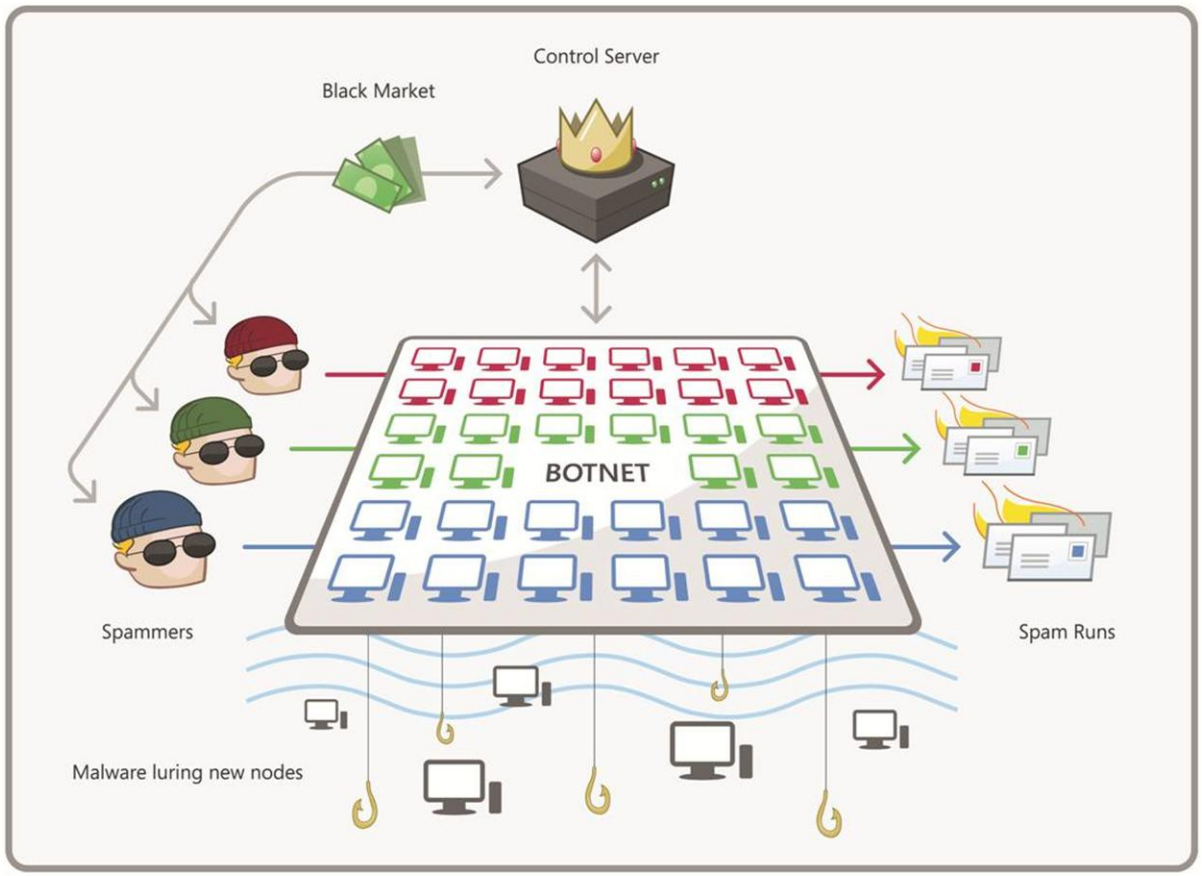
犯罪基盤としてのボットネットと対策の事例

マイクロソフト（株）
チーフセキュリティアドバイザー
高橋　正和

ボットネット



未承諾電子メールの87%はボットネットが原因でおこる。

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

DDoS攻撃–
2008年中の攻撃
190,000件

出典：Internet Security
http://internet-security.suite101.com/article.cfm/botnets_guilty_for_87_of_2009_global_spam_mail#ixzz0eysy7BTj
Namestnikov, Yuri. "The Economics of Botnets," Kaspersky Lab. 2009年

Waledac：2009年7月～12月

Hotmailは18日間でマルウェア「Waledac」に感染したコンピュータからのトラフィック6億5,100万件を遮断

39カ国におけるボットネット上位10位

マイクロソフトは、 96,223台のマシンからWaledacを駆除した。

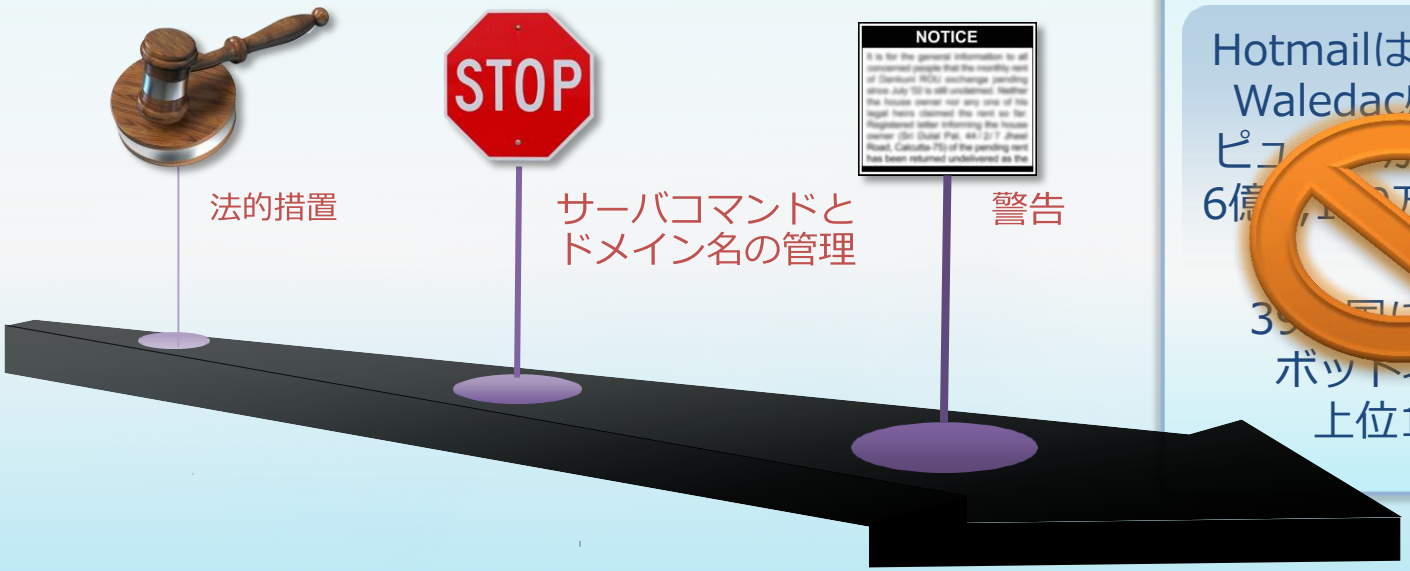
出典：マイクロソフトデジタル犯罪ユニット、
マイクロソフトマルウェアプロテクションセンター、2010年3月

Microsoft

ボットネット

WALEDACボットネット「遮断」アプローチ

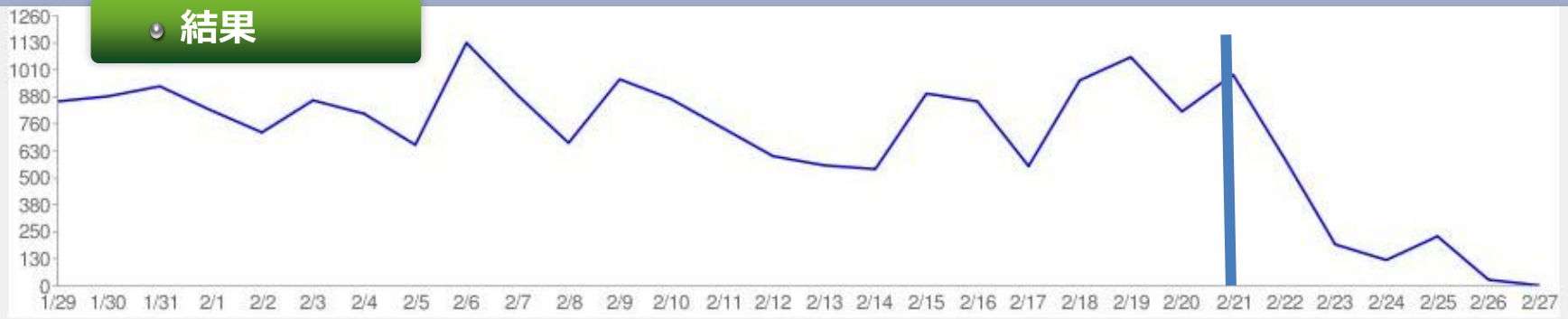
短期的 – 先例を作る



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

3[redacted]る
ボットネット
上位10位

結果



Microsoft

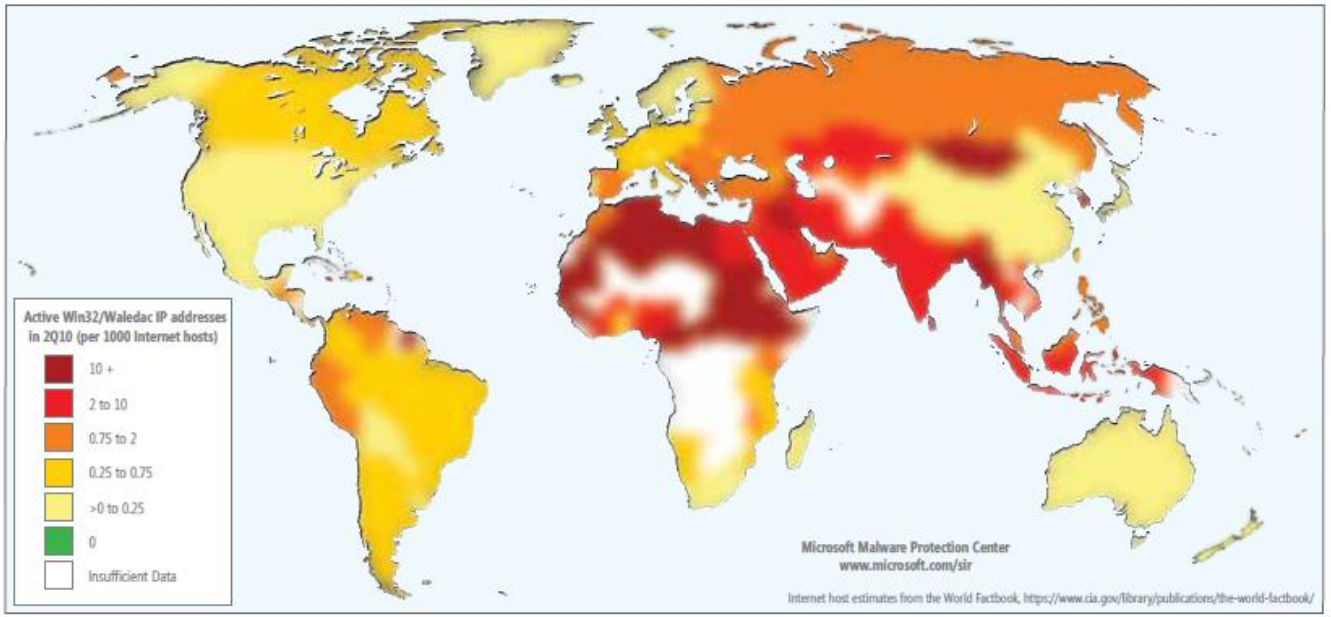
WALEDAC TAKE DOWN

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

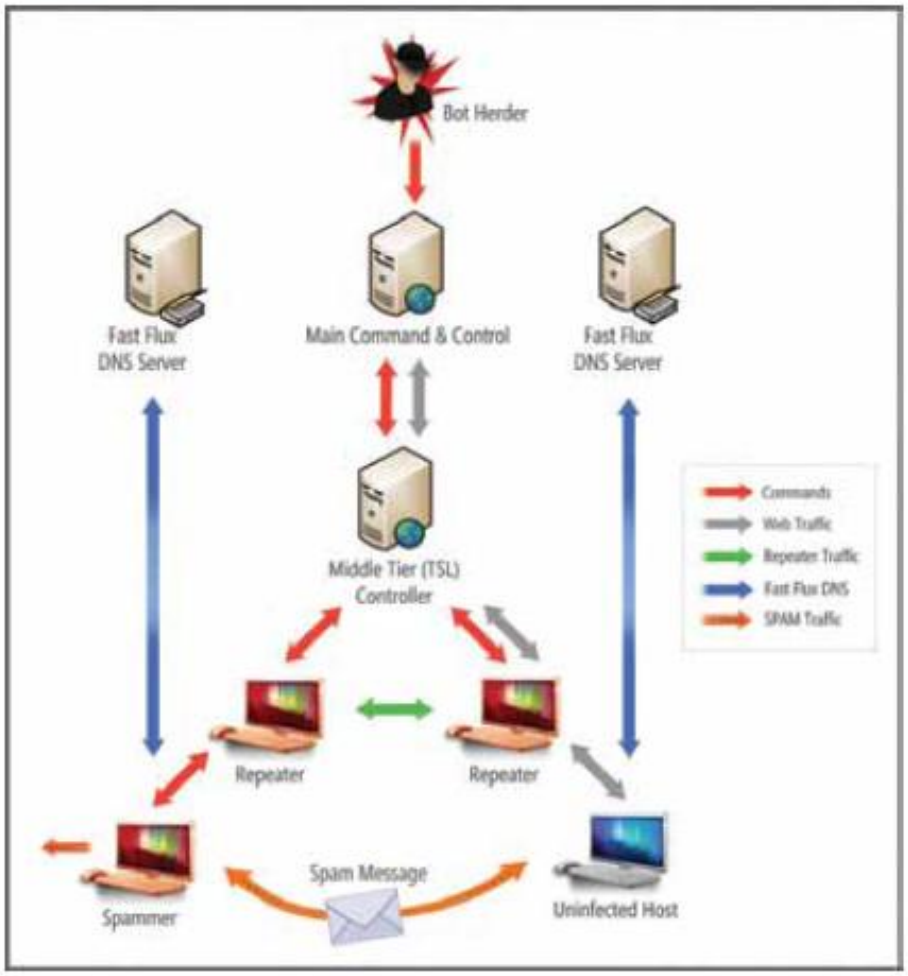
FIGURE 17. Active IP addresses in the Win32/Waledac botnet in 2Q10, per 1000 Internet hosts



- 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

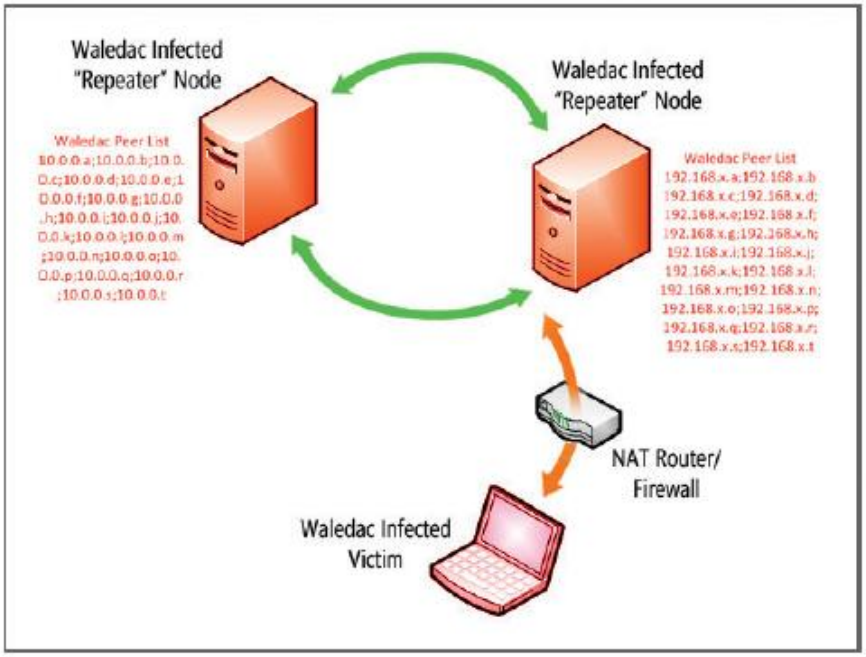
FIGURE 18. The Win32/Waledac tier infrastructure



- 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



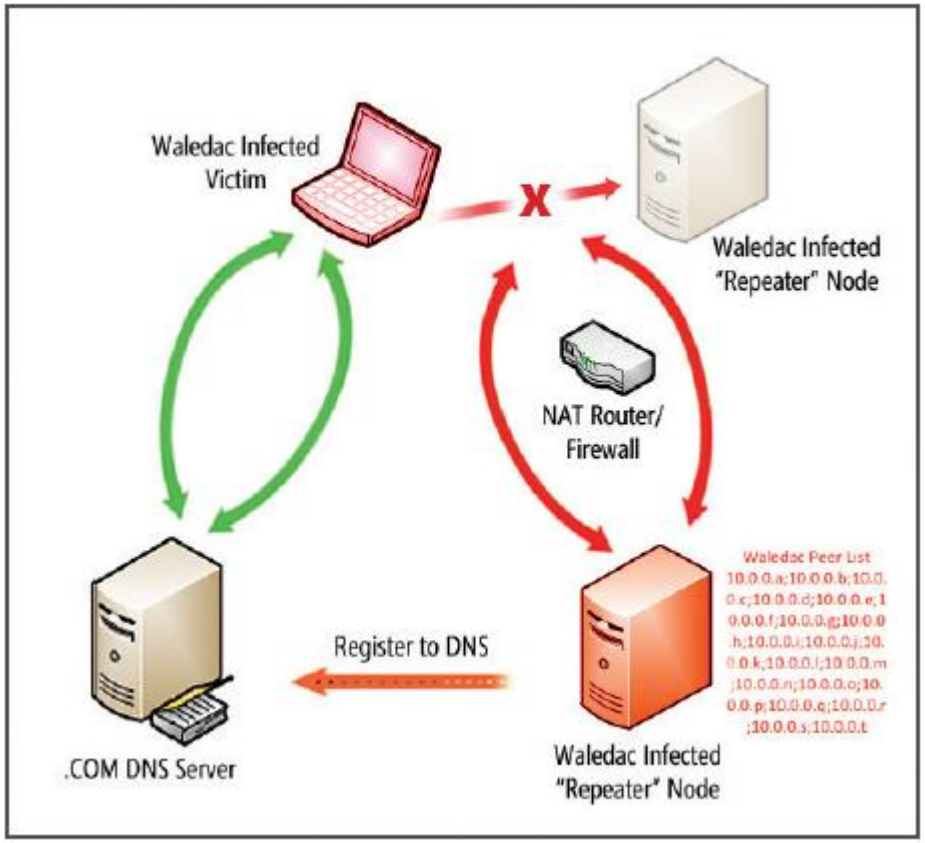
- PCがWaledacに感染すると、スパマー・ノードか、リピーターノードに分類される。
  - PCが、プライベートIPを使っている場合は、WaledacのHTTPを使った指揮命令が利用できないと判断し、スパマー・ノードに割り当てられる。
  - グローバルIPを利用し、TCP/80を使ってアクセスができる場合は、リピーター・ノードとして割り当てられ、Fast Flux DNSに組み込まれる。

- 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

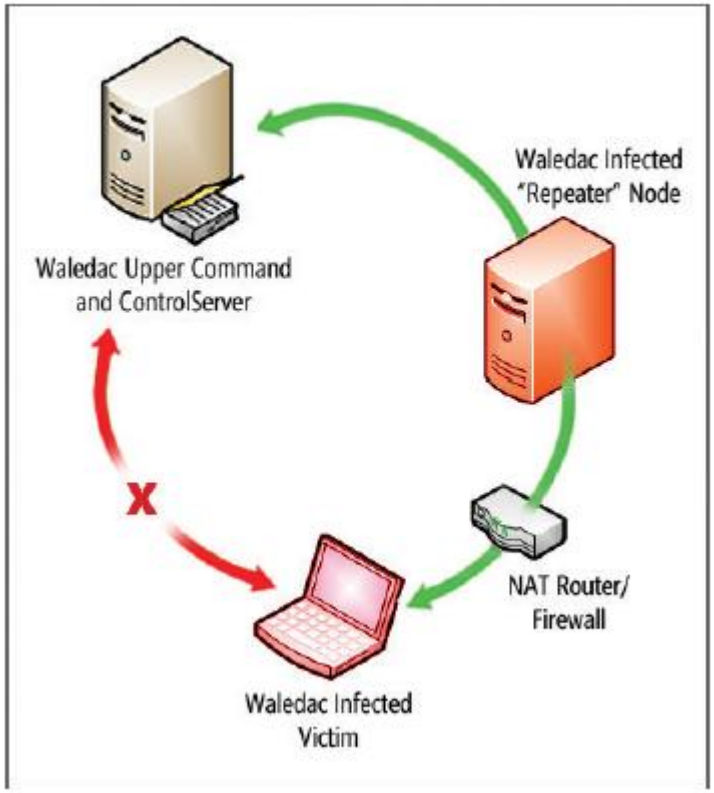
FIGURE 20. Win32/Waledac peering list exchange using fast flux DNS



- 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

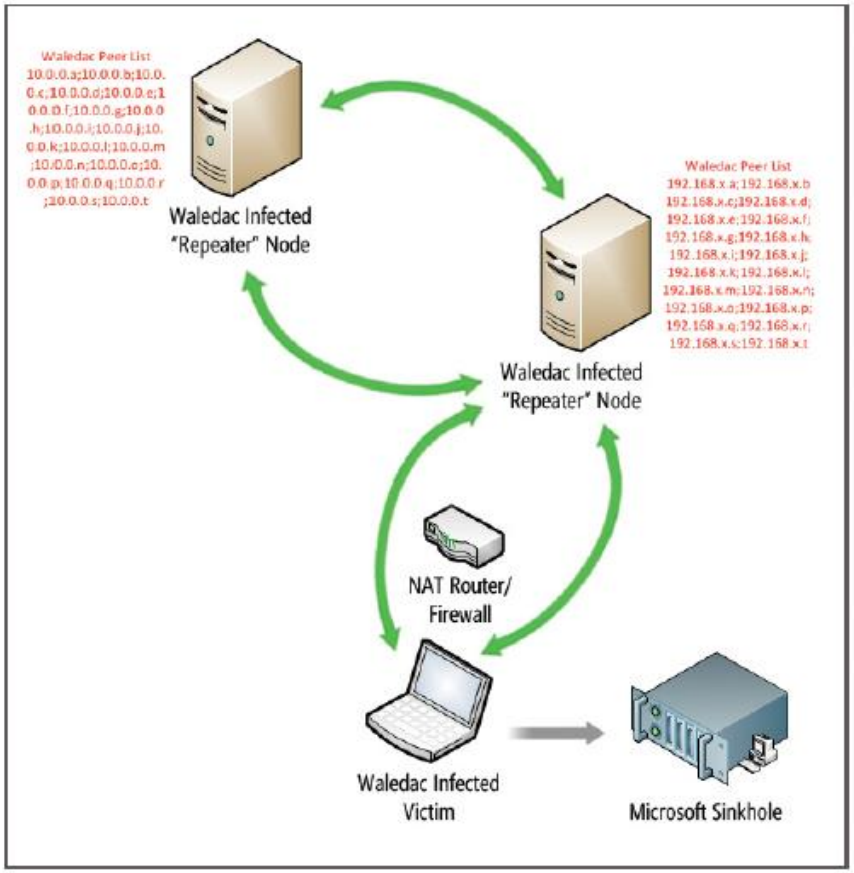
FIGURE 21. Win32/Waledac proxy function through the repeater tier



- 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。

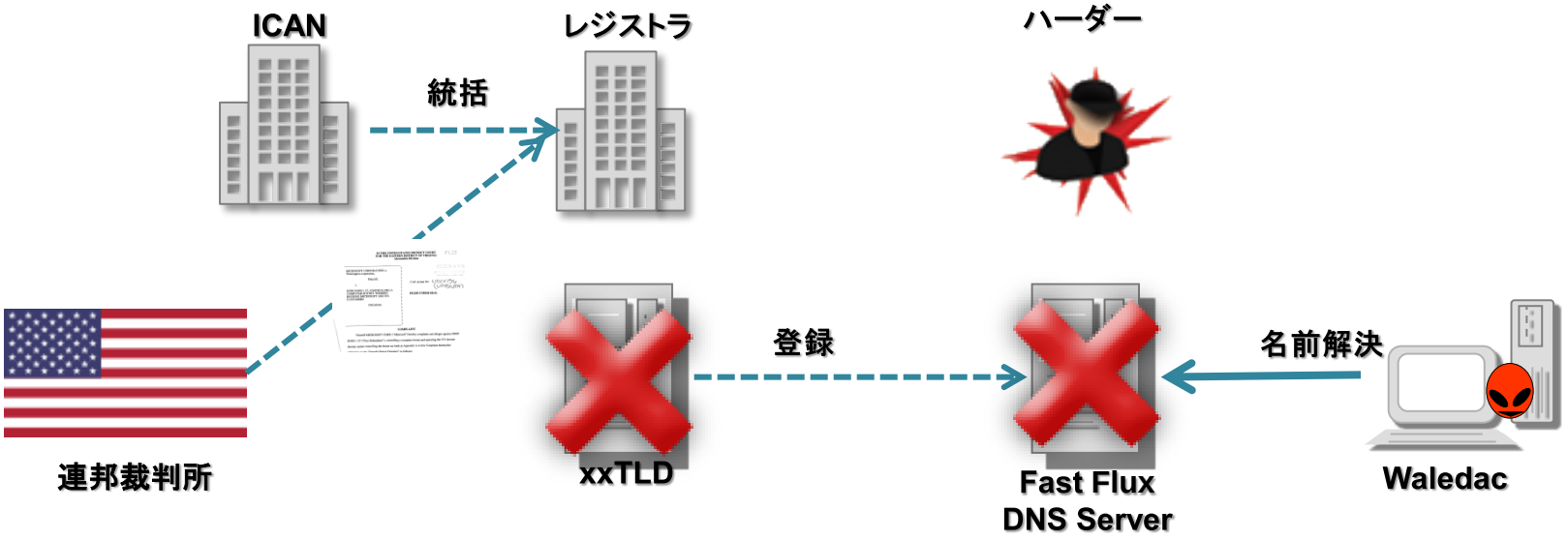
DNSの対策：ホスト名の削除

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



一方的な暫定措置 (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）

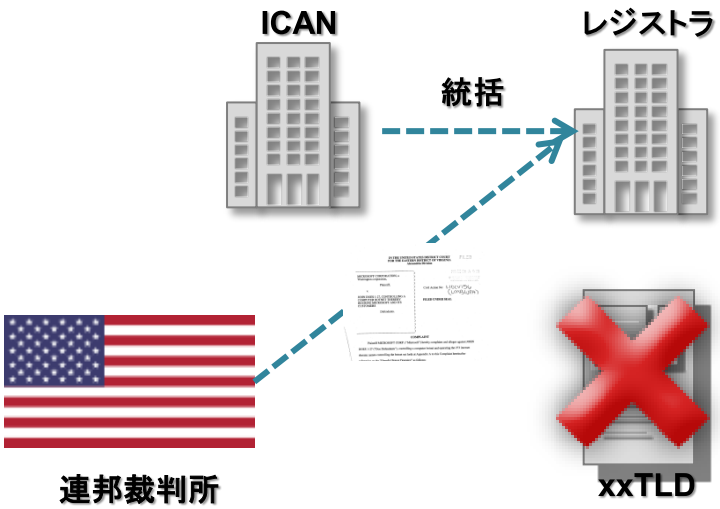
強制力がないため、必ずしも実施されない

DNS サーバーの Take Down

ハーダーが保持をしているか、レジストラが管理をしているケースが多い

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



一方的な暫定措置
(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倍場合に、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

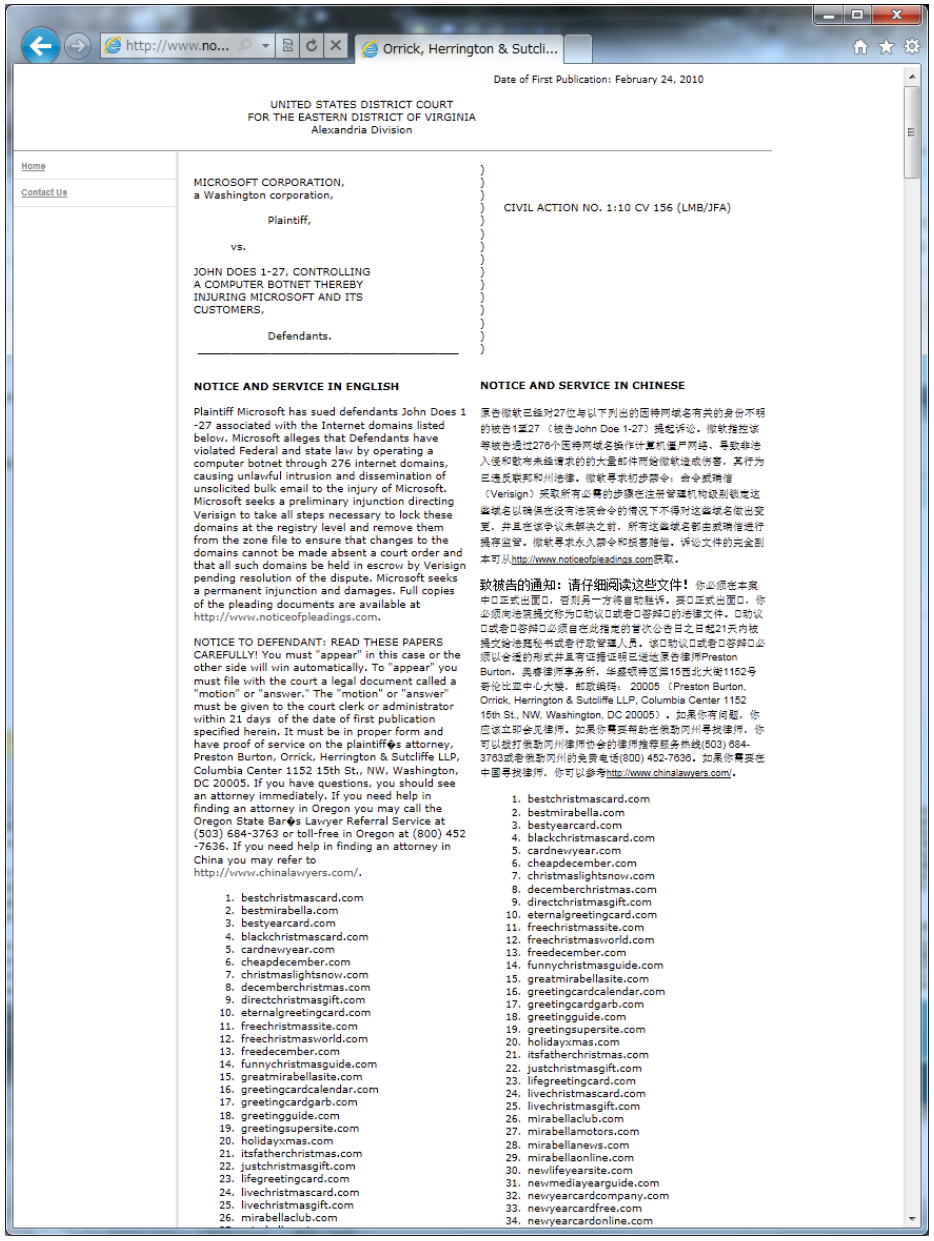
Defendants.

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.no... Orrick, Herrington & Sutcli...

Date of First Publication: February 24, 2010

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

Home
Contact Us

MICROSOFT CORPORATION, a Washington corporation,

Plaintiff,

vs.

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

Defendants.

CIVIL ACTION NO. 1:10 CV 156 (LMB/JFA)

NOTICE AND SERVICE IN ENGLISH

Plaintiff Microsoft has sued defendants John Does 1 -27 associated with the Internet domains listed below. Microsoft alleges that Defendants have violated Federal and state law by operating a computer botnet through 276 internet domains, causing unlawful intrusion and dissemination of unsolicited bulk email to the injury of Microsoft. Microsoft seeks a preliminary injunction directing Verisign to take all steps necessary to lock these domains at the registry level and remove them from the zone file to ensure that changes to the domains cannot be made absent a court order and that all such domains be held in escrow by Verisign pending resolution of the dispute. Microsoft seeks a permanent injunction and damages. Full copies of the pleading documents are available at http://www.noticeofpleadings.com.

NOTICE TO DEFENDANT: READ THESE PAPERS CAREFULLY! You must "appear" in this case or the other side will win automatically. To "appear" you must file with the court a legal document called a "motion" or "answer." The "motion" or "answer" must be given to the court clerk or administrator within 21 days of the date of first publication specified herein. It must be in proper form and have proof of service on the plaintiff's attorney, Preston Burton, Orrick, Herrington & Sutcliffe LLP, Columbia Center 1152 15th St., NW, Washington, DC 20005. If you have questions, you should see an attorney immediately. If you need help in finding an attorney in Oregon you may call the Oregon State Bar's Lawyer Referral Service at (503) 684-3763 or toll-free in Oregon at (800) 452 -7636. If you need help in finding an attorney in China you may refer to http://www.chinalawyers.com/.

1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com

NOTICE AND SERVICE IN CHINESE

原告微软已经对27位与以下列出的因特网域名有关的身份不明的被告1至27（被告John Doe 1-27）提起诉讼。微软指控该等被告通过276个因特网域名操作计算机僵尸网络、导致非法入侵和散布未经请求的的大量邮件同始微软造成伤害。其行为已违反联邦和州法律。微软寻求初步禁令，命令威瑞信（Verisign）采取所有必需的步骤在注册管理机构级别锁定这些域名以确保在没有法院命令的情况下不得对这些域名做出变更，并且在该争议未解决之前，所有这些域名都由威瑞信进行维存监管。微软寻求永久禁令和损害赔偿。诉讼文件的完全副本可从http://www.noticeofpleadings.com获取。

致被告的通知：请仔细阅读这些文件！你必须在本案中□正式出庭□，否则另一方将自动胜诉。要□正式出庭□，你必须向法院提交称为□动议□或者□答辩□的法律文件。□动议□或者□答辩□必须自在此指定的首次公告日之日起21天内被提交给法院秘书或者行政管理人员。该□动议□或者□答辩□必须以合适的形式并且有证据证明已送达原告律师Preston Burton，奥睿律师事务所，华盛顿特区第15西北大街1152号哥伦比亚中心大楼，邮政编码： 20005 （Preston Burton, Orrick, Herrington & Sutcliffe LLP, Columbia Center 1152 15th St., NW, Washington, DC 20005）。如果你有问题，你应该立即会见律师。如果你需要帮助在俄勒冈州寻找律师，你可以拨打俄勒冈州律师协会的律师推荐服务热线(503) 684-3763或者俄勒冈州的免费电话(800) 452-7636。如果你需要在中国寻找律师，你可以参考http://www.chinalawyers.com/.

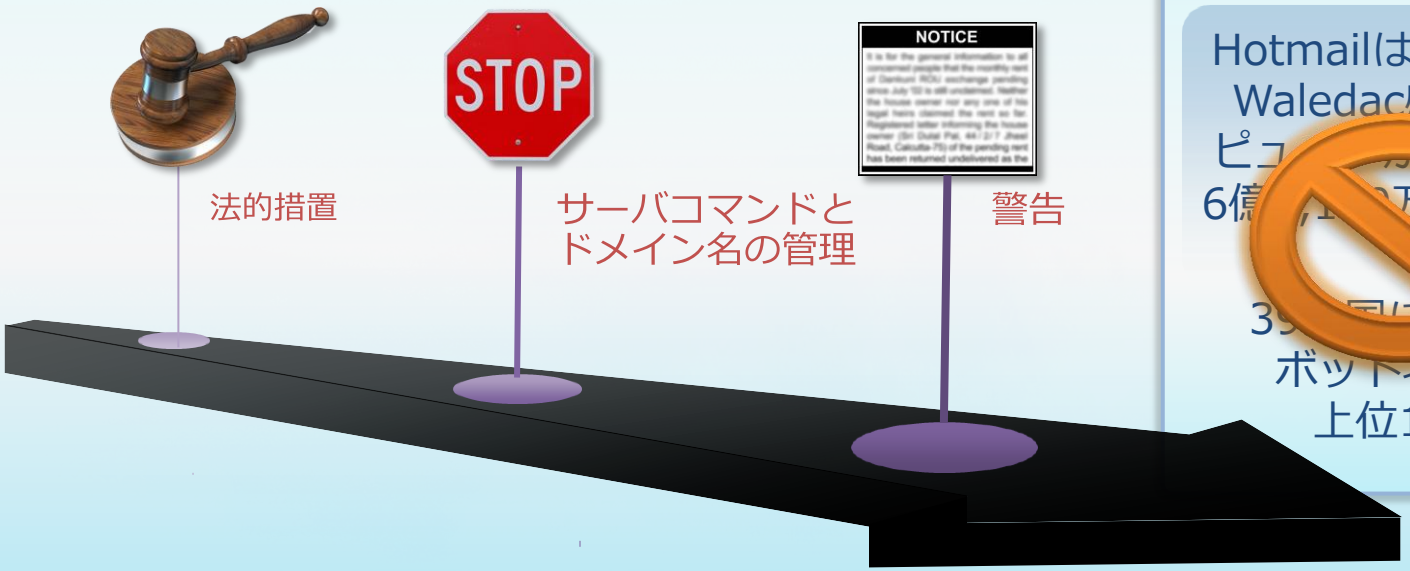
1. bestchristmascard.com
2. bestmirabella.com
3. bestyearcard.com
4. blackchristmascard.com
5. cardnewyear.com
6. cheapdecember.com
7. christmaslightsnow.com
8. decemberchristmas.com
9. directchristmasgift.com
10. eternalgreetingcard.com
11. freechristmassite.com
12. freechristmasworld.com
13. freedecember.com
14. funnychristmasguide.com
15. greatmirabellasite.com
16. greetingcardcalendar.com
17. greetingcardgarb.com
18. greetingguide.com
19. greetingsupersite.com
20. holidayxmas.com
21. itsfatherchristmas.com
22. justchristmasgift.com
23. lifegreetingcard.com
24. livechristmascard.com
25. livechristmasgift.com
26. mirabellaclub.com
27. mirabellamotors.com
28. mirabellanews.com
29. mirabellaonline.com
30. newlifeyearsite.com
31. newmediayearguide.com
32. newyearcardcompany.com
33. newyearcardfree.com
34. newyearcardonline.com

http://www.noticeofpleadings.com/

ボットネット

WALEDACボットネット「遮断」アプローチ

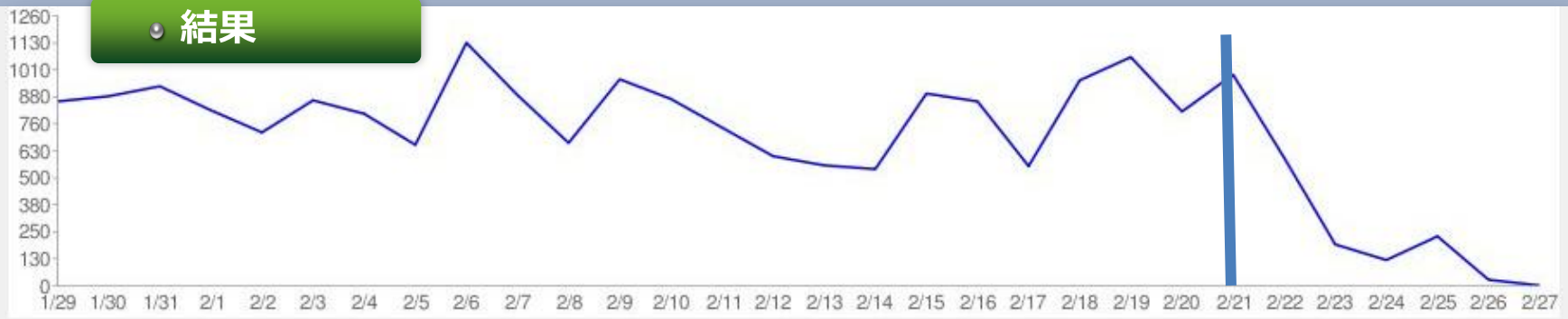
短期的 – 先例を作る



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

3[redacted]る
ボットネット
上位10位

結果



Microsoft

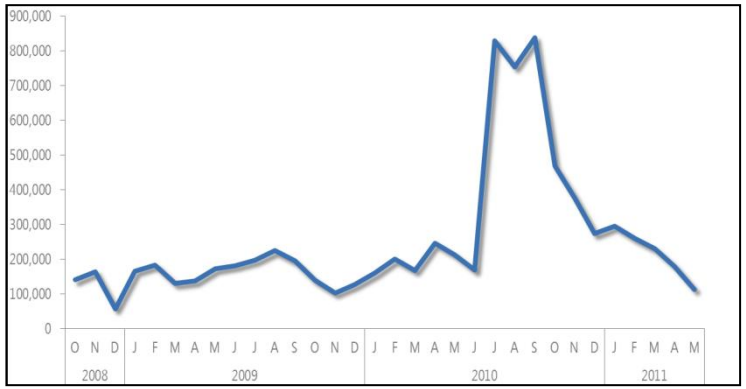
マイクロソフト　セキュリティ　インテリジェンスレポート
スペシャルエディション

Rustockの脅威と戦い

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

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

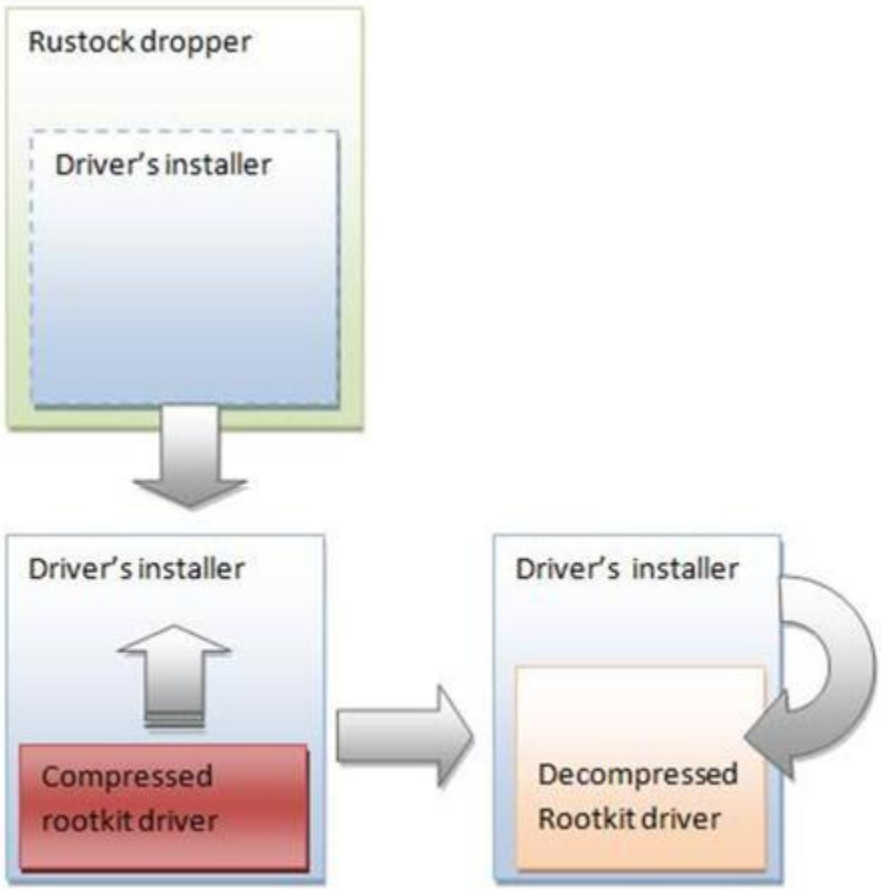


マイクロソフトのマルウェア対策ソリューションによる Win32/Rustock の検出数 (2008 年 10 月～ 2011 年 5 月)

- 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

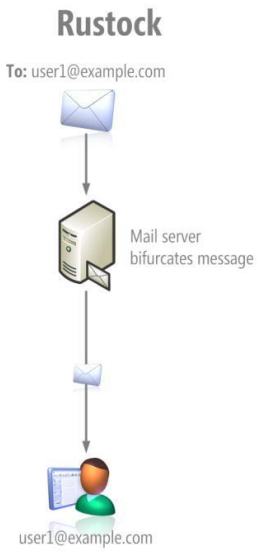
- ドロッパー
  - ユーザーモードで実行
  - C&Cから、ルートキットドライバーの複合化とドロップ
  - ポリモーフィック型、
  - 静的な文字列は使わない
  - RC4で暗号化しaPLibで圧縮
- ドライバーインストーラー
  - システムドライバーに成りすまし、カーネルモードで実行
  - Beep.sys, null.sys等の置き換え
  - ハードコード化されたファイル名とランダムなファイル名
- ルートキットドライバー
  - カーネルモードで実行
  - INT 2eh割り込みを賜与してユーザーモードボットクライアントと通信
  - SSDT*をフックし、自身を除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

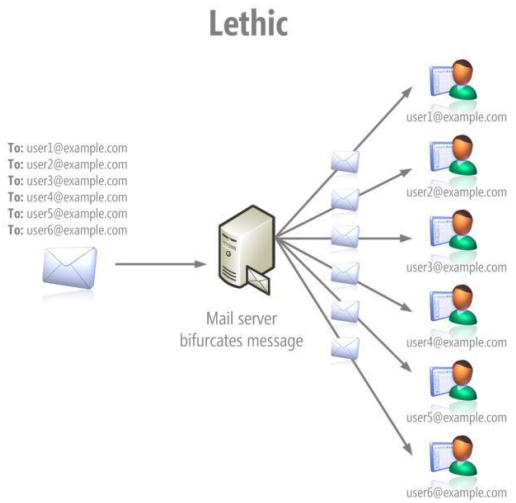


*SSDT: System Service Dispatch Table

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

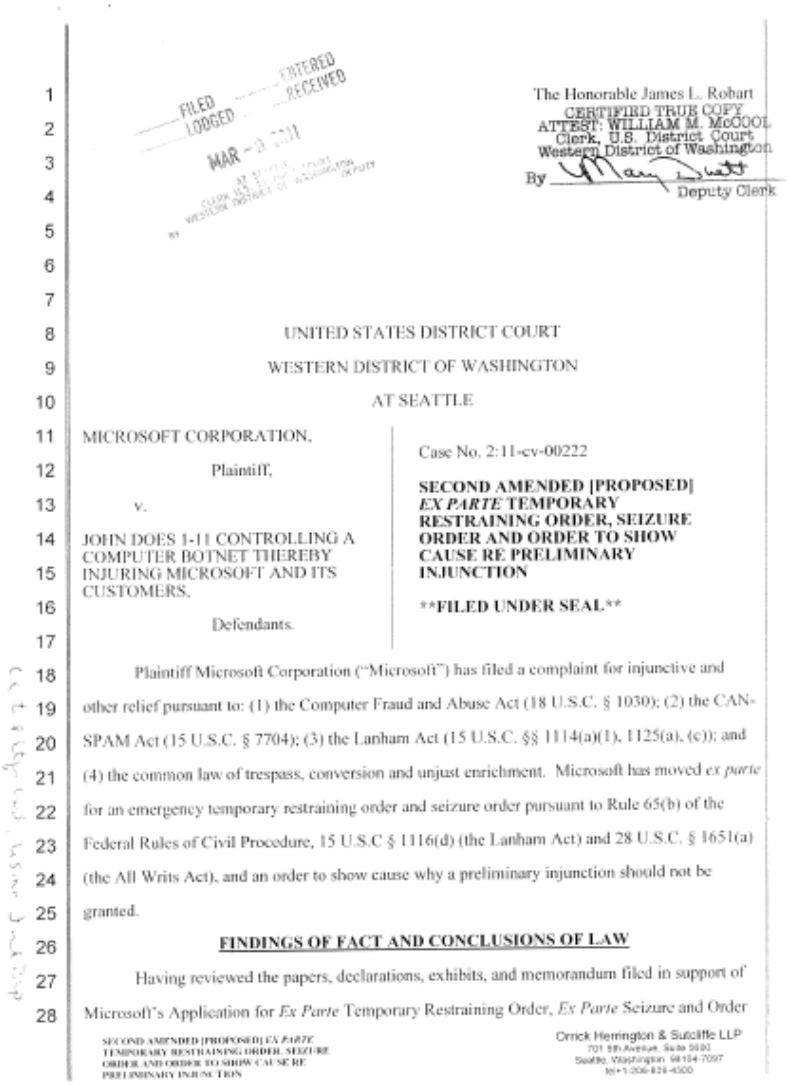
- マルウエアの追加インストール
  - 既知のRustock ドロッパー（Win32/Harnig）に感染させる
  - 対話的な操作を行わずに5分間で左表のマルウエアをダウンロード・インストール
  - これらのマルウエアは、さらに別のマルウエア等をダウンロード（多層構造のダウンローダー）

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
  - C&Cのアドレスをボットにハードコード

裁判における Rustock の対処



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

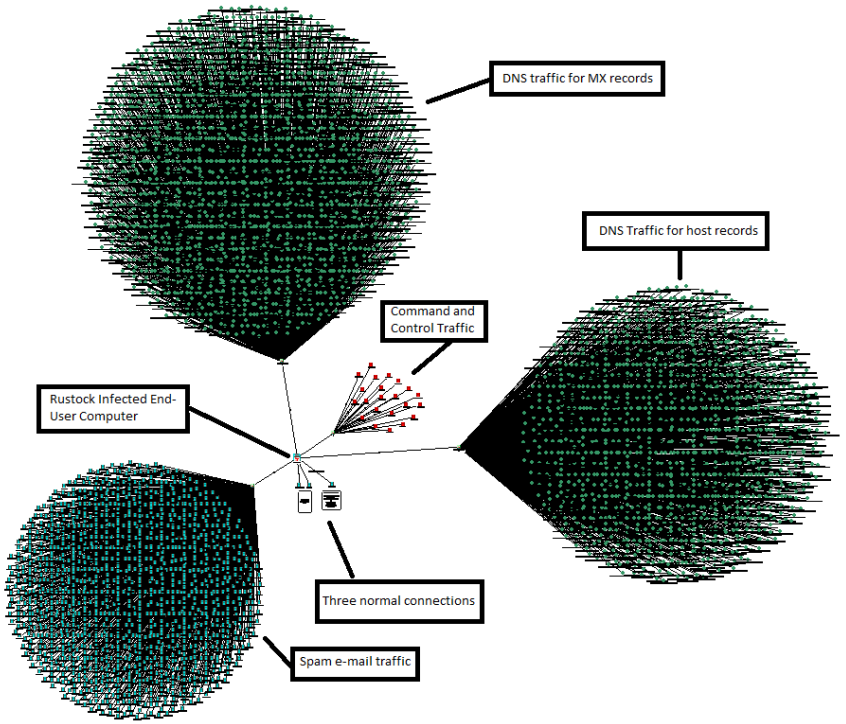
- ハードディスク20台の解析結果
  - スパムを送信するためのソフトウェアとデータ
    - 数千個の、メールアドレス、ID/パスワードの組み合わせを含んだテキストファイル
    - 42万個以上の電子メールアドレス
    - マイクロソフトや製薬会社の商標を不正に利用したテンプレート
  - ロシアのIPアドレスに対するサイバー攻撃に利用されていたことを示すデータ
  - 匿名インターネットアクセスを提供するノードとして使用
    - 電子メールテンプレート、商標、電子メールアドレスなどを保存する Rustockシステムへの匿名アクセスを提供するために使用したとみられる
- サー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

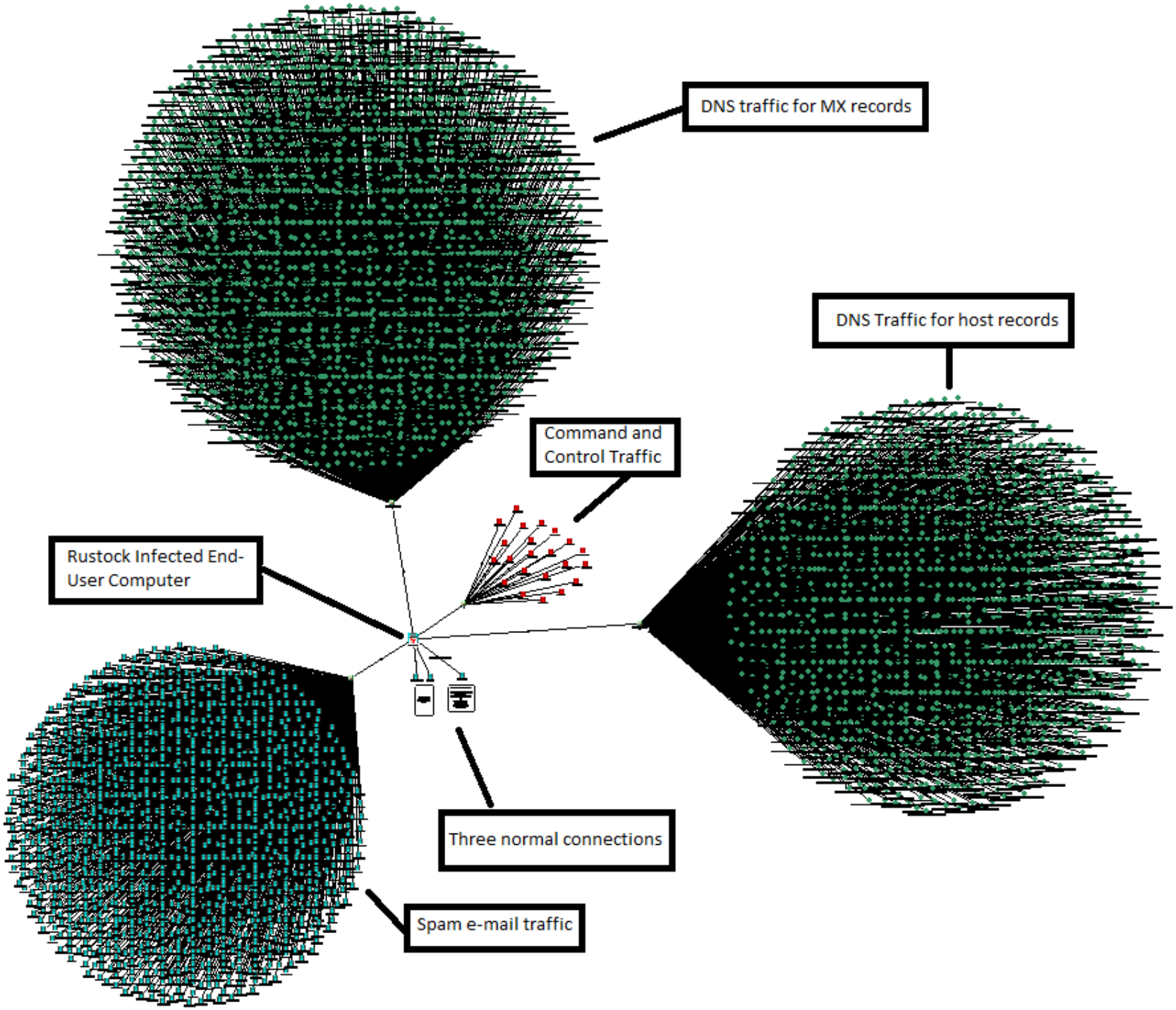
Rustock に関する統計

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

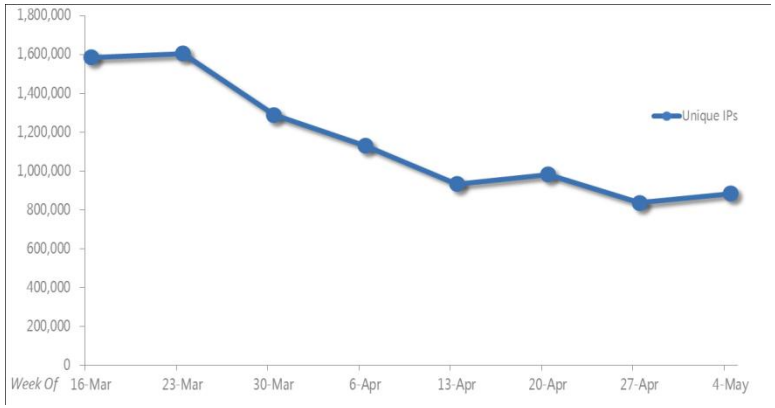
- Rustockのネットワーク活動

  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

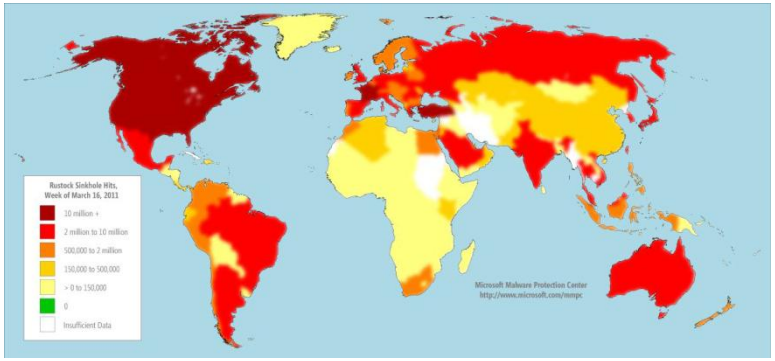


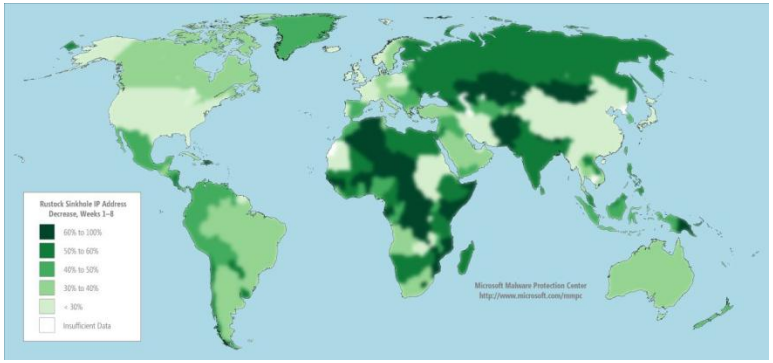

DNS traffic for MX records
DNS Traffic for host records
Command and Control Traffic
Rustock Infected End-User Computer
Three normal connections
Spam e-mail traffic

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

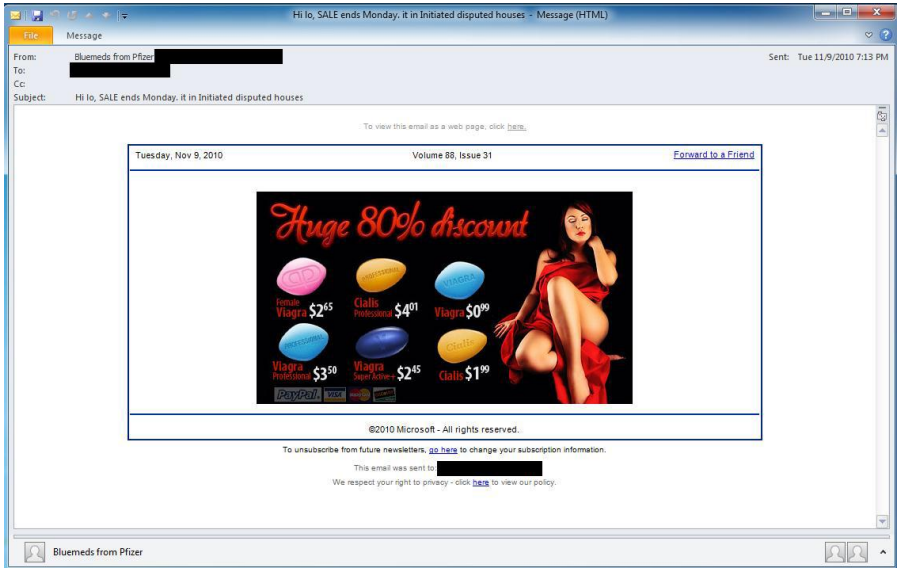
- 地理的な分析

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

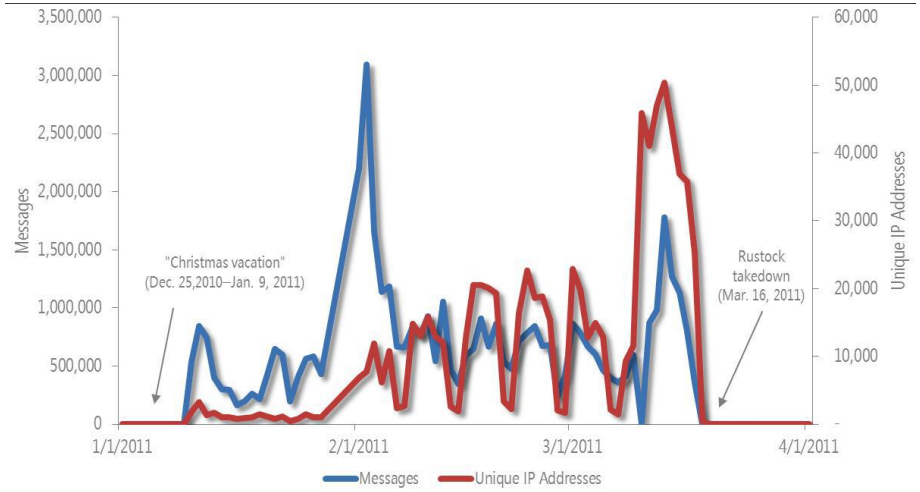
スパムに関する統計

- 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
    - 不適切な有効成分を含む
    - 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ことを阻止し、誰にとっても安全で信頼できるインターネットの実現が可能となります