DNS シンクホールの効果検証のための学内クライアントの名前解決状況の分析

笠置友里* 中村將** 池部実* 吉田和幸***
（大分大学 *工学部知能情報システム工学科 **工学研究科工学専攻 ***学術情報拠点情報基盤センター）

1 はじめに

ボットは攻撃者が用意した C&C サーバに定期的に接続し，攻撃者からの命令を受信した後に，DDoS 攻撃や spam 送信などの不正な活動をする．そのため，ボットの C&C サーバへの接続を阻止することでボットの活動を停止できる．C&C サーバへの接続防止の手法のひとつに，DNS シンクホール[1]がある．この手法では，DNS キャッシュサーバはブラックリストを保持し，クライアントから C&C サーバの FQDN の問合せを受けた場合，本来の回答とは異なる偽の回答を返すことで C&C サーバへの接続を阻止する．本研究では学内の DNS キャッシュサーバが C&C サーバの FQDN の問合せを受けているかを調査し，DNS シンクホールによる C&C サーバへの接続阻止の効果を検証する．

2 DNS シンクホール

攻撃者は C&C サーバを介してボットに命令を送信し，DDoS 攻撃や spam 送信などのサイバー攻撃をする．DNS シンクホールとは，C&C サーバとボットの接続を阻止する手法である．DNS シンクホールによる C&C サーバとボットの接続阻止の流れを図 1 に示す．

(1)ボットは攻撃者からの命令を受信するために，C&C サーバの FQDN を DNS キャッシュサーバに問い合わせる．

(2)DNS キャッシュサーバは自身の持っているブラックリストの FQDN と問い合わせ FQDN が一致すると，DNS キャッシュサーバの管理人によって設定された偽の回答を返す(例：127.0.0.1)．

(3)DNS キャッシュサーバが偽の回答を返すことにより，ボットは C&C サーバに接続することができなくなる．

図 1. DNS シンクホールによる C&C サーバとボットの接続阻止の流れ

3 問い合わせログとブラックリストの照合

DNS シンクホールを用いることにより C&C サーバへの接続防止の効果検証のために，学内ホストの中に C&C サーバと見られる不正ドメインの FQDN を問い合わせているホストが存在しているかを調査した．Malware Domain List[2]が公開している 2016 年 7 月 6 日時点の 2,578 件の不正な FQDN のブラックリストと学内 DNS キャッシュサーバの問い合わせログを照合した．大分大学の DNS キャッシュサーバは複数存在するが，今回の調査では工学部知能情報システム工学科のネットワークに設置した DNS キャッシュサーバ 1 台を対象に照合した．

4 検出した問い合わせの分析結果

2016 年 1 月～6 月の 6 ヶ月間の問い合わせログ 55,828,519 件を調査した．照合の結果，ブラックリストに記載されている FQDN に該当する問い合わせを 11 件検出した．1 ヶ月ごとの検出した不正 FQDN の問い合わせ件数を表 1 に，問い合わせ内容の一部を表2に示す．今回検出した 11 件の問い合わせの間隔は不定期であり，送信元 IP アドレスは 5 件存在した．不正な FQDN は 3 件検出され，A レコードと AAAA レコードを問い合わせていた．検出した問い合わせの中には， ウェブサイトを閲覧した際にスクリプトにより自動的に不正な URL へ誘導する問い合わせが含まれていた．このような問い合わせはドライブバイダウンロード攻撃につながる危険性がある．

表 1. 1 ヶ月ごとの検出した問い合わせ件数

月	1 月	2 月	3 月	4 月	5 月	6 月
件数	0 件	4 件	0 件	2 件	5 件	0 件

表 2. 検出した問い合わせ内容

年-月-日	時刻	名前解決対象の FQDN	レコード
2016-2-11	16:29:29	www.xenon.com.au	A
2016-2-11	16:29:29	www.xenon.com.au	AAAA
2016-4-27	15:49:52	www.daidegasforum.com	A
2016-4-27	15:49:52	www.daidegasforum.com	AAAA
2016-5-19	14:50:59	js.tongji.linezing.com	A

5 まとめと今後の展開

DNS シンクホールの効果検証のため，学内クライアントの名前解決状態を調査した．調査した半年間では 11 件のブラックリストに掲載されているドメインの問い合わせが存在し，それらの中にはドライブバイダウンロード攻撃につながる可能性がある問い合わせが含まれていた．ドライブバイダウンロード攻撃は，クライアントの知らないうちにマルウェアをダウンロードさせインストールする危険性がある．ドライブバイダウンロード攻撃につながる名前解決は阻止する必要がある．今回調査対象とした DNS キャッシュサーバを DNS シンクホールとして設置し，不正 FQDN の接続を阻止する．今後は検出した 5 件の IP アドレスが不正 FQDN の問い合わせの他にどのような問い合わせをしているかを分析し，C&C サーバやドライブバイダウンロード攻撃につながる不正な FQDN への問い合わせが存在するかを調査する．

参考文献

[1] 八木毅，秋山満昭，村山純一：コンピュータネットワークセキュリティ．コロナ社．2015

[2] Malware Domain List. http://www.malwaredomainlist.com/mdl.php.