LAC
ともに、イキル

JAPAN SECURITY OPERATION CENTER

INSIGHT

vol.17

2017年9月25日

JSOC Analysis Team

JSOC JAPAN SECURITY OPERATION CENTER

JAPAN SECURITY OPERATION CENTER

JSOC INSIGHT vol.17

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

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】
2017 年 4 月 1 日 ～ 2017 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。

※本文書の情報提供のみを目的としており、記述を利用した結果生じる、いかなる損失についても株式会社ラックは責任を負いかねます。
※本データをご利用いただく際には、出典元を必ず明記してご利用ください。
(例　出典：株式会社ラック【JSOC INSIGHT vol.17】)
※本文書に記載された情報は初回掲載時のものであり、閲覧・提供される時点では変更されている可能性があることをご了承ください。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

2　エグゼクティブサマリ

本レポートは、集計期間中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。

■　WannaCry の感染事例

システム上の文書、画像、動画などのファイルを暗号化し、それらのファイルの復号を条件として金銭を要求するランサムウェアのひとつである、「WannaCry」に感染したと考えられる重要インシデントを確認しています。WannaCry は感染拡大を試みる機能を有しており、感染した端末は組織の内部ネットワークおよび外部のどちらに対しても感染活動を行います。内部ネットワークのシステムが感染すると、多数のファイルが暗号化され、さらに他のシステムへ感染が広がり、組織の業務に大きな支障をきたす恐れがあります。

WannaCry はセキュリティパッチが公開されている脆弱性を狙っており、かつ無効化を推奨されていた Windows の機能「SMBv1」を介して感染活動を行うことが知られています。今回の事例で、定期的なソフトウェアのアップデート、各種設定の見直しがインシデントを防ぐ鍵となることを再認識させられました。

■　DDoS 攻撃に関連する通信が増加傾向

SNMP、DNS、NTP をはじめとした、DDoS 攻撃の踏み台として利用可能なサービスの探査通信を定常的に検知しています。本探査通信により、外部ネットワークからDDoS攻撃の踏み台として利用できると判明した場合、対象サーバがDDoS攻撃に加担させられる可能性があります。なお、SOCにてNTPの探査通信の検知件数が一時的に急騰していることが確認できており、DDoS 攻撃の準備が行われたと推測しています。

このような探査通信は別のサービスに対しても、継続して発生すると予想されます。また、組織の管理下にあるサーバがDDoS攻撃に加担した場合、社会的な責任を追及される可能性があるため、サーバに対する定期的なセキュリティ診断や設定見直しを実施ください。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

3　JSOC におけるインシデント傾向

3.1　重要インシデントの傾向

JSOC では、ファイアウォール、IDS/IPS、サンドボックス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、攻撃の成功を確認もしくは被害が発生している可能性が高いと判断した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	緊急事態と判断したインシデント ・お客様システムで情報漏えいや Web 改ざんが発生している ・マルウェア感染通信が確認でき、感染が拡大している
	Critical	攻撃が成功した可能性が高いと判断したインシデント ・脆弱性をついた攻撃の成功やマルウェア感染を確認できている ・攻撃成否が不明だが影響を受ける可能性が著しく高いもの
参考インシデント	Warning	経過観察が必要と判断したインシデント ・攻撃の成否を調査した結果、影響を受ける可能性が無いもの ・検知時点では影響を受ける可能性が低く、経過観察が必要なもの
	Informational	攻撃ではないと判断したインシデント ・ポートスキャンなどの監査通信や、それ自体が実害を伴わない通信 ・セキュリティ診断や検査通信

図 1 に、集計期間(2017 年 4 月～6 月)において発生した重要インシデントの件数推移を示します。

本集計期間に発生した重要インシデントの合計件数は、前集計期間の 332 件から増加し、353 件でした。

インターネットからの攻撃により発生した重要インシデントの傾向として、4 月下旬から 5 月上旬にかけて(図 1-①)、OpenSSL の脆弱性(HeartBleed)[1]を悪用した攻撃による重要インシデントが多く発生しました。本重要インシデントが多く発生した主な要因は、新たにご契約いただいたお客様環境で、本脆弱性による重要インシデントが継続して発生したことでした。本脆弱性情報の公開から 3 年が経ちますが、いまだに本脆弱性による重要インシデントが発生しています。本脆弱性は、サーバのログ等から攻撃の有無を確認することが困難であること、さらにサービスの提供そのものには直接影響を及ぼさないため、脆弱性の存在に気付いていない OpenSSL 利用者がまだ数多くいると考えられます。

ネットワーク内部から発生した重要インシデントは、5 月中旬(図 1-②)に多く発生しました。依然とし

[1] JSOC INSIGHT vol.5 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
https://www.lac.co.jp/lacwatch/pdf/20141112_jsoc_n001w.pdf

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

て Ursnif に感染したと考えられる重要インシデントが多く発生しており、同時期に不審なファイルが添付されたメールを多数確認していることから、利用者が不審な添付ファイルを実行し感染したため、件数が増加したものと考えられます。また、WannaCry への感染が疑われる重要インシデントも本集計期間で確認しました。

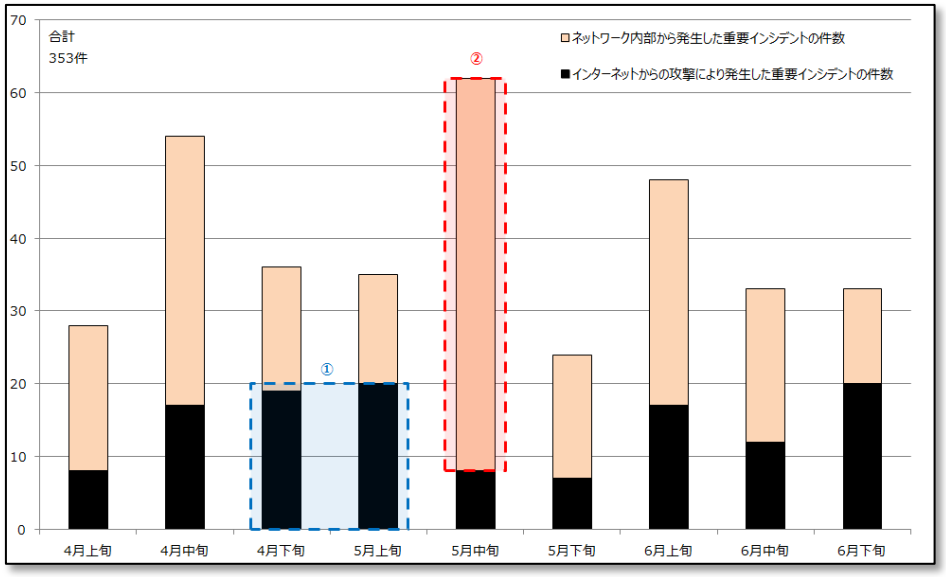


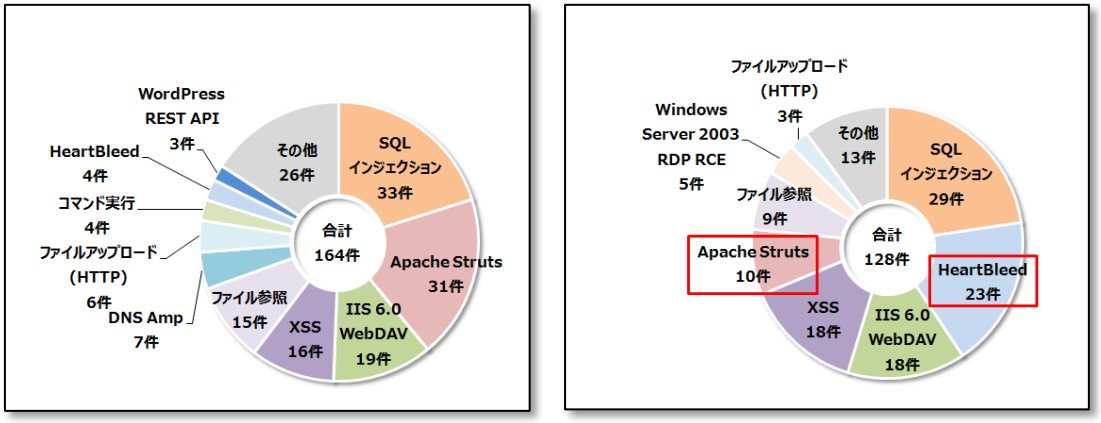
図 1 発生した重要インシデントの件数推移(2017 年 4 月~6 月)

図 2 に、インターネットからの攻撃により発生した重要インシデントの内訳を示します。

インターネットからの攻撃により発生した重要インシデントの件数は、前集計期間の 164 件から減少し、128 件でした。Apache Struts の脆弱性を悪用した攻撃による重要インシデントの件数が減少し、HeartBleed を悪用した攻撃による重要インシデントの件数が増加しました。他の分類においては特徴的な増減は見られませんでしたが、全体的に減少傾向が見られ、前集計期間と比較した件数が減少したと考えられます。

Apache Struts に関する重要インシデントが減少した原因は、前集計期間で多数発生した S2-045 の脆弱性を悪用した攻撃による重要インシデントが、本集計期間で発生しなかったためでした。本脆弱性を悪用した攻撃自体は継続して多数検知していることから、Apache Struts を利用している環境において、本脆弱性への対策が完了したことがうかがえます。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.



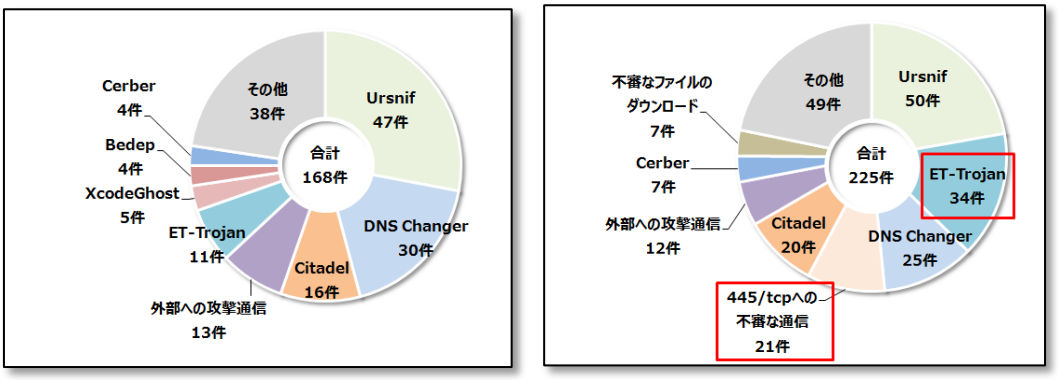
(a) 1～3 月　　(b) 4～6 月

図 2 インターネットからの攻撃により発生した重要インシデントの内訳

図 3 に、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を示します。

ネットワーク内部から発生した重要インシデントの発生件数は、前集計期間の 168 件から増加し、225 件でした。ET-Trojan に感染したことによる重要インシデントの件数が多数増加し、内訳の多くを占めました。また、Ursnif や DNS Changer の感染による重要インシデントも、依然として多く発生しています。

445/tcp への不審な通信に、ランサムウェアのひとつである WannaCry に感染した可能性がある重要インシデントが含まれています。本重要インシデント発生時は、WannaCry 感染時に発生する通信を検知対象としたシグネチャがまだリリースされていませんでした。しかし、特定のサービスが稼動しているホストを探索するスキャン通信を検知対象としたシグネチャが、内部ネットワーク間の通信、及び内部から外部への通信を短時間で多数検知しており、検知状況などから WannaCry に感染した可能性があると判断しました。WannaCry の詳細につきましては、4.1 で紹介します。



(a) 1～3 月　　(b) 4～6 月

図 3 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

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

3.2　注意が必要な通信について

集計期間で注意が必要な通信や、大きな被害には発展していないもののインターネットからの攻撃で検知件数が多い事例について紹介します。

表 2 に、集計期間において多数検知した通信を示します。

表 2 多数検知した通信

概要	JSOC の検知内容	検知時期
110.85.4.102 からの攻撃	前集計期間から引き続き、110.85.4.102(中国)から脆弱性スキャンを検知しました。 4 月中旬に脆弱性スキャンは収束したものの、5 月の上旬に同送信元からの不審なファイルのアップロードを試みる攻撃を検知しました。	1 月下旬～ 4 月中旬、 5 月上旬
Disk Sorter に存在するバッファオーバーフローの脆弱性を悪用した攻撃	4 月中旬に、Disk Sorter Enterprise に存在するバッファオーバーフローの脆弱性(CVE-2017-7230)を悪用した攻撃を検知しました。本ソフトウェアに存在するオーバーフローの脆弱性に関する PoC は複数公開されており、GET メソッドを使用した PoC[2]と検知内容が一致しました。検知した攻撃の多くは 79.135.55.204(イタリア)から発生しており、インターネットに公開されている IPv4 アドレスに対して総当りに攻撃を実施しているように見受けられました。	4 月中旬
SSH に関するファイルの参照	5 月上旬に、SSH に関する設定不備を狙ったファイル参照を検知しました。 参照の対象は、SSH における秘密鍵の保存先として一般的に使用される、.ssh/id_rsa や.ssh/id_dsa といったパスの参照を特に多く検知しました。	5 月上旬

[2] Disk Sorter Enterprise 9.5.12 – 'GET' Buffer Overflow(SHE)
https://www.exploit-db.com/exploits/41666/

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

概要	JSOC の検知内容	検知時期
183.129.160.229 からの攻撃	5 月上旬に、183.129.160.229(中国)から S2-045 や HeartBleed の脆弱性を悪用した攻撃を検知しました。 また、5 月中旬に公開された、Joomla!に存在する SQL インジェクションの脆弱性(CVE-2017-8917)[3]を悪用した攻撃も脆弱性情報の公開直後から検知しました。この送信元だけでなく、脆弱性情報が公開された直後は該当の攻撃通信を多数検知する傾向があるため、注意が必要です。	5 月上旬～中旬
185.22.187.227 からの攻撃	5 月中旬に、185.22.187.227(トルコ)から WordPress REST API の脆弱性[4]を悪用した攻撃を検知しました。	5 月中旬
36.62.162.205 からの攻撃	5 月下旬に、36.62.162.205(中国)から脆弱性スキャンを検知しました。検知内容から、Web アプリケーション脆弱性スキャナである NetSparker を使用していると考えます。	5 月下旬

[3] Joomla! Developer Network Security Announcements [20170501] – Core – SQL Injection
https://developer.joomla.org/security-centre/692-20170501-core-sql-injection.html

[4] JSOC INSIGHT vol.16 4.1 WordPress REST API の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20170704_jsoc_j001t.pdf

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

4　今号のトピックス

4.1　WannaCry の感染事例

2017 年 5 月 12 日より、WannaCry と呼ばれる[5]マルウェアへの感染が世界規模で発生しました[6]。WannaCry はランサムウェアの一種であり、感染拡大を行うワームの特徴を持ちます。これまで確認されたランサムウェアは、メールの添付ファイルや不正な Web アクセス(ExploitKit 等)を感染経路とするものが一般的でした[7]。しかしながら、WannaCry は Windows の SMB サービスに存在する脆弱性(CVE-2017-0144)を悪用し、ネットワーク経由で感染を拡大するワーム機能を有していました。本脆弱性を含む MS17-010 の脆弱性に対する修正プログラムを適用していない端末が、インターネットから接続可能な状態で稼動していたため、大規模な感染に繋がった可能性が考えられます。SOC においても、WannaCry の感染活動と推測される通信を検知し、重要インシデントとしてお客様へ連絡しています。

4.1.1　WannaCry で確認されている挙動について

WannaCry は、以下の動作を行うことが各ベンダより報告されています[8,9]。

■　サンドボックスなどの動的解析回避

自身が解析環境で実行されているかを判別するために、存在しないドメインへのアクセスを試みます。サンドボックスなどの解析環境では、存在しないドメインへのアクセスに対して、何らかのレスポンスを返すネットワークを構成することがあるためです。

この動作を逆手にとると、特定のドメインにアクセスができれば WannaCry を停止させることができます。そのため、WannaCry が通信を行う未登録のドメインを研究者らが取得し、Sinkhole 化させる動きがありました。今回 Sinkhole 化されたドメインは WannaCry のキルスイッチ・ドメイン[10]とも呼ばれています。

---

5 Wana Decrypt0r、WannaCryptor、WCRY 等とも呼ばれる。

6 Indicators Associated With WannaCry Ransomware
https://www.us-cert.gov/ncas/alerts/TA17-132A

7 JSOC INSIGHT vol. 11 4.2 ランサムウェア感染通信の検知について
https://www.lac.co.jp/lacwatch/pdf/20160517_jsoc_m001t.pdf

8 マルウェア解析奮闘記 WannaCry の解析
http://blog.macnica.net/blog/2017/05/wanacry-8ff1.html

9 ランサムウェア「WannaCry」対策ガイド rev.1
https://www.lac.co.jp/lacwatch/report/20170519_001289.html

10 Player 3 Has Entered the Game: Say Hello to 'WannaCry'
http://blog.talosintelligence.com/2017/05/wannacry.html

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

■　ファイルの暗号化および身代金の要求

文書、画像、動画、データベースなどの 170 種類以上の拡張子のファイル[11]を暗号化し、ファイル名の末尾に「.WNCRY」という文字列を追加します。その後、身代金を要求する画面(図 4)を表示します。

図 4　WannaCry 感染時の身代金を要求する画面

■　Tor 利用による通信の秘匿化

ファイルの暗号化キーを C2 サーバへ送信します。WannaCry の C2 サーバは「.onion」ドメインで作成されているため、Tor ブラウザをダウンロードし、Tor 経由でのアクセスを行います。

■　ネットワーク経由での感染拡大

WannaCry の感染活動には The Shadow Brokers(TSB)が 2017 年 4 月に公開したツール「ETERNALBLUE」とバックドア「DoublePulsar」を使用します。ETERNALBLUE は Microsoft Windows で実装されている Server Message Block(SMB)サービスにおける任意コード実行可能な脆弱性 CVE-2017-0144 を悪用します。なお、TSB が公開したツール群や機密情報などについては後述の付録 1　を参照ください。

[11] WCry/WanaCry Ransomware Technical Analysis
https://www.endgame.com/blog/technical-blog/wcrywanacry-ransomware-technical-analysis

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

図 5[12]に WannaCry による感染拡大の概要を示します。

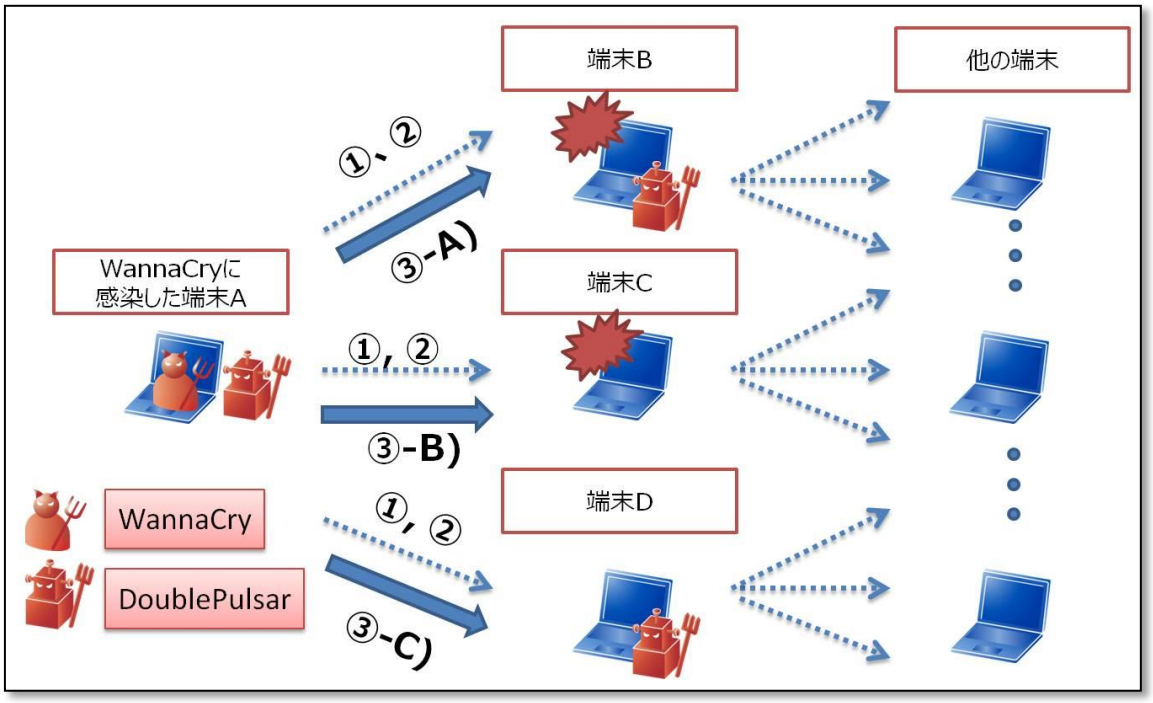


図 5 WannaCry の感染拡大概要

① 445/tcp への接続可否を調査する
② ①の調査にて、接続できる場合、以下の追加調査を行う
- SMB サービスの脆弱性(CVE-2017-0144)の存在確認
- DoublePulsar の存在有無

③ ②の調査の結果により、以下の動作を行う

A) 脆弱性が存在し、すでに DoublePulsar が設置されている場合
DoublePulsar 経由で WannaCry を作成、実行する

B) 脆弱性が存在するが、DoublePulsar は設置されていない場合
脆弱性を悪用し、DoublePulsar を設置した後、WannaCry を作成、実行する

C) 脆弱性は解消されているが、すでに DoublePulsar が設置されている場合
DoublePulsar 経由で WannaCry を作成、実行する
脆弱性は解消され、かつ DoublePulsar が設置されていない場合
該当端末への感染はせず、別端末の調査行為(①、②)を再開する

[12] WannaCry 2.0（＋亜種)におけるワーム活動の詳細と残存する DoublePulsar について
http://www.mbsd.jp/blog/20170629.html

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

WannaCry に感染した端末は、ネットワーク上に存在する他の端末に対して ETERNALBLUE を使用して感染拡大を試みます。組織内のネットワークだけでなく外部ネットワークに対しても感染活動が行われるため、急速な感染拡大が発生したと考えられます。

4.1.2 WannaCry の感染通信の検知事例

図 6 に 4 月 1 日から 6 月 30 日までの 445/tcp に対するポートスキャンの検知件数を示します。WannaCry の情報が公開された 5 月 12 日直後に、ポートスキャンの検知が急増しました。これは特定のお客様において WannaCry の感染拡大活動が多く発生したためです。お客様の対処が完了した後も、5 月 12 日以前と比較してポートスキャンの検知件数は多く発生しており、WannaCry の亜種の活動、もしくは攻撃者の調査活動が活発化したと考えられます。

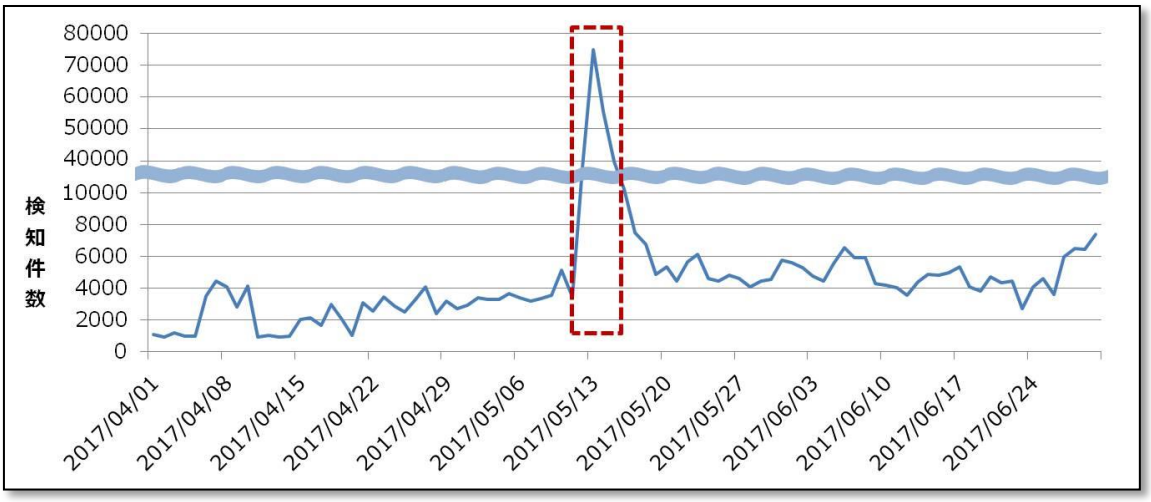
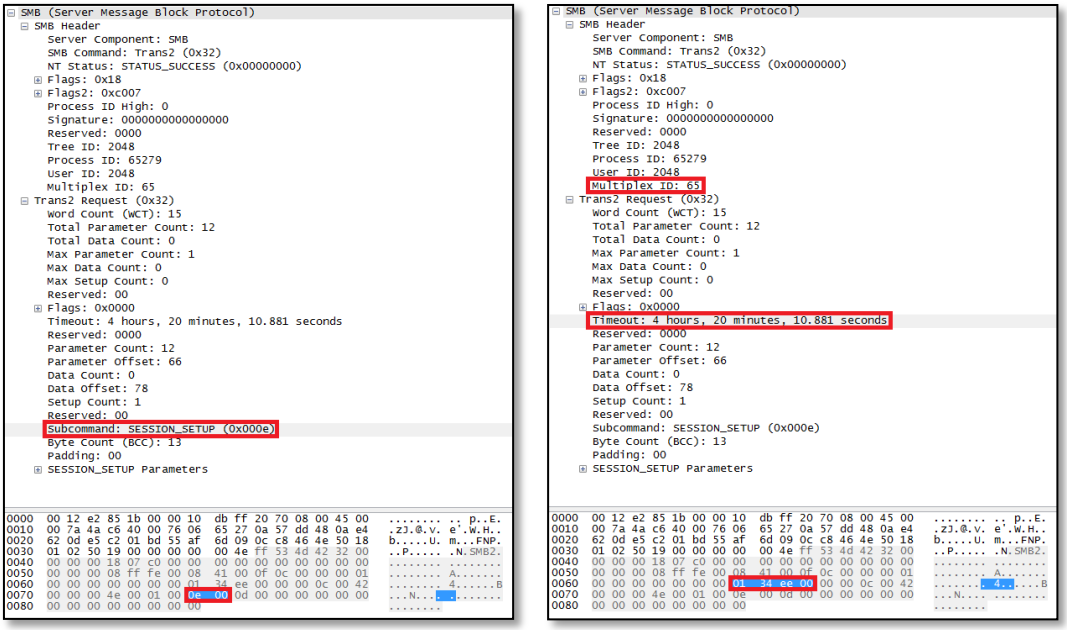


図 6 445/tcp ポートスキャンの検知件数推移

お客様環境において、内部ネットワーク間および内部ネットワークから外部ネットワーク宛に、445/tcp への不審な通信を短期間に多数検知しました。このような検知状況は、何らかのマルウェアに感染した可能性があることから、重要インシデントと判断しています。その後、WannaCry 感染時の通信や ETERNALBLUE 実行時の通信を検知するシグネチャが追加されました。シグネチャの追加後、お客様環境において図 7 で示す 445/tcp への不審な通信を検知しました。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

図 7 は、図 5 ①において発生する通信の一部で、DoublePulsar が設置されているかを確認する通信です。この通信は、SMB 通信では通常使用しないコマンド(TRANS2_SESSION_SETUP) [13]を用いており [図 7 (a)]、Timeout フィールドおよび Multiplex ID フィールド [図 7(b)]の値を利用し、バックドアに対して命令を送信します。



(a) SESSION_SETUP サブコマンド　　(b) Multiplex ID および Timeout 値

図 7 TRANS2_SESSION_SETUP サブコマンドによるバックドアの確認

Timeout フィールドに記述された値は以下の式により、3 種類の命令としてデコードされます[14]。

$$0\text{xff}\,\&\left((x)+(x>>8)+(x>>16)+(x>>24)\right)=\begin{cases}0\text{x23} & (\text{バックドアの存在確認})\\ 0\text{xc8} & (\text{コード実行})\\ 0\text{x77} & (\text{バックドアの削除})\end{cases}$$

[13] 2.2.6.15 TRANS2_SESSION_SETUP (0x000E)
https://msdn.microsoft.com/en-us/library/ee441654.aspx

[14] BROKERS IN THE SHADOWS: Analyzing vulnerabilities and attacks spawned by the leaked NSA hacking tools
https://blog.checkpoint.com/2017/05/25/brokers-shadows-analyzing-vulnerabilities-attacks-spawned-leaked-nsa-hacking-tools/

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

図 7 の Timeout フィールドの値である「01 34 ee 00」を上記の式に当てはめた場合、計算結果が 0x23 となるため、当該通信はバックドアが存在しているかを確認する通信であることがわかります。図 7 のような通信が組織内の端末より大量に発生している場合、WannaCry の感染拡大活動を行っている可能性が高いと考えます。SOC では、内部ネットワーク間の当該通信を検知しており、かつ内部ネットワーク間および内部ネットワークから外部ネットワーク宛に、445/tcp への不審な通信を短期間に多数検知していたため、当該通信を重要インシデントと判断しています。

Multiplex ID フィールドは、実行する命令コードに対する応答内容の取得に用います。0x41 を Multiplex ID フィールドの値として命令コードを送信することで、バックドアの存在確認の場合には、Multiplex ID フィールドの値が 0x41 に対して、0x51 として返ってくるとバックドアが存在していることを示します。同様に 0x41 に対して、0x41 が返ってくるとバックドアが存在していないことを示します。

4.1.3 WannaCry の対策

WannaCry 感染拡大時に悪用される MS17-010 の対象範囲を表 3 に示します。WannaCry による影響の大きさを考慮して、サポートが終了した Windows XP と Windows Server 2003 のセキュリティ更新プログラムが Microsoft 社により例外的に公開されています[15]。このセキュリティ更新プログラムを適用していない場合、WannaCry およびその亜種に感染する可能性があります。

表 3 MS17-010 の対象範囲

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

WannaCry の対策を以下に示します。MS17-010 の対象範囲の Windows を利用している場合、可能な限り早期に対策することを推奨します。

[15] 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/

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

【WannaCry への対策】

- MS17-010 のセキュリティ更新プログラム[16]を適用し、再起動を行う
- ウイルス対策製品の定義ファイルを最新の状態にする
- SMBv1 を無効化する

WannaCry は DoublePulsar を利用して感染拡大を行うランサムウェアです。よって、組織の内部ネットワーク上のシステムが感染した場合、内部感染が拡大し多数のシステム上のファイルが暗号化されることで組織の業務に多大な影響を与えます。また、WannaCry の亜種や同種の自動感染型のランサムウェアが確認されており[17]、DoublePulsar の新バージョンをマルウェア感染に用いるバックドアとして利用する例も報告されています[18]。加えて、DoublePulsar とは別種のバックドアが設置されている可能性もあります。そのため、以下で示す WannaCry だけに限らず、マルウェアへの根本的な対策が必要です。

【WannaCry などのマルウェアへの根本的な対策】

- サポートが終了した OS を使用しない
- 最新バージョンのソフトウェアを利用する
- 内部端末から異常なトラフィックが発生していないか、ネットワーク監視を行う
- ウイルス対策ソフトにて定期検査を行う
- 不要なサービスポートを公開しない

WannaCry の対策およびその他の根本的な対策については、対策ガイドを公開しています[19]。本レポートと併せてご参照ください。

---

16 マイクロソフト セキュリティ情報 MS17-010 - 緊急
https://technet.microsoft.com/ja-JP/library/security/ms17-010.aspx

17 WannaCry の危機再び。新たな拡大感染型ランサムウェア GoldenEye/Petya が全世界で拡散中。
https://www.lac.co.jp/lacwatch/people/20170628_001319.html

18 NSA から流出したバックドアの進化版、Petya の DoublePulsarV2.0 を分析する
http://www.checkpoint.co.jp/threat-cloud/2017/07/brokers-shadows-part-2-analyzing-petyas-doublepulsar v2-0-backdoor.html

19 ランサムウェア「WannaCry」対策ガイド rev.1
https://www.lac.co.jp/lacwatch/report/20170519_001289.html

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

4.2 DDoS 攻撃に関する通信の検知傾向

UDP によるサービスを踏み台とした DDoS 攻撃の準備段階として、踏み台に利用可能な DNS や NTP、SNMP などのサービスが稼動しているホストを、攻撃者が定常的に探査していることが検知傾向からわかります。本集計期間において、探査に関する通信のうち、NTP の monlist 機能が有効になっているサーバを探査する通信の検知件数が急激に増加しました。また、DDoS 攻撃の機能を有している、IoT 機器に感染しボットネットを構築するマルウェア Mirai[20]に感染させる攻撃も増加しました。

4.2.1 UDP によるサービスを踏み台とした DDoS 攻撃の概要

図 8 に、UDP によるサービスを踏み台とした DDoS 攻撃として、アンプ攻撃(リフレクター攻撃)[21]の概要を示します。

UDP の通信はセッションの確立を行わないため、容易に送信元を偽装できます。そのため、攻撃者は踏み台ホストに対して、送信元 IP アドレスを DDoS 攻撃の対象である IP アドレスに偽装したリクエストを送信することで、踏み台ホストからのレスポンスを攻撃対象のホストへ送信させるリフレクター攻撃が可能です。

リフレクター攻撃の踏み台として利用されるサービスの代表例として、DNS や NTP、SNMP などのサービスが挙げられます。これらのサービスは、主に UDP を使用していることからリフレクター攻撃の踏み台として利用可能な場合が多い他、リクエストに対するレスポンスの通信量が大きい(増幅率が高い)ため、探査の対象とされています。このような増幅率の高いサービスを踏み台として利用することにより、DDoS 攻撃の効率を向上させた攻撃をアンプ攻撃といいます。

[20] JSOC INSIGHT vol.14 4.1 IoT 機器の乗っ取りを試みる攻撃の検知
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

[21] 技術解説：「DNS Reflector Attacks(DNS リフレクター攻撃)」について
https://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

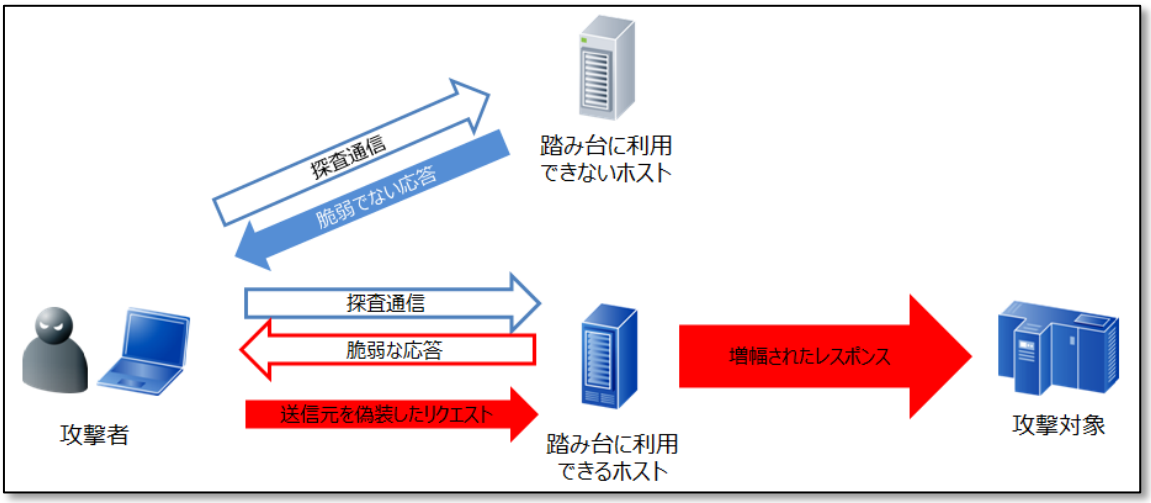


図 8 UDP によるサービスを踏み台としたアンプ攻撃(リフレクター攻撃)

4.2.2 アンプ攻撃に関する検知事例

表 4 に、アンプ攻撃に関する検知事例を示します。

本集計期間において、DNS および SNMP のサービスを利用したアンプ攻撃に関する通信の検知件数は、大きな増減が見られませんでした。しかし、NTP サービスの monlist 機能に対する探査通信は、検知件数が多数増加しました。

表 4 リフレクター攻撃およびアンプ攻撃に関する検知事例

サービス	探査通信の概要と検知状況	増幅率
DNS	外部から再帰問い合わせを試みるリクエストや、外部へのサイズの大きいレスポンスを検知しています。外部からの再帰問い合わせが可能な状態になっている場合、非常に高い増幅率のレスポンスが発生する可能性があります。	数十倍 ～数百倍
NTP	ntpd に実装されている monlist 機能に対するリクエストを検知しています。monlist は、過去に行った NTP 通信の一覧を返す機能です。本機能が有効な場合、非常に高い増幅率のレスポンスが発生する可能性があります。	数十倍 ～数百倍
SNMP	外部へのサイズの大きいレスポンスを検知しています。踏み台として利用する条件として、サービスが外部に公開されている他、コミュニティ名が判明しているといった追加条件が必要ですが、デフォルトの設定で運用されている場合が多く見受けられます。上記の条件を満たした場合、非常に高い増幅率のレスポンスが発生する可能性があります。	～数千倍

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

図 9 に、NTP サービスの monlist 機能に対するリクエストの件数推移を示します。
6 月 2 日から 3 日(図 9-①)の短い期間にのみ検知件数が増加しました。

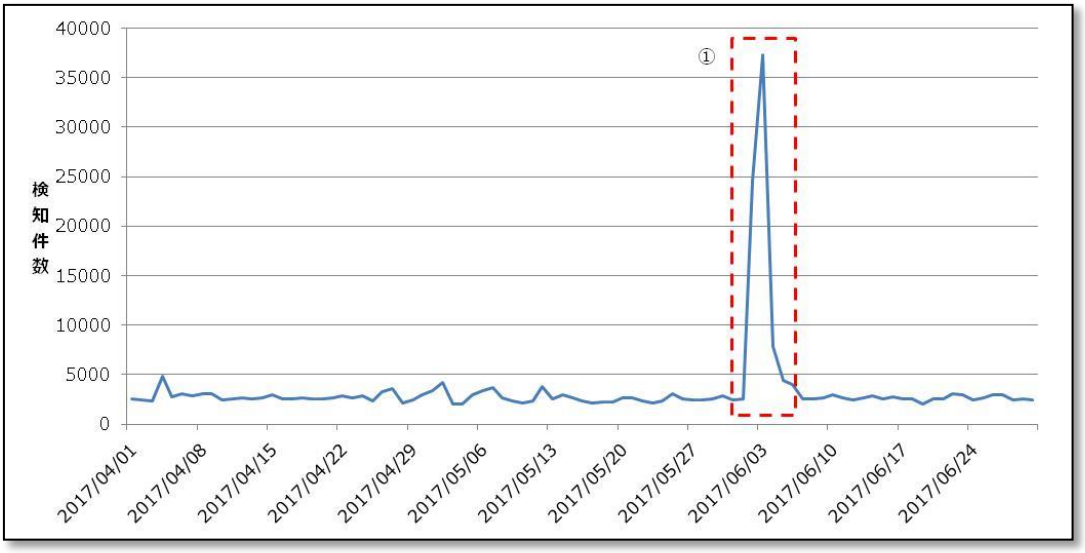


図 9 NTP サービスの monlist 機能に対するリクエストの件数推移

図 10 に、検知件数が増加した期間(図 9-①)の monlist リクエストについて、送信元 IP アドレスの保有国ごとで件数を集計した結果を示します。

検知件数の増加した期間におけるリクエストは、9 割以上が中国に割り当てられている IP アドレスを送信元としており、中国からのリクエストが 6 月 2 日から 3 日までの期間で大幅に増加していました。本リクエストのいずれにおいても、同一送信元から長時間の継続検知が確認されず、サイズの大きいレスポンスの検知も確認されなかったため、DDoS 攻撃の踏み台として利用するためのリクエストではなく、DDoS 攻撃の踏み台として利用可能なホストを探査する通信であると考えます。増加した探査通信の送信元 IP アドレスによる検知実績を調査したところ、過去に不審な通信の検知が確認できないことから、本期間においてのみ、踏み台として利用可能なホストを探査したものと考えられます。その他の国は、検知件数が増加する前の 6 月 1 日から 3 日間の検知件数に大きな件数の変化は見られませんでした。なお、政治、事案などの状況によって、このような DDoS 攻撃や探査が増加することがありますが、今回は本事象に関連するニュースや統計情報等は、公開情報からは確認できておりません。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

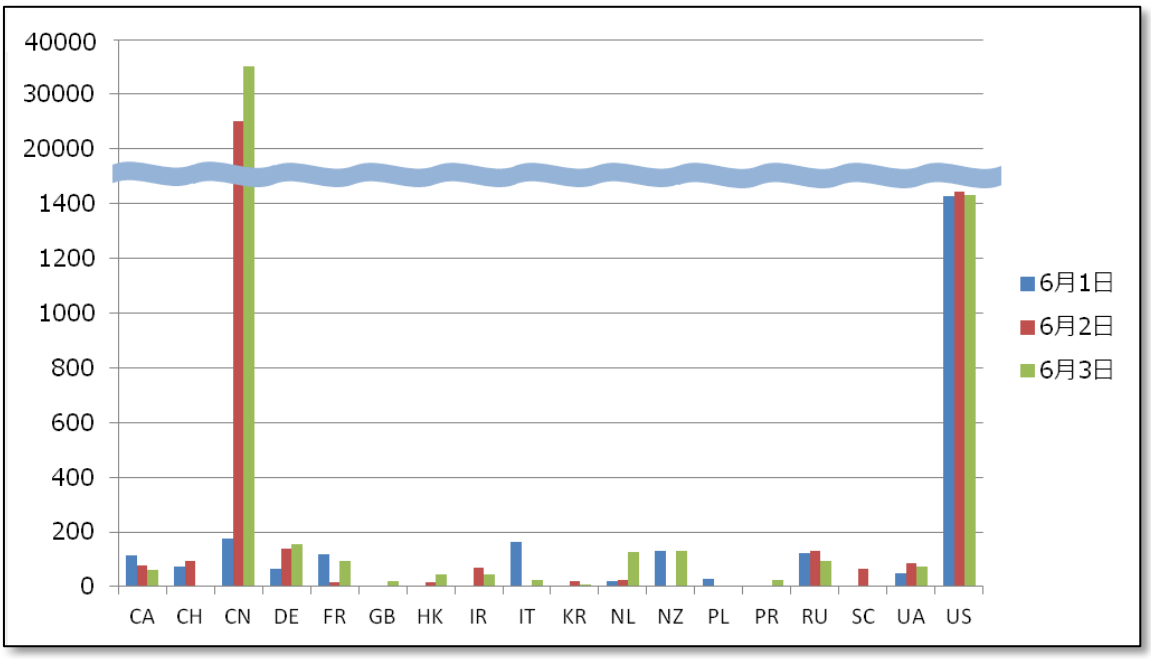


図 10 検知件数増加期間における送信元 IP アドレス保有国ごとの検知件数推移

4.2.3 Mirai に感染させる攻撃の検知傾向

SOC において、IoT 機器を悪用するマルウェア「Mirai」による攻撃通信が、6 月 20 日以降に検知件数が増加していることを確認しました。その 9 割以上の送信元が中国に割り当てられている IP アドレスであり、セキュリティ対策に不備のある中国製品が国内にて広く出回っていることが、原因の一つとして考えられます。図 11 に Mirai に関する攻撃の検知件数を示します。

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

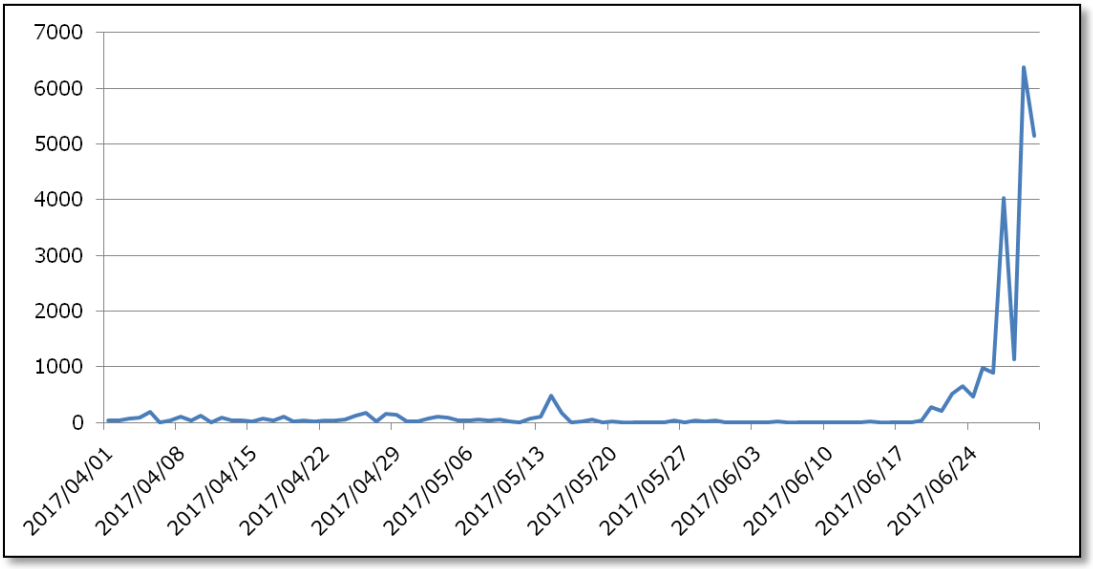


図 11 Mirai に関する攻撃の検知傾向

また、Mirai の感染拡大を試みる通信の特徴として、攻撃対象の IP アドレスをランダムに選択する点と試行回数が少ない点が挙げられます。SOC 全体において、単一送信元から複数の送信先に対する攻撃を検知していない点と、執拗な攻撃を行わず複数回の検知がない点から、今回増加した通信は感染拡大を試みる通信を検知したものと考えられます。

4.2.4 対策

DDoS 攻撃に関しては、DDoS 攻撃の被害者となるだけではなく加害者となってしまう場合があります。そのため、DDoS 攻撃に加担してしまわないための対策が必要です。IoT 機器を活用する上での対策は JSOC INSIGHT Vol.14 を参照ください。

【UDP によるサービスを踏み台とした DDoS 攻撃への対策】

- サービスを意図せず外部へ公開していないか確認する
  - 外部へ公開する必要がある場合はアクセス制限を実施する
  - サービスに認証が実装されている場合、推測が困難な認証情報を設定する
- 公開しているサービスに関する脆弱性情報が公開されていないか確認する
- 内部から外部への不審なトラフィック増がないか確認する

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

付録 1 The Shadow Brokers が公開した検証コードの数々

2016 年 8 月、「The Shadow Brokers(TSB)」と名乗るハッカー集団が複数の検証コードを公開しました。これらの検証コードにはアメリカ国家安全保障局(NSA)がハッキングに利用したとされるツールも含まれており、注目が集まりました。とくに、Cisco 社製品のコード実行の脆弱性(通称:EXTRABACON)はゼロデイ攻撃として悪用される懸念があったため、SOC から注意喚起を行いました[22,23]。

EXTRABACON の情報公開を封切りに、TSB は手に入れた情報を数回に分けて公開しました。主な情報公開の内容を表 5 に示します。

表 5 The Shadow Brokers が公開した情報一覧

公開日	タイトル	主な検証コード、公開した情報
2016/08/13	Equation Group Cyber Weapons Auction - Invitation	・ EPICBANANA ・ EXTRABACON
2016/10/31	Message #5 - TrickOrTreat	・ NSA がハッキングしたサーバリスト ・ ハッキングに使用したツール群
2016/12/14	Message #6 - BLACK FRIDAY / CYBER MONDAY SALE	・ ツール一覧のスクリーンショット
2017/04/10	Don't Forget Your Base	・ 2016/08 に公開したツール群の解凍パスワード
2017/04/14	Lost in Translation	・ ETERNALBLUE ・ ESTEEMAUDIT ・ EXPLODINGCAN ・ DoublePulsar

5 番目の公開情報「Lost in Translation」には、4.1 で取り上げた WannaCry の感染を拡大するために用いられた ETERNALBLUE を含みます。Lost in Translation にて公開された主な検証コードを表 6 に示します。

[22] Cisco 社製品における SNMP の脆弱性（CVE-2016-6366）について
https://www.lac.co.jp/lacwatch/people/20160823_000399.html

[23] JSOC INSIGHT vol.14 第 4 章 4.2 Cisco 社製品のコード実行の脆弱性（CVE-2016-6366）について
https://www.lac.co.jp/lacwatch/pdf/20170110_jsoc_j001t.pdf

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

表 6 Lost in Translation にて公開した主な検証コード

コードネーム	悪用する脆弱性	攻撃対象のサービス
ETERNALBLUE	MS17-010	SMB (445/tcp)
ETERNALCHAMPION		
ETERNALROMANCE		
ETERNALSYNERGY		
ESTEEMAUDIT	CVE-2017-9073	RDP (3389/tcp, udp)
EXPLODINGCAN[24]	CVE-2017-7269	WebDAV (80/tcp, 443/tcp)

表 6 のうち、ETERNALBLUE、ESTEEMAUDIT、EXPLODINGCAN の 3 種が対応している脆弱性を狙った攻撃については、SOC にて通信の検知実績があります。

図 12 に、ESTEEMAUDIT の検証コードを利用したと考えられる通信の検知例を示します。
実際に SOC の検証環境下にて検証コードを実行した際にも、図 12 の赤枠部が見受けられたため、本通信は TSB が公開したツールを利用したものであると判断できます。

今回 4.1 にも取り上げた WannaCry を筆頭に、今後も TSB の検証コードやペイロードが基となる攻撃ツールやマルウェアが猛威を振るう状況が容易に想定できます。2017 年 6 月より、TSB は「TheShadowBrokers Monthly Dump Service」と命名し、月額制で情報公開するサービスを展開しました。この情報を購入したユーザも存在[25]しており、販売された情報をベースとしてゼロデイ攻撃が行われるなどの状況が推測されるため、今後も注目して情報収集しておくべきハッカー集団の一つといえます。

[24] JSOC INSIGHT vol. 16 第 4 章 4.3 IIS 6.0 の WebDAV 機能における任意コード実行の脆弱性
https://www.lac.co.jp/lacwatch/pdf/20170704_jsoc_j001t.pdf

[25] TheShadowBrokers are NOT Making America Great again!!!
https://steemit.com/shadowbrokers/@fsyourmoms/theshadowbrokers-are-not-making-america-great-again

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

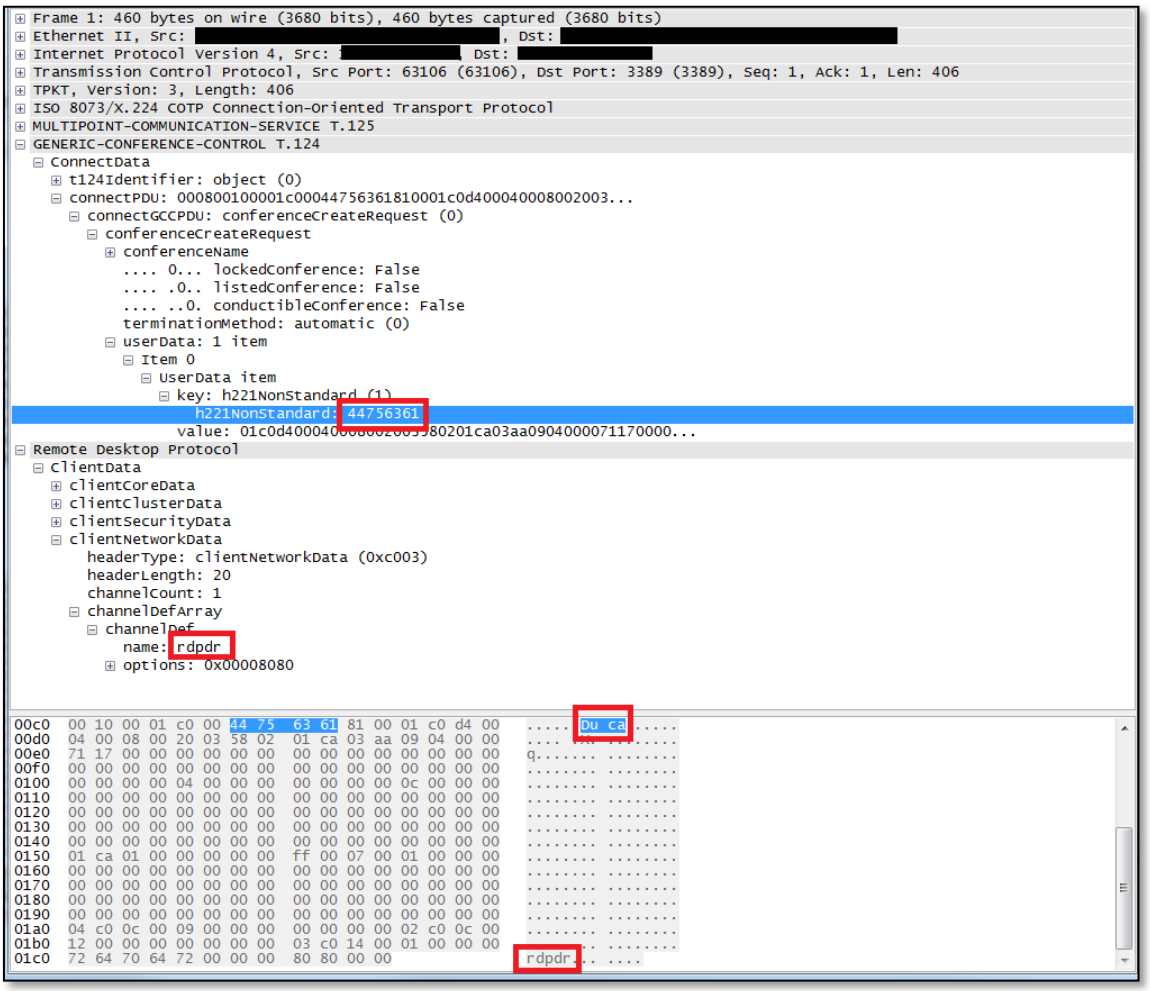


図 12 ESTEEMAUDIT と考えられる通信の検知例

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

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.17
【執筆】
阿部 翔平 / 久米 潤一郎 / 園田 真人 / 髙井 悠輔
(五十音順)

Copyright© 2017 LAC Co., Ltd. All Rights Reserved.

JSOC

JAPAN
SECURITY OPERATION
CENTER

LAC ともに、イキル

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
TEL：03-6757-0113（営業）
E-MAIL：sales@lac.co.jp
https://www.lac.co.jp/

LAC、ラックは、株式会社ラックの商標です。JSOC(ジェイソック)、
JSIG(ジェイシグ)は、株式会社ラックの登録商標です。

その他、記載されている製品名、社名は各社の商標または登録商標です。