レポート

平成 30 年2月 14 日

「Eternalblue」又は「Doublepulsar」を悪用した攻撃活動等と考えられるアクセスの増加等について

- 「Eternalblue」又は「Doublepulsar」を悪用した攻撃活動等と考えられるアクセスの増加
- Oracle WebLogic Server の脆弱性（CVE-2017-10271）を標的とした攻撃活動等の観測

1 「Eternalblue」又は「Doublepulsar」を悪用した攻撃活動等と考えられるアクセスの増加

警察庁では、平成 29 年 12 月以降、攻撃ツール「Eternalblue」又は「Doublepulsar」を悪用した Microsoft Windows を標的とする攻撃活動等と考えられるアクセスの増加を観測しています（図1）。

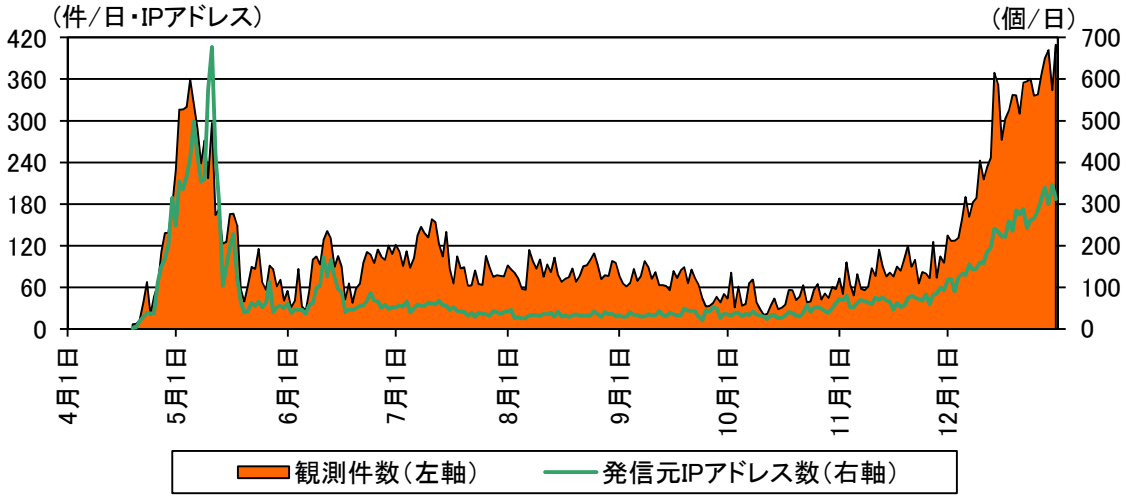

図1 「Eternalblue」又は「Doublepulsar」を悪用した攻撃活動等と考えられる通信の観測件数及び発信元 IP アドレス数の推移（WannaCry によるものを除く）（H29.4.1～12.31）

4月 14 日に「The Shadow Brokers」を名乗る集団が、「Eternalblue」及び「Doublepulsar」をはじめとする複数の攻撃ツールをインターネット上に公開しました。警察庁の定点観測システムにおいては、4月 19 日以降、これらツールに関する特徴的な SMB パケットを継続して観測しており、同時期からインターネット上で「Eternalblue」を用いた攻撃活動又は「Doublepulsar」に感染した機器の攻撃活動等が実施されていたことが考えられます。

5月 12 日からは、世界各国でランサムウェア「WannaCry」[i] の被害が報告されるようになりました。「WannaCry」は同一ネットワーク（LAN）内及びインターネット上の機器に、以下の2種類の手法[ii] により感染活動を行います。

【手法 A】 脆弱性 MS17-010 が修正されていない場合は、当該脆弱性を悪用してバックドア「Doublepulsar」を感染させる。その後、「Doublepulsar」を経由して「WannaCry」を送り込む。

【手法 B】 感染対象の機器にパッチが適用されており、手法 A に失敗した場合には、第三者によって既に「Doublepulsar」に感染させられていないか確認する。「Doublepulsar」に既に感染していた場合には、これを経由して「WannaCry」を送り込む。

警察庁においては、5月 12 日以降、【手法 A】又は【手法 B】の特徴を有する通信を観測しています。【手法 A】の特徴を有する通信は、5月 11 日以前には観測されていないことから、当該通信は「WannaCry」の感染活動に起因するものと考えられます。他方、【手法 B】の特徴を有する通信は、次の2つの攻撃活動又は探索と同一の特徴を有するため、【手法 A】及び【手法 B】の特徴を有する通信が連続して同一の発信元 IP アドレスから観測された場合には、その【手法 B】の特徴を有する通信も、「WannaCry」の感染活動によるものと判断できます。

- 「Eternalblue」を悪用した攻撃活動又は脆弱性が存在する機器の探索
- 「Doublepulsar」感染機器に対する攻撃活動又は感染機器の探索

「Eternalblue」、「Doublepulsar」及び「WannaCry」に関連する通信についてまとめたものが、表1です。

表1 「Eternalblue」、「Doublepulsar」及び「WannaCry」に関連する通信

	想定される通信の目的	備考
通信1	「WannaCry」の感染活動（手法 A）	「WannaCry」の感染活動で用いられる通信には、「Eternalblue」を解析して動作を簡素化した結果が流用された可能性が高いことが判明している[iii]
通信2	「Eternalblue」を悪用した攻撃活動又は脆弱性が存在する機器の探索	同一の発信元 IP アドレスから、通信1及び通信2が連続して観測された場合には、「WannaCry」の感染活動と判断可能
	「Doublepulsar」感染機器に対する攻撃活動又は感染機器の探索	
	「WannaCry」の感染活動（手法 B）	

[i] 「WannaCrypt」、「WanaCrypt0r」、「WanaDecryptor」、「Wcrypt」、「Wcry」等と呼ぶ場合があります。また、メールへの添付等で感染拡大を試みた古いバージョンと区別するため、新しいバージョンのものを特に「WannaCry 2.0」と呼ぶ場合もあります。

[ii] 「第三のプレイヤーがやってきた：「 WannaCry 」の出現」
https://gblogs.cisco.com/jp/2017/05/wannacry/
「ランサムウェア「WannaCry／Wcry」のワーム活動を解析：侵入／拡散手法に迫る」
http://blog.trendmicro.co.jp/archives/14920

[iii] 「WanaCrypt0r Ransomworm」
https://baesystemsai.blogspot.com/2017/05/wanacrypt0r-ransomworm.html

警察庁では、通信1及び通信2を継続して観測しており、その多くは発信元 IP アドレスが同一であることから、「WannaCry」又はその亜種による感染活動が未だに継続しているということがわかります。

しかしながら、12 月以降、通信1と比較して通信2の割合が増加し、通信1とは異なる発信元 IP アドレスからの通信2の観測が散見されるようになりました。このことから、「Eternalblue」を悪用した脆弱性 MS17-010 が未修正の機器を標的とする攻撃活動や、既に「WannaCry」や他の攻撃者によって感染させられた「Doublepulsar」を悪用する攻撃活動が実施されている可能性があります。

以上のことから、Microsoft Windows が稼動している機器を利用している場合には、改めて以下の対策を実施することを推奨します。

- MS17-010 等の 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 を常に最新の状態にしてください。Microsoft Windows XP 等の Microsoft 社のサポート対象期間外の製品についても、「WannaCry」の発生を受けて例外的なパッチ提供[i]が行われています。
- MS17-010 が未適用の Microsoft Windows が稼動している機器を直接インターネットに接続していた場合には、既に「WannaCry」、「Doublepulsar」又はその他のマルウェアに感染し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。
- Microsoft Windows が稼動している機器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 が稼動している機器は、可能であれば 445/TCP 及び 3389/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。直ちに 445/TCP 全体を遮断することが困難な場合には、SMBv1（SMB 1.0）機能を無効にする回避策も検討してください。
- 各組織の管理者は組織内の通信トラフィックを確認し、「WannaCry」の感染拡大活動や、キルスイッチのドメインへの接続等が発生していないか確認してください。また、「Doublepulsar」スキャンツール等を活用して、組織内に「Doublepulsar」に感染した機器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　Oracle WebLogic Server の脆弱性（CVE-2017-10271）を標的とした攻撃活動等の観測

Oracle WebLogic Server は Oracle 社が開発販売するソフトウェア製品であり、Java EE でウェブアプリケーションを作成する際に利用されるアプリケーションサーバです。平成 29 年 10 月 17 日、Oracle 社から Oracle WebLogic Server に存在する脆弱性（CVE-2017-10271）[i] が公表されました。同社は、当該脆弱性が悪用された場合、未認証でネットワーク経由による攻撃が可能としています。

警察庁においては、12 月 23 日以降、国外のウェブサイトに当該脆弱性を悪用する攻撃コードが公開されていることを確認しています。同攻撃コードは、Oracle WebLogic Server が初期設定で管理用ポートとして使用する 7001/TCP に対して細工した HTTP リクエストを送信することにより、サーバ上で不正にコマンドを実行するものでした。

また、同 23 日からは、7001/TCP を宛先ポートとする当該脆弱性を悪用する攻撃活動等も観測しました（図2）。観測した攻撃活動等は、いずれも脆弱性が存在する特定のパスに対する HTTP リクエストであり、以下の2種に大別されました。

- HTTP POST リクエストにより、実際に脆弱性を悪用してサーバ上で不正にコマンド実行を試みる活動
- HTTP GET 又は HTTP HEAD リクエストにより、脆弱性が存在するパスにアクセス可能であるか探索を実施する活動

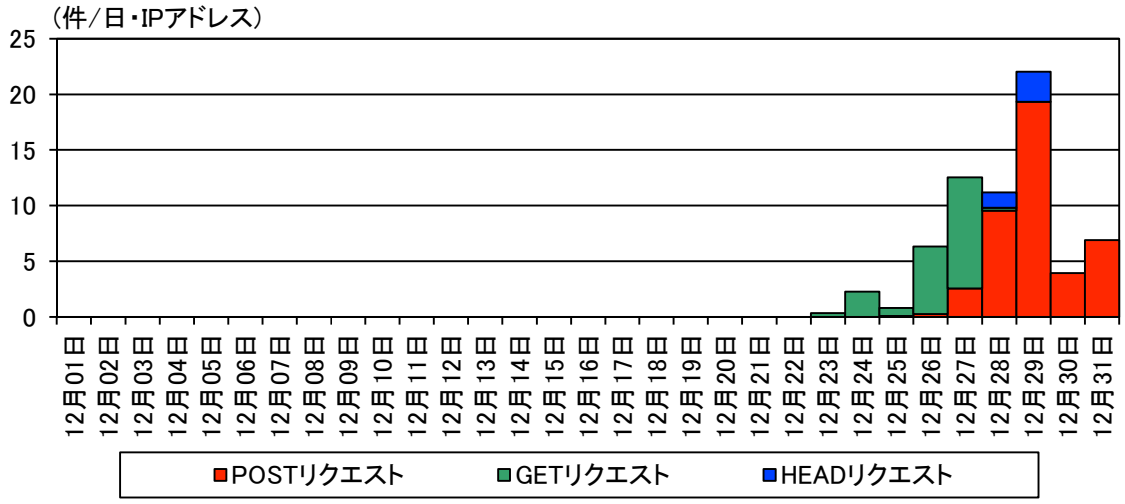

図2　Oracle WebLogic Server の脆弱性（CVE-2017-10271）を悪用する攻撃活動等の推移（HTTP リクエスト別）

[i]「Oracle Critical Patch Update Advisory – October 2017」
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html#AppendixFMW
「Text Form of Oracle Critical Patch Update – October 2017 Risk Matrices」
http://www.oracle.com/technetwork/security-advisory/cpuoct2017verbose-3236627.html#FMW
「JVNDB-2017-008734　Oracle Fusion Middleware の Oracle WebLogic Server における WLS Security に関する脆弱性」
http://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-008734.html

観測した攻撃活動の中には、Linux（UNIX）及び Microsoft Windows の双方で稼動している Oracle WebLogic Server を標的として、外部のウェブサーバからファイルをダウンロードし、更に同ファイルの実行を試みるものも確認できました（図3）。これは、Oracle WebLogic Server が動作するサーバ上で何らかの不正プログラムの実行を企図しているものと考えられます。

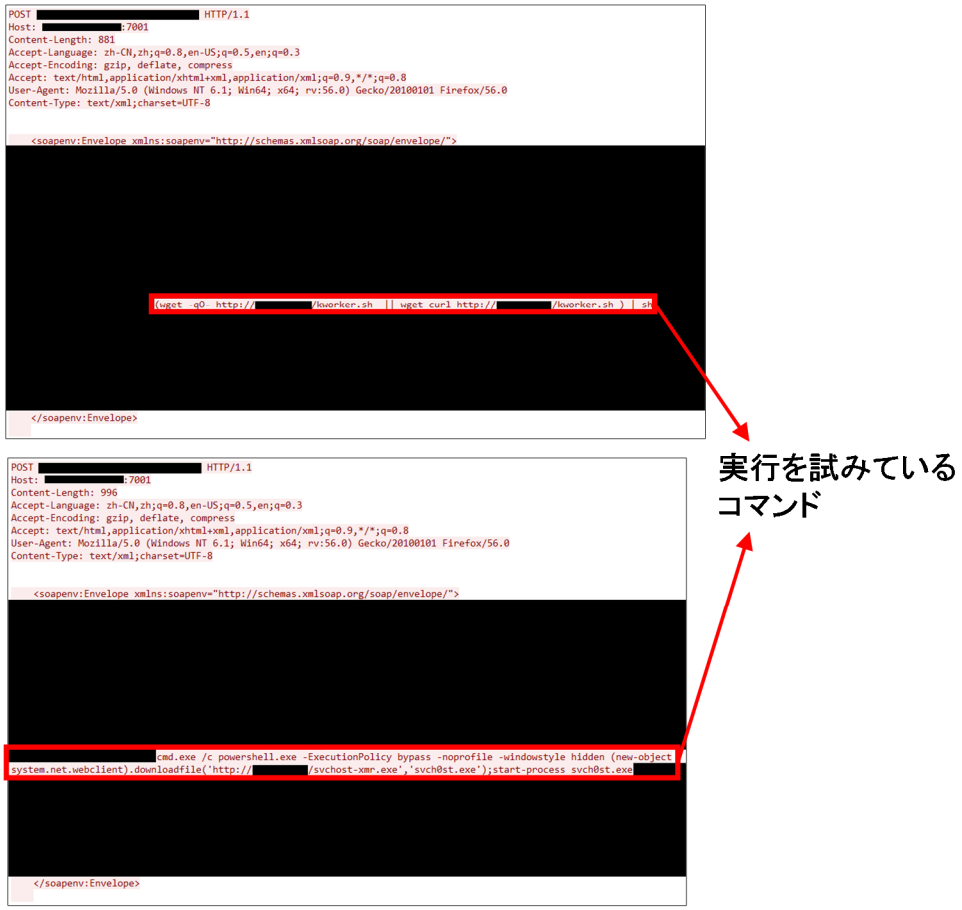

図3　Oracle WebLogic Server の脆弱性（CVE-2017-10271）を標的とした攻撃活動の観測例（上：Linux（UNIX）を標的とするもの、下：Microsoft Windows を標的とするもの。一部をマスキング）

Oracle WebLogic Server を利用している場合には、以下の対策を実施することを推奨します。

- Oracle 社から当該脆弱性の修正プログラムが提供されているので、速やかにアップデートを実施してください。
- Oracle WebLogic Server の管理用に利用される 7001/TCP 等、一般の利用者がアクセスする必要がないポートについては、インターネットからのアクセスを遮断する又は特定の IP アドレスからのみアクセスを許可する等の適切なアクセス制限を実施してください。
- アップデートされないまま管理用ポートがインターネットからアクセス可能となっていた Oracle WebLogic Server は、既に攻撃を受けている可能性があります。該当するサーバ等に不審なプロセス、ファイル及び通信等が存在しないか確認してください。