2016 年 2 月 1 日

遠隔操作ウイルスの制御に DNS プロトコルを使用する事案への注意喚起

株式会社ラック

当社は、複数の企業の緊急対応調査で、ある特定の遠隔操作ウイルス（RAT:リモートアクセスツール）が、攻撃者からの指令を伝達する指令サーバ（C2 サーバや C&C サーバとも呼ばれます）との通信に、DNS（Domain Name System）プロトコル（通信手順）を悪用していることを確認しました。
本注意喚起をお読みになった方は、自組織の DNS サーバの動作状況もしくはネットワーク上で送受信されている DNS パケットの確認を行っていただくことをお勧めします。

経緯と概要

当社が運営する緊急対応サービス「サイバー119」は、昨年の後半より複数の大手企業様より遠隔操作ウイルスに関連する対応要請を受け、調査を行ってまいりました。
これらの事案で発見された遠隔操作ウイルスを調査したところ、攻撃者がインターネット側から企業内ネットワークで動作する遠隔操作ウイルスを操る際に、DNS プロトコルを使用する DNS トンネリングとも言われる手口を利用していることが確認されました。
これまでの代表的な遠隔操作ウイルスにおいては、Web 閲覧で用いられる HTTP（S）プロトコルを使用し、Web サーバを模した指令サーバを使用しています。しかしながら今回は DNS サーバを模した指令サーバを構築していることが確認されました。

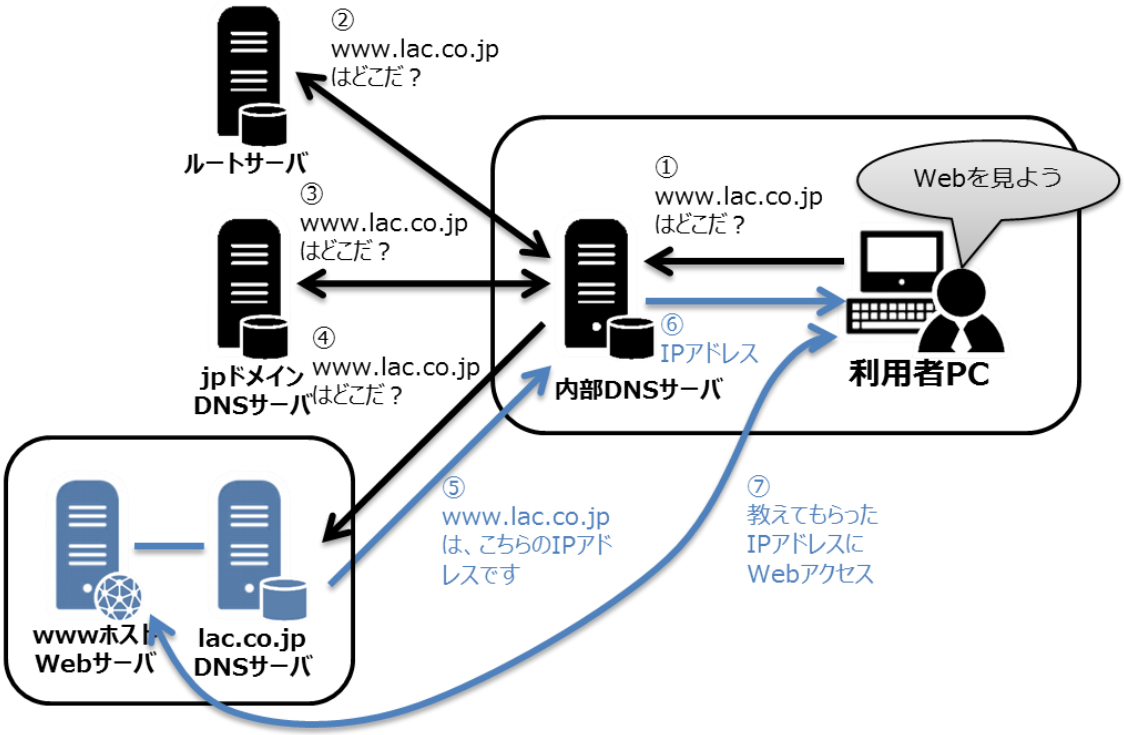

図 1：Web 閲覧における DNS の動き

DNS プロトコルはインターネットにおいて、ドメイン名（FQDN）から IP アドレスなどの情報を得るために DNS サーバとの通信に使用されるプロトコルで、ほとんどの企業でこのプロトコルの制限は行っていません。また、反応速度を重視し、DNS 問い合わせの記録（アクセスログ）の保持を行っていない企業がほとんどであり、攻撃者と遠隔操作ウイルスの交信状況を把握することが困難です。

攻撃者は、各企業における DNS の運用状況を十分に把握しており、DNS パケットを使用してインターネットと企業内部のネットワーク間での指令のやり取りを秘密裏に行う手口を用いていると考えられます。

この脅威は、多くの企業にとって従来のセキュリティ対策における盲点といえます。当社としては、広くその危険性を理解していただき、何らかの対応をお願いするために本日、一般公開いたしました。

DNS を用いた指令サーバとの通信

当社が調査した事案においては、何らかのサイバー攻撃により遠隔操作ウイルスが仕込まれたクライアントコンピュータから、通常のものとは考えられない DNS パケットが送出されていることが確認されました。

攻撃者が用意したと見られる DNS サーバに対して、遠隔操作ウイルスが次のような DNS 問い合わせ（FQDN を含む DNS クエリ)を模したパケットを送出しています。

time	type	query
197.436563000	TXT	HMAb**********.abcde.example.co.jp
197.436614000	TXT	z7Zc**********.abcde.example.co.jp
197.436654000	TXT	H2P8**********.abcde.example.co.jp
197.583133000	TXT	HMAb**********.abcde.example.co.jp
197.587123000	TXT	z7Zc**********.abcde.example.co.jp
197.593304000	TXT	H2P8**********.abcde.example.co.jp
198.645641000	TXT	4uc0**********.abcde.example.co.jp
198.645776000	TXT	MJbk**********.abcde.example.co.jp
198.645904000	TXT	tPg0**********.abcde.example.co.jp
198.652529000	TXT	4uc0**********.abcde.example.co.jp
198.658656000	TXT	MJbk**********.abcde.example.co.jp
198.664786000	TXT	tPgQ**********.abcde.example.co.jp
199.722159000	TXT	vjHD**********.abcde.example.co.jp
199.722279000	TXT	EwFJ**********.abcde.example.co.jp
199.722421000	TXT	ZhTD**********.abcde.example.co.jp
199.726541000	TXT	vjHD**********.abcde.example.co.jp
199.730360000	TXT	EwFJ**********.abcde.example.co.jp
199.734118000	TXT	ZhTD**********.abcde.example.co.jp
200.782882000	TXT	RoYh**********.abcde.example.co.jp
200.783054000	TXT	FfhL**********.abcde.example.co.jp
200.783155000	TXT	TNBB**********.abcde.example.co.jp
200.789800000	TXT	RoYh**********.abcde.example.co.jp
200.795985000	TXT	FfhL**********.abcde.example.co.jp
200.802182000	TXT	TNBB**********.abcde.example.co.jp
201.859412000	TXT	MfcY**********.abcde.example.co.jp
201.859558000	TXT	S++6**********.abcde.example.co.jp
201.859687000	TXT	Nunz**********.abcde.example.co.jp
201.866535000	TXT	MfcY**********.abcde.example.co.jp
201.872924000	TXT	S++6**********.abcde.example.co.jp
201.879116000	TXT	Nunz**********.abcde.example.co.jp
202.935669000	TXT	s0dh**********.abcde.example.co.jp
202.935862000	TXT	j24K**********.abcde.example.co.jp
202.935973000	TXT	+030**********.abcde.example.co.jp
202.942586000	TXT	s0dh**********.abcde.example.co.jp
202.948746000	TXT	j24K**********.abcde.example.co.jp
202.954903000	TXT	+030**********.abcde.example.co.jp
203.481753000	TXT	PLwa**********.abcde.example.co.jp
203.481919000	TXT	ngTt**********.abcde.example.co.jp
203.482026000	TXT	jBdH**********.abcde.example.co.jp
203.489342000	TXT	PLwa**********.abcde.example.co.jp
203.495426000	TXT	ngTt**********.abcde.example.co.jp
203.501824000	TXT	jBdH**********.abcde.example.co.jp
204.558159000	TXT	joOf**********.abcde.example.co.jp
204.558303000	TXT	Lzif**********.abcde.example.co.jp
204.558417000	TXT	OROA**********.abcde.example.co.jp
204.566594000	TXT	joOf**********.abcde.example.co.jp
204.574018000	TXT	Lzif**********.abcde.example.co.jp
204.580848000	TXT	OROA**********.abcde.example.co.jp
205.634498000	TXT	y+r6**********.abcde.example.co.jp
205.634649000	TXT	HKaN**********.abcde.example.co.jp
205.634750000	TXT	mmX1**********.abcde.example.co.jp
205.641417000	TXT	y+r6**********.abcde.example.co.jp
205.647608000	TXT	HKaN**********.abcde.example.co.jp
205.653792000	TXT	mmX1**********.abcde.example.co.jp
206.710912000	TXT	1ErG**********.abcde.example.co.jp
206.711031000	TXT	vCli**********.abcde.example.co.jp
206.711133000	TXT	Ss9K**********.abcde.example.co.jp
206.717764000	TXT	1ErG**********.abcde.example.co.jp
206.723976000	TXT	vCli**********.abcde.example.co.jp
206.730148000	TXT	Ss9K**********.abcde.example.co.jp
207.787243000	TXT	i73y**********.abcde.example.co.jp
207.787404000	TXT	ZYWP**********.abcde.example.co.jp
207.787504000	TXT	oJqu**********.abcde.example.co.jp
207.795014000	TXT	i73y**********.abcde.example.co.jp
207.801789000	TXT	ZYWP**********.abcde.example.co.jp
207.807908000	TXT	oJqu**********.abcde.example.co.jp

図 2:確認された不正な DNS パケットの一部

time はキャプチャされたパケットの相対的な時間（秒）を表し、type は DNS レコードの種類、query が DNS クエリを表します。
クエリに含まれるドメイン名（example.co.jp）、サブドメイン名（abcde）、ホスト名部分は、実際の情報ではなく例示用に書き換えています。
サブドメイン名（abcde）は標的を特定する文字列か作戦名を表していると推察され、当社にて解析したマルウェアが使用しているドメインには、他に 4 つのサブドメインが存在することが確認されています。したがって、同じマルウェアは、複数の他の組織にも使用されている可能性があります。

実際の DNS リクエストでは、**10 秒程度の短い時間の間に、指令サーバとの通信と考えられる DNS クエリを送信しています。FQDN のホスト名部分には、暗号化されていると考えられる 30 文字以上の文字列が埋め込まれています。**
指令サーバである DNS サーバが稼動していれば、これらの TXT レコードのクエリを送信したクライアント PC に対して応答を行われると考えられますが、検体の解析を行った時点では該当 DNS サーバは既に存在せず、遠隔操作ウイルスへの指令の内容などは確認できませんでした。指令サーバが稼動していた場合は、命令が暗号化された上で、送信されるものと推察できます。

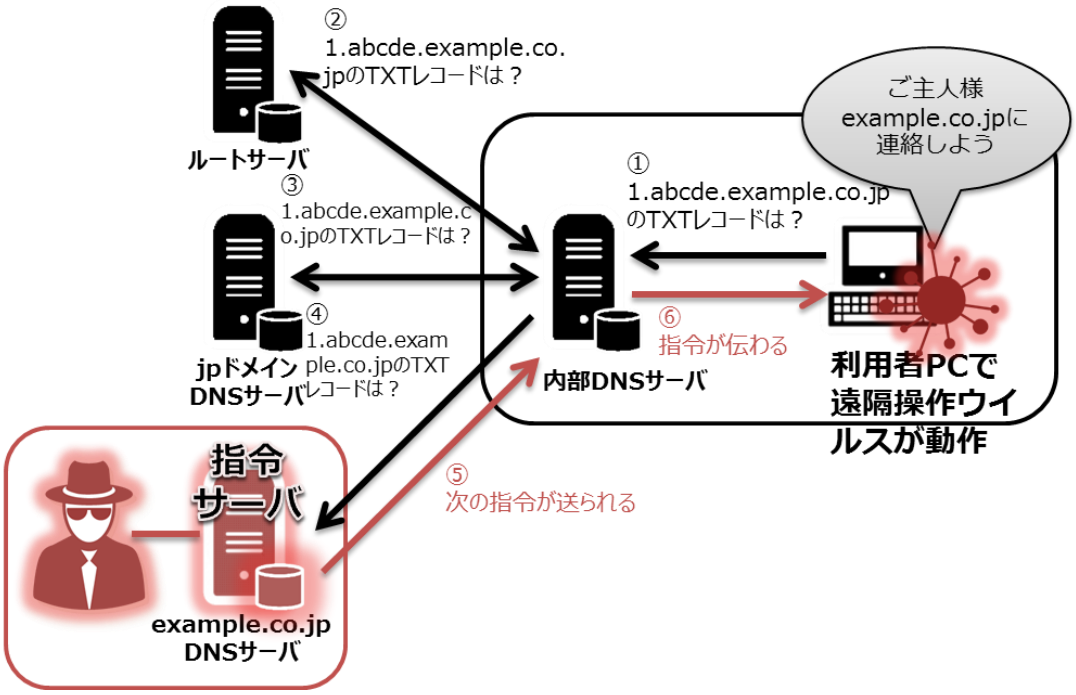

図 3:遠隔操作ウイルスの制御に DNS を用いた不正な行動の動き

なお、DNS パケットの内容や送信頻度などの情報は、あくまでも当社が調査した事案で確認されたものです。そのため DNS レコードの種類、送信頻度、ホスト名の長さや文字列は、変化する可能性があります。

この脅威が深刻である理由

今回の注意喚起で明らかにした「DNS サーバを模した指令サーバとの通信」という脅威は、以下の理由で企業にとっては深刻な問題となります。

1. 使用されている DNS 通信単体では、特に異常があるわけではない。そのため、次世代型 FW やプロキシ、IDS などで検知することは困難。
2. DNS リクエストがシステムに及ぼす負荷を懸念して、多くの DNS ではログを収集していない。そのため、不正なリクエストが行われたか否かを確認することは困難。
3. 指令サーバは生存期間が短いため、事後に調査しても何が行われたかを詳細に把握することは困難。
4. 遠隔操作ウイルスは攻撃対象に対してカスタマイズされているため、ウイルス対策ソフトでは検知が困難。

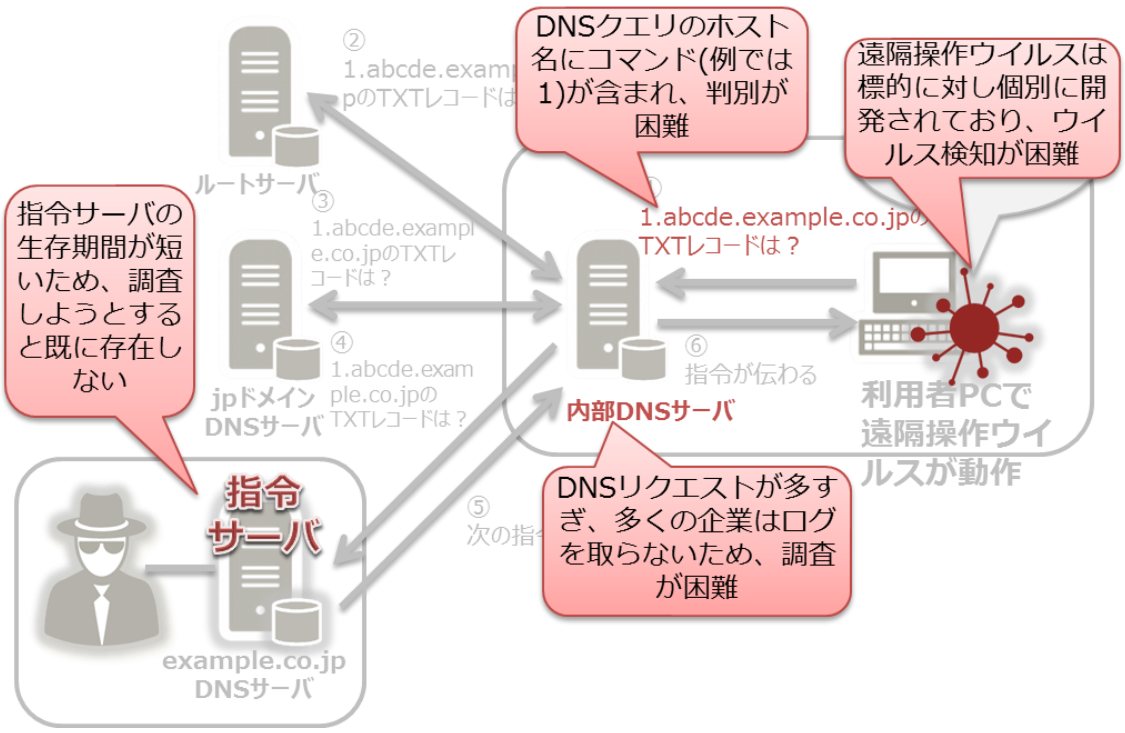

図 4:企業にとって DNS プロトコルを悪用した脅威への対応が困難な理由

推奨する対応方法

本注意喚起で指摘した脅威は、DNS プロトコルを悪用したものです。DNS はインターネットの根幹を支えるシステムであることから、DNS へのアクセスを停止したり、ドメイン名や DNS サーバを頻繁に切り替えることが出来るため、ブラックリストによるブロックで防ぐことも難しいのが現実です。
本脅威への対応例としては、次のような策が考えられます。

1　現在の DNS サーバへのアクセス状況を確認する
前項「DNS を用いた指令サーバとの通信」にあるような、不正な DNS 通信を発見するため、次のような作業を行います。

1.1 内部 DNS のアクセスログから不正なリクエストを発見する

DNS への要求は、インターネット通信が行われるたびなされるため、非常に大量にアクセスログが記録されます。このログの記録が DNS の動作負荷の増大につながる可能性があります。そのため、サーバの負担を確認しながらログの取得を行ってください。

その後、取得したログから、前項「DNS を用いた指令サーバとの通信」にあるような不正な DNS リクエストの有無を確認します。

1.2 ネットワークパケットを収集し不正なリクエストを発見する

DNSサーバはインターネットアクセスの根幹を構成する重要なサービスです。ログ取得の悪影響を考慮する場合、DNS サーバへの UDP/53 および TCP/53 に対するパケットをキャプチャし、調査する方法もあります。その後、取得したログから、前項「DNS を用いた指令サーバとの通信」にあるような不正な DNS リクエストの有無を確認します。

収集したネットワークパケットの調査に関しては、当社の情報漏えいチェックサービスが対応可能です。

また、ネットワークパケットの収集および分析に関しては、当社子会社のネットエージェントが提供している「PacketBlackHole」をご活用いただけます。

ネットエージェント株式会社「PacketBlackHole 特設ページ」

E-mail: pbh-sales@netagent.co.jp Tel: 03-5619-1341

2 指令サーバとして稼動している DNS 通信（UDP/53,TCP/53）を拒否する

不正な DNSリクエストが確認された場合、DNS のフォワード制限、もしくはファイアウォールなどにより指令サーバへの DNS 通信を拒否するよう設定してください。

3 DNS アクセスの制限と、プロキシサーバの活用

可能であれば、内部 DNS での名前解決は企業内部ネットワークのみに制限して社外の DNS サーバにフォワードしない設定とし、Web などインターネットのサイトへのアクセスはプロキシサーバ経由でのアクセスに制限します。

4 不正なパケットを送出しているクライアントを特定する

不正なパケットを送出している IP アドレスは、ログやパケットキャプチャの内容から判断します。また、インターネットアクセスを想定していないシステム(特に制御システムや重要な情報を扱うシステム)に設置する内部 DNS サーバの接続状況を確認し、インターネットに対して通信する必要がない場合はその内部 DNS サーバは隔離します。

5 遠隔操作ウイルスの隔離

遠隔操作ウイルスは、標的型攻撃で用いられるように標的となる組織に特化して開発されていることが多く、ウイルス対策ソフトでは発見できない場合もあります。遠隔操作ウイルスを発見した場合は、感染機器をネットワークから隔離すると共に、ウイルスの検体ファイルは削除せず、ご利用のウイルス対策ソフトベンダに検体提供し、パターンファイルの更新などを行ってください。また、ウイルス検体の特定、侵入による被害状況の確認が必要となる場合は、当社の緊急対応サービス「サイバー119」など、調査サービスを活用されることをお勧めします。

参考情報

Tunneling Data and Commands Over DNS to Bypass Firewalls
https://zeltser.com/c2-dns-tunneling/
Detecting DNS Tunneling
http://www.sans.org/reading-room/whitepapers/dns/detecting-dns-tunneling-34152

以上