dnsops.jp Summer Day 2016
2016.6.24

「マルウェア不正通信ブロックサービス」の提供開始に伴う

マルウェア不正通信のブロック状況について

NTTコムエンジニアリング株式会社
サービスNW部 サービスNW部門
佐藤 正春

・OCN DNSサーバの運用、保守
・OCN DDoS対策装置の運用、保守
・NTTCom Cloud用DDoS対策装置(一部)の運用、保守

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

背 景

マルウェアによるセキュリティ上の被害は増加の一途をたどっています。

例えば、マルウェアを悪用したサイバー犯罪の一つであるインターネットバンキングの不正送金について、国内の被害額は2015年上半期約15億円4,400万円と過去最悪の金額に達しています(警察庁調べ)。不正な通信の被害を避けるためには、利用者が個々にセキュリティ対策を行う必要がありますが、感染していても気づかないような挙動をするものも多く、対策を浸透させるのは容易ではありません。

これをうけNTT Comは、国内最大のインターネット接続サービス「OCN」をはじめとした対象サービスをご契約いただいているお客さまに、より安全・安心にインターネットをご利用いただくため、お客さまがお申し込みや設定をすることなく、また無料でご利用いただけるマルウェア対策サービスを提供します。

このような取り組みは、国内ISPとして初めてです。

参考：マルウェアの被害例

	カテゴリ	マルウェア/概要	被害規模等	内容等
1	不正送金	世界規模で感染拡大した口座情報窃取により不正送金を行う「Game Over Zeus」	被害額(警視庁発表) 14億円(2013年度) 29億円(2014年度) 31億円(2015年度)	・金融機関を装い偽画面を表示させ各種情報を窃取、当該利用者の口座から第三者へ不正送金を行う ・FBI,ユーロポール等が世界的駆除作戦を展開、警察機関を通じてOCNへも協力要請あり ・世界で100万台の端末が感染、うち20%が日本国内感染 ・OCNにおいても約4,000ユーザの感染を確認
2		主に日本を標的として感染拡大した口座情報窃取により不正送金を行う「VAWTRAK」		・主に日本を標的として口座番号やパスワードなどの各種情報を窃取、不正送金を行う ・警視庁が国内各ISPに駆除作戦協力要請を実施 ・警察機関により世界中で約8.2万台、日本国内で約4.4万台の感染端末を特定 ・OCNにおいても約8,000ユーザの感染を確認
3		「Banking Trojan」		・Windowsのプロセスに不正プログラムを挟み込み、ネットバンキング利用時に各種情報を窃取。感染後、被害者は偽装サイトにしかアクセスできなくなる。
4		「Man In The Browser」		・正規のネットバンキングのページ全面に、偽のポップアップを表示させて各種情報を窃取するマルウェア
5	個人情報漏洩	「i.JTB」における顧客情報の流出	約827万件 (2016年6月)	・氏名、性別、生年月日、メールアドレス、住所、郵便番号、電話番号、パスポート番号、パスポート取得日などが流出 ・JTB、dトラベル、yahooトラベル、DeNAトラベル、auトラベル
6		「日本年金機構」における加入者情報の流出	約125万件 (2015年6月)	・加入者の基礎年金番号、氏名、生年月日、住所などの情報が流出
7		「東京大学」における職員/学生の個人情報の流出	約3.6万件 (2015年6月)	・職員/学生のID、パスワード、氏名、学生証番号などが流出
8		「早稲田大学」における職員/学生の個人情報の流出	約3,300件 (2014年12月)	・職員/学生の氏名、性別、メールアドレス、内線番号、学籍番号などの情報が流出

ガイドラインの改定

2015年11月30日
電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインの改定について

総務省において9月9日に「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第二次とりまとめ」が公表されたことから協議会を開催し、研究会の「第二次とりまとめ」を踏まえた追加修正を行い第4版を作成

3.
DNS の機能を悪用したDDoS 攻撃に用いられている名前解決要求に係る通信への対処として、DNSサーバを通過する全ての名前解決要求に係るFQDNを常時確認し、リストに基づいて、FQDNが一致する場合に当該名前解決要求に係る通信を遮断することについて追加しました。
（第5条 1　攻撃通信への対応　(1) サイバー攻撃等に係る通信の遮断 イ　事業者設備に支障が生じる場合(ｵ)）

DNSAmp攻撃、ランダムサブドメイン攻撃への対処

5.
C&C サーバ等との通信の遮断における有効な同意として、個別の同意を取得していない場合であっても、契約約款等に基づく事前の包括同意として、マルウェア感染端末とC&Cサーバ等との通信をレピュテーションDBに基づいて遮断することについて追加しました。（同　(2) レピュテーションＤＢの活用　(ｱ)）

マルウェア対策

News Release

2016.2.1

国内ISPとして初めて、マルウェアによる情報漏洩から利用者を守る
「マルウェア不正通信ブロックサービス」の無料提供を開始
～お客さまによるお申し込みも設定も不要、不正通信を判別して自動ブロック～

1. NTTコミュニケーションズ(略称:NTT Com)は、インターネット接続サービス「OCN」の利用者など*1を対象に、2016年2月1日より「マルウェア不正通信ブロックサービス」を無料で提供開始します。
2. 「マルウェア」とは、パソコンなどの機器に損害を与えることを目的に、悪意をもって作られたソフトウェアやコード類の総称です*2。マルウェアに感染したパソコンなどの機器は、悪意のある第三者が設置した外部のC&Cサーバー*3と通信を行い、インターネットバンキングにおける不正送金や、マイナンバーやパスワードなどの個人情報漏洩といった被害をもたらす可能性があります。
3. 本サービスは、マルウェアが外部のC&Cサーバーと通信を行おうとすると、通信の内容(宛先情報)からそれを検知*4し、アクセスを遮断*5することでお客さまの被害を防ぐものです。
4. このように、通信の宛先情報に基づいて不正な通信をブロックするサービスを提供することは、国内の事業者として初めての試みです。
5. なお、お客さまによるお申し込みや設定は一切不要で、対象サービスをご利用のすべてのお客さまに対して無料で提供します。

新聞報道等

読売新聞（2月1日）

サイバー攻撃 自動で遮断

NTTコム 今月から無償サービス

NTTコミュニケーションズは1日から、国内シェア（占有率）トップのインターネット接続サービス「OCN」などで、パソコンにサイバー攻撃を仕掛ける相手との通信を自動で遮断する取り組みを始める。

利用者全体が対象で、国内のネット接続事業者では初めての対応という。国内では通信の秘密を侵害する恐れがあるとして遮断は行われてこなかったが、昨年9月に総務省の研究会が一定の条件下で遮断できるとの報告書をまとめていた。

サービスは無償で、ウイルスに感染したパソコンが遠隔操作され、不正送金や情報流出といった被害が生じることを防ぐ。あらかじめ登録された悪質なサーバーとの通信を検出すると、該当する通信だけを自動で遮断し、利用者に感染や通信の遮断をメールで通知。登録された悪質なサーバー上のサイトを見ようとした場合も遮断される。

ウイルス対策ソフトで感染を防ぐことができなかった場合でも、通信を遮断すれば個人情報流出といった被害を最小限に食い止めることができる。宛先の文字列で判別するため、不正な通信が遮断されても、メールやインターネットなどの通信はそのまま使える。

金融機関の多くは、自社のインターネットバンキングでそれぞれサイバー攻撃対策を取っている。これに対し今回のサービスはネット接続事業者が、幅広い利用者を対象に、パソコンが不正に操作されることなどから守ってくれるものだ。ただ、すべてのサイバー犯罪を防げるものではない。偽のホームページで他人のパスワードやクレジットカード情報を得る「フィッシング」などには注意が必要になる。

警察庁の調査では、インターネットバンキングの2014年の不正送金の被害額は29億円を超え、前年から倍増するなど、対策が急務になっている。

NTTコミュニケーションズの通信遮断サービスのイメージ

フジサンケイビジネスアイ（2月2日）

NTTコム、不正送金防止サービス

NTTコミュニケーションズは1日、マルウエア（悪意のあるソフトウエア）に感染したパソコンなどの機器がネットバンキングで不正送金しようとしたり、パスワードなどの個人情報を盗聴（ろうえい）しようと作動していることを自動で検知し、遮断するサービスを始めた。同社のインターネット接続サービス「OCN」利用者ら向けに無料で提供する。

日経産業新聞（2月3日）

不正サーバーと通信を自動遮断

NTTコム

NTTコミュニケーションズは、マルウエア（悪意のあるソフトウエア）に感染したパソコンからの情報漏洩を防ぐサービスを同日始めたと発表した。攻撃者が設置した外部サーバーとの通信を自動検知して遮断する。

「マルウェア不正通信ブロックサービス」はNTTコムの個人向けネット接続サービス「OCN」や企業向けデータ通信サービスを使う顧客向け。自動検知に使う情報は業界ガイドラインに基づき通信の宛先情報に限る。申し込みや設定作業は不要で利用料は無料。

News Release

総務省
MIC Ministry of Internal Affairs and Communications

ご意見・ご提案 English Google™カスタム検索 検索

アクセシビリティ簡易支援ツール

総務省トップ > 広報・報道 > 報道資料一覧 > マルウェアに対する被害未然防止の実施

報道資料

平成28年2月26日

マルウェアに対する被害未然防止の実施

近年、コンピュータマルウェア※1感染を原因とするインターネットバンキングの不正送金等の被害が続けており、我が国におけるマルウェア感染に対する対策が求められています。
このような状況を踏まえ、本年2月より、総務省は、「官民連携による国民のマルウェア対策支援プロジェクト（Advanced Cyber Threats response InitiatiVE（略称「ACTIVE」））」を通じたマルウェア感染者の被害未然防止の取組を開始しました。

※1 マルウェア：悪意のあるソフトウェアの総称であり、コンピュータに感染することによって、不正送金や 情報窃取などの遠隔操作を自動的に実行するプログラムのこと。

1 背景

昨今、個人情報の窃取を目的とするマルウェアや、特定のサービスに対するDDoS攻撃※2を行うマルウェアが大きな脅威となっています。インターネットバンキングによる不正送金等の被害に代表されるように、マルウェアに感染した端末は、C&Cサーバ※3の指令を受けて個人情報を窃取される可能性があるとともに、他者へのサイバー攻撃の踏み台としても利用される可能性があります。
しかしながら、マルウェアの高度化に伴い、アンチウイルスソフトによるマルウェアの駆除が難しくなってきているため、マルウェアによる被害を軽減するための新たな方策が求められています。

※2 DDoS攻撃：分散型サービス妨害攻撃（Distributed Denial of Service）。多数のコンピュータから一斉に大量のデータを特定宛先に送りつけることにより、当該宛先のネットワークやサーバを動作不能にする攻撃。
※3 C&Cサーバ：Command and Control サーバの略であり、外部から侵入して乗っ取ったコンピュータを多数利用したサイバー攻撃において、コンピュータ群に対して攻撃者からの指令を送り、制御を行うサーバコンピュータのこと。

2 実施内容

このような状況を踏まえ、本年2月より、総務省は、実証プロジェクト「ACTIVE」において、安心・安全なネットワーク環境の実現に向けて、一般財団法人日本データ通信協会 テレコム・アイザック推進会議と連携し、今年度から新たに被害未然防止の取組を開始しました。
本取組は、同推進会議から国内のインターネット・サービス・プロバイダ（ISP）事業者へ「ACTIVE」において得られたC&Cサーバに関する情報提供を行い、各ISP事業者において、当該情報に基づき、マルウェアとC＆Cサーバ間の通信を抑止するとともに、マルウェアに感染した端末の利用者への注意喚起を行うことで被害を軽減するものです。
なお、本取組については、総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」に準じております。

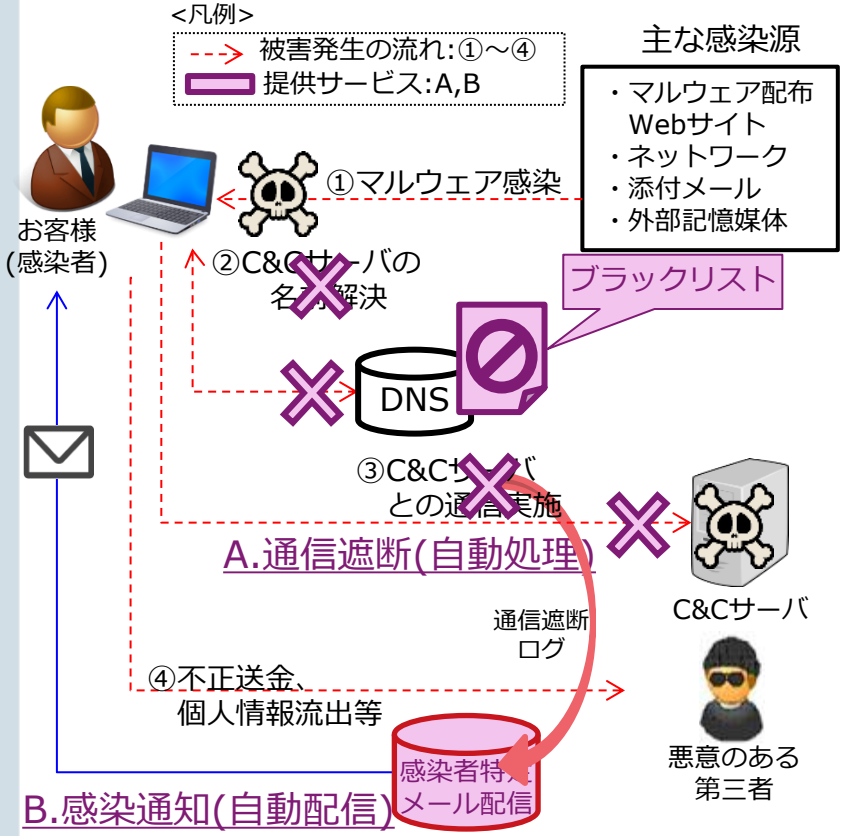
（参考）「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第二次とりまとめ」及び意見募集の結果の公表
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html

連絡先
総務省情報流通行政局情報セキュリティ対策室
道方課長補佐、棚田係長
電話：03-5253-5749 FAX：03-5253-5752

サービス概要

[マルウェア感染と被害拡大防止の仕組み]

お客様の端末がマルウェアに感染、C&Cサーバからの遠隔指令により悪意のある第三者にて不正送金/個人情報流出等の被害が発生



・C&Cサーバとの通信を遮断する事で不正送金/情報流出等を防止
・お客様の端末がマルウェアに感染している旨を通知/駆除案内

サービス仕様	A.マルウェア感染端末とC&Cサーバ(※1)の通信遮断(※2) B.該当者に対して感染通知の実施(※3)
対象サービス	・C-OCN(2種:光,ADSL,モバイル等) ・B-OCN(4種,6種,7種:光,ADSL,モバイル等) ・UNOインターネット接続,G-VPNインターネット接続
対象外サービス	・3,5,8種,IPバックボーンサービスはDNSをお客様が用意するため対象外 (但し、3,5,8種はオプションのDNSサービス利用時は対象) ・IP-VPN,eVLANはインターネット接続提供なしのため対象外
提供形態	・対象サービスにデフォルト提供 [約款改定に伴う包括同意での実施](※4) ・デフォルト提供を希望しないお客様へはサービス非適用となる仕組みを用意[オプトアウト](※4)
料金	無料(申込み不要)

[今後のサービス仕様の拡張について]

・将来的には①マルウェア感染を防止するサービスの提供を検討

(※1)Command and Control server:マルウェア感染端末等を遠隔操作する際に用いられるサーバ
(※2)ブラックリストに該当するドメインに対するDNSの名前解決を行わない。通信遮断精度向上のためMSSや外部機関のリスト情報等の活用を今後検討
(※3)通知時にマルウェア感染駆除/防止に効果があるセキュリティ商材やCLA(統合ログ分析サービス)等をMSSと連携して勧奨。通知については、VAWTRAK感染注意喚起において配信実績あり
(※4)「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会(2015年7月)」にて整理済み

（参考）通知文面

※非常に重要なお知らせのため、OCNからのメールを希望されていない方
にもお送りすることをご了承ください。

【重要】マルウェア感染に関するご注意

日頃より、OCNサービスをご利用いただき誠にありがとうございます。

お客さまがご契約のOCN回線（お客さま番号 N999999994 ）
でご利用のパソコンやスマートフォン等がマルウェア(※1)に感染した
可能性があり、お客さまの被害を防ぐため不正な通信を遮断しました。

不正通信遮断月 ：2016年3月

本対応により、マルウェア感染による不正な通信は
一時的に遮断しております。活動が一時的に中断していますが、
マルウェアに感染している可能性がございますので以下のサイトを
ご確認のうえ、対策を実施していただくことをお勧めします。

【ウイルス対策ソフト等をご利用でない場合】
ウイルス対策ソフトをインストールすることをお勧めします。
以下のホームページもしくは弊社窓口までお問い合わせください。

【ウイルス対策ソフト等をご利用の場合】
ウイルス対策ソフトを最新化することをお勧めします。
具体的な方法については、各ウイルスソフトメーカにお問い合わせください。
また、マルウェア感染駆除のご相談については以下のホームページ
もしくは弊社窓口までお問い合せください。

ホームページはこちらをご覧ください
⇒ http://s.ocn.jp/mal

(※1)マルウェアとは、パソコンやスマートフォン等に感染し、
第三者への不正送金を行ったり、個人情報等を盗み取るなどの
悪意のあるソフトウェアの総称です。

今後ともOCNをご愛顧いただきますよう、よろしくお願い申し上げます。

電話によるお問い合わせ
OCNテクニカルサポート　0120-047-558
受付時間 10:00から18:00(土日祝日含む、年末年始を除く)

メールによるお問い合わせ
OCNテクニカルサポート
https://support.ntt.com/ocn/inquiry/input/pid220000038y

発行:エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町1-1-6

以降は会場にて