

MWS2012 2A3-1

DCWG(DNS Changer Working Group)における連携について

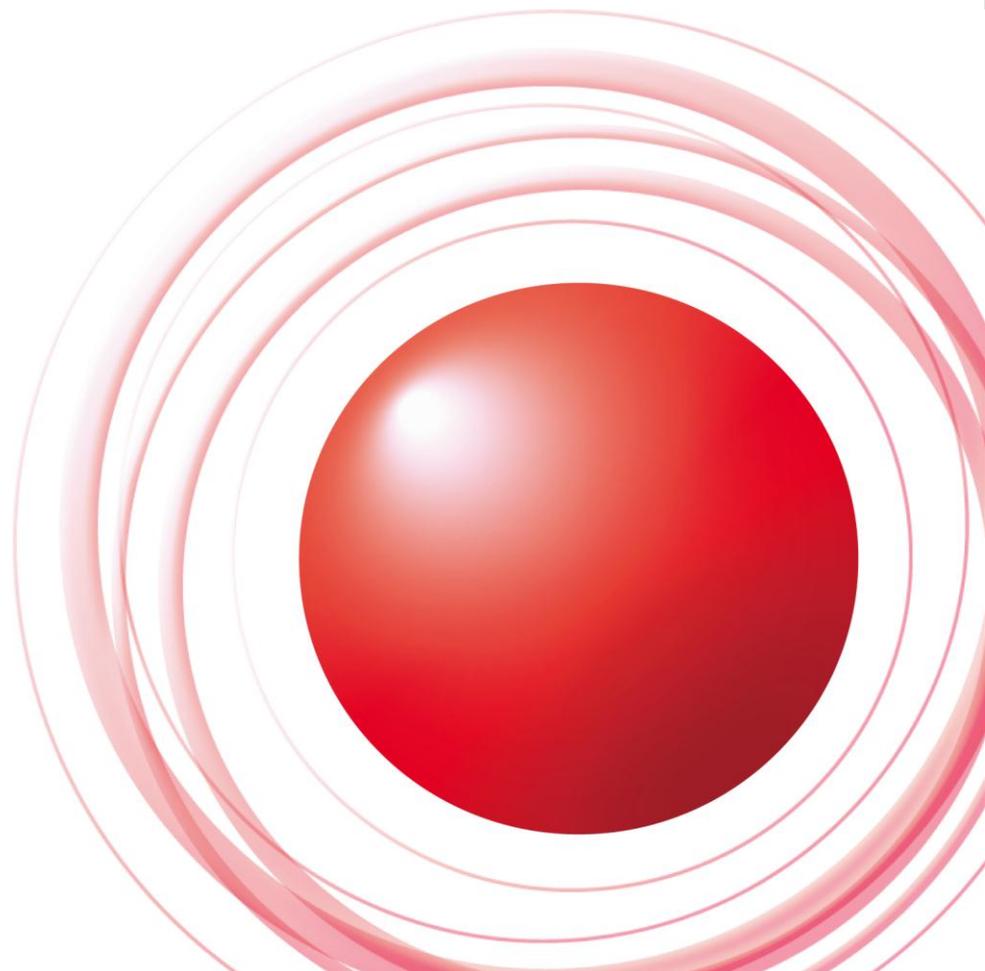


2012/10/31

株式会社インターネットイニシアティブ
サービスオペレーション本部セキュリティ情報統括室

齋藤 衛

Ongoing Innovation



自己紹介



齋藤 衛(さいとう まもる)

株式会社インターネットイニシアティブ サービス本部 セキュリティ情報統括室 室長
1967年生まれ。1993年中央大学大学院 理工学研究科 管理工学専攻修了。

1995年株式会社インターネットイニシアティブに入社。法人向けファイアウォールサービスに従事した後、法人向けセキュリティサービスの 開発(マネージドセキュリティサービス、IDSサービス、DDoS対策サービスなど)、セキュリティサービス担当プロダクトマネージャを経て、現職。

2001年よりIIJグループの緊急対応チーム IIJ-SECTの活動を行う(IIJ-SECTは2002年に**FIRST**に加盟)。**テレコムアイザックジャパン**、**日本シーサート協議会**、**日本セキュリティオペレーション事業者協議会**、**テレコム・セプター**など複数の団体の運営委員。総務省「スマートフォンとクラウドセキュリティ研究会」構成員、安心・安全インターネット協議会P2P研究会、永遠のビギナー対策研究会、安心ネットづくり促進協議会 児童ポルノ対策作業部会 技術者SWGなど複数の団体で活動を行う。共訳書として「ファイアウォール構築 第二版」(オライリー・ジャパン)。IIJ-SECTの活動は平成21年度「経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)」を受賞。

DCWGIにおける連携について

DNS Changer の現状

- マルウェアは同定され、ウイルス対策ソフトウェアなどで駆除可能となっている。
- 行為者(犯人)グループは逮捕され、犯行に用いられたサーバインフラは停止させられている。
- 感染者救済のためのDNSサーバが用意され、約8カ月間にわたって駆除のための猶予が与えられた。その結果、大きな実害を生むことなくインシデント自体が終了している。

“DNS Changer”は二度と被害を生まない。

Agenda

DNS Changerとそのテイクダウン

DNS Changerの感染者対策

DCWGについて

DNS Changerとそのテイクダウン

Operation Ghost Click: アンチウイルスベンダ、FBI、DCWG

Trend Micro Incorporated
Research Paper
2012

OPERATION GHOST CLICK The Rove Digital Takedown

By: Forward-Looking Threat Research Team

トレンドマイクロ社「Rove Digitalの壊滅」
https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81



DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse web sites, send e-mail, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

<http://www.fbi.gov>
<http://www.fbi.gov/contact-us>

122.456.789
987.654.321 — Legitimate DNS

Manhattan U.S. Attorney Charges Seven Individuals for Engineering Sophisticated Internet Fraud Scheme That Infected Millions of Computers Worldwide and Manipulated Internet Advertising Business

Malware Secretly Re-Routed More Than 4 Million Computers, Generating at Least \$4 Million in Fraudulent Advertising Fees for the Defendants

Operation Ghost Click
International Cyber Ring That Infected Millions of Computers

11/09/11

Six Estonian nationals have been arrested and charged with running a sophisticated fraud ring that infected millions of computers worldwide with a virus and manipulated the multi-billion-dollar Internet advertising industry. Users of infected computers were redirected to fraudulent websites, and their computers were made vulnerable to other kinds of malicious software.

http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911

DCWG

Home News Detect Fix Protect Networks ISPs Victim Rights

Find out if you have been violated and infected with DNS Changer. No software will be downloaded to perform the check.

If you think you are infected, please follow take action to fix your computer now.

Protect your computer from DNS Changer.

Don't Panic!

If you are reading this page, it means you are NOT infected with DNS Changer. Your device might still be violated with other malware. We recommend safe computing practices to protect your self while on-line. Information here is a starting place to start <http://www.dcwg.org/protect/>.

What is the DNS Changer Malware?

On November 8, the FBI, the NASA-OIG and Estonian police arrested several cyber criminals in "Operation Ghost Click". The criminals operated under the company name "Rove Digital", and distributed DNS changing viruses, variously known as TDSS, Alureon, TidServ and TDL4 viruses. You can read more about the arrest of the Rove Digital principals here, and in the FBI Press

<http://www.dcwg.org/>

Georgia Tech,
Internet Systems Consortium,
Mandiant,
National Cyber-Forensics and
Training Alliance,
Neustar, Spamhaus, Team
Cymru, Trend Micro,
University of Alabama at
Birmingham, (匿名のISP)

<http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business>

DNS Changerとそのテイクダウン

DNS Changerに関するいくつかの事実

- 感染端末のDNSの参照先を犯行グループの用意した参照用DNSサーバに変更するマルウェア。
- 感染した端末はDNSのクエリに対し、偽のDNS応答受ける。
- Microsoft Windowsおよび Apple Mac OS。
- 世界規模で最大400万台の感染。
- 感染経路はWeb参照によるdrive by download もしくは偽の動画再生ソフトによる(FBIのプレスリリースより)。
- 犯人グループの逮捕。偽DNSサーバ環境の接收。
- その後、感染者の救済が実施された。
- 2012年7月9日(日本時間)をもって大きな混乱を起こすことなく、インシデント対応自体が終了。

DNS Changerとそのテイクダウン

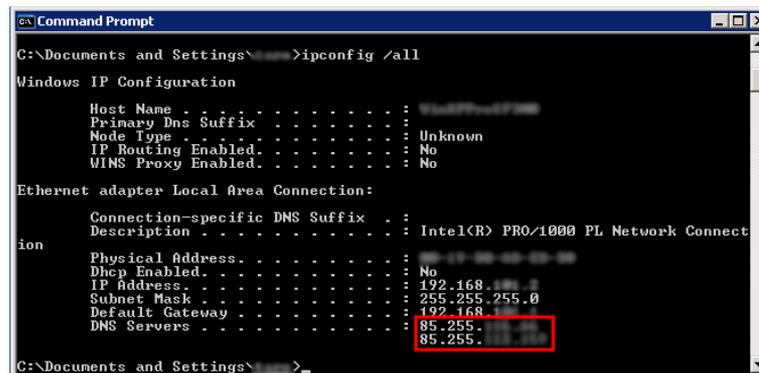
DNS Changer対策 timeline (犯人グループ逮捕まで)

日時	状況
2005	DNS Changer 検体複数のアンチウイルスベンダによる検出 (TDSS、FAKEAVとの関連含む)
2006	トレンドマイクロによる犯人グループ把握 (「Rove Digitalの壊滅」より)
2008	テイクダウンの努力
	9月 カリフォルニアのホスティング企業 Atrivo が上流IXにより操業停止
	10月 エストニアのドメイン事業 Estdomains ICANNよりレジストラ契約停止
2009	Nelicash アフィリエイトプログラム FAKEAVのインストール
2011年11月08日	検挙 FBI、オランダ警察、エストニア警察など 7名起訴、6名が逮捕(ロシア人1名は逃亡中)

DNS Changerとそのテイクダウン

マルウェアによる名前解決の変更

- OSのアップデートや、アンチウイルスソフトのパターンファイル更新を阻害する目的に実施されることが多い。
 - MyDoom(2004)ではhostsファイルにエントリを追加することにより更新を阻害。
 - 他のマルウェア変更の手法としては、ARP cache poisoning によるものや、DNS poisoningによるもの、マルウェア自身がDHCPサーバの機能を有するものも知られている。
- DNS Changer においては、OSの参照用 DNSサーバの設定を変更する手法が用いられていた。



```
Command Prompt
C:\Documents and Settings\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : 
Primary Dns Suffix . . . . . : 
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

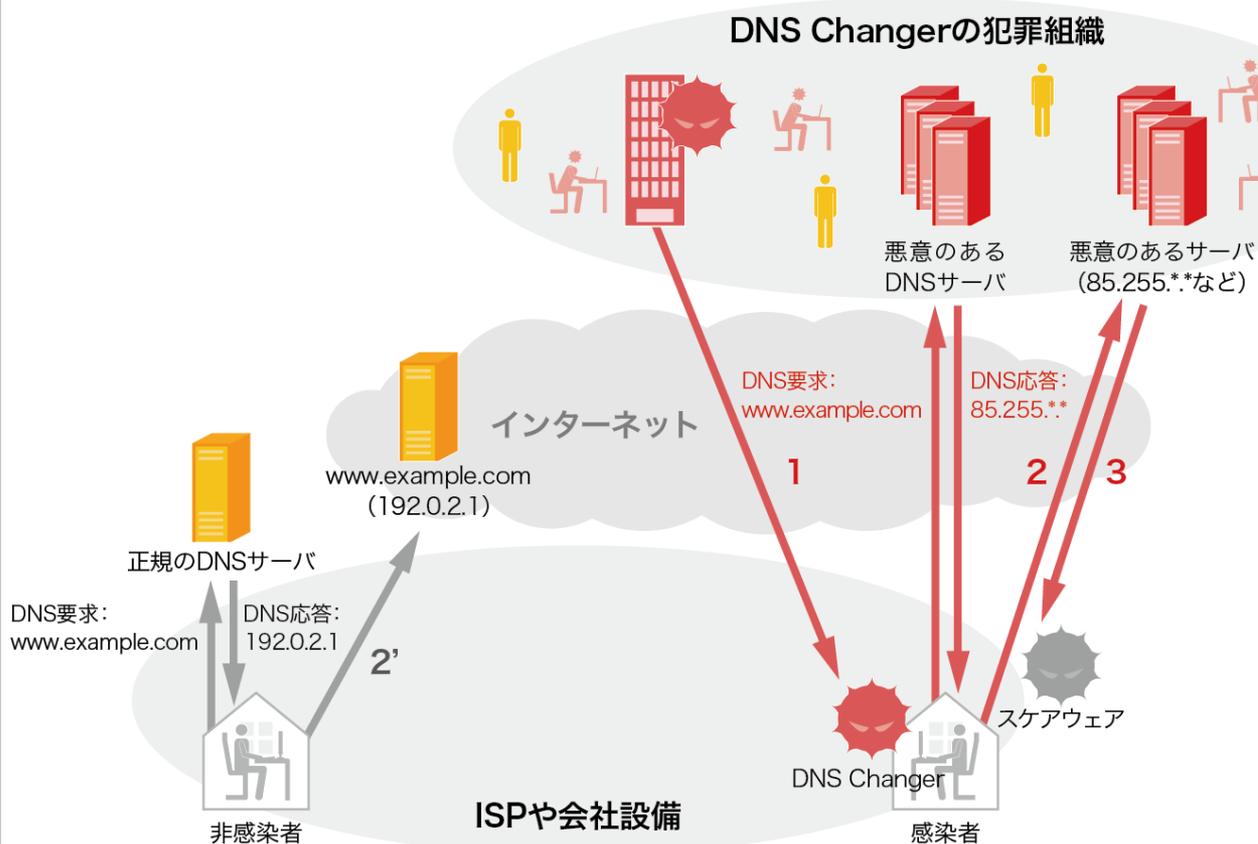
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Intel(R) PRO/1000 PL Network Connect
   ion
   Physical Address. . . . . : 
   Dhcp Enabled. . . . . : No
   IP Address. . . . . : 192.168.
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . : 192.168.
   DNS Servers . . . . . : 85.255.
                        85.255.
```

IJ Internet Infrastructure Review (IIR) Vol.15 より
<http://www.ij.ad.jp/company/development/report/iir/015.html>

DNS Changerとそのテイクダウン

マルウェアとしてのDNS Changerの挙動



1. ソーシャルエンジニアリング(動画再生ソフトウェアに偽装したファイルをダウンロードさせるなど)やドライブバイダウンロードで感染させ、DNS設定を悪意のあるサーバに書き換える。
2. 検索エンジンなど、特定のサイト(例では、www.example.com)にアクセスすると、悪意のあるDNSサーバに問い合わせに行くため、悪意のあるサーバに誘導されてしまう。
- 2'. 非感染者の場合、ISPなどのDNSサーバが設定されて正常なDNSの応答が返るため、利用者の要求通りのサーバに接続される。
3. 悪意のあるサーバからスケアウェアをダウンロードさせるなどして、利用者から金銭を詐取る。

DNS Changerとそのテイクダウン

DNS Changerの被害

- 偽DNSのエントリ1万4千
 - 検索エンジン Google, Yahoo!, Bing, Ask.com
 - 広告事業 Google Ads, Overture, Doubleclick
 - ソフトウェア更新サーバ マイクロソフト、アドビ、セキュリティ対策ソフト
 - アダルトサイト、出会い系サイト
 - ドメイン事業者 (使用されていないドメインのハイジャック)
 - wikileaks.orgなどのアクセス数の多いサイト
 - マルウェアTDSSなどのサーバ
- 利用者の被害
 - 検索結果からの不正サイトへの誘導
 - 検索結果のHTMLの改ざんなどではなく、DNSクエリにより検索結果をクリックしたことを検知し、DNSのレスポンスを改ざんした
 - FAKEAVのライセンス料
- 広告産業への被害
 - 有名サイトの広告の置き換え
- その他
 - 犯人グループが用意した広告へのアフィリエイト課金



図13: DNSチェンジャーに感染したコンピュータの被害者が閲覧した「amazon.com」のWebページ

トレンドマイクロ「Rove Digitalの壊滅」より
https://inet.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=81

DNS Changerとそのテイクダウン

DNS Changerのその他の挙動

- MBRに感染し、駆除後も再起動により再び設定変更をする。
- ホームルータのDNSの設定変更を試みる(IJでは実際の被害は未確認)
 - UTSTARCOM,routers from BNSL(India),D-Link,Linksys,OpenWRT/DD-WRT,A-Link,Netgear,ASUS ZVMODELVZ Web Manager, SMC など(ISCのMerike KaeoによるNanog54 Security BoFの発表資料より)
- スケアウェア(FAKEAV)のインストール。



FAKEAV(AntiMalware)の様子
<http://www.threatexpert.com/report.aspx?md5=9f09ff8dba53c3f3734295528297d015>



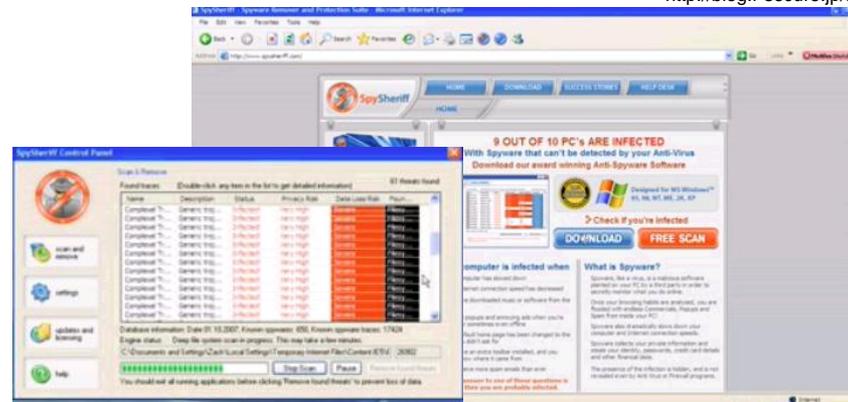
FAKEAV(Protection Center)の様子
<http://www.mcafee.com/japan/security/virD.asp?v=DNSChanger.bu>



FAKEAV(MacGuard)の様子
<http://blog.f-secure.jp/archives/50605046.html>



FAKEAV(WindowsAntiSpyware)の様子
<http://www.gfi.com/blog/movie-time-dns-changer-trojan/>



FAKEAV(SpySheriff)の様子 <http://www.youtube.com/watch?v=ve5KU01JYA8>

DNS Changerの感染者対策

犯人グループの逮捕

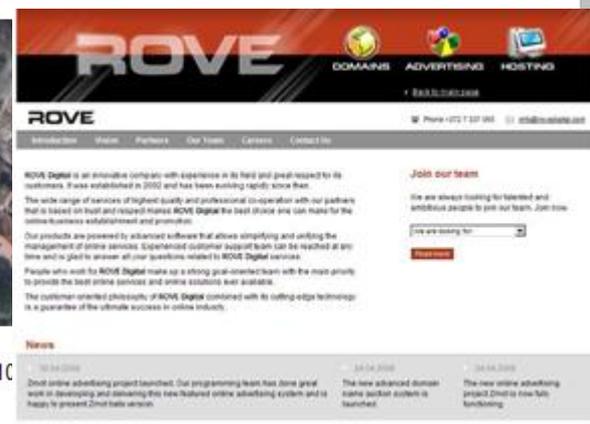
- エストニアに本拠地を持つRove Digital を親会社にした企業グループ

U.S. v. Tsastsin, et al.

COUNT	CHARGE	DEFENDANTS	MAXIMUM PENALTIES
1	Wire fraud conspiracy	VLADIMIR TSAASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	30 years in prison
2	Computer intrusion conspiracy	VLADIMIR TSAASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	10 years in prison
3	Wire fraud	VLADIMIR TSAASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	30 years in prison
4	Computer intrusion (furthering fraud)	VLADIMIR TSAASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	Five years in prison
5	Computer intrusion (transmitting information)	VLADIMIR TSAASTSIN ANDREY TAAME TIMUR GERASSIMENKO DMITRI JEGOROV VALERI ALEKSEJEV KONSTANTIN POLTEV ANTON IVANOV	10 years in prison
6	Money laundering	VLADIMIR TSAASTSIN	30 years in prison
7	Engaging in monetary transactions of value over \$10,000 involving fraud proceeds	VLADIMIR TSAASTSIN	Per count: 10 years in prison



Google Maps image of ROVE offices at Lai 6, Tartu, Tartumaa 510



Vladimir Tsastšin (aka "SCR"), head of ROVE Digital in Tartu



Members of Estonian police carrying DNSChanger servers and routers out of the Rove Digital office Tartu, Estonia on the 9th of November, 2011.



The forensic bus of the central criminal police of Estonia parked outside Rove Digital offices on the 9th of November, 2011.

<http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business>

F-Secure 社のMikko HippunenのPinterest より<http://pinterest.com/mikkohypponen/case-dns-changer/>

Agenda

DNS Changerとそのテイクダウン

DNS Changerの感染者対策

DNS Changerの遺した課題

DNS Changerの感染者対策

感染者対策のtimeline(日本時間)

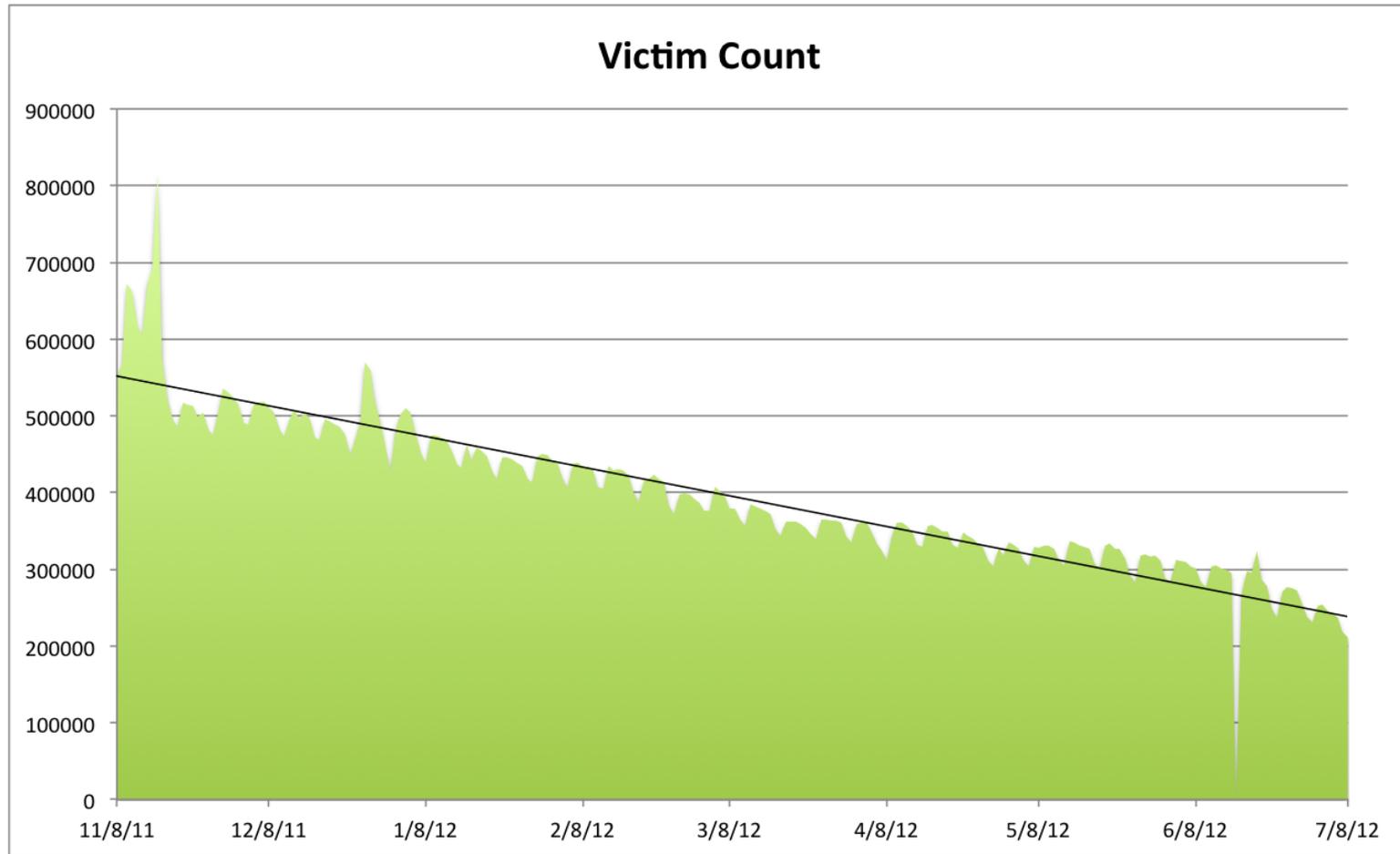
日時	状況
2011年11月04日	DCWG.orgのドメイン登録。
2011年11月08日	(Rove Digital 犯人グループ逮捕当日) (世界の感染台数は551,436) ISCによる感染者対策のDNS参照サーバ稼働開始。偽参照用DNSサーバが停止しても、感染者は正常にインターネット接続ができるようにした(2012年3月9日まで)。
2012年02月06日	NANOG 54 ISCの Merike Kaeo による ISP 向け発表。
2012年02月27日	IIJ-SECT blog「DNS Changerマルウェア感染に関する注意喚起」。
2012年2月末	JPCERT/CCやTelecomISAC JapanなどのWorkingGroupで対応を検討。 国内ISP個別の注意喚起活動。
2012年03月06日	JPCERT/CC「DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起」。 感染者の参照用DNSサーバの運用期間120日館延長の米国連邦裁判所命令。 (世界の感染台数は407,927)
2012年03月07日	IIJ-SECT blog「DNS Changerマルウェア感染に関する注意喚起(続報)」。
2012年05月22日	JPCERT/CC DNS Changer「DNS Changer マルウェア感染確認サイト公開のお知らせ」。
2012年05月23日	Google 検索の結果への注意喚起 “Notifying users affected by the DNSChanger malware”。
2012年05月30日	Telecom-ISAC Japan「DNS Changer マルウェア感染に関する注意喚起について」。
2012年06月04日	Facebook 感染者のログイン時に警告を開始 “Notifying DNSChanger Victims”。
2012年07月09日	感染者用DNSサーバの運用停止。(世界の感染台数は210,851)
2012年07月10日	IIJ-SECT blog「DNS Changer - FBIによるDNSサーバの運用停止後の状況とまとめ」。

※感染者数はすべてDCWGの資料より引用

<http://www.dcwg.org/wp-content/uploads/2012/07/dcwg-unique-ips-20120709.pdf>

DNS Changerの感染者対策

感染者数減少の様子



DNS Changer Working Group
<http://www.dcwg.org/last-day-of-dcwg-data/>

DNS Changerの感染者対策 一般向けの注意喚起



- ▶ HOME
- ▶ IIJ-SECTについて
- ▶ IIJセキュリティ情報統括室について
- ▶ MITFについて
- Security Diary
- ▶ リンク
- ▶ IIJ
- ▶ Internet Infrastructure Review (定期発行技術レポート)
- + お問い合わせ
- + 個人情報保護ポリシー
- + Twitter @IIJSECT
- + RSS

Security Diary

HOME > Security Diary > DNS Changerマルウェア感染に関する注意喚起

Diary

DNS Changerマルウェア感染に関する注意喚起

2011年11月、DNS Changer と呼ばれるマルウェアのC&Cサーバが差し替え、活動を封じ込められました。その後の懸念点などがNetwork Operators' Group) で話し合われています。その資料サーバと同様のIPアドレスで正規のDNSサーバが運用されているが3月8日に迫っています。DCWG (DNS Changer Working Group) 45万の感染未確認が観測されており、まだ感染したままのユーザーが多くなっています。事実上、インターネットの利用ができなく

DNS Changer[1]は、Webの検索結果を改ざんしたり、閲覧中置き換えて表示するなどの行為を行ないます。例えば、スパイと、その検索結果をスクリーンショット (偽ウイルス対策ソフト) などで、悪意のあるソフトウェアをインストールさせ、

DNS Changerの感染者であるかは、DCWGにも記載されている設定値をチェックすることである程度判断できます[3]。また、ページはFBIの資料やDCWGのWebページに記載されており、ある可能性が高いです。FBIではDNSサーバのIPアドレスを含まれるかを検査するWebページも公開しています。IIJの調べると、他のプロセスにコードインジェクションを行なった上でDNSサーバの設定を変更し、悪意のあるDNSサーバを強制する

IIJ-SECT blog
<https://sect.iiij.ad.jp/d/2012/02/245395.html>

JPCERT/CC
Japan Computer Emergency Response Team Coordination Center

安全・安心なIT社会のための、国内・国際連携を支援する

お問い合わせ | 採用情報 | サイトマップ | English

最新情報を取得 (RSS) | メールマガジン | HTTPS | モバイル

検索

Home > 情報提供 > 注意喚起 > 2012 > DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起

トップページ

情報提供

- ・ 注意喚起
- ・ 早期警戒
- ・ 脆弱性対策情報
- ・ Weekly Report
- ・ インターネット 定点観測
- ・ インシデントの報告
- ・ インシデント対応とは?
- ・ インシデントの報告
- ・ インシデント対応状況
- ・ 各種登録
- ・ 製品開発者登録
- ・ メーリングリスト
- ・ 制御システムセキュリティ
- ・ 制御システムセキュリティ
- ・ ラーニング
- ・ セキュアコーディング
- ・ 技術メモ
- ・ ライブラリ
- ・ 公開資料
- ・ 四半期レポート
- ・ 研究・調査レポート
- ・ CSIRTマテリアル

DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起

最終更新: 2012-03-07

コンピュータセキュリティ対策チーム

各位

JPCERT-AT-2012-03-06 (付)

2012-03-07 (3)

<<< JPCERT/CC Alert 2012-03-06 >>>

DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起

<https://www.jpCERT.or.jp/at/2012/at120008.html>

1. 概要

JPCERT/CC では、DNS 設定を書き換えるマルウェア (以下、DNS Changer に関する情報) を入手しました。DNS Changer は2007年頃にはじめて検出されたマルウェアですが、DNS Changer に感染した PC は、現在でも世界中で数万以上存在し、日本国内でも相当数の PC が感染しているとのことです。

また、2011年11月に米国連邦捜査局 (FBI) により、不正な DNS サーバに差し替えられ、正常な DNS サーバに置き換えられています。しかし、このサーバの運用は2012年3月9日 (日本時間) に停止する計画となっているため、DNS Changer に感染したままの PC は、2012年3月9日 (日本時間) 以降、

<https://www.jpCERT.or.jp/at/2012/at120008.html>

DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起

最終更新: 2012-03-07

コンピュータセキュリティ対策チーム

各位

JPCERT-AT-2012-03-06 (付)

2012-03-07 (3)

<<< JPCERT/CC Alert 2012-03-06 >>>

DNS 設定を書き換えるマルウェア (DNS Changer) 感染に関する注意喚起

<https://www.jpCERT.or.jp/at/2012/at120008.html>

1. 概要

JPCERT/CC では、DNS 設定を書き換えるマルウェア (以下、DNS Changer に関する情報) を入手しました。DNS Changer は2007年頃にはじめて検出されたマルウェアですが、DNS Changer に感染した PC は、現在でも世界中で数万以上存在し、日本国内でも相当数の PC が感染しているとのことです。

また、2011年11月に米国連邦捜査局 (FBI) により、不正な DNS サーバに差し替えられ、正常な DNS サーバに置き換えられています。しかし、このサーバの運用は2012年3月9日 (日本時間) に停止する計画となっているため、DNS Changer に感染したままの PC は、2012年3月9日 (日本時間) 以降、

DNS Changer マルウェア感染に関する注意喚起について

情報通信基盤の安心・安全を確保するために活動している一般財団法人日本データ流通協会 (JDC) と、アイザック推進会議 (存在地: 東京都港区、会長: 稲垣久夫 (NECビッグロップ株式会社)) 以下、Telecom-ISAC Japan 社、インターネットの安定運用に関わる各業の検出および対応に努むる者であります。

US-CERT の情報によると、DNS Changer と呼ばれるマルウェアに感染したユーザーは、2012年7月8日以降、DNS の名前解決ができなくなり、インターネットの利用ができなくなります。そのため、本注意喚起ではネットワークに対して、DNS Changer 感染有無の確認方法と、感染時の対策について説明します。

- DNS Changer ウイルスとは
- 本注意喚起の背景
- DNS Changer 感染の確認方法
- DNS Changer 感染時の対策
- 参考情報 ISP のサポートページ

■ DNS Changer ウイルスとは

DNS Changer は Ghost Click や TDS、TDL、Zlob、Alureon などの名称で知られており、感染した場合には、DNS サーバの設定が犯罪者の用意した DNS サーバに変更され、その結果、ユーザーは不正なサイトに誘導されるなどの被害があったり、知らぬ間に犯罪者の活動に加担するようになります。

■ 本注意喚起の背景

2011年11月、FBI (米連邦捜査局) は関係機関との協力の下、この犯罪グループを捜索、逮捕し、犯罪者の用意した不正な DNS サーバなどの関連を実行しました。さらに、このDNSサーバを安全なDNSサーバに置き換えることで、感染者がインターネット利用を継続できるようになりました。ただし、この実行措置は期限付きであり、現在では2012年7月8日までとなっています。そのため、本注意喚起では、各ユーザーのパソコンがDNS Changer に感染し、DNS設定が書き換えられているかどうかを確認し、その場合の対策方法を紹介します。

■ DNS Changer 感染の確認方法

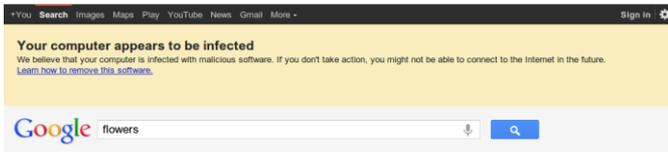
次のIPアドレスにDNSサーバが設定されている場合には、2012年7月8日以降、DNSの名前解決ができなくなり、インターネットを利用できなくなります。

64.26.176.0	---	64.26.191.255
67.210.0.0	---	67.210.15.255
77.67.82.0	---	77.67.82.255
85.255.113.0	---	85.255.127.255
93.188.160.0	---	93.188.167.255
213.109.64.0	---	213.109.79.255

<https://www.telecom-isac.jp/news/news20120530.html>

DNS Changerの感染者対策

感染者への警告



<http://googleonlinesecurity.blogspot.jp/2012/05/notifying-users-affected-by-dnschanger.html>

Your computer or network might be infected

Facebook has partnered with an alliance of public and private organizations to raise awareness about malware. Through that alliance we received information that your computer, home network, or office network may be at risk and infected with a type of malware called "DNSChanger".

For more information about DNSChanger malware, to see if your systems are infected, and to learn how to clean them, please visit the the DNSChanger Working Group website: <http://www.dcwg.org/> and click on the 'Detect' link.

This type of malware, if left on your systems, will prevent you from accessing the Internet after July 9, 2012. This includes your access to all websites, email, and chat.

[Click here for more information](#) **Continue**

<https://www.facebook.com/notes/facebook-security/notifying-dnschanger-victims/10150833689760766>

JPCERT/CC © 安全・安心なIT社会のための、国内・国際連携を支援する
JPCERT コーディネーションセンター

DNS Changer マルウェア感染確認サイト

✖ DNS Changer マルウェアに感染している可能性がります

(1) ウイルス対策ソフトウェアの更新ファイルを最新に更新して、スキャンを行ってください。
※ 一部のウイルス対策ソフトウェア手元には、以下のウイルス対策ソフトウェアの検知に必要な対応がなっていない。

Kaspersky Labe TDSSKiller
<http://support.kaspersky.co.jp/faq/faqid-208389215>

McAfee Labs Siteguard
<http://www.mcafee.com/japan/security/siteguard.asp>

Microsoft Windows Defender Offline
<http://windows.microsoft.com/ja-jp/windows/what-is-windows-defender-offline>

Microsoft Safety Scanner
<http://www.microsoft.com/security/scanner/ja-jp/default.aspx>

Norton Power Eraser
<http://security.symantec.com/what/pe.aspx>

Trend Micro Housecall
<http://us.trendmicro.com/ja/tools/housecall/>

(2) DNS Changer マルウェア感染確認サイトにて再度アクセスいただき、再び感染の可能性ありと検知された場合は、参照している999 DNS 変更を確認してください。
※ DNS Changer の感染し、かつ DNS 変更を実施するケースは確認しています。

(3) JPCERT/CC、及び IPA への報告をお願いします。

JPCERT/CC
インフォメーション
<http://www.jp-cert.or.jp/foim/>

IPA
ウイルス対策に関するお問い合わせ
<http://www.ipa.go.jp/secure/infocenter/infocenter.html>

※ 本サイトは、IPアドレス、DNS、および DNS サーバに関するお問い合わせ、お問い合わせの受付時間を確認してください。
Web アクセスに Proxy を使用している場合は、正しい確認が必要な場合があります。

Copyright © 2012 JPCERT/CC. All Rights Reserved.

<http://dns-ok.jp-cert.or.jp/>

DNS Changer Check-Up



DNS Resolution = RED

Your computer is using the DNS Changer nameservers and is therefore probably infected.

<http://www.dns-ok.us/>

感染者が参照用に利用するDNSサーバを掌握しているため、特定のサイトのDNS検索もとをチェックすることにより、感染者の判定を行うことができる。

DNS Changerの感染者対策

日本国内における対処(ISPとして)

- モチベーション
 - 「インターネットが使えない！」と、いわれたくない。サポートコストの増加が嫌。
- 情報の質と状況把握の問題
 - DCWGを信用してよいか。
 - エンタープライズ向けサービスを除き、機器設定を運用管理するサービスが少ない。
 - そもそも利用者の選択により外部のDNSサービスを参照することがある(たとえば google public DNSなど)。実際の通信に利用されるDNSサーバを知る方法がない。
 - どうやって駆除方法を提供するか。
- 個別対応人的コストの問題
- 結果として多くのISPにおいては次の対応を行った。
 - 利用者一般向けの注意喚起。
 - DCWGより感染者情報の提供を受けての個別対応。
- 日本国内の感染者数は7月9日時点で5,522。

Agenda

DNS Changerとそのテイクダウン

DNS Changerの感染者対策

DCWGについて

DCWGIについて

DNS Changer対策成功のポイント

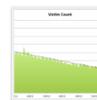
- 最終的な対策イメージを持った人がいた。
 - トレンドマイクロの Forward-looking Threat Research のリサーチャー Feike Hacquebord、Paul Ferguson。
 - およびFBI。
- WG側の登場人物が自分の役割以上の働きをした。
 - ウイルス対策ソフトベンダ、法執行機関、DCWGメンバー（大学、研究機関、セキュリティベンダ、団体など）。
- 多くの外部組織によるDCWGの活動への協力があつた。
 - CSIRT、オンラインサービス、ISP、業界団体、報道など。

DCWGIについて

DNS Changer対策成功のポイント(2)

- DCWGIの機能

- 感染状況の観測(感染者用DNSサーバ)。
- 対策者(たとえばISP)へのリーチ。
- 対策に必要な情報の、必要なタイミングでの提供。
- 第三者からの信頼に足るプレゼンス。
- 一般へのアウトリーチ。



Last Day of DCWGI Data
On July 9, 2012 By bgreene

July 8th 2012 is the last day we collect DNS data on the DNS Changer Victims. The total "unique IPs" and last day of infections per DNS Top Level Domain Country Code (TLD CC) are linked below. Now that this phase of the remediation exercise is over, researchers will collect all the data and compare [...]

[Read Full Article →](#)



Updated DNS Changer Infection Data
On July 6, 2012 By bgreene

Lots of people have been asking for updated data. Thanks to one of our volunteers, we have the latest dump: Daily Unique IPs connecting to the clean DNS servers up to June 27th 2012 – dcwg-unique-ips-up-to-June-27 Daily Unique IPs in July 2012 – dcwg-unique-ips-July-2012 Current List of Infections by [...]

[Read Full Article →](#)



DNS Changer – Top 25 ASNs
On June 13, 2012 By bgreene

Top 25 ASNs seen on Monday, June 11th who have DNS Changer infections communicating with the DCWGI Clean DNS servers. +-----+ |asn |unique_ips | +-----+ | 9839 | 15568 | 3269 | 13406 | | 7922 | 11964 | 3320 | 9250 | 7132 | 6743 | | 3215 | [...]

[Read Full Article →](#)



Top DNS Changer Infections by Country
On June 13, 2012 By bgreene

Here is our latest country based on Country codes for Monday, June 11th: +-----+ |cc |unique_ips | +-----+ | US | 69517 | IT | 26494 | IN | 21302 | GB | 19589 | DE | 18427 | FR | 10454 | CN | 10304 | [...]

[Read Full Article →](#)



Updated DNS Changer Data – Daily Count of Unique IP Addresses
On June 13, 2012 By bgreene

The following is our latest figures on the number of unique IP addresses communicating with the DNS Changer "Clean Servers." +-----+ |date |unique_ips | +-----+ | 2011-11-08 | 551436 | 2011-11-09 | 567937 | 2011-11-10 | 672972 | 2011-11-11 | 661664 | 2011-11-12 | 617054 | 2011-11-13 | [...]

[Read Full Article →](#)



Geo Movie of DNS Changer Infections – Jan 2012 to Mar 2012
On June 12, 2012 By bgreene

Yet another Shadowserver.org illustration to explore the geographic view of DNS Changer infections from Jan 2012 to Mar 2012.

[Read Full Article →](#)

Word Map of DNS Changer infections by

Hilbert Map of DNS Changer Infections

DCWGIについて

Interview with Dr. Feike Hacquebord (トレンドマイクロ松川さん thanx.)

- トレンドマイクロが法執行機関に捜査するように働きかけたことがすべてのきっかけ。
- DCWGIは非公式に始めたもので、当初お互いに顔見知りの小規模なグループ(15名以下)だった。犯人逮捕後、他のウイルス対策ソフトベンダ、ISP、Google, Facebookなどが参加。
- WGでは当初は犯人に注目した活動を行い、逮捕後は対策に向けた活動に注力した。ISCはサーバテイクダウン後に感染ユーザがオンラインでいられるようにDNSサーバを運用。後にGoogle, Facebook, ISPなどが注意喚起活動を行った。
- このようなWGは秘密保持のために可能な限り小規模で行われるべきだろう。検察が立件を決意しなければそもそも犯人逮捕は望めないなので、法執行機関へのサポートは非常に重要なことである。

DCWGIについて

コミュニティによる対策: 日本での事例

- Antinny対策(2004-2006)
- Botnet対策(2004-2006)
~CCC(2006-2011)
~MWS(2008-)

我々にもできるんです。

- 「遠隔操作ウイルス」?

DCWGIについて

お願い:MWS2012参加者の皆様へ

- マルウェア対策の本当の終了とはなにかをイメージしましょう。
- そのために、自分がもう少し手を広げると何ができるかを考えよう。
- 他人がもう少し何かをすると役に立つかと考えよう。
- MWSは対策コミュニティ形成に非常に大きなチャンスです。ぜひ活用しましょう。

まとめ

DNS Changerの遺した課題

- DNS Changerとそのテイクダウン
- DNS Changerの感染者対策
- DCWGについて
 - 最終的な対策のイメージ
 - 日本における事例
 - お願い

ご清聴ありがとうございました

お問い合わせ先 IIJインフォメーションセンター
TEL: 03-5205-4466 (9:30~17:30 土/日/祝日除く)
info@ij.ad.jp
<http://www.ij.ad.jp/>

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japan は、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。©2012 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。