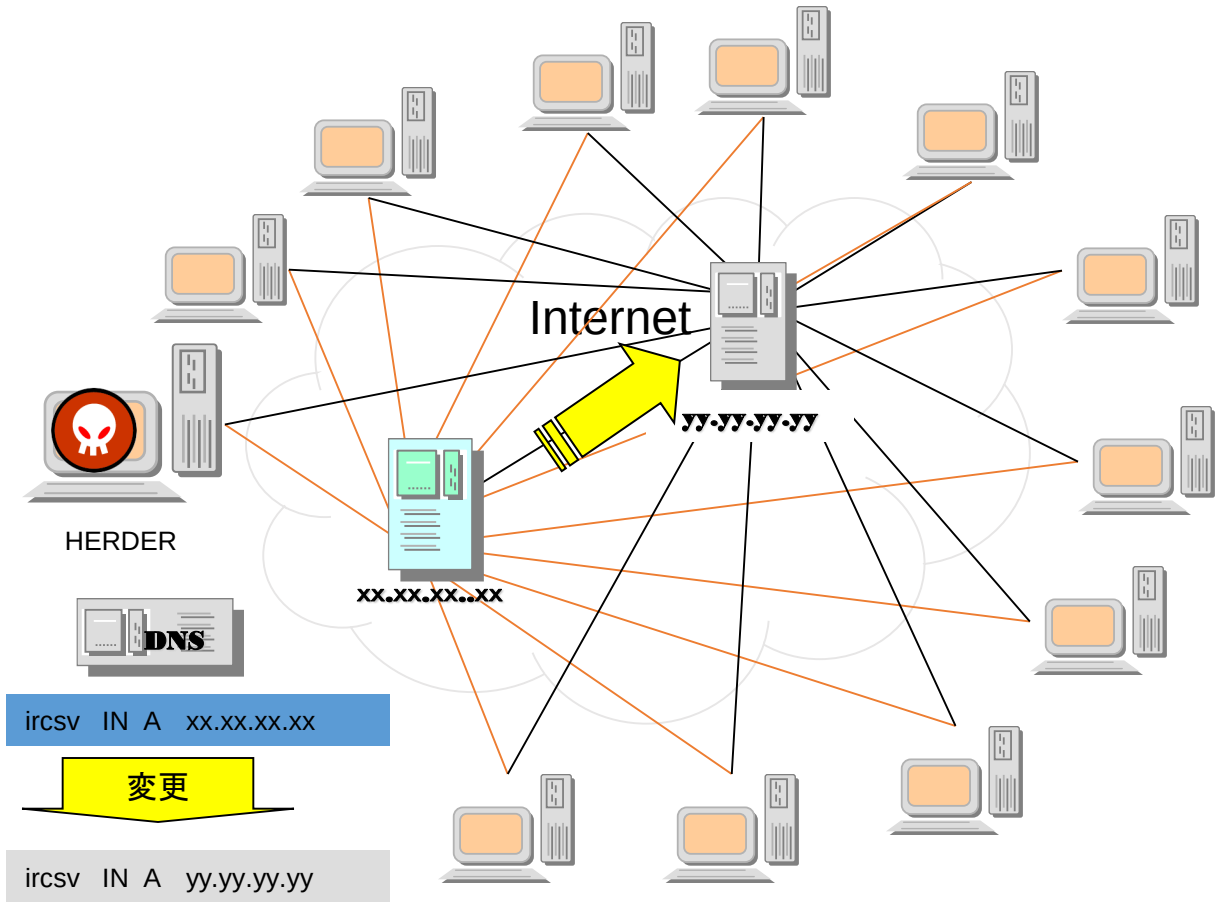


- IRCメカニズムを利用することで、感染したウイルス（ボット）の制御を実現した。
- IRCは、複数のサーバによって、クラスタリングを行うことが出来るので、リアルタイム性が高く、堅牢なシステムが構築できる

ボットネット：複数のIRCサーバの利用



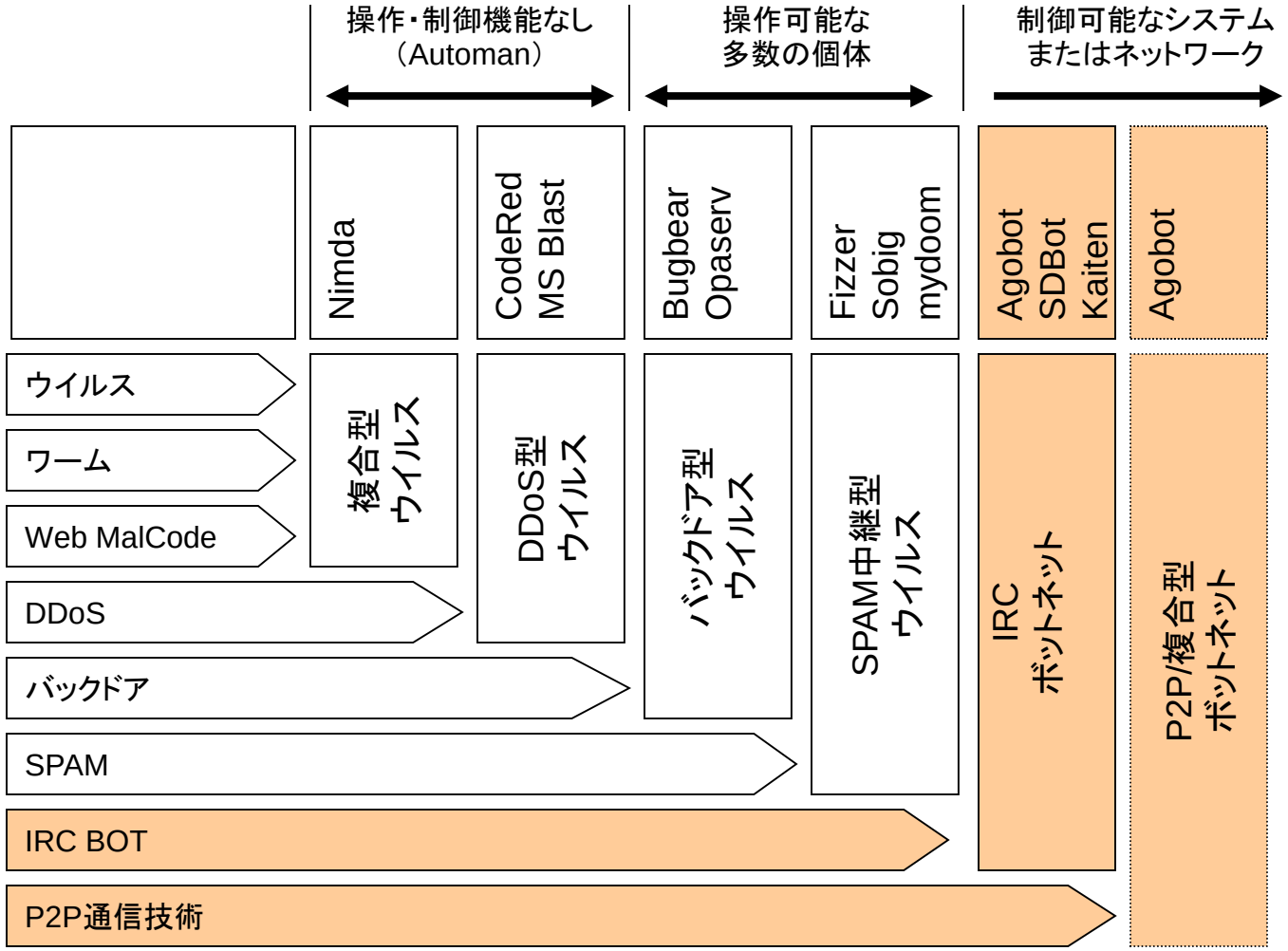
DNS変更によるIRCサーバの移動



IRCボットネットのシステム的な問題点

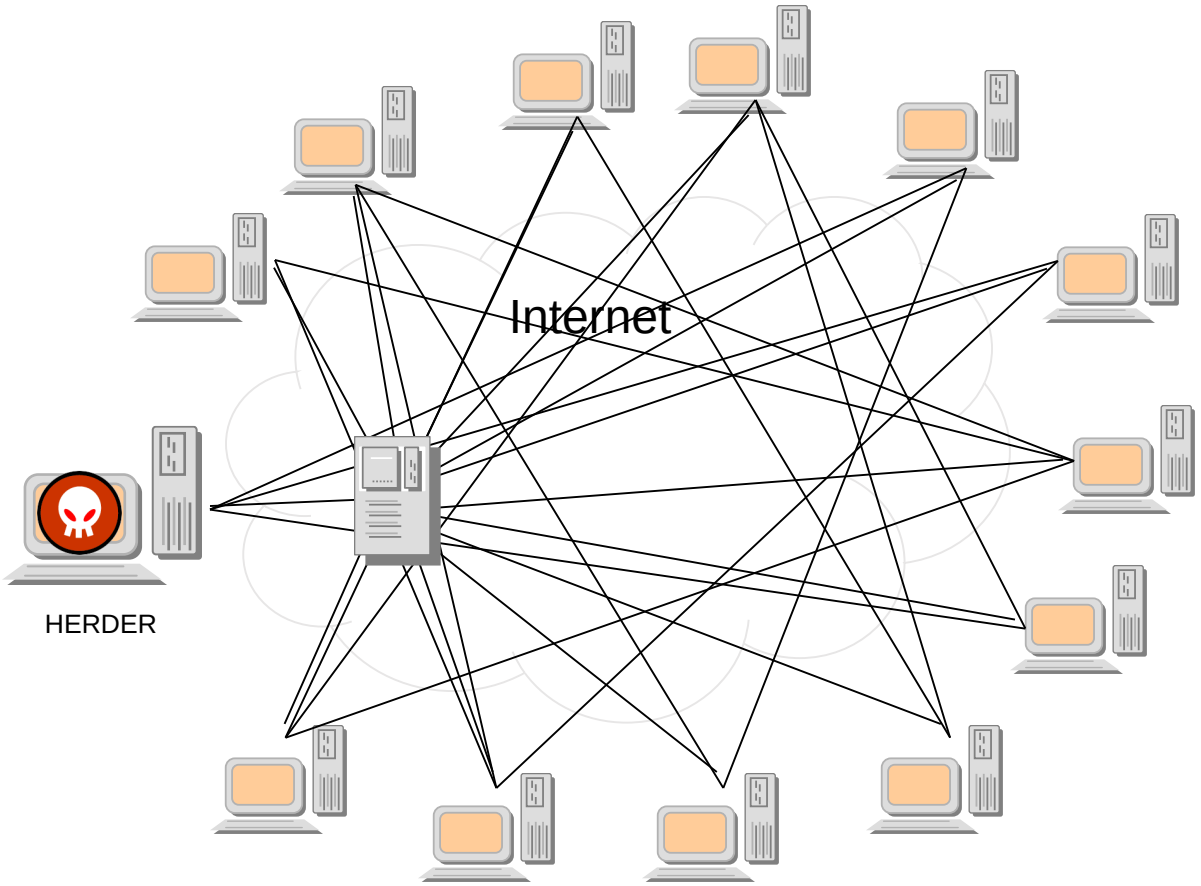
- IRCサーバを停止させる事で、攻撃に対処できる可能性がある
  - DDoSの停止を行う場合、IRCサーバをダウンさせることで、ボットとIRCサーバの通信を遮断し、攻撃を止めることが出来る可能性がある。
- IRCサーバへのアクセスから、ボットを見つけることが可能
  - IRCサーバのIPアドレスや、FQDNに対するDNSアクセスにより、ボットを見つけることが可能であり、このボットに対して、何らかの対処が出来る可能性がある
- ダウンロードの際の過負荷
  - ボットの更新を行う際に、ターゲットとなるサーバ（Web, FTP等）にアクセスが集中するため、ボットの規模に制限があるものと思われる。

ボットによる解決（分散システム）

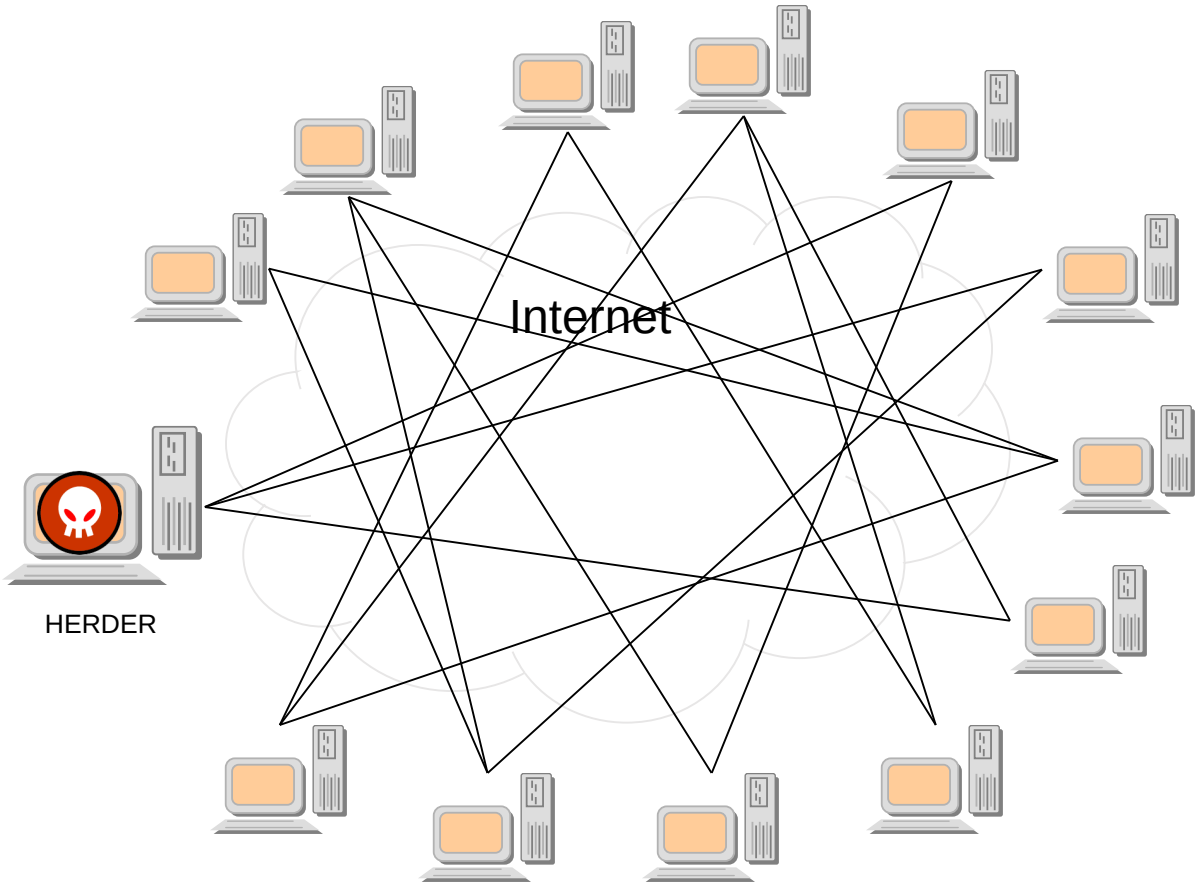


- P2Pを併用することで、より堅牢なネットワークを構成することが出来る。

Hybrid P2Pボットのイメージ



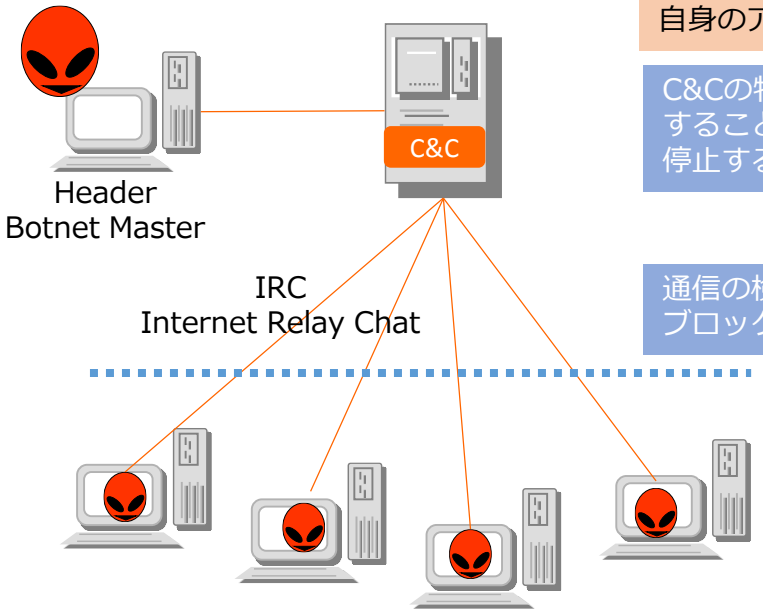
Pure P2Pボットネットのイメージ



ボットネットTakedownとアーキテクチャの推移

ボットネットの推移

初期のボットネット
IRCボットネット

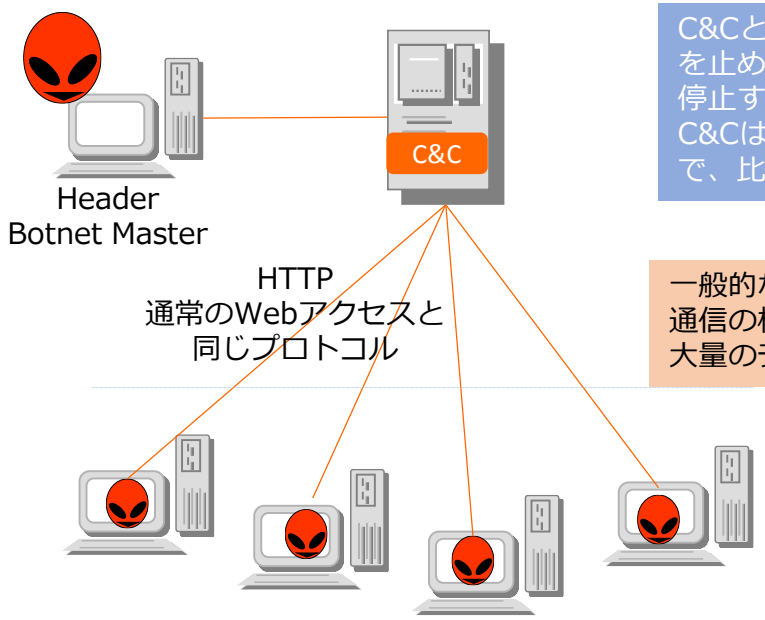


IRCの機能を利用して、大量の感染ノードを制御し、攻撃などの命令や、自身のアップデートなどを行う

C&Cの特定が容易で、これを停止することで、ボットネットは活動を停止する

通信の検出とブロックが比較的容易

初期のボットネット
HTTPボットネット



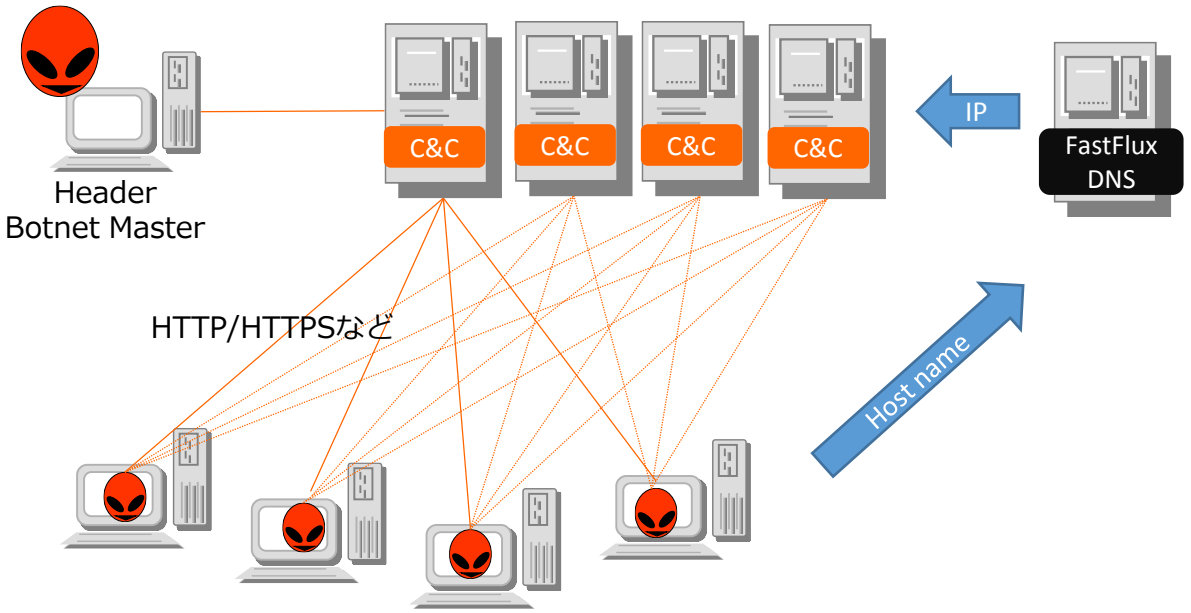
C&Cとして稼働するWebサーバーを止めれば、ボットネットは活動を停止する
C&Cは、ボットの通信を調べることで、比較的容易に判定できる

一般的な通信との区別がつきにくく、通信の検出とブロックが困難
大量のデータ転送も可能

ボットネットの推移：FastFluxとDGA

FastFlux DNSを使った HTTPボットネット

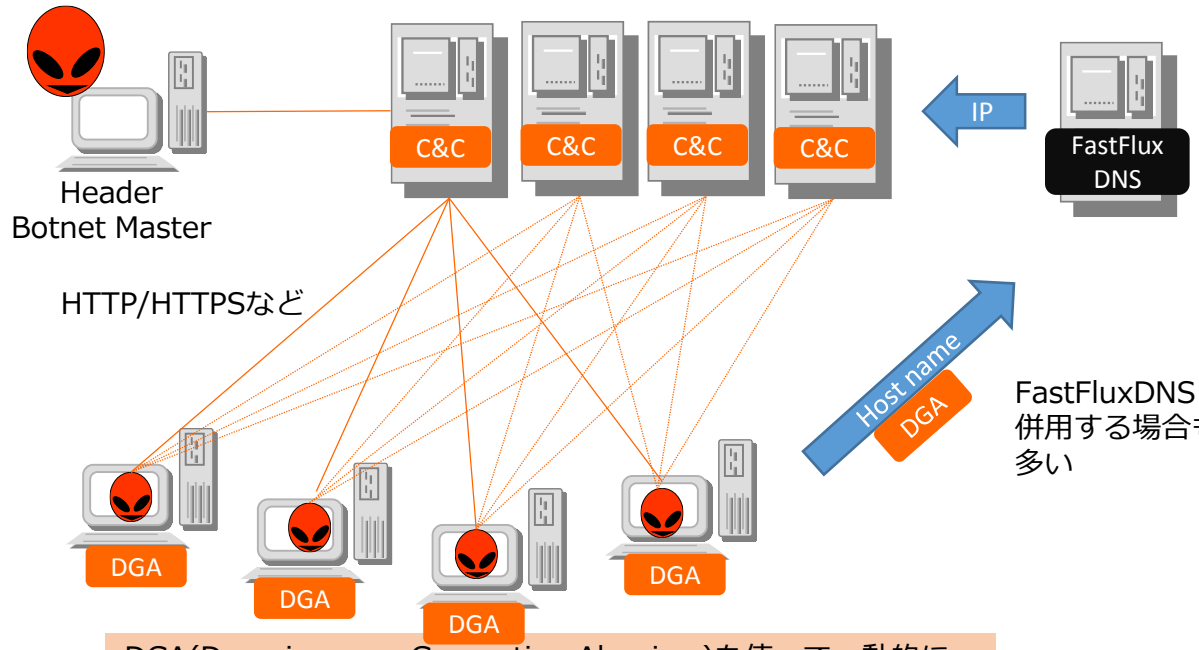
C&Cのホスト名に割り当てるIPアドレスを頻繁に変更することで、特定のC&Cを停止しても、すぐに他のIPアドレスで稼働するホストがC&Cとして稼働するようになる



ホスト名（DNS）を停止することで、C&Cとの通信が停止

DGAを使った ボットネット

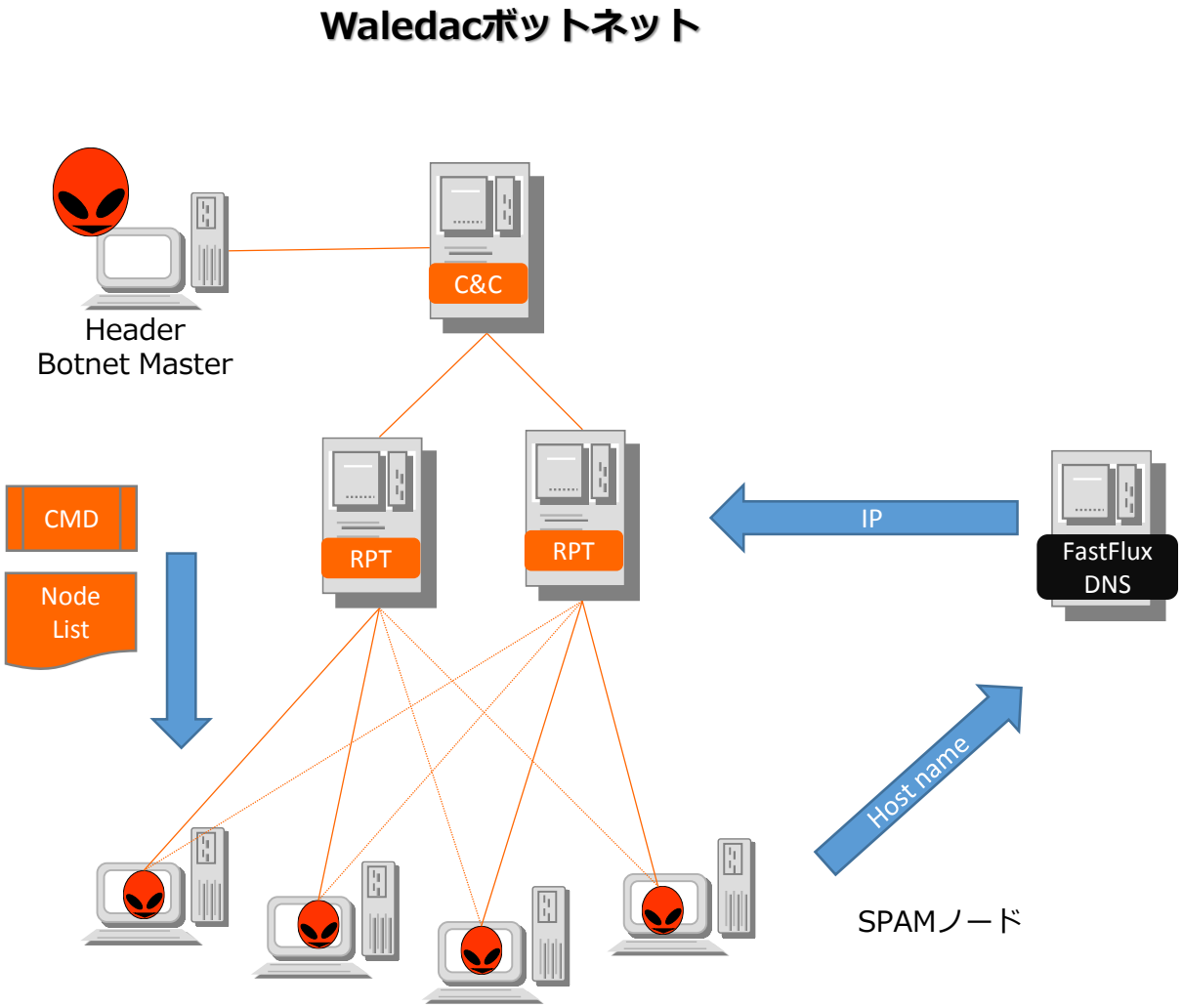
DGAを解析し、先にホスト名を差し押さえることで、C&Cを停止



FastFluxDNSと併用する場合も多い

DGA(Domain name Generation Algorism)を使って、動的にC&Cのホスト名を自動生成する。
ホスト名は、時刻などによって刻々と変化する。
ある時刻のC&Cを停止しても、一定時間後には、別のホスト名がC&Cとなるため、ボットネットが復活する

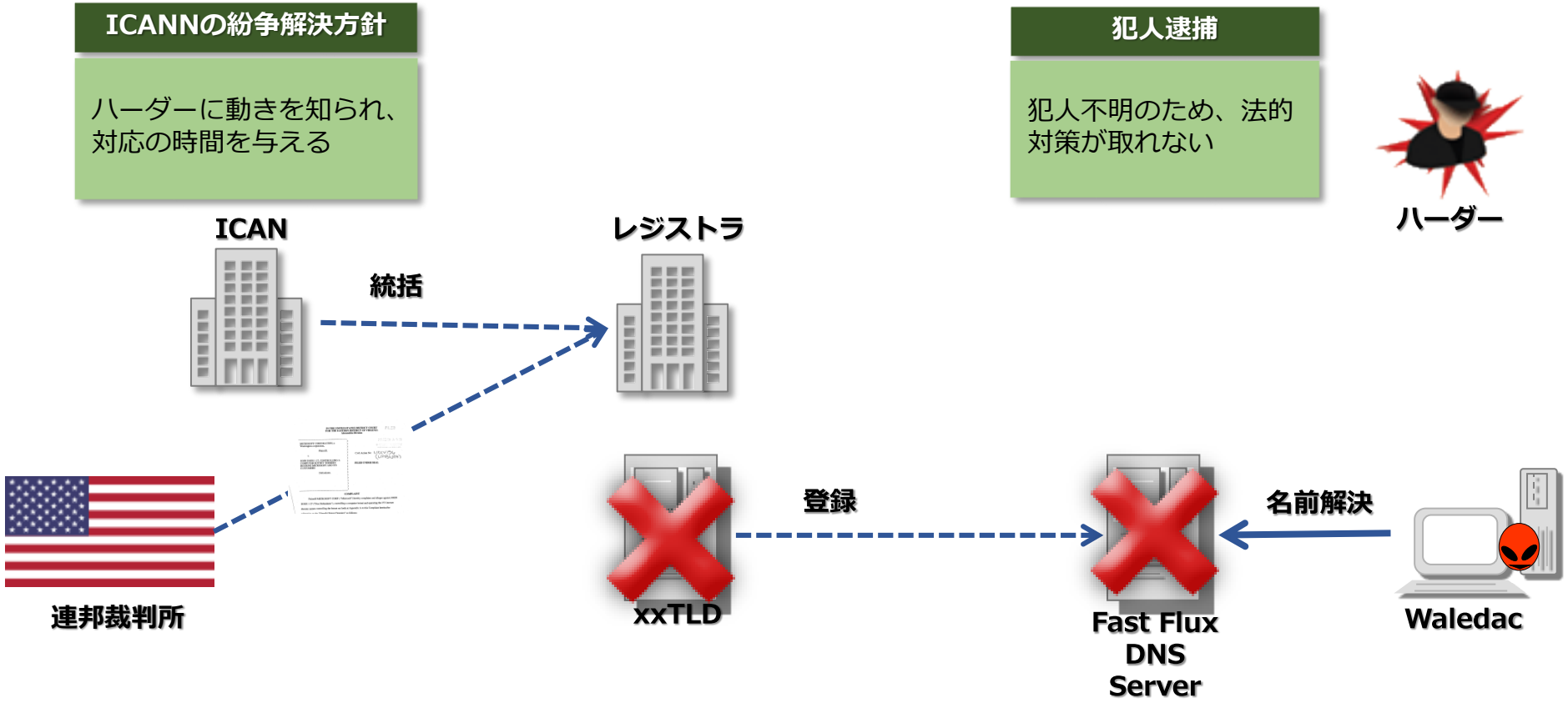
ボットネットの推移:P2Pの利用



RPT(Repeter)ノードと、SPAMノード間で、P2Pネットワークを構築。
ノードリストは、RPTノードが管理し配布をする。
隣接ノードが見つからない場合は、FastFluxDNSを使って、RPTノードを見つけるリカバリー処理が行われる。

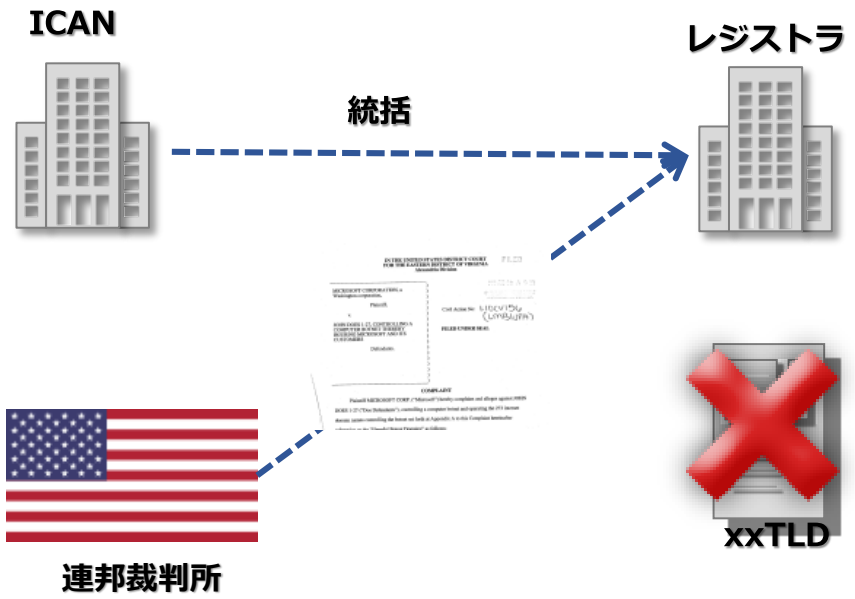
Waledacを停止させるためには、
P2Pのノードリストに偽の情報を入れ込むことに加えて、
リカバリー用に用意されているホスト名についても、
偽の情報を入れ込む必要がある

DNSの対策：ホスト名の削除



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史なしに、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

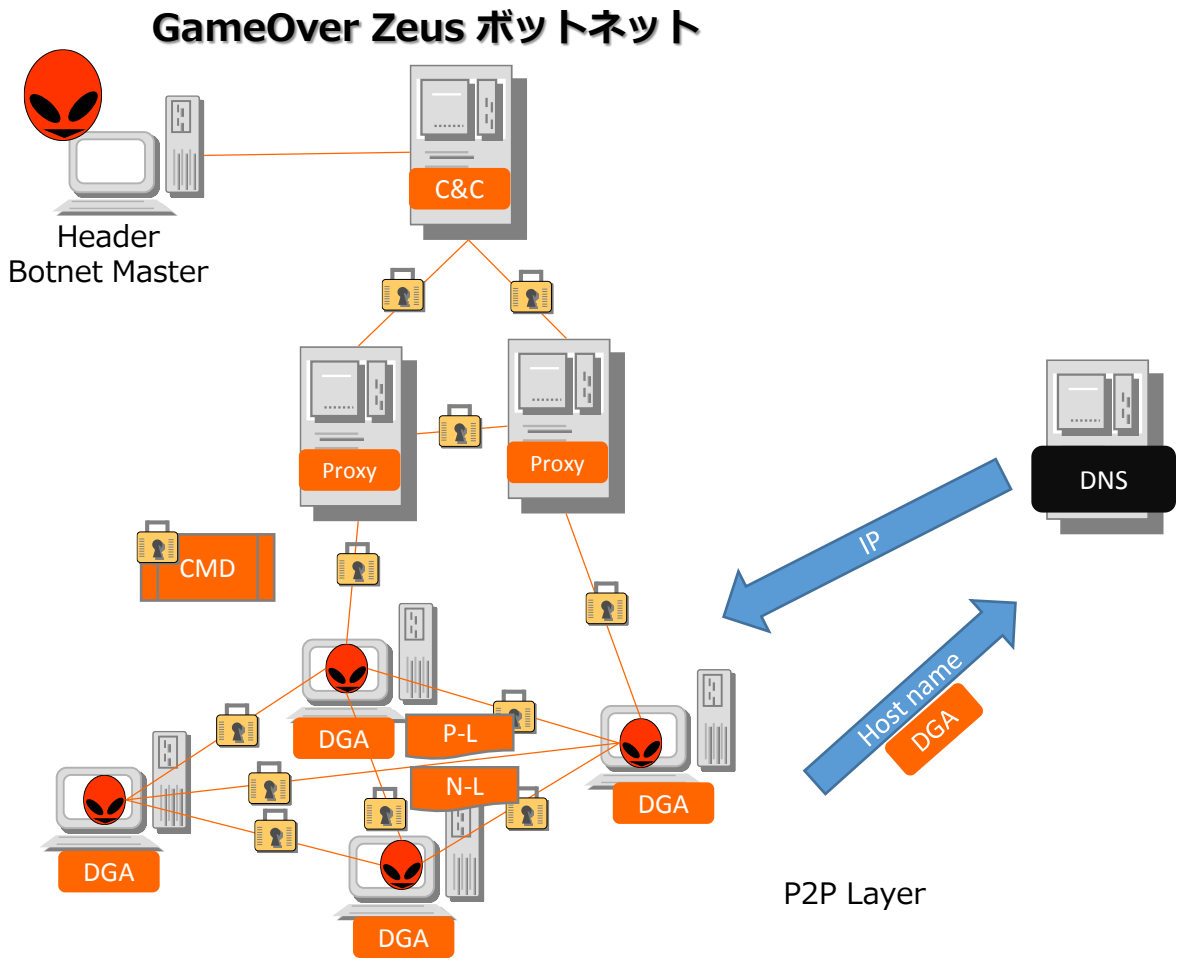
適法手続権利の維持を保証するため、ドメイン登録者に、訴状を送ると共に、電子メール、FAX、書簡による通知を行い、加えて、サイトを作成し、訴訟に関する書面をすべて掲載の上、これをメディアなどを通じて周知
www.noticeofpleadings.com

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。

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

ボットネットの推移:P2P・認証・署名



P2PレーヤとProxyレーヤでP2Pを構築。ノードリストは、ハードコードされたBoot用で始まり、隣接ノードとの通信の中で、メンテナンスを行う。
ノード間の重要なやり取りには、RSA-2048の署名が行われる。
ノードが見つからない場合は、DGAを使って隣接ノードを取得する。
各ノードがユニークIDを持ち、ノードリストの交換には、署名する仕組みになっていること、常にアクティブなノードのリストを残す設計になっていることから、Waledacなどで利用した、偽のノードリストを使って、隣接ノードとの接続を遮断することが難い。

C&CやProxyの遮断と、DGAで利用されるホスト名の差押えが必要
ノードが世界各国に分散しているため、各国法執行機関の連携が必要となる

参考資料

- **Microsoft takes on global cybercrime epidemic in tenth malware disruption**
  - http://blogs.technet.com/b/microsoft_blog/archive/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption.aspx

- **Microsoft helps FBI in GameOver Zeus botnet cleanup**
  - http://blogs.technet.com/b/microsoft_blog/archive/2014/06/02/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup.aspx
- **マイクロソフトが GameOver Zeus ボットネットのクリーンアップで FBI に協力**
  - http://blogs.technet.com/b/jpsecurity/archive/2014/06/04/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup.aspx
- **警察庁：インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について
～国際的なボットネットのテイクダウン作戦～**
  - http://www.npa.go.jp/cyber/goz/

http://www.microsoft.com/en-in/news/stories/cyber.asp

msn

Microsoft Cybercrime Cen...

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

MS QSC QUL Potal Web コンピュータ関係 趣味 地震 調査 Tools ALK CSL Facebook https--manage.windo... Install Office JARTIC JCOP

Microsoft

Microsoft India Stories

News Center

Meet the global warriors against cybercrime

From Redmond to Bangalore-the global battle against cybercrime

http://www.microsoft.com/en-in/news/stories/cyber.aspx

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

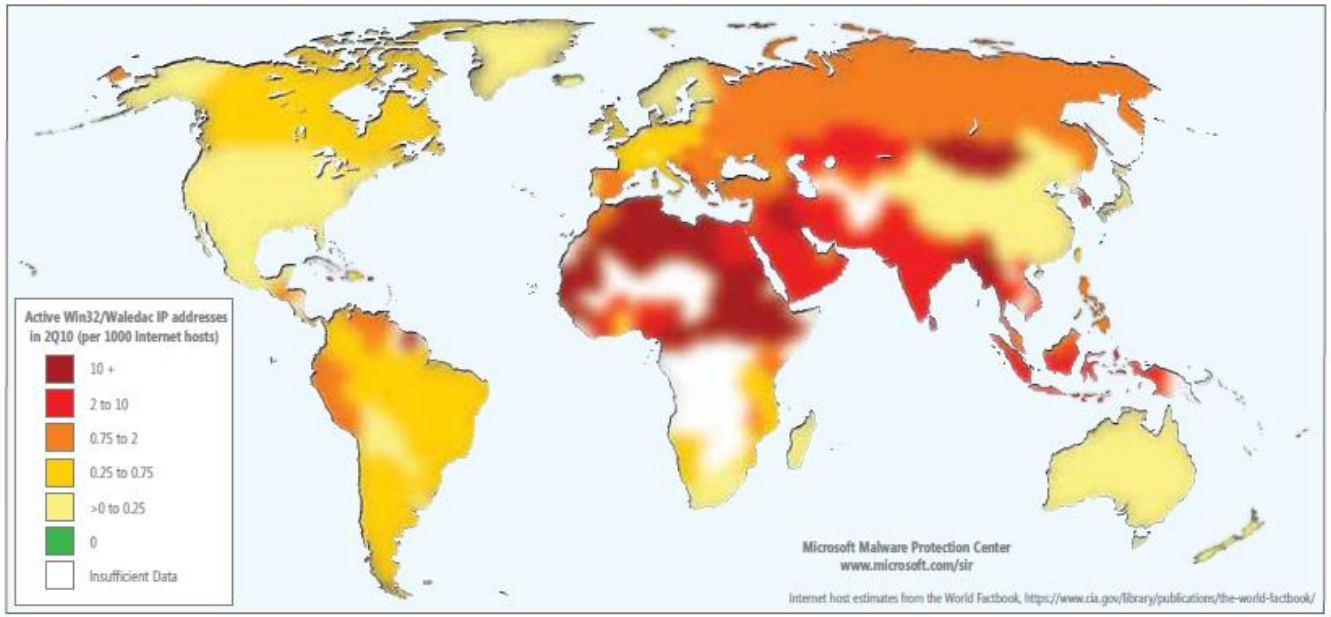
Waledac Take down

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

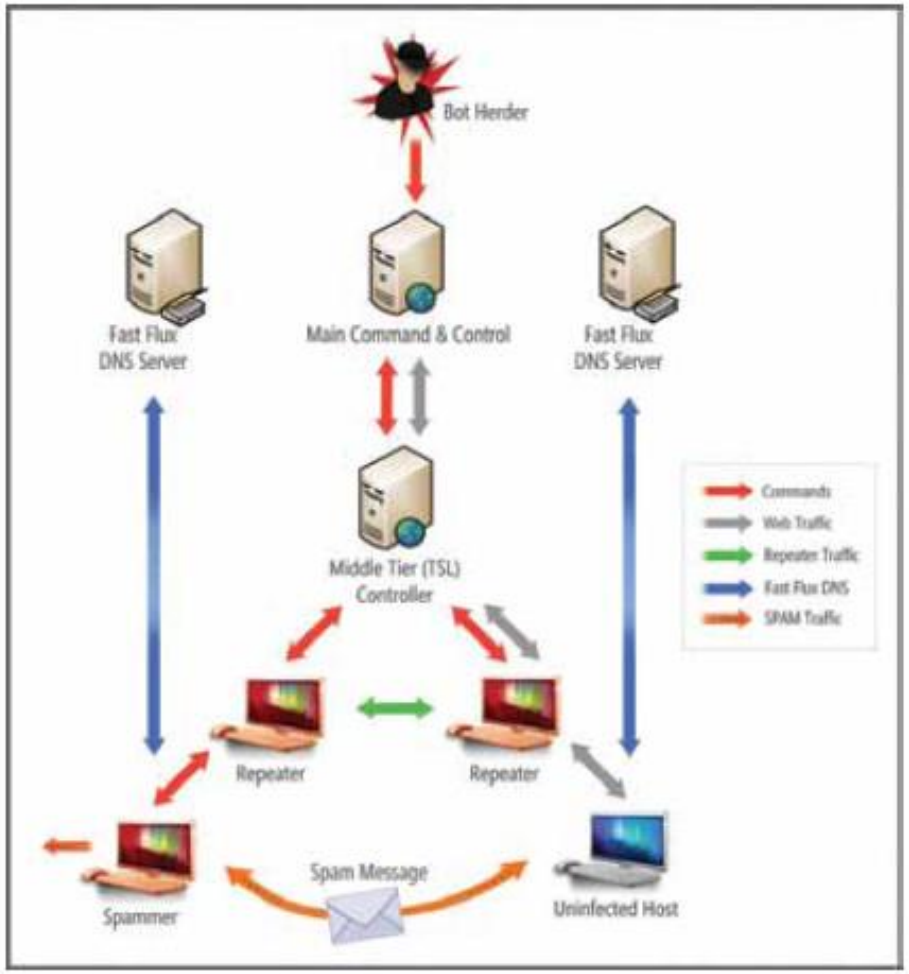
FIGURE 17. Active IP addresses in the Win32/Waledac botnet in 2Q10, per 1000 Internet hosts



- 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

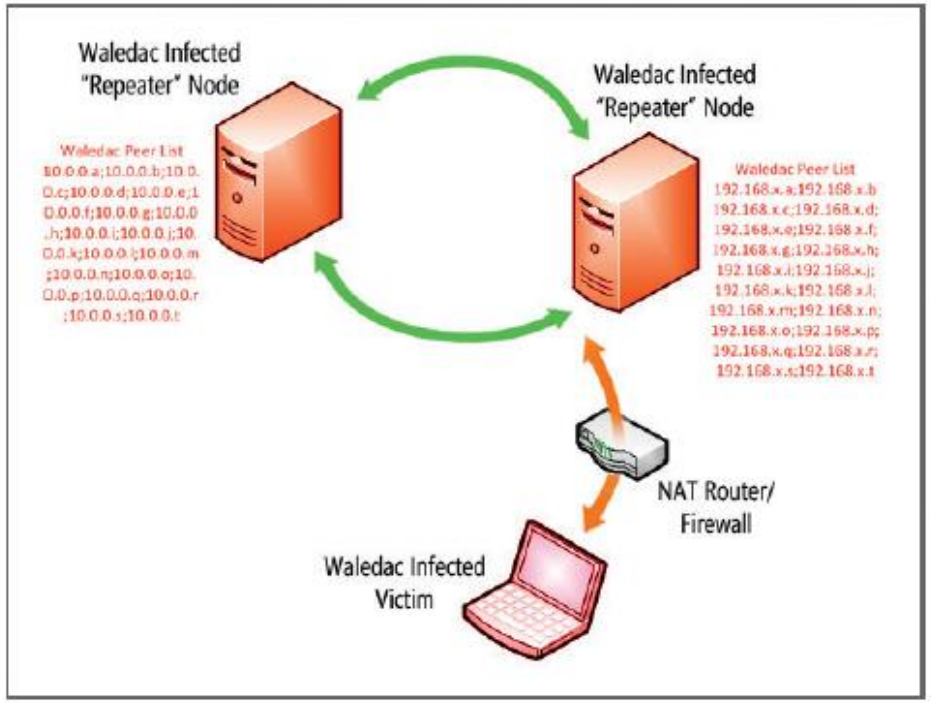
FIGURE 18. The Win32/Waledac tier infrastructure



- 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

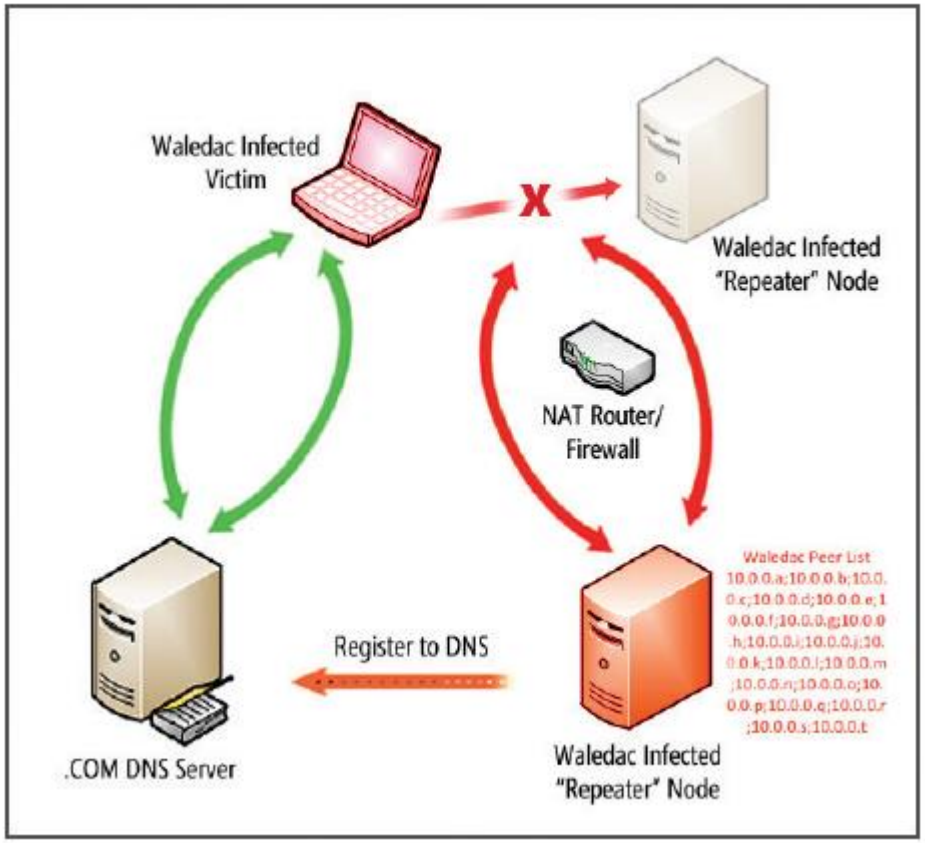
FIGURE 19. Win32/Waledac peering list exchange between infected spammer node and repeater node



- 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

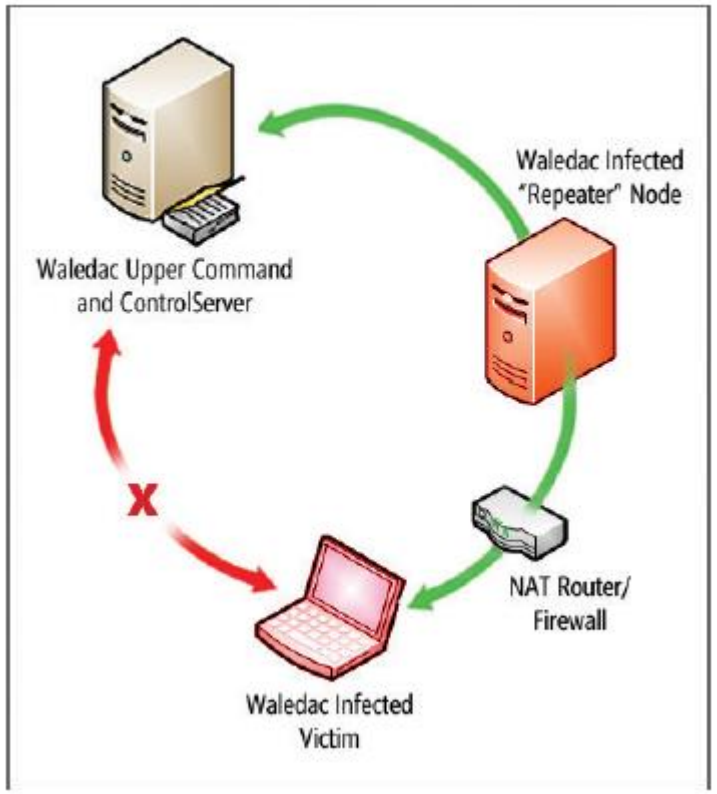


- リピーターノードの Fast Flux DNSへの登録
  - リピーター・ノードが一定期間オンランだと、信頼できるノードとして、DNSに登録され、Waledacボットネットの制御に利用される。

- 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

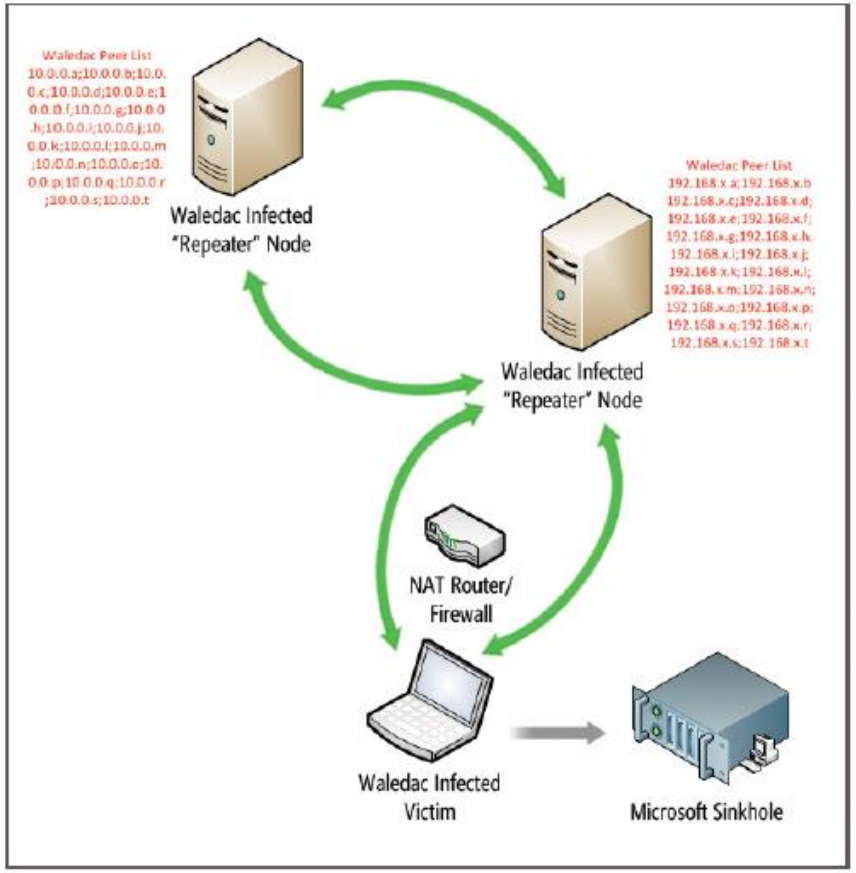
FIGURE 21. Win32/Waledac proxy function through the repeater tier



- 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。

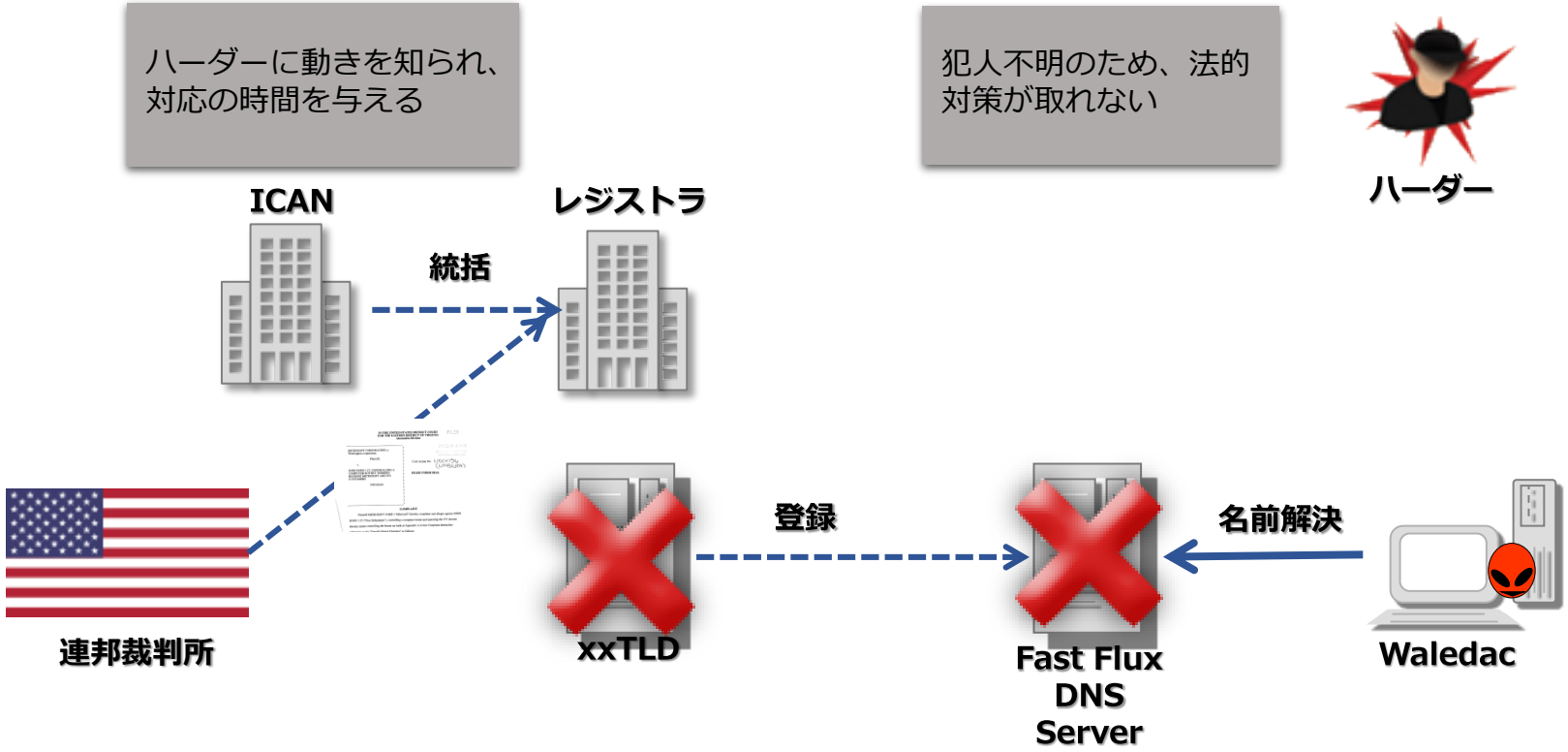
DNSの対策：ホスト名の削除

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



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）

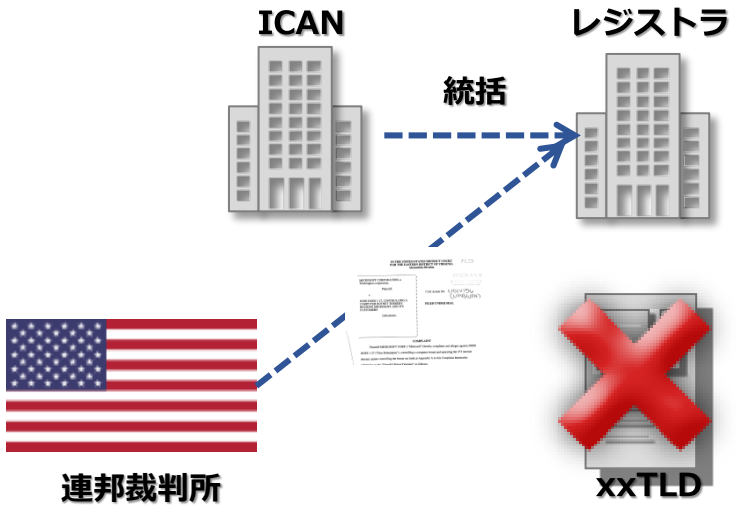
強制力がないため、必ずしも実施されない

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。

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

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

FILED

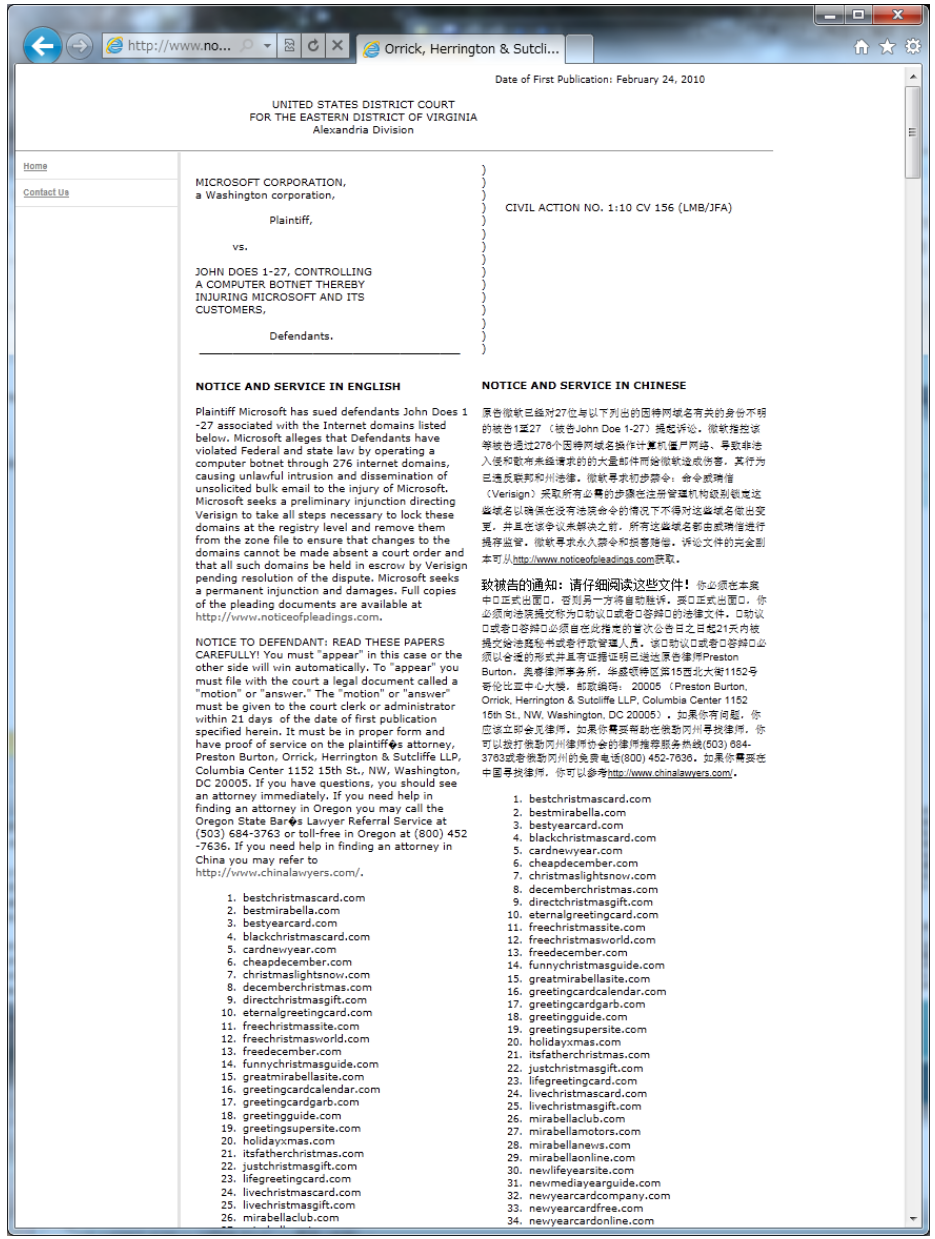
2010 FEB 22 A 9:03

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:

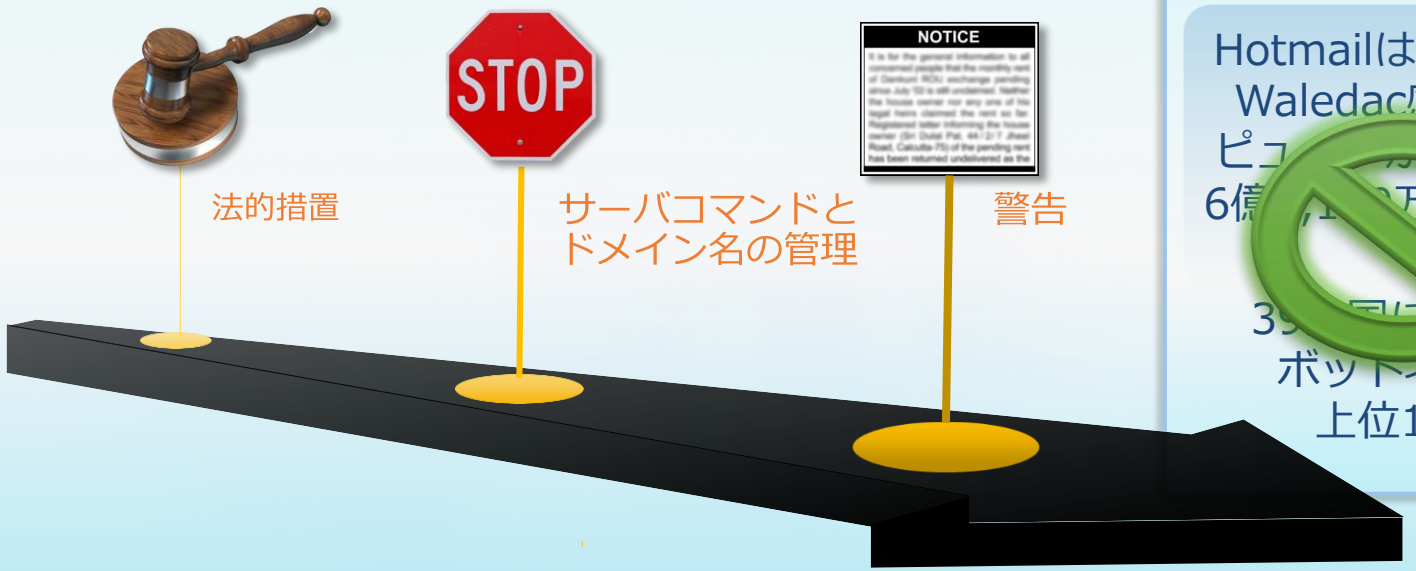


http://www.noticeofpleadings.com/

ボットネット

WALEDACボットネット「遮断」アプローチ

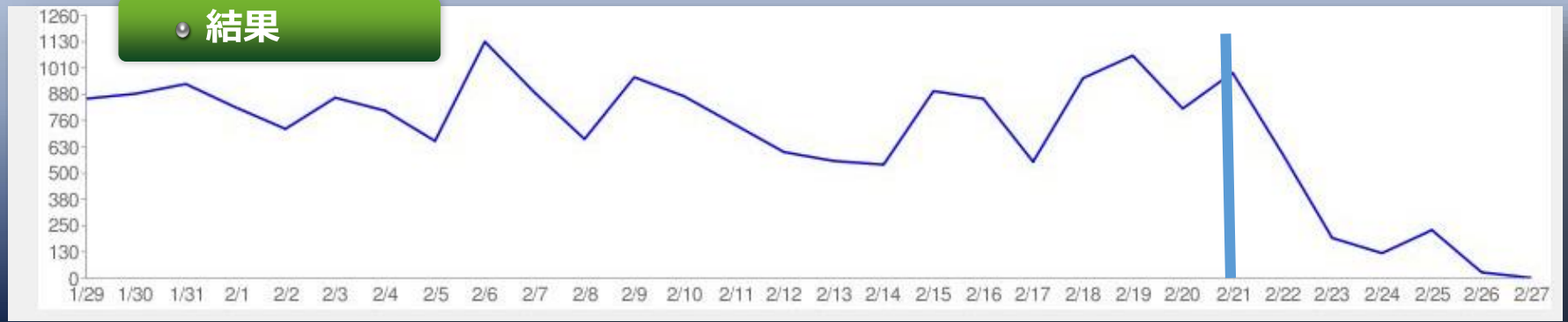
短期的 – 先例を作る



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

3[illegible]る
ボットネット
上位10位

- 結果

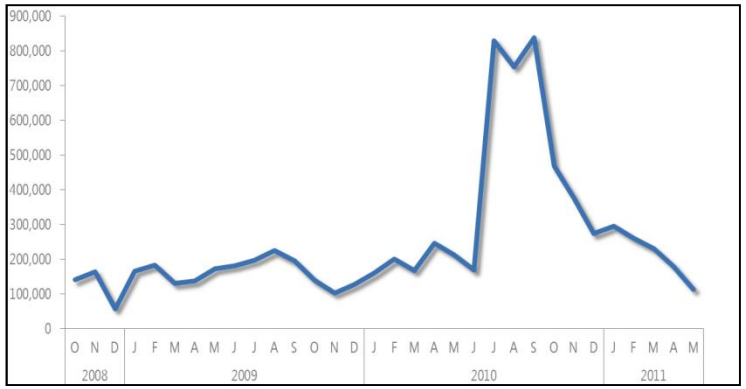


Microsoft

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

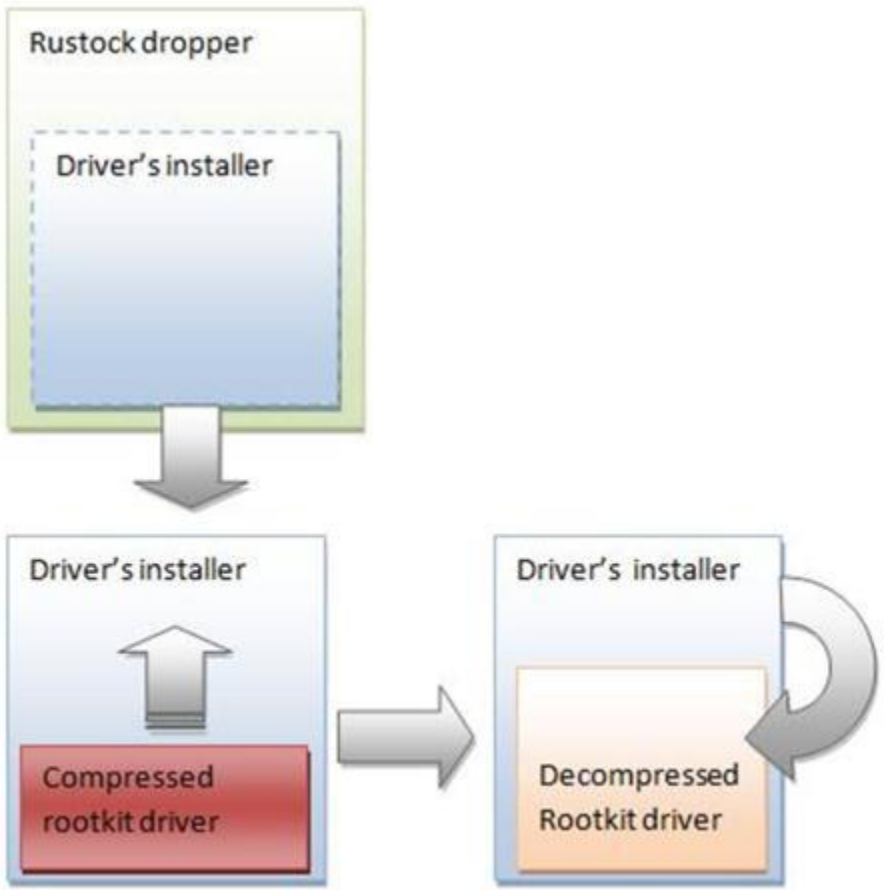


マイクロソフトのマルウェア対策ソリューションによる Win32/Rustock の検出数 (2008 年 10 月～ 2011 年 5 月)

- 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

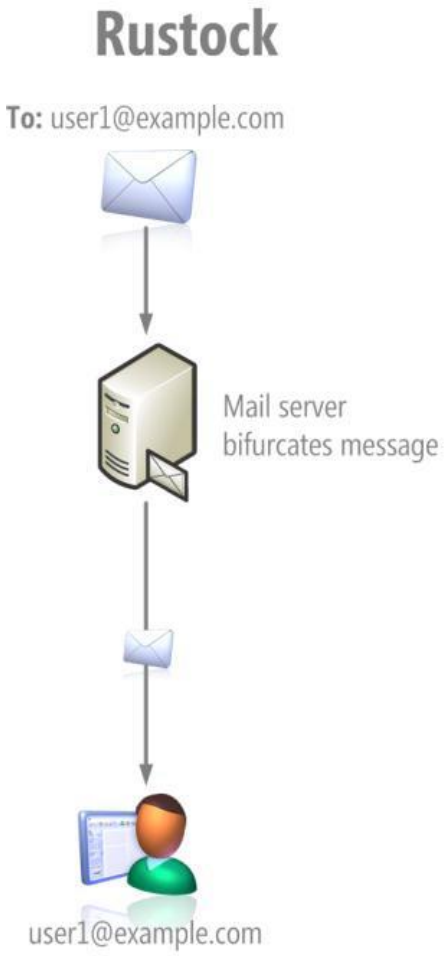
Rustockの構成

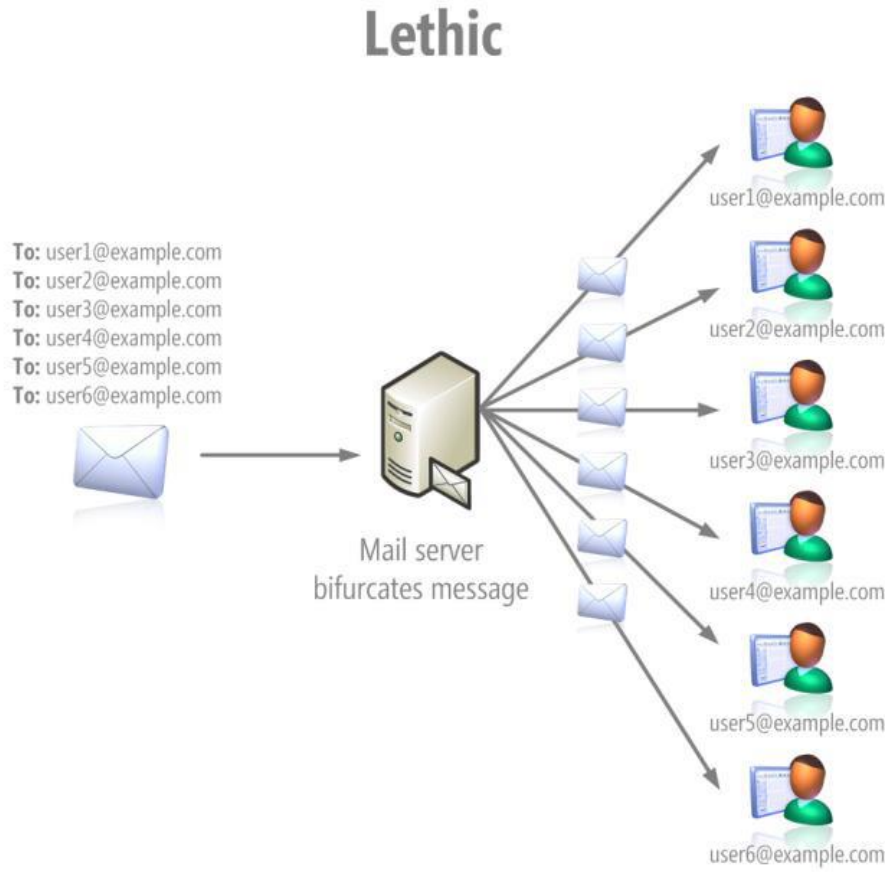
- ドロッパー
  - ユーザーモードで実行
  - C&Cから、ルートキットドライバーの複合化とドロップ
  - ポリモーフィック型、
  - 静的な文字列は使わない
  - RC4で暗号化しaPLibで圧縮
- ドライバーインストーラー
  - システムドライバーに成りすまし、カーネルモードで実行
  - Beep.sys, null.sys等の置き換え
  - ハードコード化されたファイル名とランダムなファイル名
- ルートキットドライバー
  - カーネルモードで実行
  - INT 2eh割り込みを賜与してユーザーモードボットクライアントと通信
  - SSDT*をフックし、自身を除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

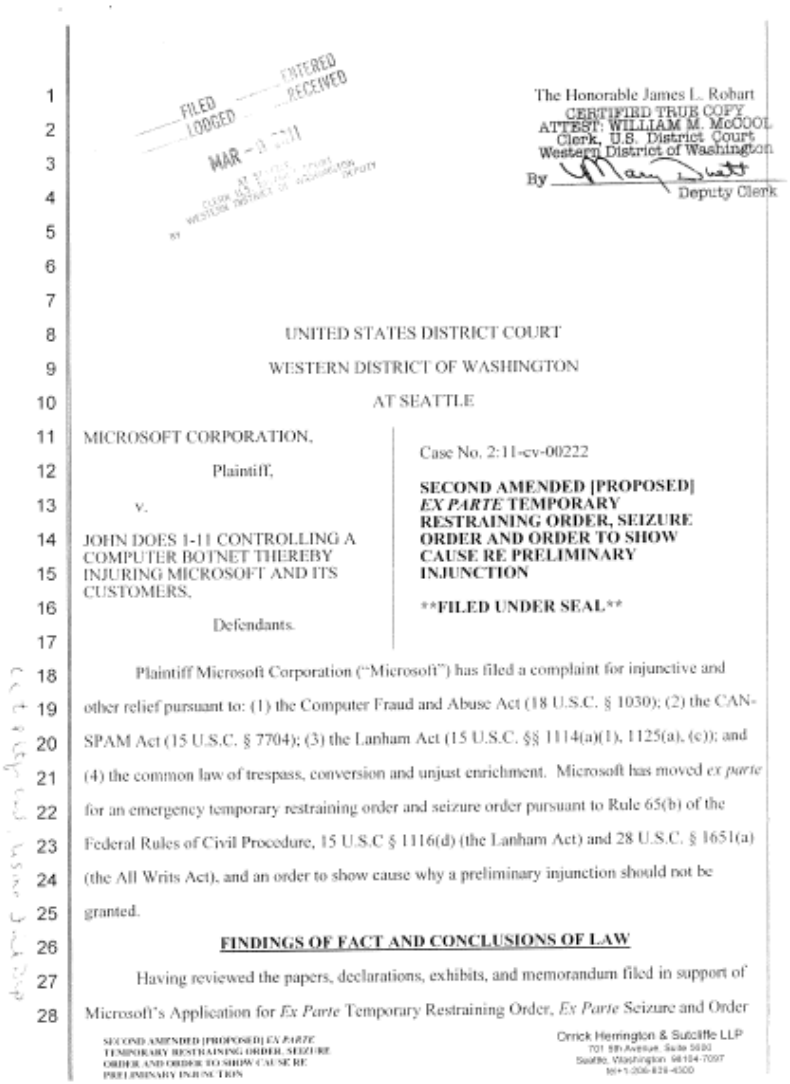
- マルウエアの追加インストール
  - 既知のRustock ドロッパー（Win32/Harnig）に感染させる
  - 対話的な操作を行わずに5分間で左表のマルウエアをダウンロード・インストール
  - これらのマルウエアは、さらに別のマルウエア等をダウンロード（多層構造のダウンローダー）

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, COURT
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

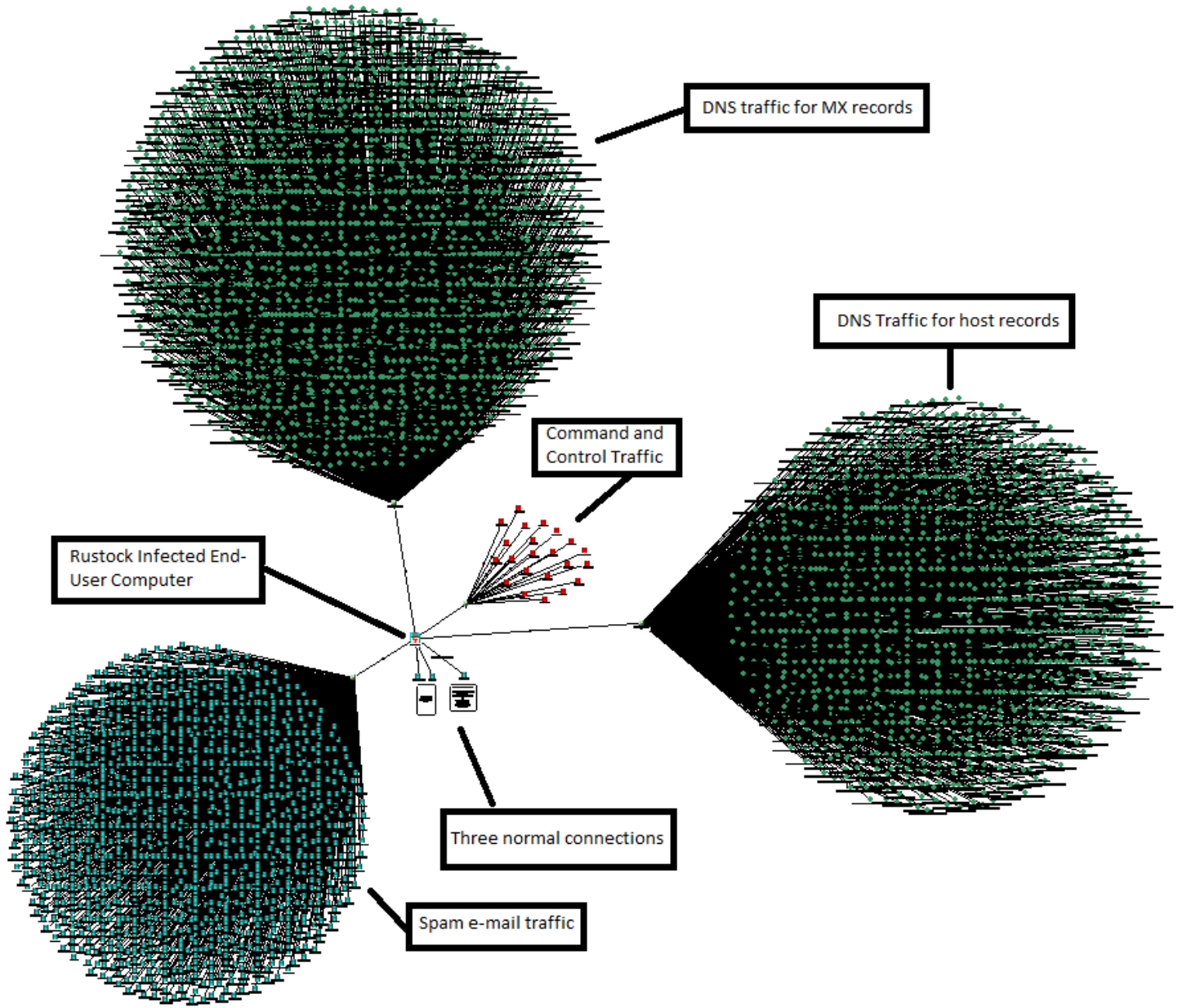
- ハードディスク20台の解析結果
  - スパムを送信するためのソフトウェアとデータ
    - 数千個の、メールアドレス、ID/パスワードの組み合わせを含んだテキストファイル
    - 42万個以上の電子メールアドレス
    - マイクロソフトや製薬会社の商標を不正に利用したテンプレート
  - ロシアのIPアドレスに対するサイバー攻撃に利用されていたことを示すデータ
  - 匿名インターネットアクセスを提供するノードとして使用
    - 電子メールテンプレート、商標、電子メールアドレスなどを保存するRustockシステムへの匿名アクセスを提供するために使用したとみられる
- サーバ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

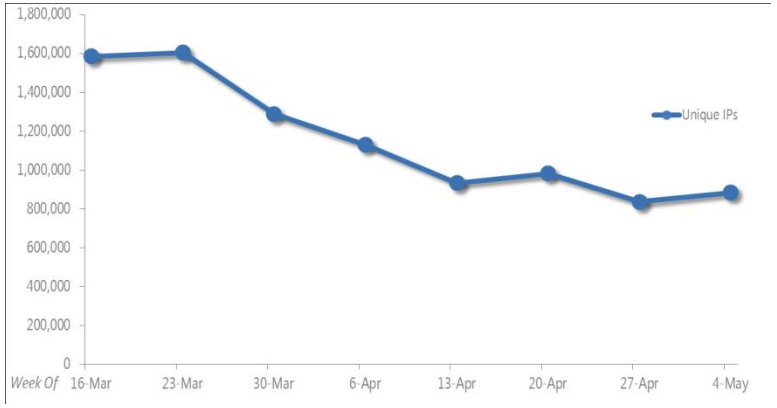
- 130万を超えるIPからRustockを検出
  - 2011/1/22　～　2011/2/4

- Rustockのネットワーク活動

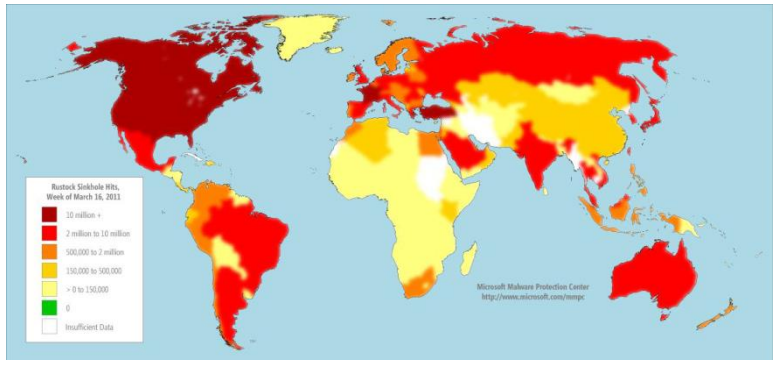
  1台のRustockに感染したPCの24分間の動き
  - 3つの通常通信
  - DNS　Aレコード　　1,406回
  - MXレコード　　2,238回
  - 送信したメールサーバ　　1,376台
  - C&C等との通信　　22回

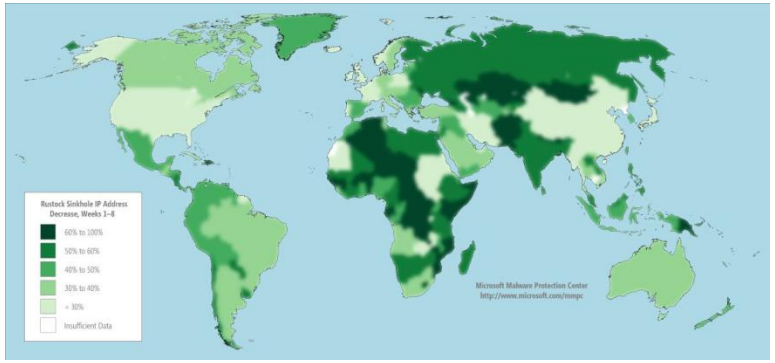


オペレーションの結果



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

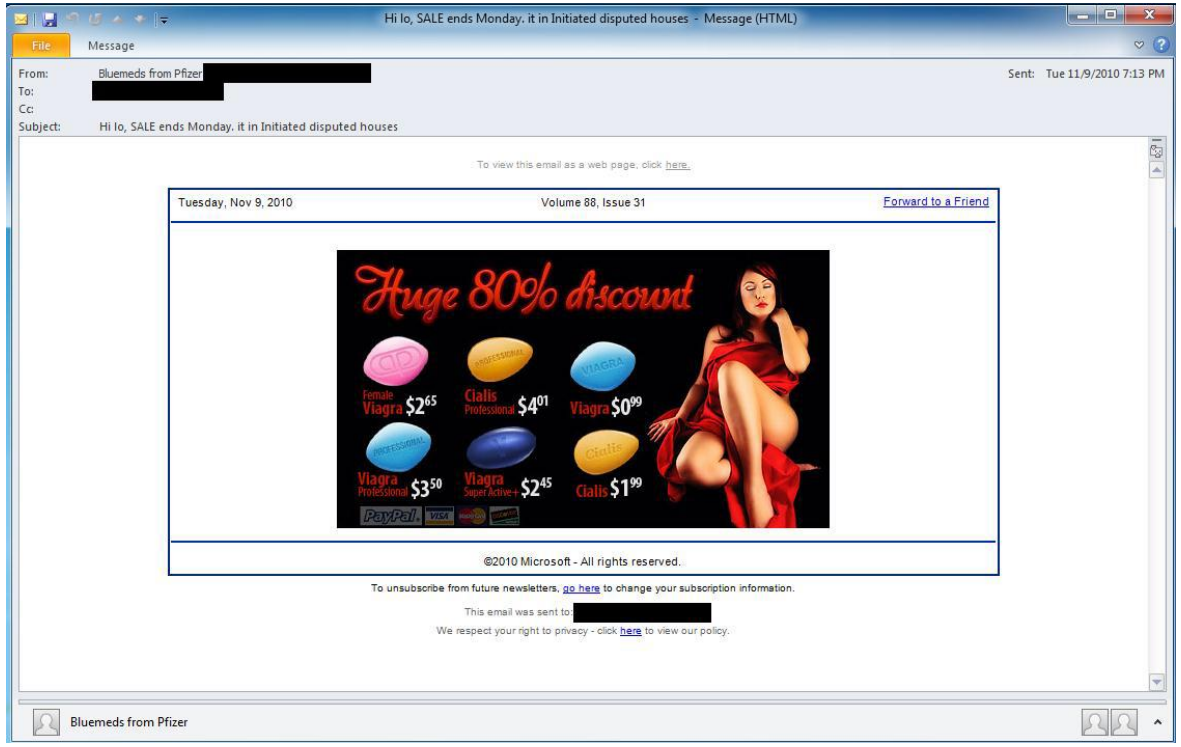
- 地理的な分析

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

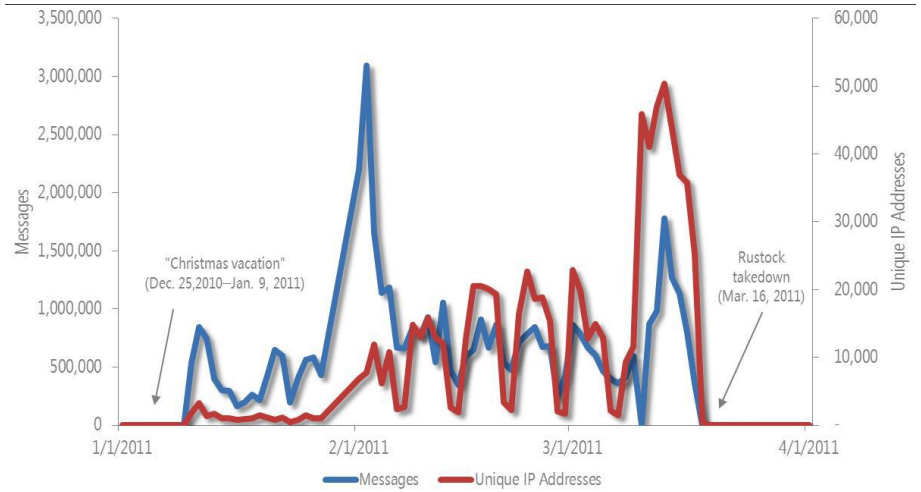
スパムに関する統計

- 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

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
- 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

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

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

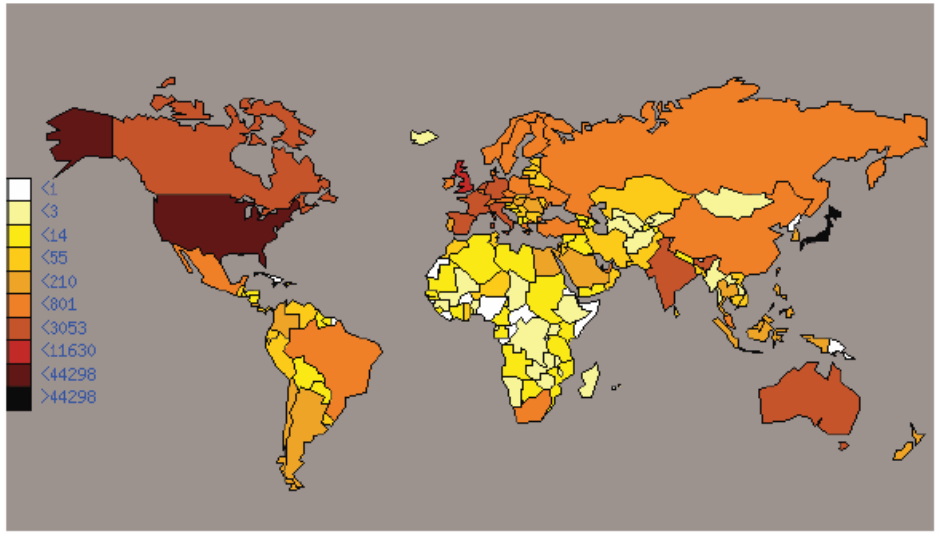
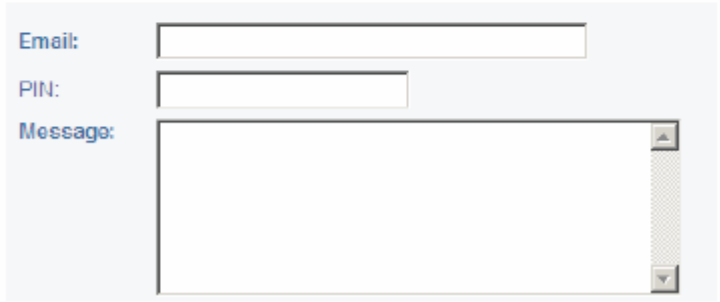


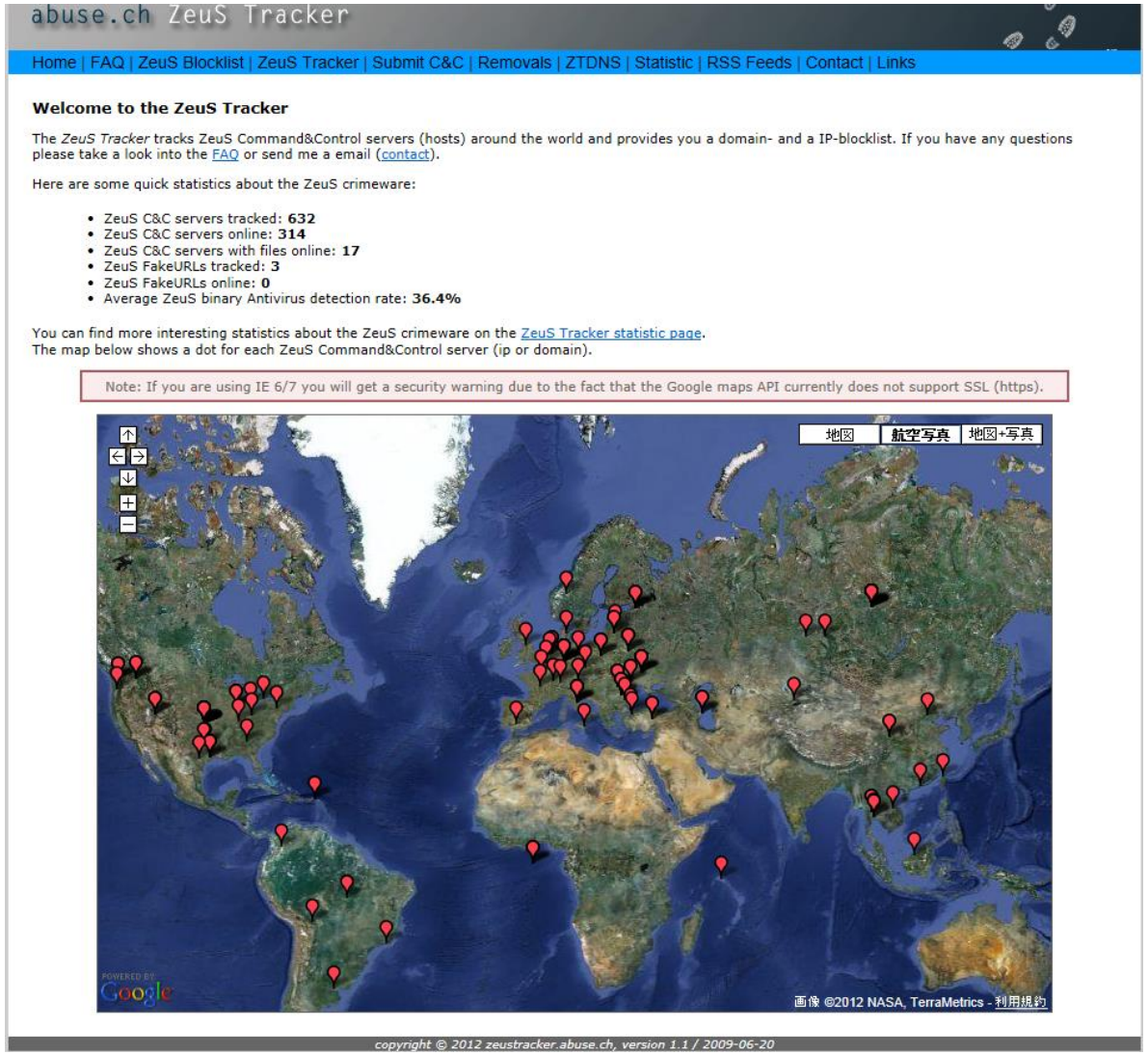
Figure 4
Web page before injection

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

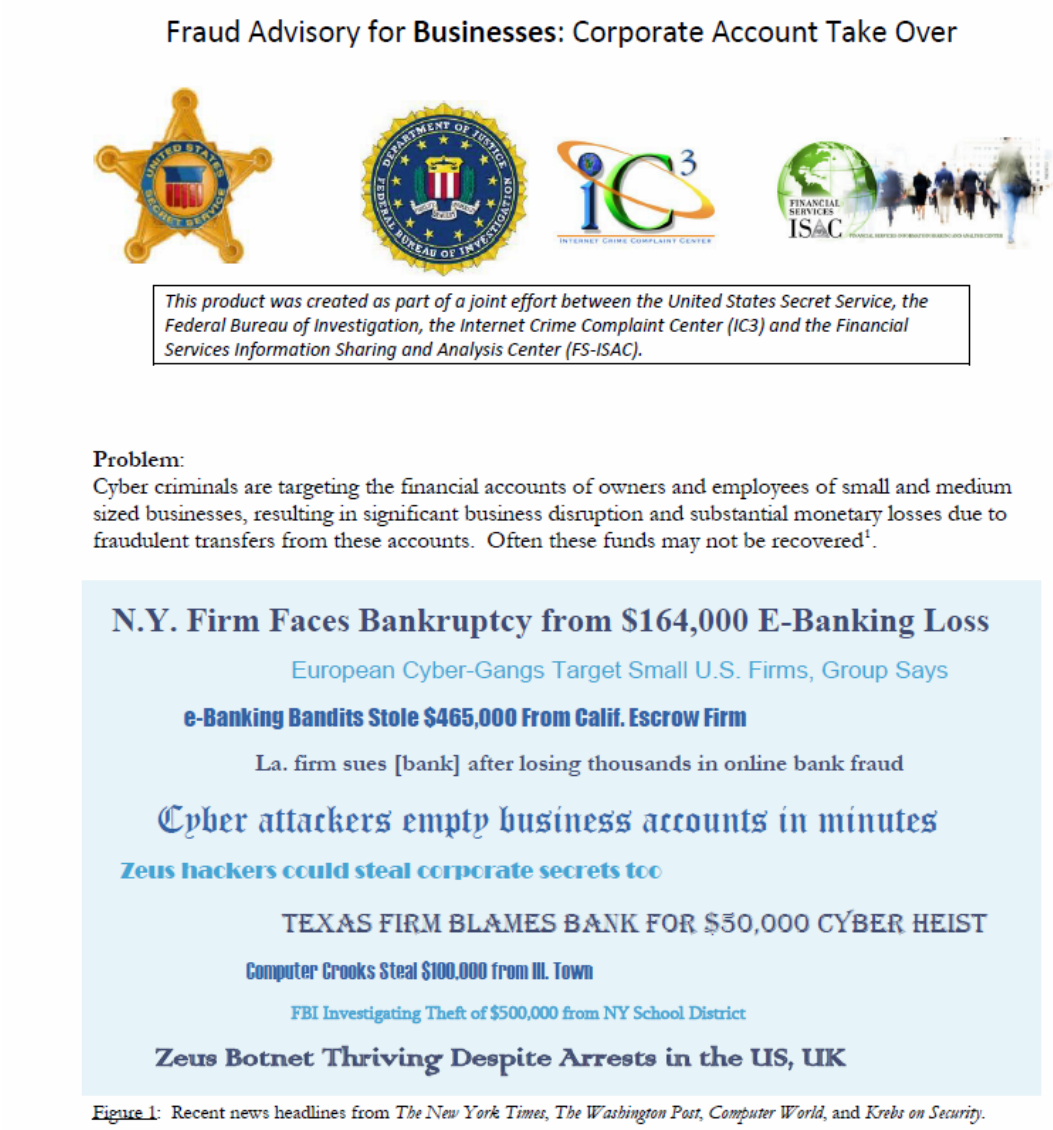
ZeuS Tracker



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*.

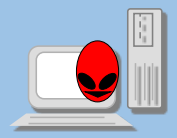
- サイバー犯罪組織は、中小規模企業の経営者と従業員の口座情報をターゲットとしている。
- これにより、重大なビジネス上の混乱と、相当額の金銭的な損失が発生している

  - 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

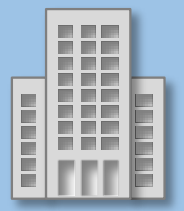
二要素認証の回避（Zeus）

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

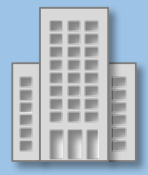


・二要素認証
乱数表
ワンタイムパスワード

二要素認証を使うオンラインバンクからの金銭を詐取

二要素認証によるログイン

Man in the Browser Attack



認証
ログイン
Top Page

口座**A**に100万円を送金

Aを**B**に書換え

口座**B**に100万円を送金

口座**A**に送金終了

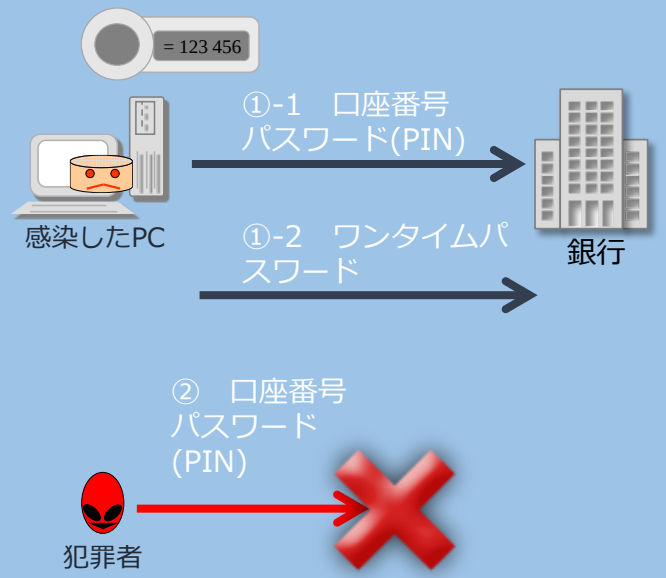
Bを**A**に書換え

口座**B**に送金終了

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

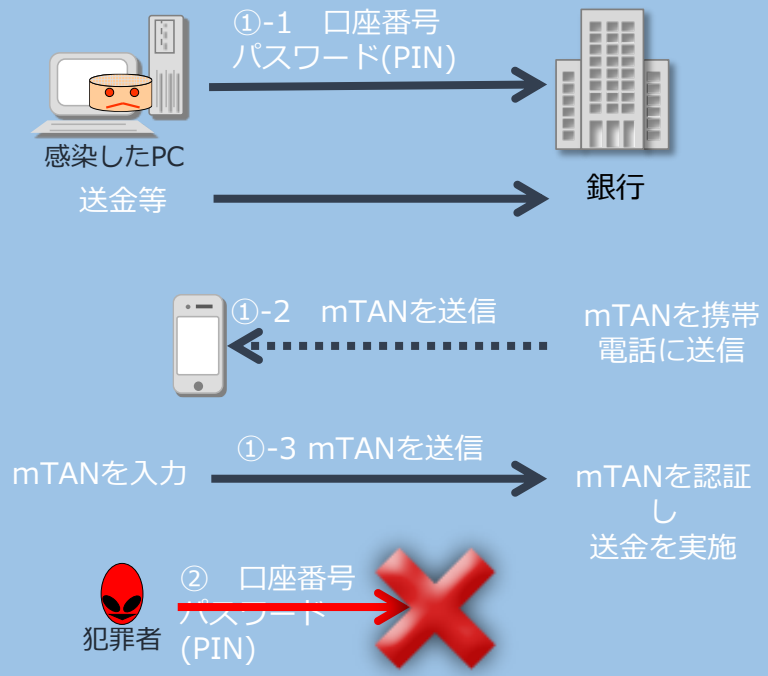
mTANに対する攻撃（SpyEye）

ワンタイムパスワードによる対策



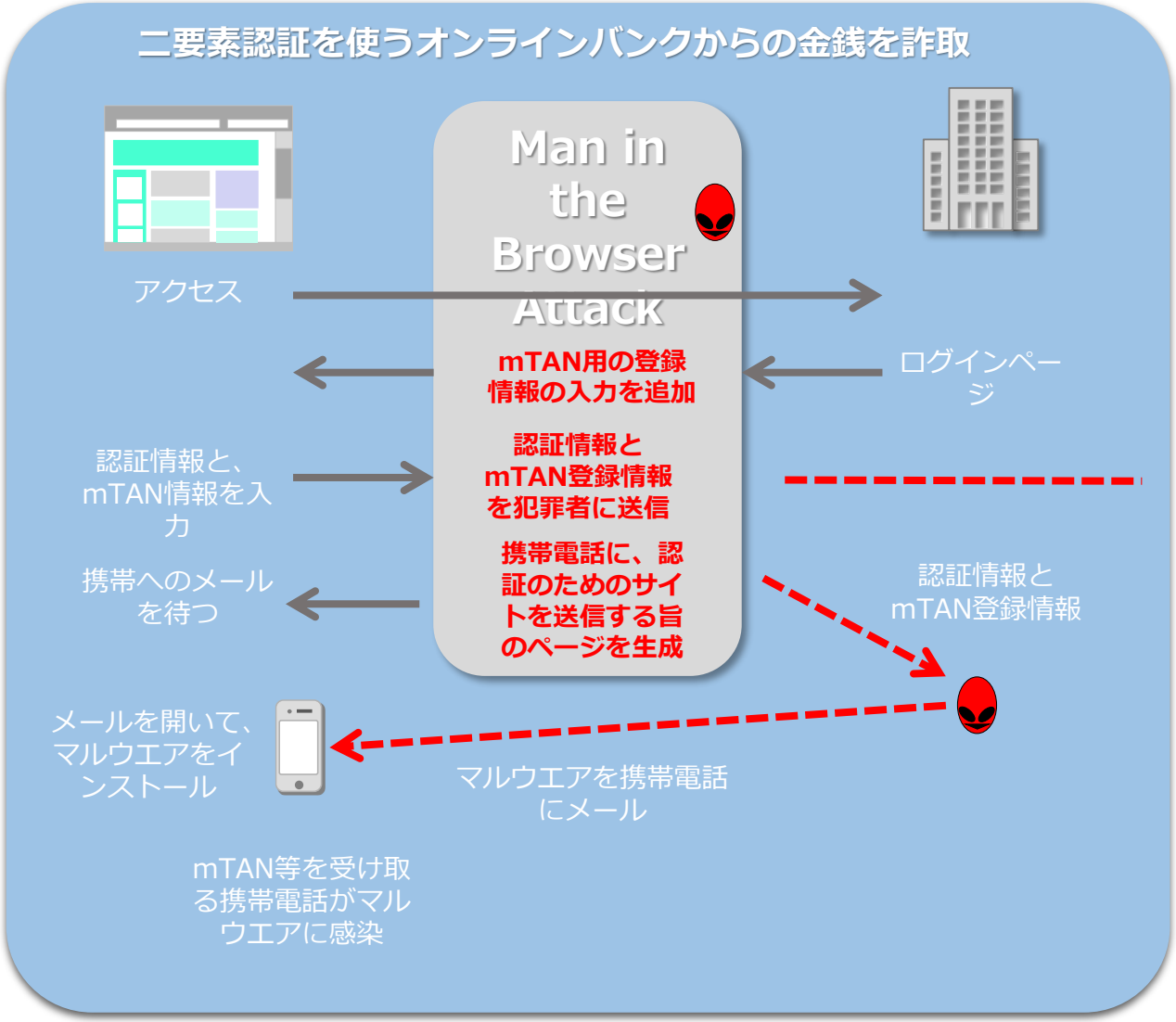
乱数表による対策
① 利用者がオンラインバンクにログインする
ワンタイムパスワードで認証する
② キーロガーがこれを詐取し、外部の犯罪者に送信する
③ 犯罪者は、認証情報を利用して、銀行から現金を引き出そうとするが、ワンタイムパスワードが取得できないため、ログインができない

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



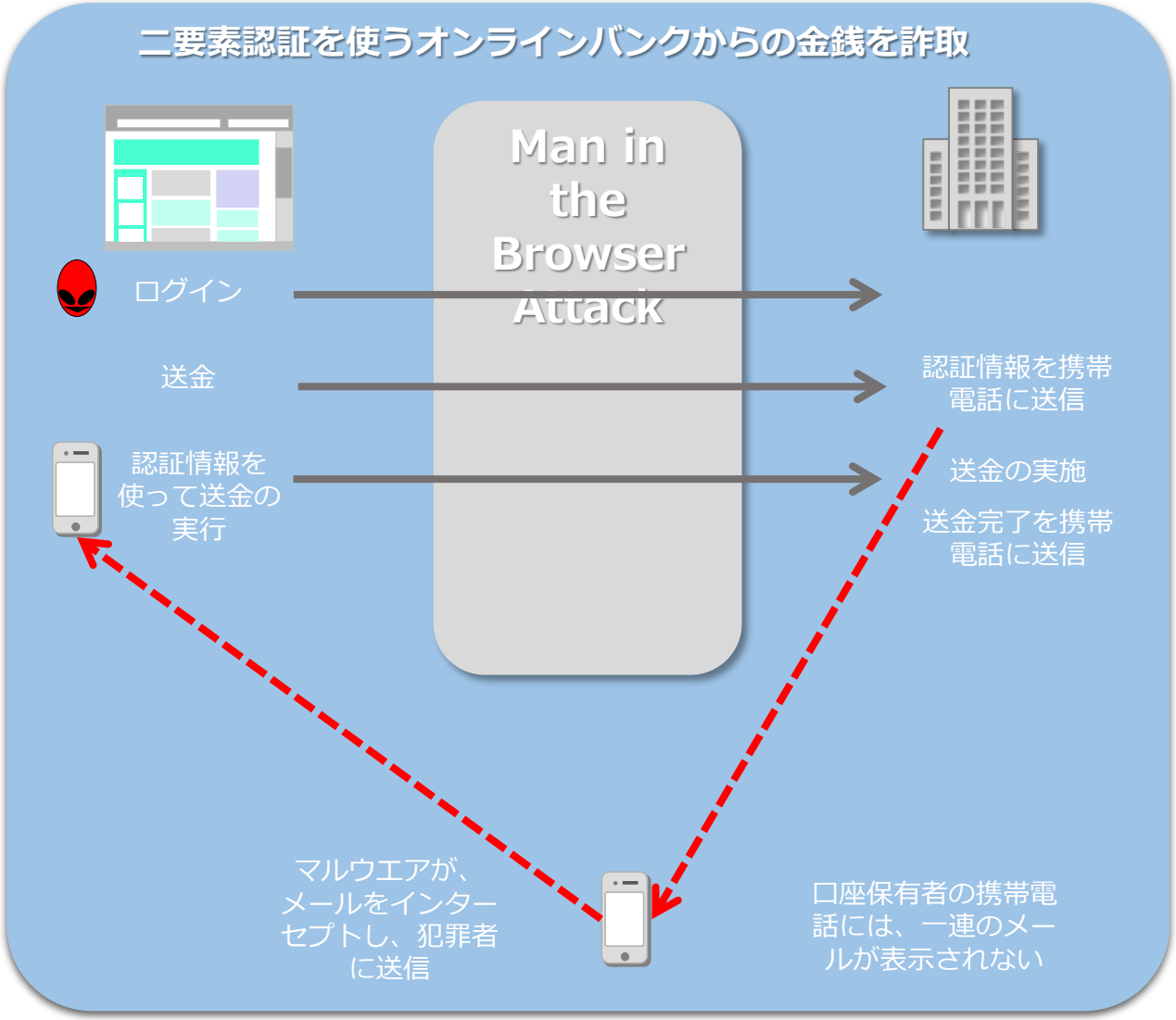
Mobile TAN (mTAN)

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



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

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

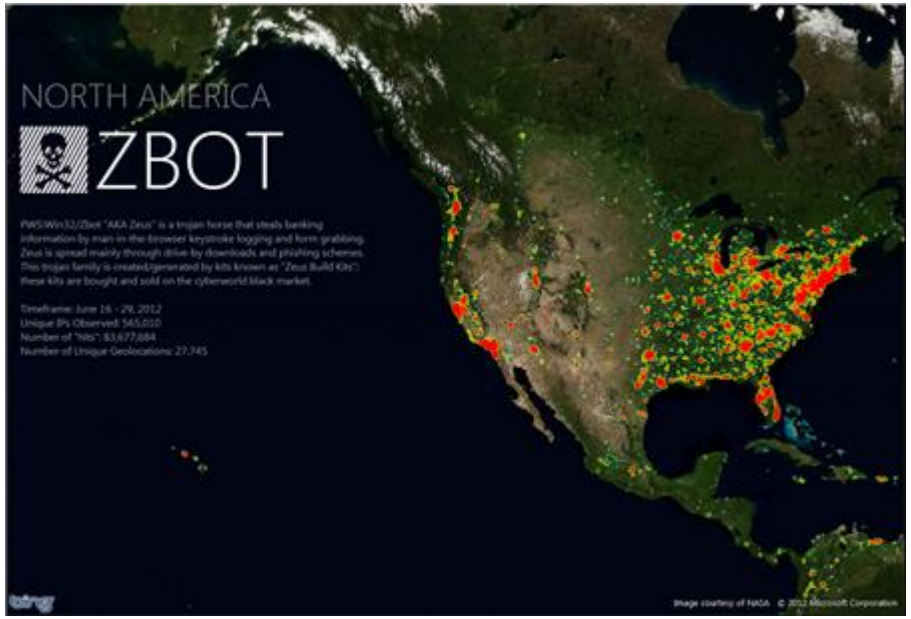
A little over three months ago, I wrote here about how Microsoft's Digital Crimes Unit, along with its financial industry partners and Kyrus Tech, took action to disrupt the dangerous Zeus botnets, known for fueling half a billion dollars in online fraud and identity left. We are pleased to announce 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

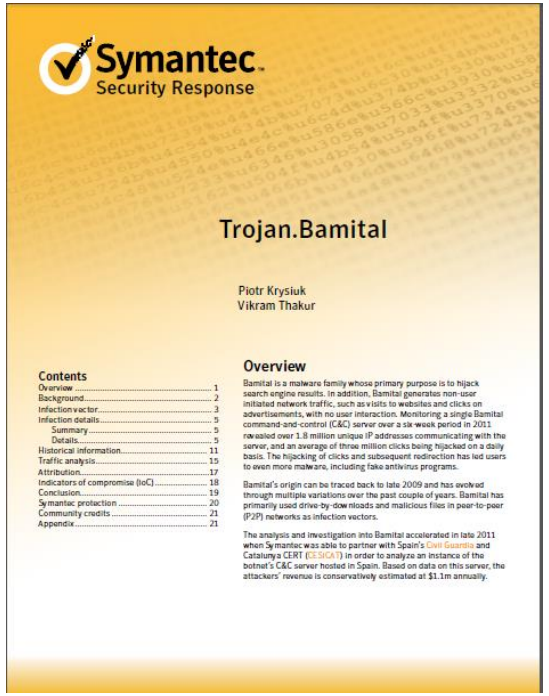


2012/3/25-31	2012/6/17-23
779,816	336,393

サイバー犯罪のコストを上げ、サイバー犯罪を抑止する

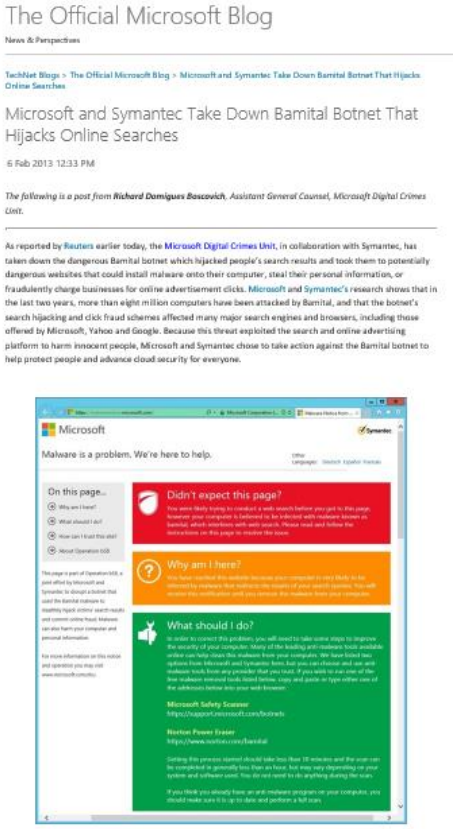
Operation b58
Bamital botnet Takedown

主要な情報ソース



Trojan.Bamital
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/trojan_bamital.pdf

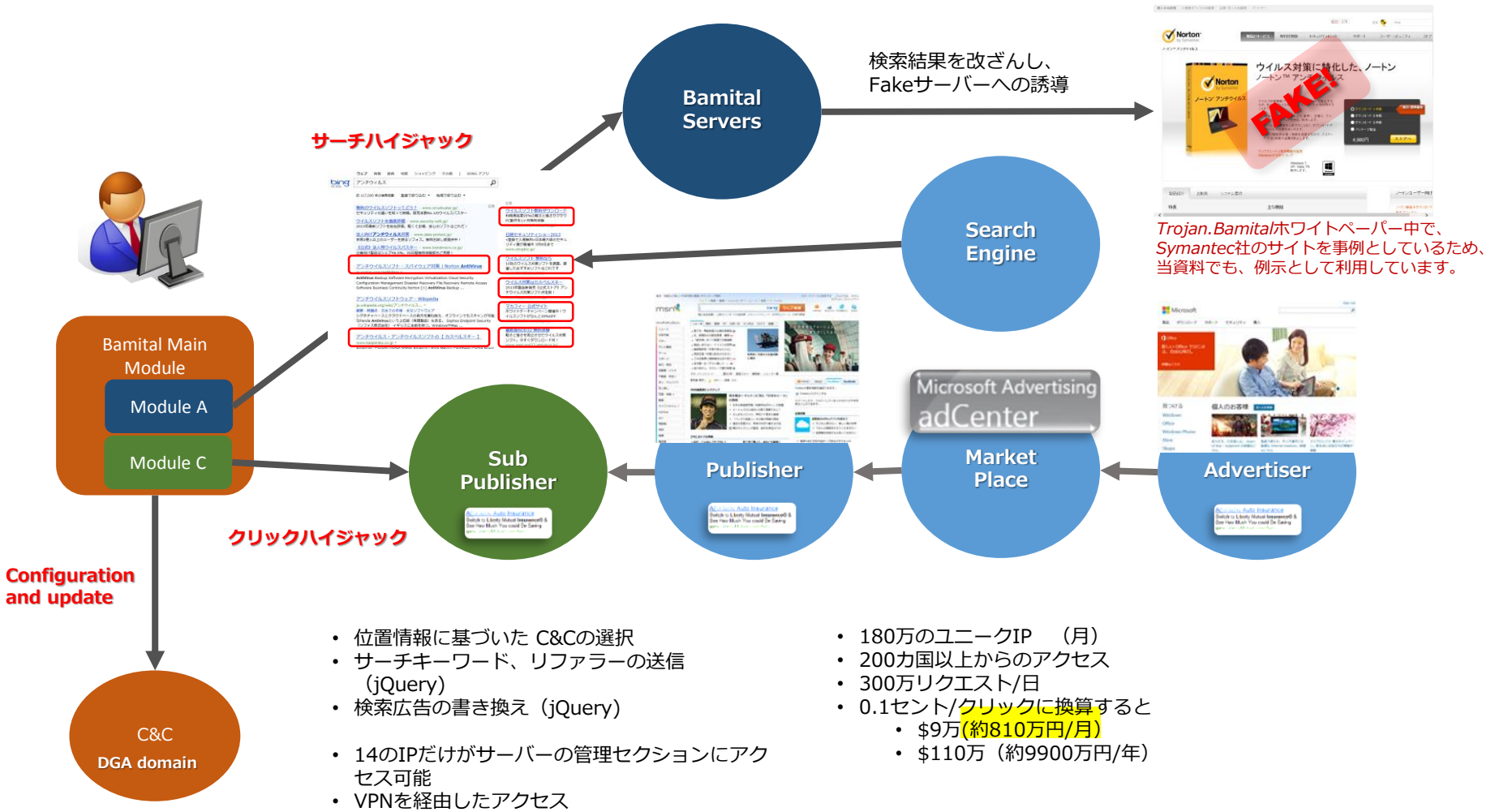
Bamitalボットネットの終焉
http://www.symantec.com/connect/blogs/bamital-0



Microsoft and Symantec Take Down Bamital Botnet That Hijacks Online Searches
http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx

Bamital Botnetの概要

Bamitalの挙動

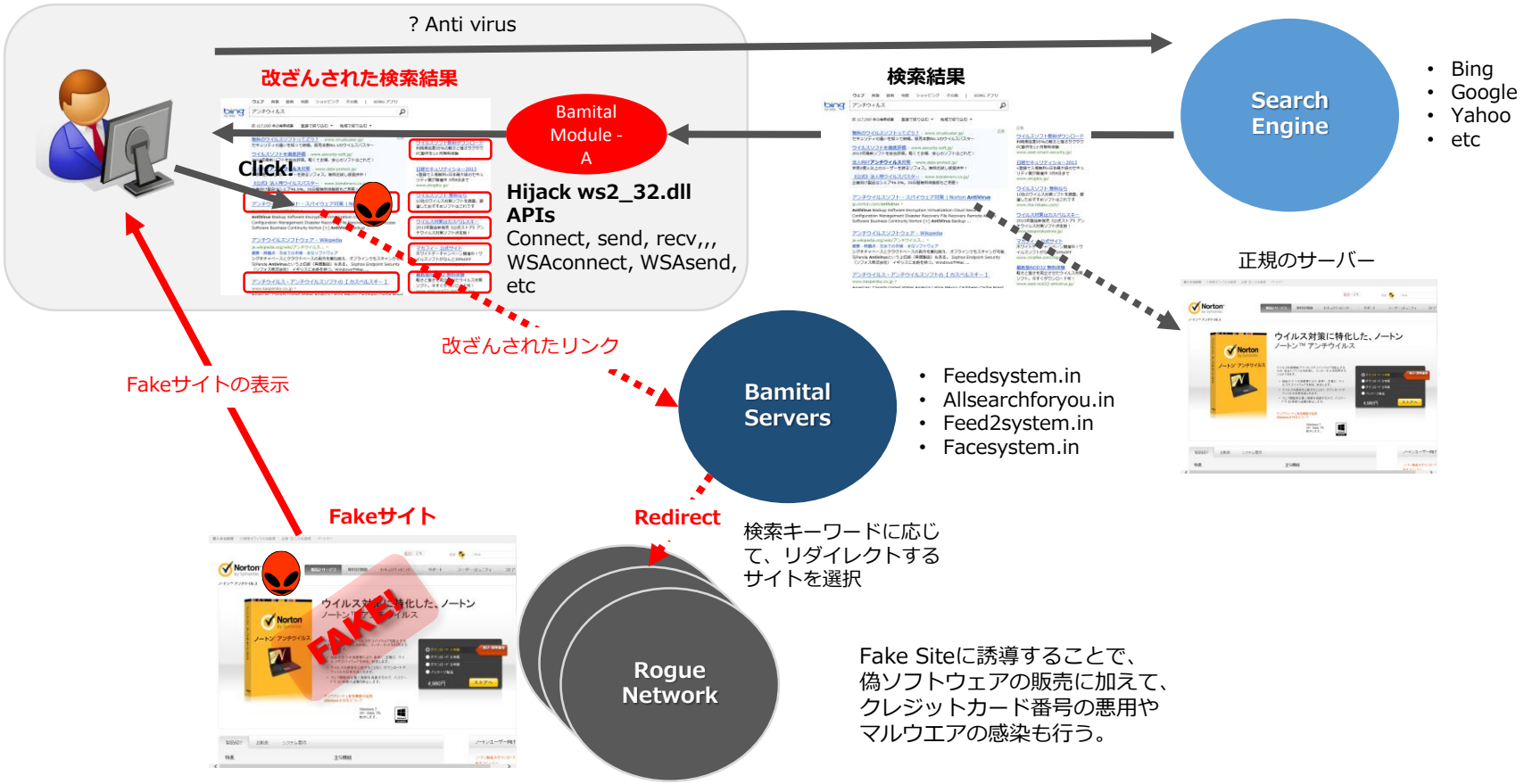


- 位置情報に基づいた C&Cの選択
- サーチキーワード、リファラーの送信（jQuery）
- 検索広告の書き換え（jQuery）

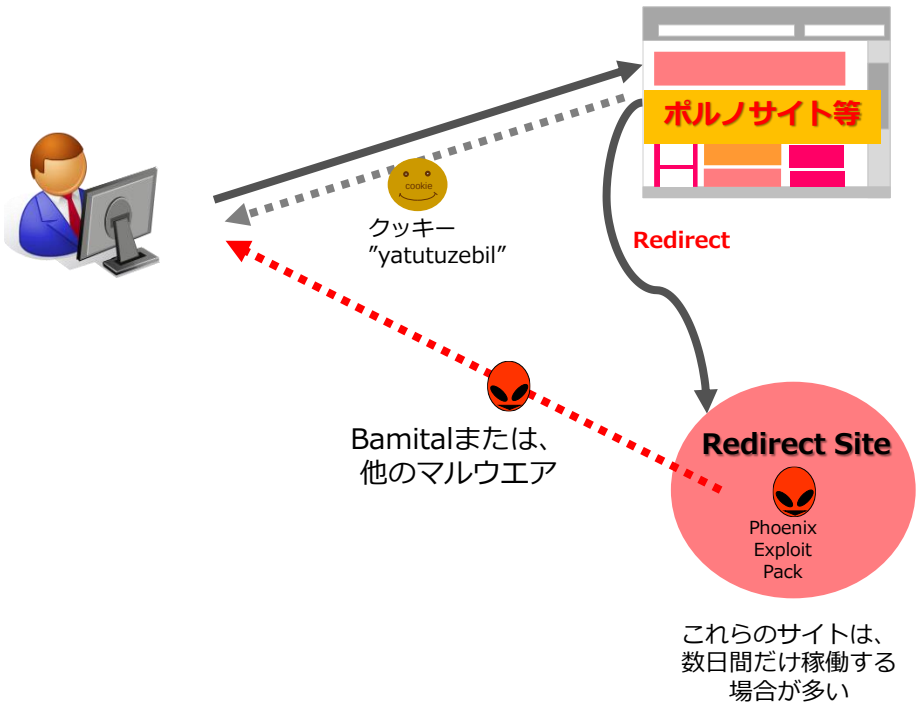
- 14のIPだけがサーバーの管理セクションにアクセス可能
- VPNを経由したアクセス
- オンライン広告ブローカーの利用

- 180万のユニークIP　（月）
- 200カ国以上からのアクセス
- 300万リクエスト/日
- 0.1セント/クリックに換算すると
  - $9万(約810万円/月)
  - $110万（約9900万円/年）

サーチハイジャックの仕組み



感染のルート(Drive by Download)



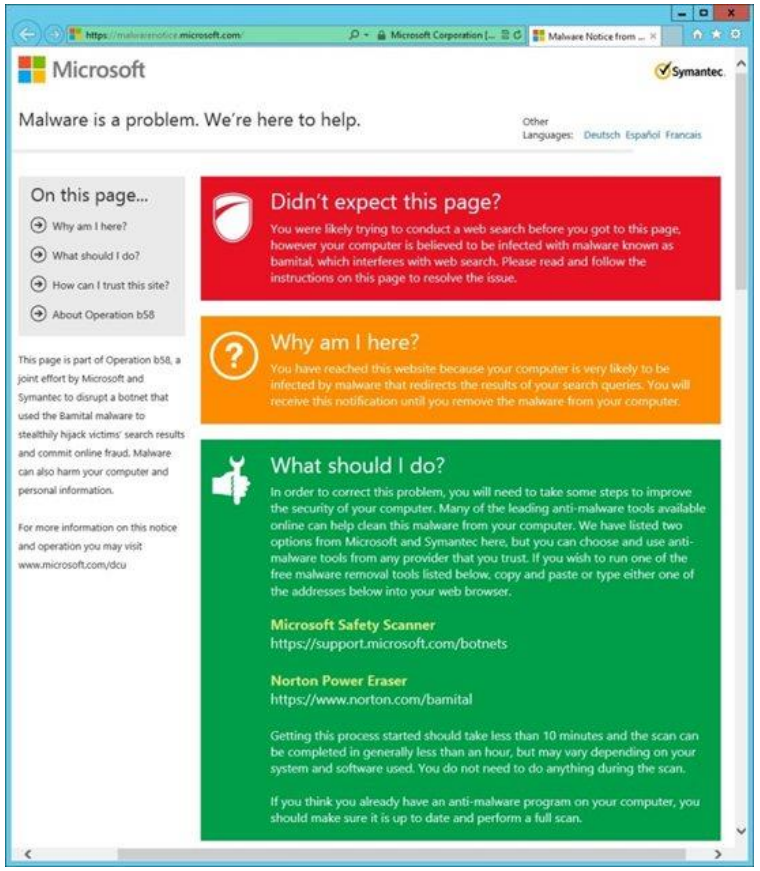
yatituzebil cookieをセットするドメイン名

- all-celeb.com
- allsearchforyou.in
- bestpornodrive.com
- beststoresearch.com
- catalogforyou.com
- catalogpornosearch.com
- celebrity-info.com
- drafsddhjk.com
- easy-statistics.in
- ekstaz.info
- facesystem.in
- famouspeopledata.com
- famouspeopleinformation.com
- findalleasy.com
- findallsimple.com
- freepornoreport.com
- freepornoshop.com
- freesearchshop.com
- localfreecatalog.com
- loveplacecatalog.com
- lovepornomoney.com
- newpornopicture.com
- newsearchnecessary.com
- newsearchshop.com
- pornobeetle.com
- pornofreecatalogs.com
- pornofreeforyou.com
- pornowinner.com
- proshopcatalog.com
- searchnecessary.com
- search-porno.info
- shopcataloggroup.com
- shop-work.com
- superstarsinfo.com
- winnerfree.com

ランダムに生成されたと思われるドメイン名

- bahufykyby.info
- basewibuxenagip.info
- cefimoqicy.info
- cohehonyhe.info
- covyqileju.info
- decogonuwy.info
- degupydoka.info
- diconybomo.info
- dixegocixa.info
- favomavene.info
- fegufidaty.info
- fenemusemy.info
- fihyqukapy.info
- fokizireheceduf.info
- fyzuvejemuxoqiw.info
- gecadutolu.info
- gybejajehekyfet.info
- hiveqemyrehinex.info
- kyqehurevynyryk.info
- lofyjisoxo.info
- loqytylukykiruf.info
- lujuhijalu.info
- luxohygity.info
- moqawowyti.info
- musututefu.info
- mysotonego.info
- negenezepu.info
- pyziviziny.info
- qecytylohozariw.info
- qokimusanyveful.info
- qudevyfiqa.info
- radohowexehedun.info
- relusibeci.info
- rulerykozu.info
- sygonugeze.info
- taqyhucoka.info
- tebejoturu.info
- vesufopodu.info
- vujygijehu.info
- vyzefykeno.info
- wezadifiha.info
- xatawihuvo.info
- xohuhynevepeqyv.info
- zuhokasyku.info
- zykuxykevu.info

Takedown



- Bamital ボットネットに係るドメインおよびIPアドレスに対する差し押さえの民事訴訟を起こし、受理される。
- Bamital に感染しているユーザーは、ボットネットのTakedownにより、検索結果がエラーとなるため、Bamitalに感染していることと対策の方法を周知するためのページを作成し、そのページに誘導した

http://blogs.technet.com/b/microsoft_blog/archive/2013/02/06/microsoft-and-symantec-take-down-bamital-botnet-that-hijacks-online-searches.aspx

オンライン広告と
クリックジャック

オンライン広告の概要

Traffic

Real or Fraudulent

Internet Users

Publishers

Sites displaying ads to their visitors
(Supply side actors)

Bing, Google, Yahoo, MSN, YouTube,
ICanHasCheezburger

Marketplace

Runs the auction

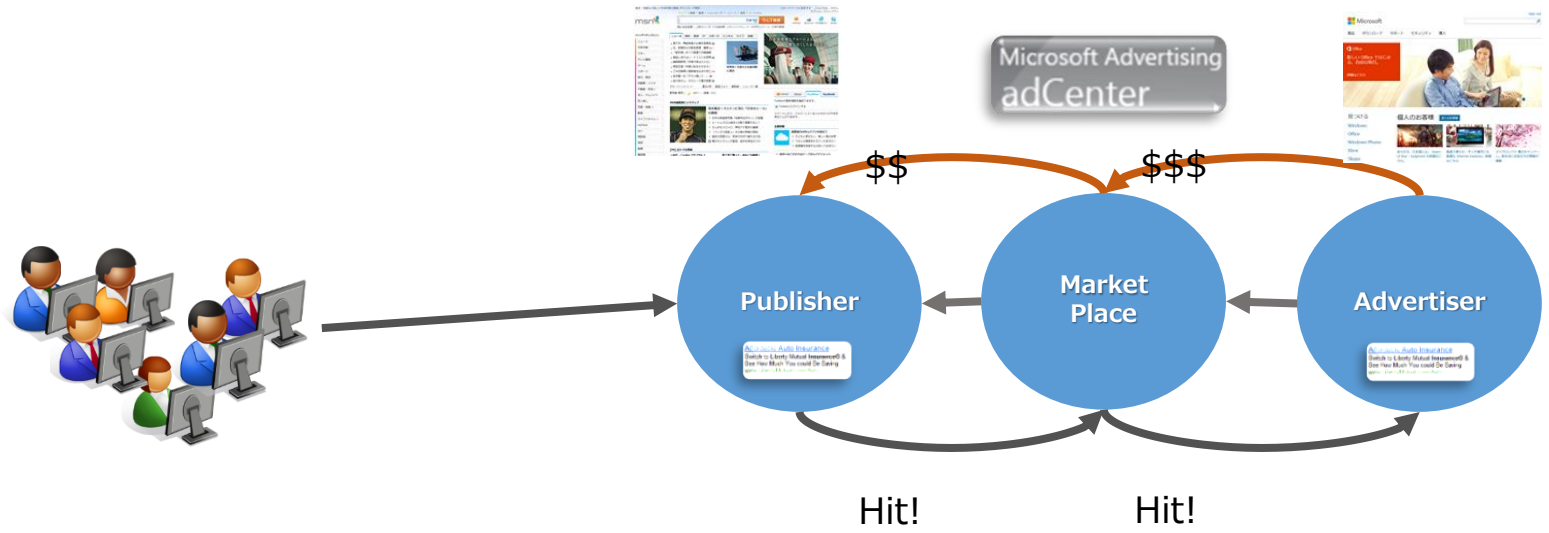
AdWords & adCenter

Advertisers

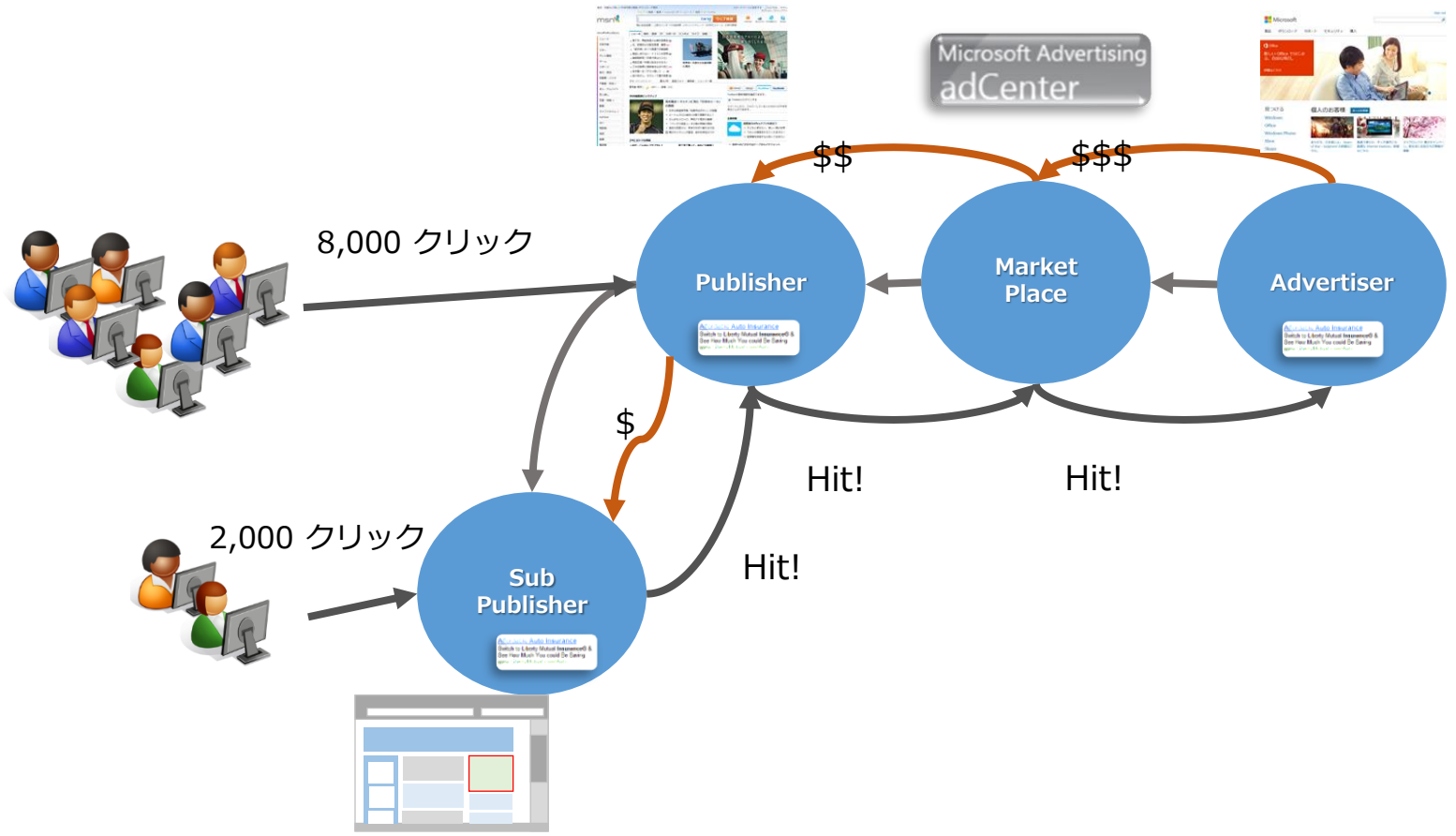
Sites wishing to acquire traffic
(Demand-side actors)

Wal-Mart, eBay, Amazon,
Progressive, Apple

オンライン広告の概要

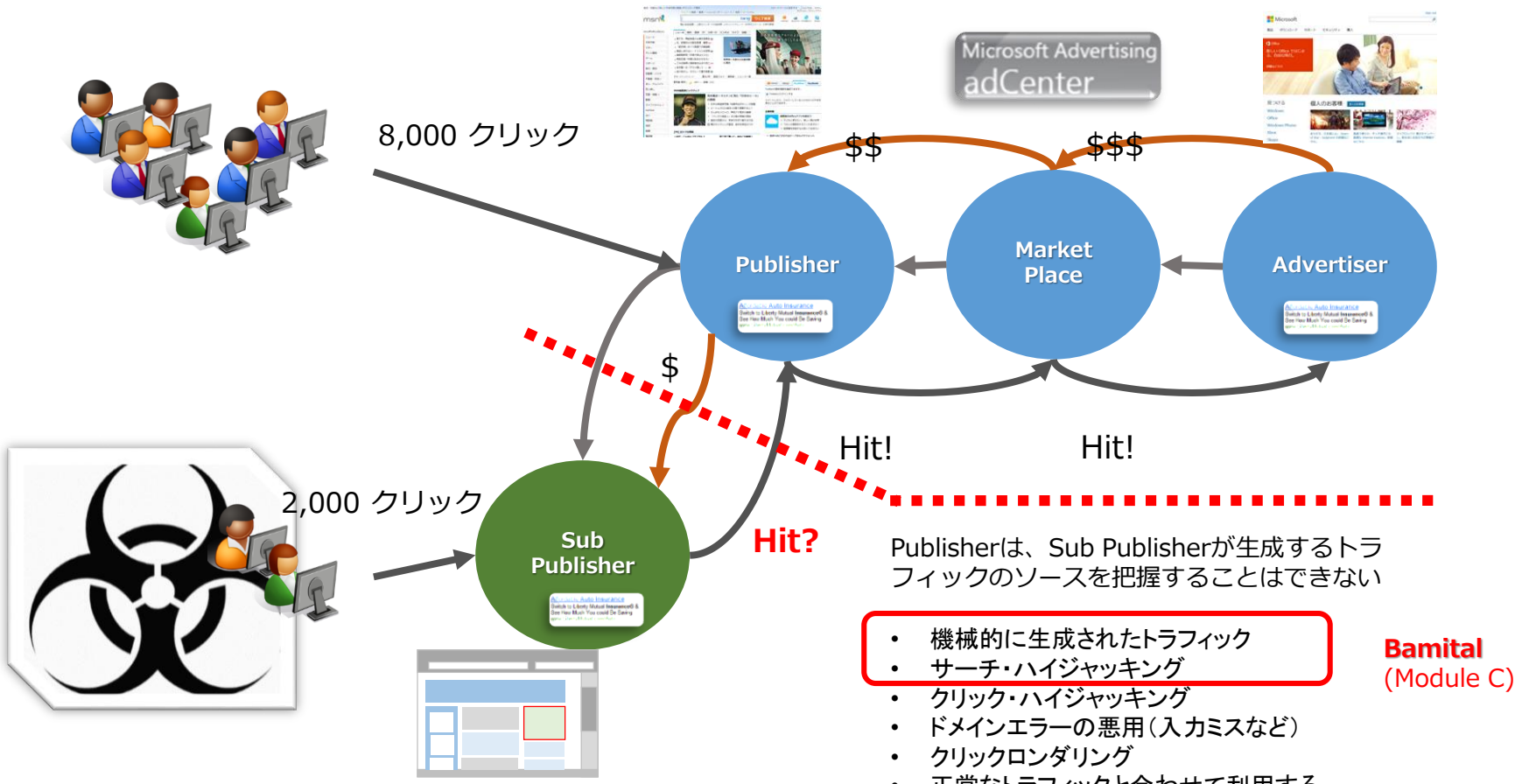

Microsoft Advertising
adCenter
$$
$$$
Publisher
Market Place
Advertiser
Hit!
Hit!

オンライン広告の再販（Sub-Syndication）



例：BLOG向けのアフェリエートプログラム

Sub-Syndicationの問題と悪用

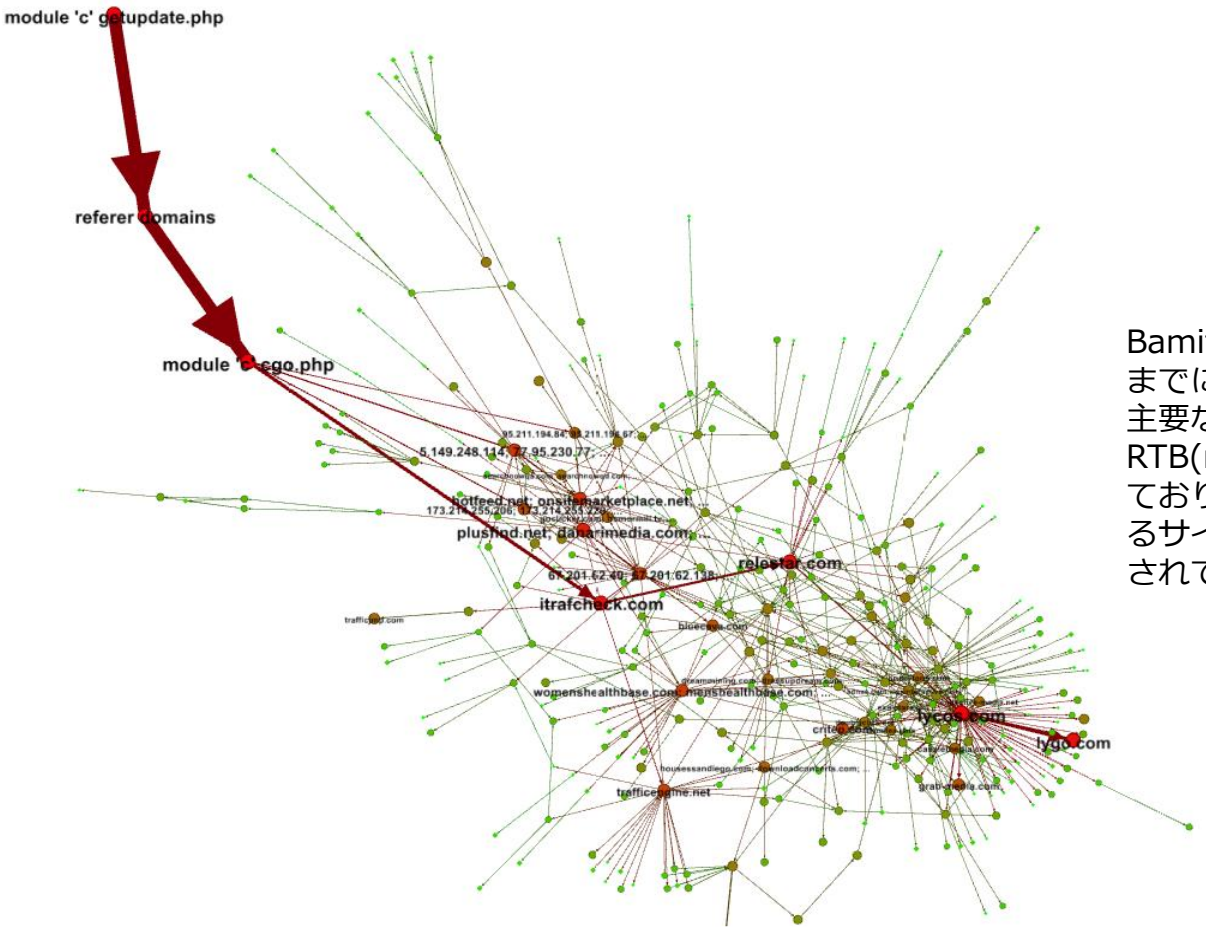


Publisherは、Sub Publisherが生成するトラフィックのソースを把握することはできない

- 機械的に生成されたトラフィック
- サーチ・ハイジャッキング
- クリック・ハイジャッキング
- ドメインエラーの悪用（入力ミスなど）
- クリックロンダリング
- 正常なトラフィックと合わせて利用する

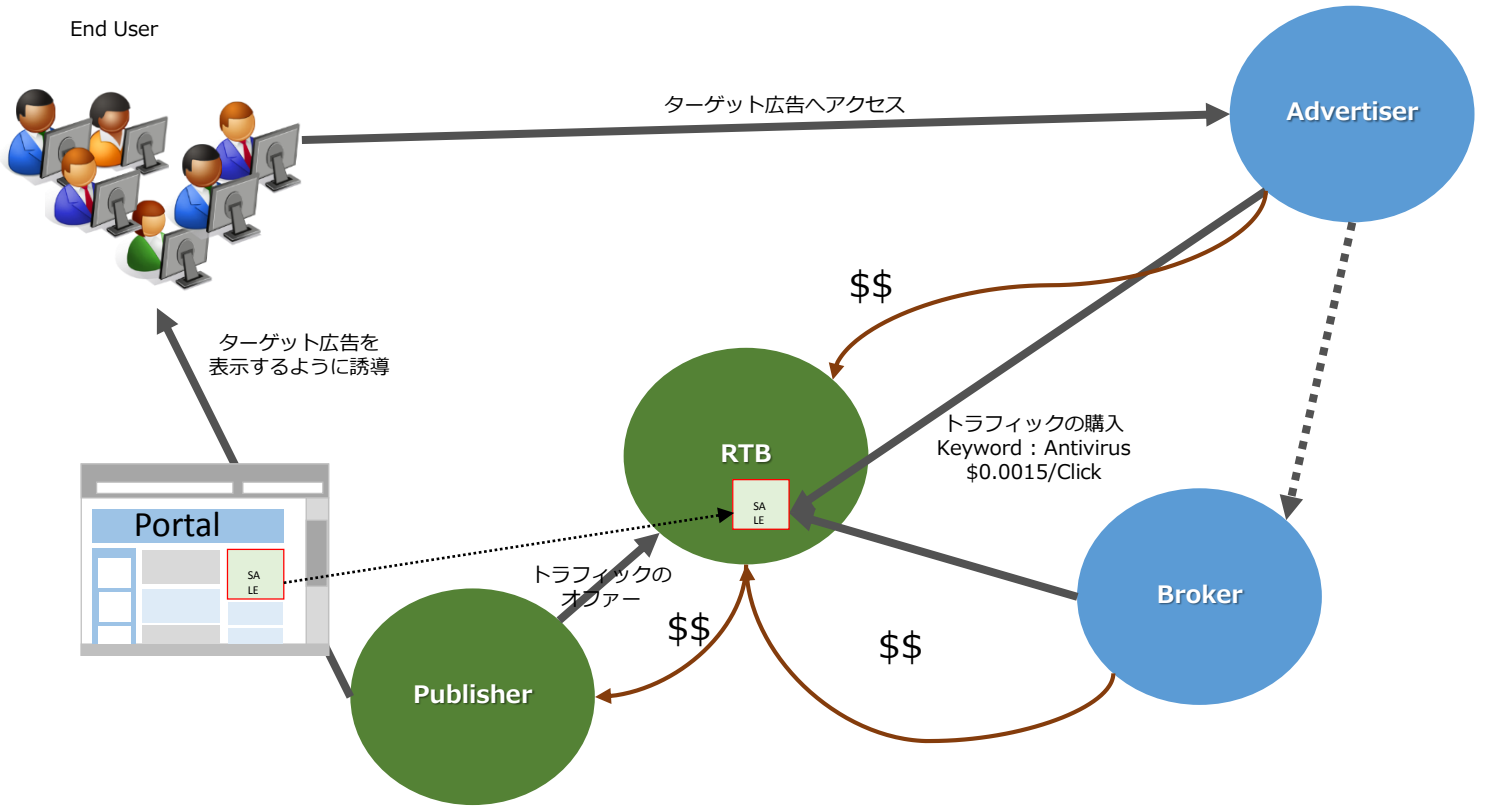
Bamital
(Module C)

Bamital Traffic Pattern

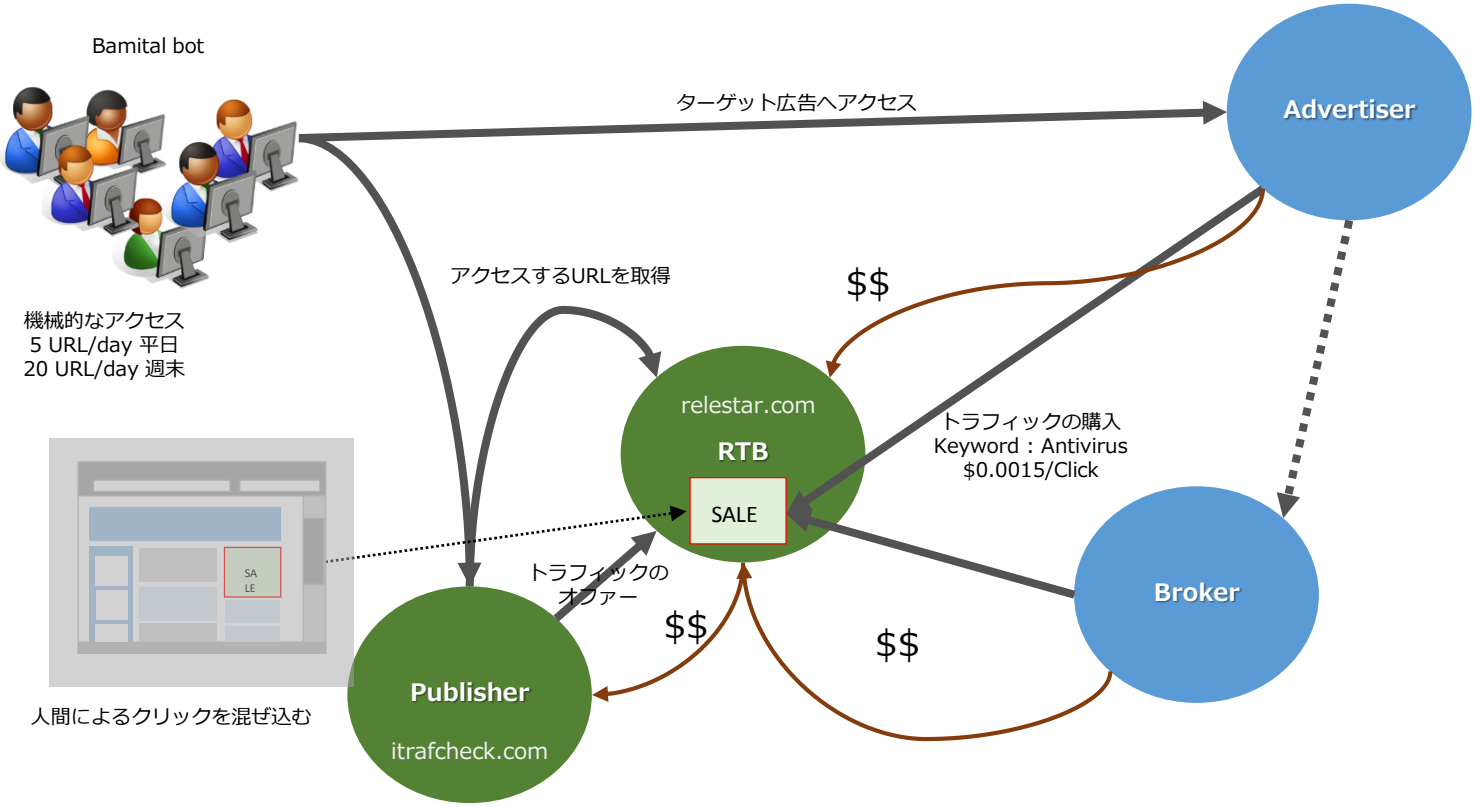


Bamitalが標的とする広告にアクセスするまでに、10以上のサイトを経由している
主要なアクセスポイントとして、
RTB(real-time bidding)サイトが含まれており、このサイトを通じて、アクセスするサイトの最適化を図っているものと推測されている

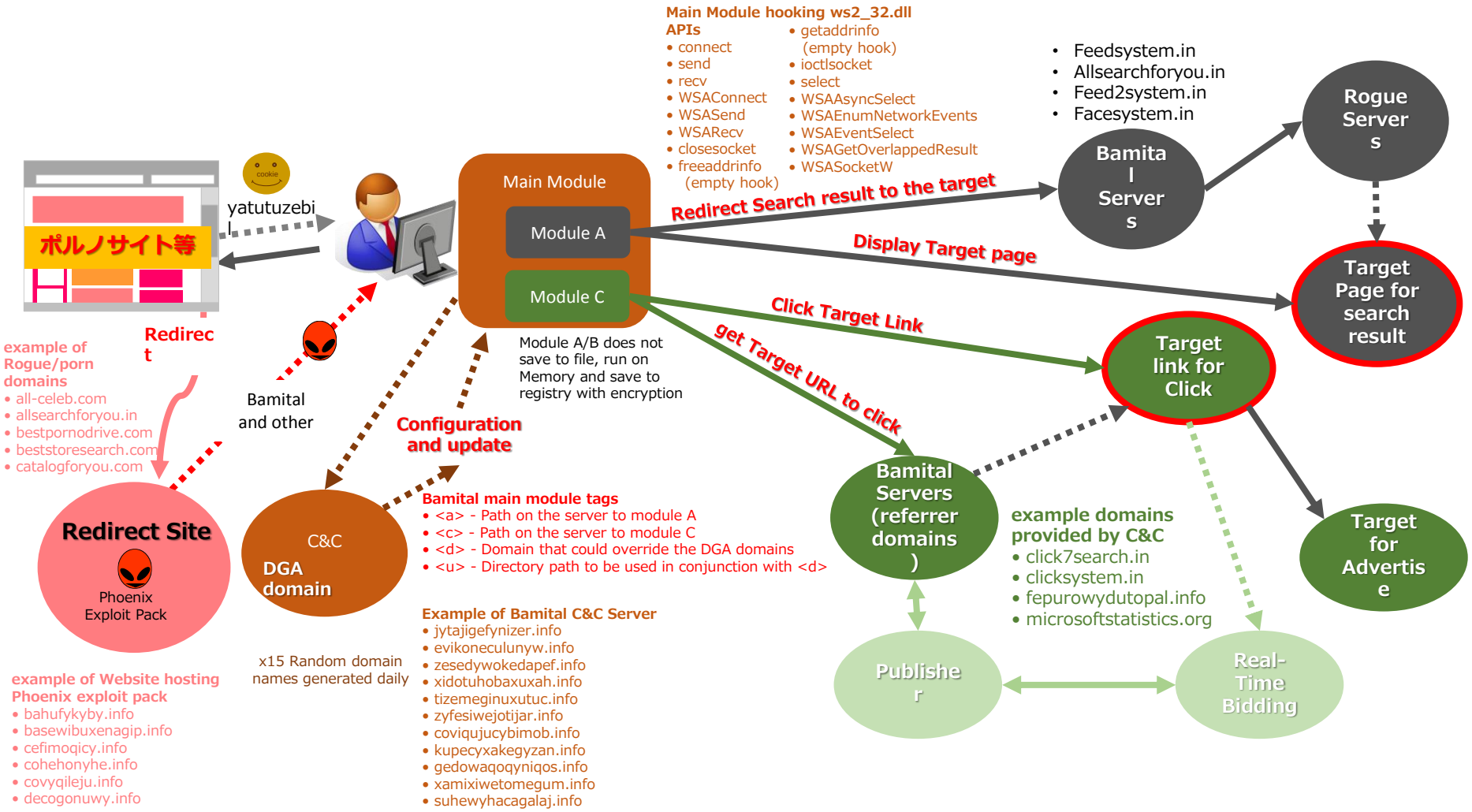
RBT(Real-time Bidding)



RBTの利用:Bamitalのケース



Bamitalエコシステム



むすび

- サイバー犯罪のターゲットとして、オンライン広告が悪用される機会が増えている。
- これらの犯罪においては、他のサイバー犯罪と同様に、ボットネットが基盤として利用されている。
- ボットネットのTakedownは、サイバー犯罪を撲滅することはできないが、ソフトウェアのセキュリティレベルの向上と共に、サイバー犯罪の投資対効果を上げ、サイバー犯罪が割りの合わないものにしていくための、重要な取り組みである。

- マイクロソフトでは、今後とも関係機関と協力して、ボットネットなどサイバー犯罪に対する取り組みを継続していく。

Operation b54

Citadel botnet

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

http://www.microsoft.com/en-us/news/Press/2013/Jun13/06-05DCUPR.aspx

Operation b54の概要

- 2013年6月5日にCitadelボットネットをTakedown
  - 民間の法執行機関の協力が効果的に機能することを示す事例となった
- 被害：キーロガー機能を使ったIDを盗み出し銀行口座からの窃盗
  - 5億ドル以上の損害、500万人以上への影響（感染）
  - 感染国：90カ国以上
    - 主要な感染国：米国、ヨーロッパ、香港、シンガポール、インド、オーストラリア
- オペレーションへの参加組織
  - FS-ISAC, NACHA, ABA,
  - Agari, A10 Networks, Nominum, Microsoft DCU
  - FBI
- オペレーションの概要
  - 民事訴訟によるオペレーション
    - Microsoftが民事訴訟によりコンピューターサーバーを含むデータと証拠を差し押さえた
      - 裁判所：North CarolinaのWestern District
      - データセンター：New JerseyおよびPennsylvania
    - 1,462のCitadelボットネットと、数百万におよぶ感染したコンピューターの通信を遮断
    - 米国外の各国に存在する Citadelに感染したコンピューターへの対応ができるように、 CERT組織に対して情報を提供
    - なお、よりリアルタイム性の高い情報を提供するため　C-TIPによる情報提供を開始
  - FBIによる法執行
    - 捜査令状に基づいた、米国内での執行
    - 各国が必要な措置ができるように、海外の法執行機関への情報を提供

オペレーションの主要メンバー

- FS-ISAC
  - 1999年に設立された、金融機関のISAC(Information Sharing and Analysis Center)
  - 金融機関で、物理的およびサイバーセキュリティに関するインシデント情報を、適切で対応可能な情報を、タイムリーに共有することで、リスクを軽減することを目的としている
- NACHA:The Electronic Payments Association
  - 電子商取引を支える ACH ネットワークの開発、管理、運用を行っている
  - 17の地域の、10,000以上の金融機関を代表する組織
- ABA : American Bankers Association
  - 米国の銀行を代表する組織で、総額14兆ドルの銀行業務と、2000万人により構成されている
- Agari: FS-ISACのパートナー
  - フィッシングなどの電子メールの脅威から守るために、インターネット上から収集した数テラバイトの電子メールをベースとした、フォレンジックデータを提供
- A10 Network
  - CitadelボットネットをTakedownするための先端技術を提供
  - 2004年に設立された、革新的なネットワークとセキュリティソリューションを提供する企業
- Nominum
  - CitadelボットネットをTakedownするための先端技術を提供
  - 通信事業者向けの DNS/DHCPサーバーを提供している(140通信事業
- FBI

ボットネットTakedown事例のご紹介

GameOver ZeusとBladabindi-Jenxcus

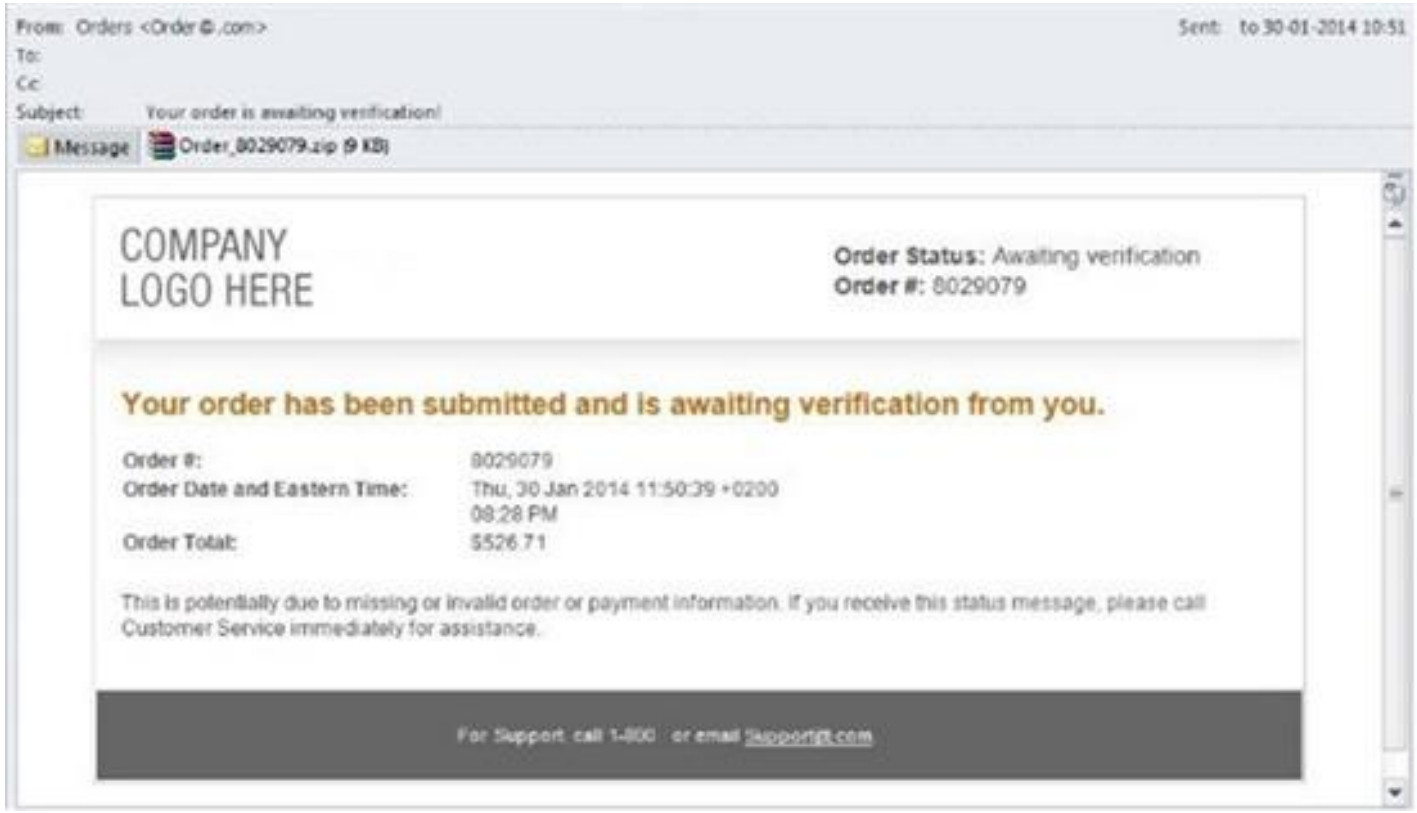
日本マイクロソフト株式会社
チーフセキュリティアドバイザー
高橋 正和

GameOver Zeus

- GameOver Zeus
  - 2011年９月に発見されたP2Pを利用するZeusの亜種
  - オンラインバンクの認証情報を盗み、ランサムウエアとしても動作する他、スパムの送信や、DDoSなどにも利用される。
  - スパムやフィッシングメッセージを通じて拡散することが多い
- 被害などの規模
  - 50 万台から 100 万台のコンピューターが感染
  - FBIは 1 億ドルを超える損失をもたらしていると予想
- Takedownの実施(2014/6/2)
  - FBIや警察庁などの各国の法執行機関が主体となりTakedownを実施、セキュリティベンダーやマイクロソフトが協力
  - FBI が登録されたドメインを差し押さえ、C&Cインフラストラクチャの一部を崩壊させた
- マイクロソフトの役割
  - P2P ネットワークの分析の実施とクリーニング ソリューションの開発
  - Shadow Server 等の協力を経て Cyber-Threat Intelligence Program (C-TIP)を通じた感染IPの提供

マイクロソフトがGameOver Zeusボットネットのクリーンアップで FBIに協力
http://blogs.technet.com/b/jpsecurity/archive/2014/06/04/microsoft-helps-fbi-in-gameover-zeus-botnet-cleanup.aspx

GameOver Zeusの攻撃メールの例



Bladabindi-Jenxcus活動基盤への対処

- Bladabindi-Jenxcus
  - 他のソフトウェアのパッケージを装うなどのソーシャルエンジニアリングを使って感染するマルウエアで、バックドアにより、攻撃者が任意の操作を行うことができる
- 被害等の規模
  - マイクロソフトのセキュリティ製品だけでも、過去12か月で740万以上の感染を検知しており、その93%がNo-IPを利用している。
- 対処
  - マイクロソフトは 6月19日に、マルウエアの数百万台ものマルウエアの感染とコントロールを行っている、Mohamed Benabdellah およびNaser Al Mutairiと、その基盤となっている無料のダイナミックDNSサービスNo-IPを運営するVitalwerks Internet Solutions, LLCに対して、ネバダ州で民事訴訟を行った。
  - 6月26日に裁判所の許可（ex patre TRO)を得て、Bladabindi - Jenxcus の基盤となる、No-IPの23のドメインのIPアドレスを、マイクロソフト社が所有する無害なIPアドレスに変更した。
  - これにより得られた情報は、Microsoft’s Cyber Threat Intelligence Program (CTIP)や、各国のCERT組織、ISPに提供される

Microsoft takes on global cybercrime epidemic in tenth malware disruption
http://blogs.technet.com/b/microsoft_blog/archive/2014/06/30/microsoft-takes-on-global-cybercrime-epidemic-in-tenth-malware-disruption.aspx

Bladabindi と Jenxcus

Bladabindi

Bladabindi は、NJ Ratと呼ばれるハッカーツールを使って作成される。
NJ Ratは公開されているツールで、自由にアイコンを変更することができる。つまり、Bladabindiは、いくつものアイコンを使い分けることで、利用者が誤って実行することによって感染する。

Bladabindi が利用するアイコンのサンプル

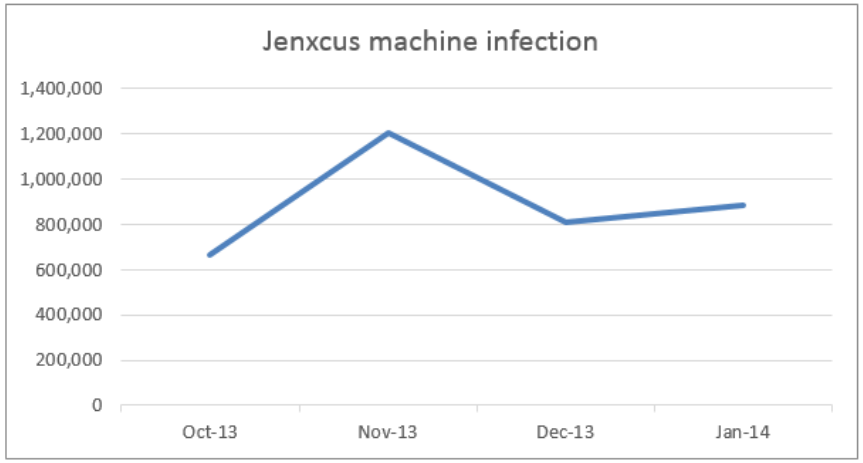
MSIL/Bladabindi
http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=MSIL/Bladabindi#tab=2

Janxcus

Janxcusは、VBScriptを使って書かれたワームで、リムーバブルメディアを使って感染することができるが、主に、他のプログラムにバンドルすることで感染を広げている。

感染するとバックドアを作り、攻撃者はリモートから感染したPCを操作することができる。
2014年2月の月例の更新で、MSRT(Microsoft Malicious Software Removal Tool ）に追加されている。

Jenxcusが感染に悪用する
偽 Flash Playerアップデートサイト



Jenxcusの感染率の推移

MSRT February 2014 – Jenxcus
http://blogs.technet.com/b/mmpc/archive/2014/02/11/msrt-february-2014-jenxcus.aspx

ボットネットのTakedownについて

- Takedownの効果
  - ボットネットのTakedownは、ボットネットの活動を停止するもので、ボットの駆除を行うものではない。
  - 今回対応をした、GameOver Zeusのように、非常に堅牢な仕組みを持ったボットネットは、何らかの方法で活動を再開する可能性が高い。
- 利用者に求められる対応
  - ボットネットが活動をしていると、アップデートを行うなどの方法で、セキュリティ対策ソフトに検知されないように活動する。
  - ボットネットの活動が停止している間は、セキュリティ製品によるボットの検知と駆除が期待できます。
  - セキュリティソフトが最新版であることを確認し、リアルタイム検知だけではなく、ハードディスク等に対する全スキャンの実施が重要。

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

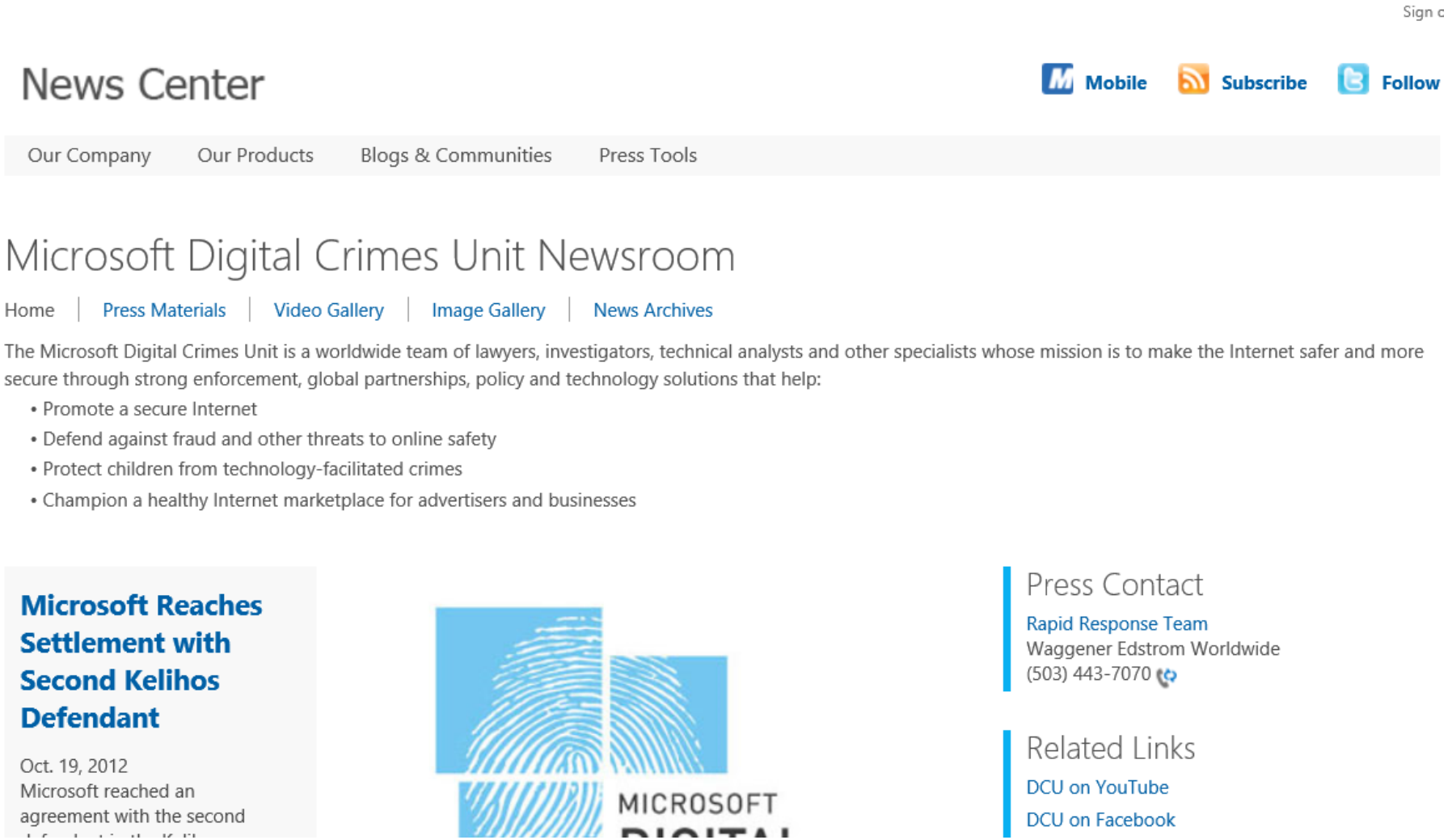
セキュリティインテリジェンスレポート

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



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

© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the
part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.