レポート

平成 29 年5月 25 日

攻撃ツール「Eternalblue」をはじめとするソフトウエアの脆弱性を悪用した攻撃等と考えられるアクセスの観測について

- 攻撃ツール「Eternalblue」を悪用した攻撃等と考えられるアクセスの観測
- IIS6.0 の脆弱性を標的とした攻撃活動等の観測
- Apache Struts 2 の脆弱性（S2-046）を有する機器の探索活動を観測

1 攻撃ツール「Eternalblue」を悪用した攻撃等と考えられるアクセスの観測

本件は、平成 29 年5月 15 日に警察庁セキュリティポータルサイト@police において概要を速報[i]したものです。その詳細については、以下のとおりです。

平成 29 年4月 14 日に「The Shadow Brokers」を名乗る集団が、Microsoft Windows の脆弱性を標的とした攻撃ツール「Eternalblue」や Microsoft Windows に感染するバックドア「Doublepulsar」などを公開しました。これら攻撃ツールの一部は、世界的な被害を発生させたランサムウェア「WannaCry」の感染活動にも悪用されています。

同集団が公開した攻撃ツールの中に Microsoft 社製品の脆弱性を標的としたものが含まれていたことを受けて、同社は同日中にブログ[ii]で、これらの問題への対応状況等を明らかにしました。同社は、公開された攻撃ツールが標的とする脆弱性は、「Windows 7」、「Windows 8.1」、「Windows 10」といったサポート対象の OS では全てパッチにより修正済みであり、「Eternalblue」が標的とする脆弱性は3月 15 日に公開された MS17-010[iii]で修正されているとしています。また同社は、当該脆弱性は Server Message Block[iv]（以下「SMB」という。）1.0 のサーバ機能に存在するものであり、悪用された場合にはネットワークを経由して遠隔から任意のコードを実行される危険性があるとしています。

また、「Doublepulsar」に感染した場合には、SMB で使用される 445/TCP ポート及びリモートデスクトップで使用される 3389/TCP ポートを介した侵入、遠隔操作等が可能になることが明らかとなっています。「Doublepulsar」に感染した端末は、445/TCP ポート及び 3389/TCP ポートへの特定のリクエストに対して特定の応答を行うことに着目して、外部からの感染確認が可能であることもわかっており、「Doublepulsar」の感染有無を確認するスキャンツールも公開されています。

「Doublepulsar」等のバックドアや「WannaCry」等のランサムウェアといった不正プログラムを、

[i] 「攻撃ツール「Eternalblue」を悪用した攻撃と考えられるアクセスの観測について」
http://www.npa.go.jp/cyberpolice/important/2017/201705151.html

[ii] 「Protecting customers and evaluating risk」
https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/

[iii] 「マイクロソフト セキュリティ情報 MS17-010 - 緊急 Microsoft Windows SMB サーバー用のセキュリティ更新プログラム (4013389)」
https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx

[iv] Microsoft Windows 等においてファイル共有等に使用される通信プロトコルであり、445/TCP ポートが使用される。

攻撃ツール「Eternalblue」と組み合わせることにより、ネットワーク経由で遠隔から感染させることが可能であることが判明しています。「Eternalblue」と「Doublepulsar」を組み合わせた攻撃手順については、具体的に解説した資料もインターネット上に公開されています。また、「Doublepulsar」及び「Eternalblue」等は、インターネット上で誰もが入手可能となっています。以上のことから、既に「Eternalblue」を悪用して「Doublepulsar」に感染させる攻撃活動が行われている可能性があります。

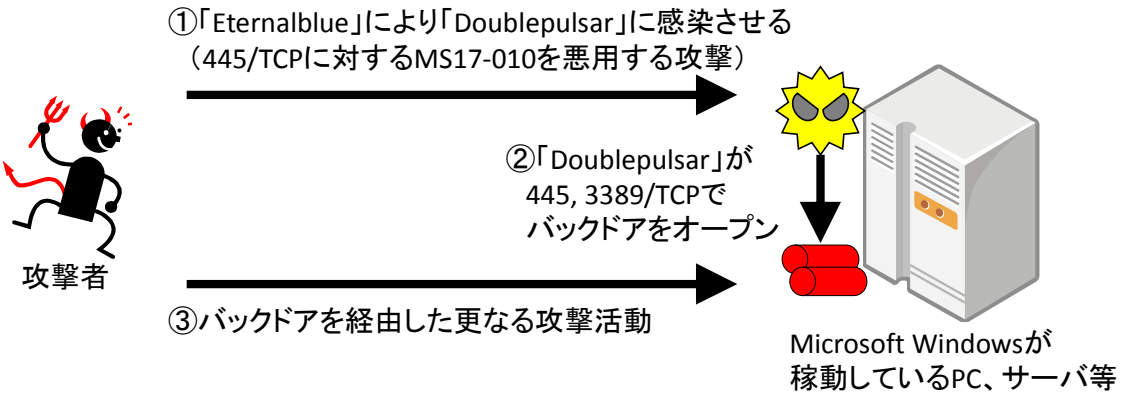

図1 「Eternalblue」と「Doublepulsar」による攻撃の概要

警察庁の定点観測システムにおいては4月 19 日以降、宛先ポート 445/TCP に対する特定の SMB ネゴシエーションパケットを観測しています（図2）。同内容は、「Doublepulsar」のスキャンツールに実装されている固有の通信内容と一致しており、「Doublepulsar」の感染有無を確認する目的であると考えられます。

一方で、SANS ISC が公開した「Eternalblue」の動作検証結果[i]によれば、「Eternalblue」を悪用する攻撃活動においても同様の445/TCP に対するアクセスが発生するものとみられます。このため、同アクセスは「Eternalblue」を悪用した MS17-010 を標的とする無差別な攻撃活動を観測している可能性も考えられます。

また、3389/TCP ポートにおいても「Doublepulsar」のスキャンツールに実装されている固有の通信と一致するアクセスが4月 23 日から断続的に増加しており、同アクセスは「Doublepulsar」の感染有無を確認する目的であると考えられます（図3）。

[i] 「ETERNALBLUE: Windows SMBv1 Exploit (Patched)」
https://isc.sans.edu/forums/diary/ETERNALBLUE+Windows+SMBv1+Exploit+Patched/22304/

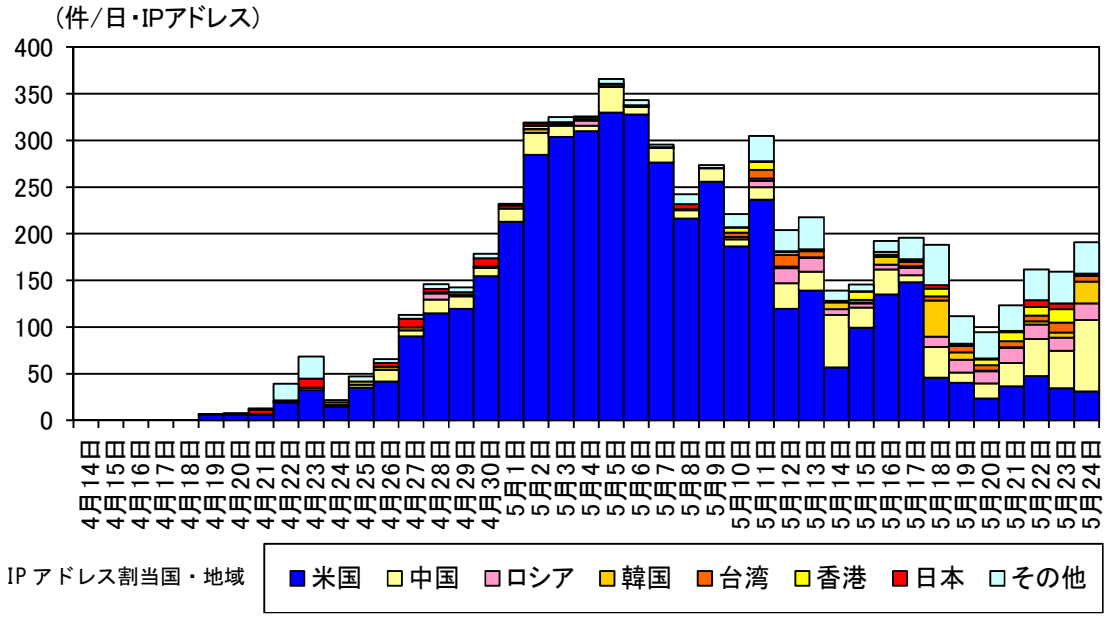

図2　攻撃ツール「Eternalblue」を悪用した攻撃等と考えられる宛先ポート 445/TCP に対するアクセス件数の発信元国・地域別推移（H29.4.14～5.24）

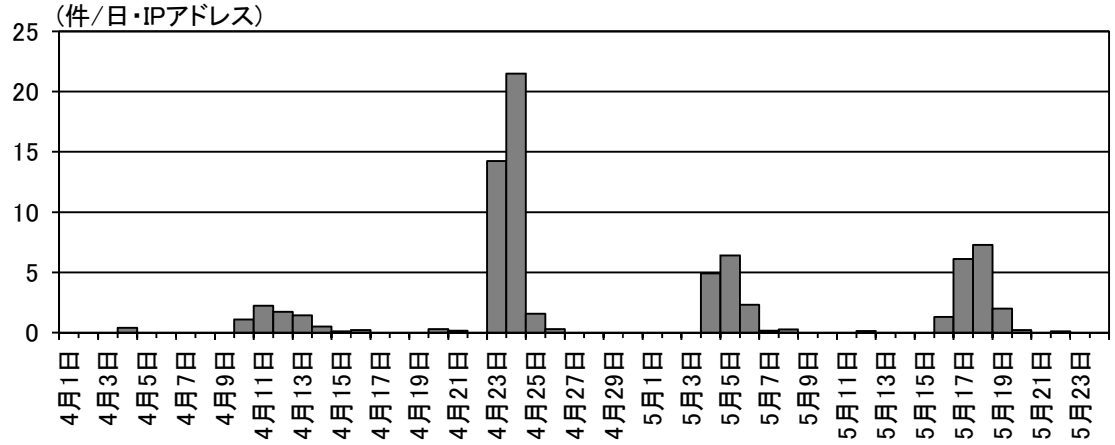

図3　「Doublepulsar」に感染した Microsoft Windows マシンの探索と考えられる宛先ポート 3389/TCP に対するアクセス件数の推移

また、5月 12 日頃からは、ランサムウェア「WannaCry」による攻撃活動が行われています。当該ランサムウェアは、「Eternalblue」を悪用した感染活動を試みるとともに、「Eternalblue」による感染に失敗した場合は既に感染している「Doublepulsar」を悪用した感染活動を行うもの [i] とされております。警察庁では、定点観測システムにおいて観測した 445/TCP ポートに対するアクセス（図2）の中に、「WannaCry」に感染した PC による感染活動の一環と思われる 5 月 12 日以降のアクセスが含まれていることを確認しております。

[i] 「Player 3 Has Entered the Game: Say Hello to 'WannaCry'」
http://blog.talosintelligence.com/2017/05/wannacry.html

当該ランサムウェアによる攻撃活動の発生を受けて Microsoft 社は、3月時点では明言していなかったサポート期間が終了している複数の製品においても MS17-010 の影響を受けることを明らかにするとともに、例外的にサポート期間対象外の製品についてもパッチを提供する旨[i]を明らかにしました。3月に公表された対象製品も含めて、MS17-010 の影響を受ける製品は表1のとおりです。

表1　MS17-010 の影響を受ける Microsoft 社製品

Microsoft Windows XP
Microsoft Windows Server 2003
Microsoft Windows Vista
Microsoft Windows Server 2008 及び Windows Server 2008 R2
Microsoft Windows 7
Microsoft Windows 8 及び Windows 8.1
Microsoft Windows Server 2012 及び Windows Server 2012 R2
Microsoft Windows RT 8.1
Microsoft Windows 10
Microsoft Windows Server 2016

以上のことから、Microsoft Windows が稼動している PC やサーバ等を利用している場合には、次の対策を実施することを推奨します。

- Microsoft Windows が稼動している PC をインターネットに接続する際は、直接接続するのではなく、ルータ等を使用して NAT を介して接続してください。自宅等ではルータを使用してインターネットに接続していても、モバイル回線を利用する場合には直接インターネットに接続される場合もあるので注意してください。
- Microsoft Windows が稼動している PC 又はサーバは、可能であれば 445/TCP ポートに対するアクセスを遮断してください。特にインターネットから当該ポートへのアクセスを許可している場合には、早急に対応を検討してください。
- インターネット接続の有無に関わらず、Microsoft 社が公開する修正パッチを直ちに適用して、利用している Microsoft Windows を最新の状態にしてください。
- 特に MS17-010 が未適用の Microsoft Windows が稼動している PC 又はサーバ等を直接インターネットに接続していた場合には、既に「Doublepulsar」の感染又はその他の攻撃活動を受けている可能性があります。不審なプロセス、ファイル及び通信等が存在しないか確認してください。
- 各組織の管理者は「Doublepulsar」スキャンツール等を活用して、組織内に「Doublepulsar」に感染した PC やサーバが存在しないか確認してください。

[i] 「ランサムウェア WannaCrypt 攻撃に関するお客様ガイダンス」
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/

2 IIS6.0 の脆弱性を標的とした攻撃活動等の観測

平成 29 年3月 27 日に、Microsoft Windows Server 2003 R2 に付属する Web サーバである IIS6.0 が有する脆弱性 [i] が公表されました。公表内容によると、当該脆弱性は WebDAV [ii] の機能が有効となっている IIS6.0 に対して、細工した PROPFIND [iii] リクエストを送信することによりサーバ上で任意のコードが実行可能となる極めて深刻なものとなっています。当該脆弱性については発見者が PoC [iv] を公開するとともに、この PoC を元に作成されたと考えられる攻撃ツールについてもインターネット上で既に公開されています。

警察庁の定点観測システムにおいては、4月 30 日及び5月 17 日に当該脆弱性を標的とした攻撃活動と考えられるアクセスを観測しました（図4）。当該アクセスを観測したのは短時間のわずかな件数のみでしたが、同アクセスには IIS6.0 が動作するサーバ上で不正なコードの実行を試みていると思われる内容が含まれていました（図5）。WebDAV 機能が有効となっている IIS6.0 に対して当該アクセスと同内容を送信すると、外部へ不正な通信が発生することを確認しています。

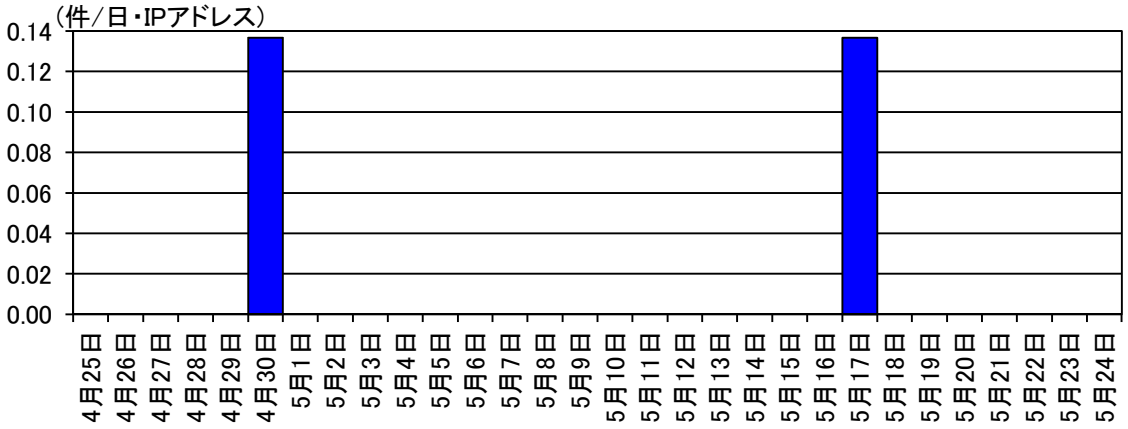

図4 IIS6.0 の脆弱性を標的とした攻撃活動と考えられるアクセス件数の推移

```
00000000  50 52 4f 50 46 49 4e 44  20 2f 20 48 54 54 50 2f   PROPFIND  / HTTP/
00000010  31 2e 31 0d 0a 48 6f 73  74 3a 20 6c 6f 63 61 6c   1.1..Hos t: local
00000020  68 6f 73 74 0d 0a 43 6f  6e 74 65 6e 74 2d 4c 65   host..Co ntent-Le
00000030  6e 67 74 68 3a 20 30 0d  0a 49 66 3a 20 3c 68 74   ngth: 0. .If: <ht
00000040  74 70 3a 2f 2f 6c 6f 63  61 6c 68 6f 73 74 2f 61   tp://loc alhost/a
00000050  61 61 61 61 61 61 e6 bd  a8 e7 a1 a3 e7 9d a1 e7   aaaaaa.. ........
```

図5 観測したアクセス内容（冒頭部分のみ抜粋）

[i] https://github.com/edwardz246003/IIS_exploit
「JVNDB-2017-002299 Microsoft Windows Server 2003 の Internet Information Services の WebDAV サービスにおけるバッファオーバーフローの脆弱性」
http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-002299.html

[ii] Web Distributed Authoring and Versioning の略であり、Web サーバ上でのファイル管理を行うために、HTTP を拡張したプロトコル

[iii] WebDAV において、ファイル等のプロパティを取得するメソッド

[iv] Proof of Concept（概念実証）の略であり、脆弱性を悪用した攻撃が可能であることを示すための簡潔な検証用プログラム

また、3月 31 日以降、脆弱性を攻撃する内容を含まない通常の PROPFIND リクエストも断続的に観測しています（図6）。さらに過去の観測状況を遡って調査したところ、平成 28 年4月から7月の間においても、通常の PROPFIND リクエストを多数観測していたことが判明しました（図7）。こうした PROPFIND リクエストは、単に WebDAV が稼動している機器を探索する目的であるとも考えられますが、PROPFIND リクエストに対する応答を確認することにより、IIS6.0 における WebDAV の有無効を確認可能であるため（図8）、当該脆弱性の影響を受ける機器の探索活動であった可能性があります。脆弱性の発見者によると、平成 28 年7月又は8月に当該脆弱性を悪用する攻撃が発生していたとされています。この攻撃活動と、その直前の4月から7月の間に通常の PROPFIND リクエストを多数観測していた事象に関連がある可能性も疑われます。

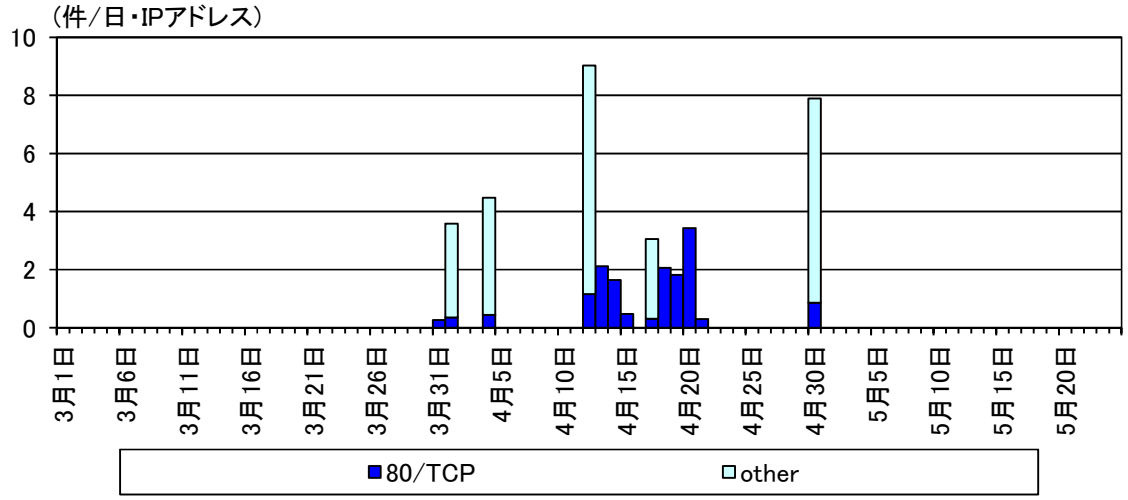

図6　通常の PROPFIND リクエストの宛先ポート別の件数推移

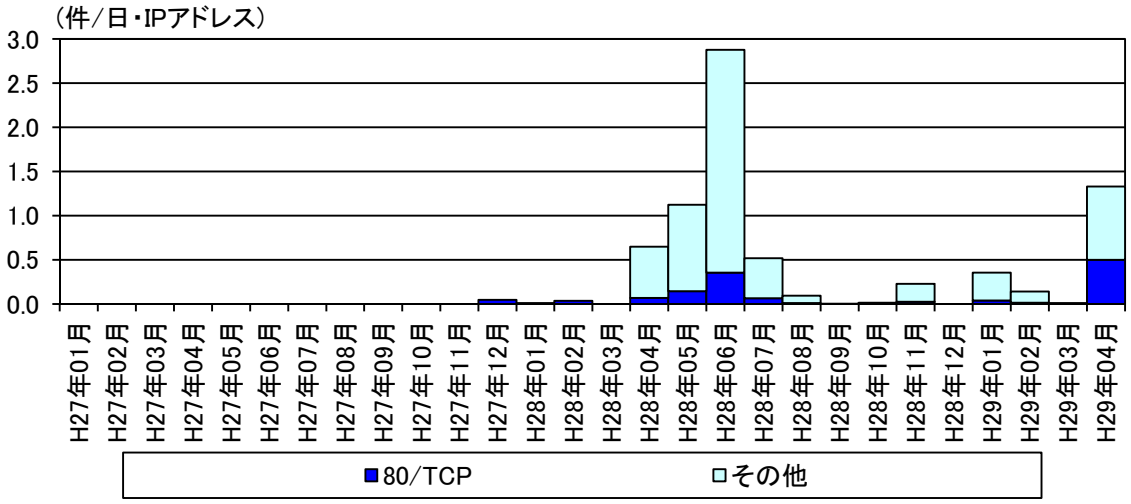

図7　通常の PROPFIND リクエストの宛先ポート別の件数推移（1日当たりの平均）

WebDAV が無効な IIS6.0 からの応答	WebDAV が有効な IIS6.0 からの応答
HTTP/1.1 501 Not Implemented Content-Length: 0 Server: Microsoft-IIS/6.0 Date: Sun, 09 Apr 2017 03:35:22 GMT	HTTP/1.1 411 Length Required Connection: close Date: Sun, 09 Apr 2017 03:38:37 GMT Server: Microsoft-IIS/6.0 Content-Type: text/html Content-Length: 50

図8 通常の PROPFIND リクエストに対する IIS6.0 からの応答例 [i]

以上のことから、IIS6.0 により Web サーバ(WebDAV サーバを含む)を運用している場合には、次の対策を実施することを推奨します。

- IIS6.0 が付属する Microsoft Windows Server 2003 及び Windows XP は、既に製造元である Microsoft 社のサポート期間が終了しています。このため、当該脆弱性に対する修正パッチも公開されていません。IIS6.0 による Web サーバ(WebDAV サーバを含む)の運用は、ただちに終了してください。
- 事情により、やむを得ずに IIS6.0 による Web サーバの運用を継続する場合には、WebDAV 機能を無効にすることにより当該脆弱性の影響を回避できる [ii] と考えられます。しかしながら、あくまでも暫定的な対策にとどめ、開発元によるサポートがある最新バージョンの OS 及び Web サーバソフトウェアへ速やかに移行してください。
- WebDAV 機能が有効となっている IIS6.0 により Web サーバ(WebDAV サーバを含む)を運用していた場合には、不審なプロセス、ファイル及び通信等が存在しないか確認してください。

[i] Server ヘッダから IIS6.0 の稼動の有無が確認可能であり、WebDAV の有効/無効によって HTTP レスポンスコードが異なる。

[ii] 「Windows Server 2003 R2 のインターネット インフォメーション サービス(IIS)6.0 における WebDAV サービスの脆弱性により、リモートから任意のコードが実行可能な脆弱性(CVE-2017-7269)に関する調査レポート」
https://www.softbanktech.jp/information/2017/20170403-01/

3 Apache Struts 2 の脆弱性（S2-046）の影響を受ける機器の探索行為を観測

Apache Struts 2 は、Java 言語で Web アプリケーションを開発する際に利用されるフレームワークです。平成 29 年3月７日に Apache Struts 2 に存在する深刻な脆弱性（S2-045）が、開発元である The Apache Software Foundation から公表[i]されました。警察庁においては、当該脆弱性 S2-045 を標的とした攻撃活動を同日から観測[ii]しています。

3月 20 日には、S2-045 と類似する脆弱性（S2-046）が公表[iii]されました。S2-045 は HTTP リクエストにおける Content-Type ヘッダを悪用することにより攻撃が可能となるものでしたが、S2-046 は Content-Disposition 及び Content-Length ヘッダを悪用することにより S2-045 と同様の攻撃を行うことが可能となるものです。開発元は、S2-045 と同様に、S2-046 も悪用された場合には、サーバ上で遠隔から任意のコードを実行される危険性があるとしています。

警察庁の定点観測システムにおいては、4月４日から断続的に S2-046 を標的としていると考えられるアクセスを観測しました（図9）。当該アクセスは、応答内容を確認することにより探索対象における S2-046 の影響の有無を確認する目的であると考えられます（図 10）。

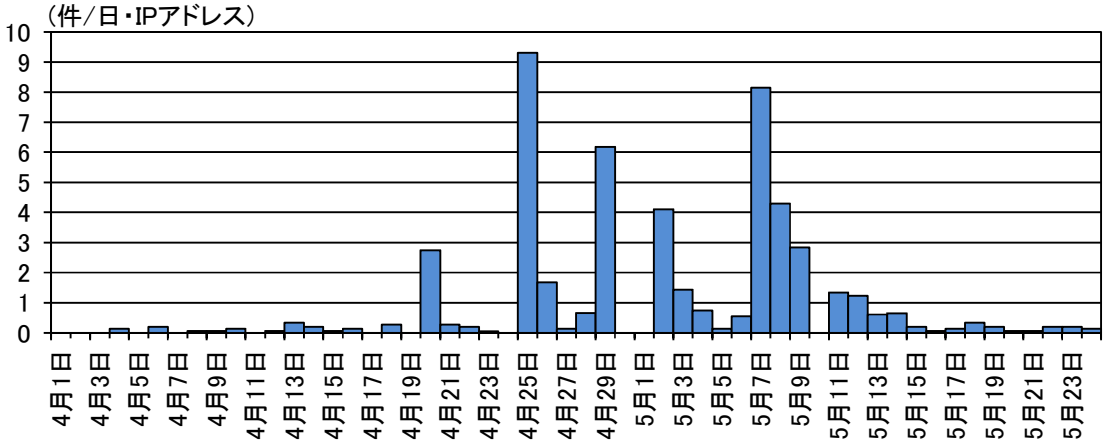

図9 Apache Struts 2 の脆弱性（S2-046）の探索行為と考えられるアクセス件数の推移

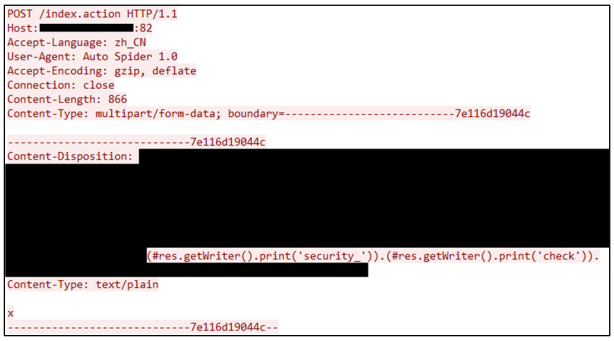

図 10 観測したアクセスの例（一部をマスキング）

警察庁の定点観測システムにおいては、S2-046 を悪用してコマンドの実行を試みる攻撃活動

[i] https://struts.apache.org/docs/s2-045.html
[ii] 「海外製ワイヤレスネットワークカメラの脆弱性を標的としたアクセスの観測等について」
http://www.npa.go.jp/cyberpolice/important/2017/201704271.html
[iii] https://struts.apache.org/docs/s2-046.html

は観測されませんでしたが、当該アクセスにより S2-046 の影響を受けることが明らかとなった機器に対しては、引き続き S2-046 を悪用する攻撃活動が行われている可能性があります。

S2-045 が Content-Type ヘッダを悪用するものであったことから、暫定的な対策として Content-Type ヘッダの内容を監視及び無害化する措置を講じていた場合であっても、Content-Disposition 及び Content-Length ヘッダを悪用する S2-046 を標的とした攻撃活動を防ぐことはできません。また、S2-045 を標的とした攻撃活動と考えられるアクセスは、4月に入ってからも継続して観測しました(図 11)。

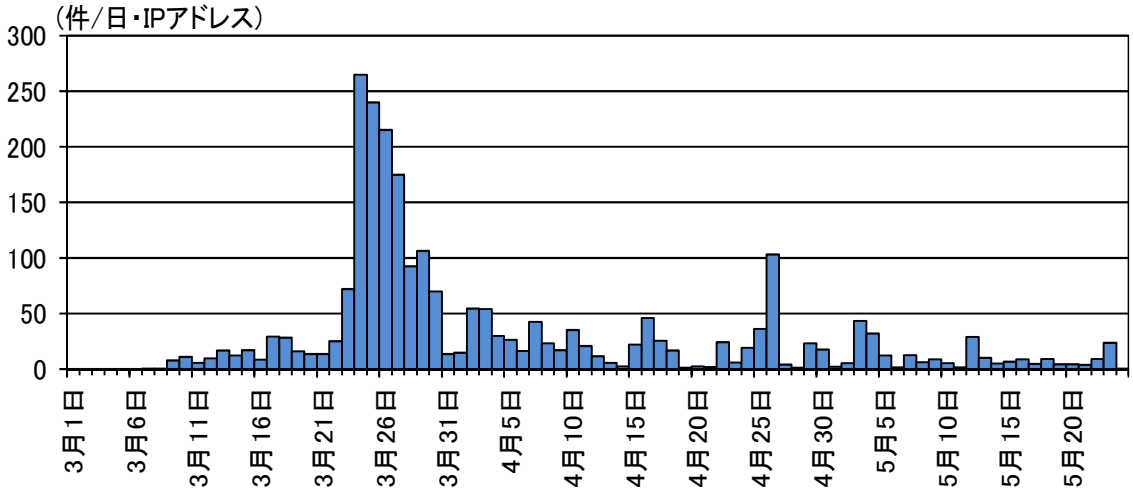

図 11 Apache Struts 2 の脆弱性(S2-045)を標的とした攻撃活動と考えられるアクセス件数の推移

以上のことから、Apache Struts 2 を使用して Web アプリケーションを運用している場合には、次の対策を実施することを推奨します。

- Apache Struts 2 を開発元から公開されている最新バージョンにアップデートしてください。
- 速やかなアップデートが困難な場合には、アップデート完了まで開発元が公表している回避策の実施等を検討してください。
- 3月7日以降も、S2-045 及び S2-046 の影響を受ける Apache Struts 2 を利用していた場合には、既に攻撃を受けている可能性が極めて高いため、不審なプロセス、ファイル、通信及びコマンド実行履歴等が存在しないか確認してください。