公開レポート

NTT DATA
Global IT Innovator

【緊急レポート】
大規模ランサムウェア感染について v1.2

株式会社NTTデータ　セキュリティ技術部　情報セキュリティ推進室
NTTDATA-CERT

2017年5月22日

© 2017 NTT DATA Corporation

目次

© 2017 NTT DATA Corporation

エグゼクティブサマリ

- 2017年5月12日から、ランサムウェア感染の世界的な拡大が報告されている。

- 被害状況（5/22時点）
  - 世界中で、150か国/30万台以上のコンピュータが感染。
  - 日本国内で、2000件の感染が判明。
  - 支払われた身代金は、総額10万1000ドル。

- 攻撃情報
  - 攻撃対象：ポート445/tcpが開いている、かつSMB※ v1が有効、かつ脆弱性CVE-2017-0145を修正するパッチMS17-010が適用されていないWindows端末
  - 攻撃手法：感染経路の全容は不明。ネットワーク経由で感染を広げる。端末上のファイルを暗号化し、300ドル相当のビットコインの支払いを要求する。
  - ランサムウェア：WannaCry（別名WannaCrypt、WannaCryptor、Wcry等）

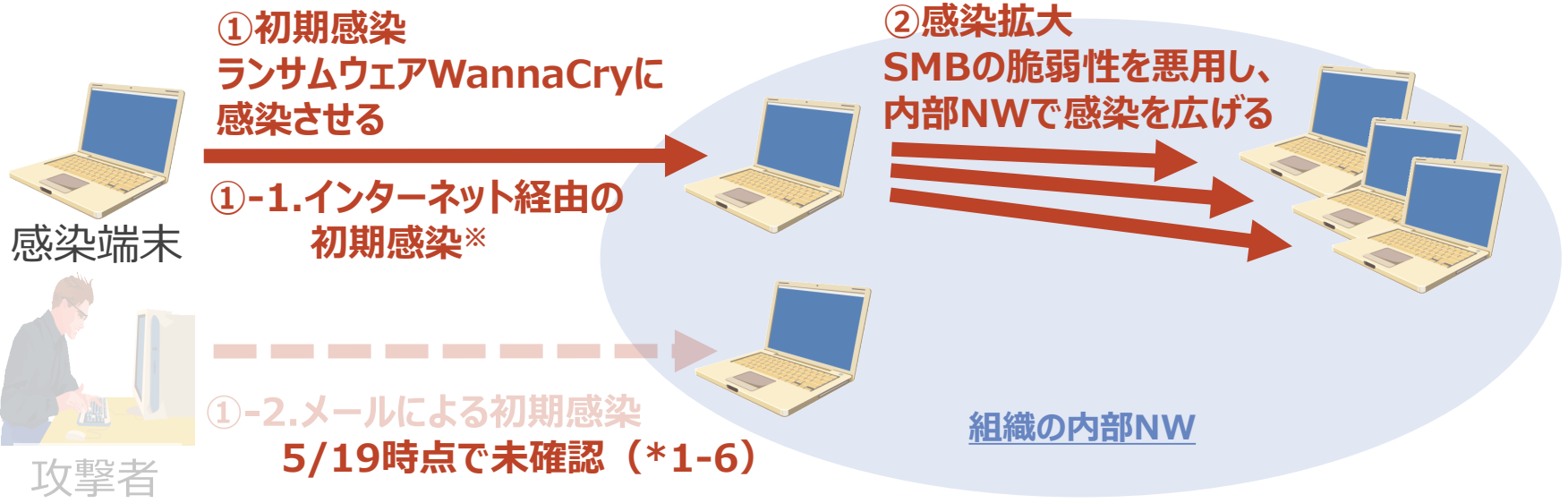
  ※SMB(Server Message Block)：Windows OSにおけるファイル共有プロトコル

- 推奨される対策
  - Windowsセキュリティパッチの最新化(MS17-010は必須)
    - ✓ 困難な場合は、SMBv1を無効化
  - 不審メールを開封しない
  - 公式サイト以外のサイトからソフトウェアをダウンロードしない

© 2017 NTT DATA Corporation

1. 本攻撃の全体像と攻撃手法

感染経路については、セキュリティベンダ等から調査報告が公開されているが、全容解明には至っていない。複数組織の調査報告から読み取れる内容をまとめ、下図に示す。（*1-1、*1-2、*1-3）



※ 持ち出し端末がモバイル接続で感染した事例報告有り。（*1-5）

攻撃対象

- ✓ ポート445/tcpが開いている、かつSMB v1が有効、かつ脆弱性CVE-2017-0145を修正するパッチMS17-010が適用されていないWindows端末（*1-7）
- ✓ Windows 10は本攻撃の影響を受けない。攻撃コードが動作しないため。（*1-4）

© 2017 NTT DATA Corporation

2. ランサムウェア感染の経緯

凡例： 関連組織の動き インシデント事例

2016/9/16	マイクロソフト、公式ブログでSMB v1のセキュリティの問題を説明して利用停止を推奨 (*2-13)
2017/1/16	米US-CERT、SMBのセキュリティ・ベストプラクティスを公開 (*2-14)
2017/3/14	マイクロソフト、SMB v1の脆弱性を修正するMS17-010を公開 (*2-15)
2017/4/14	ハッカー集団Shadow Brokersが、SMB v1を悪用するバックドアツール「Doublepulsar」を公開。4/24までに数万～十数万件が感染 (*2-18)
2017/5/12	スペインCCN-CERT、米US-CERT、WannaCryの攻撃キャンペーンについて注意喚起（*2-19、*2-20）
	マイクロソフト、修正プログラム「MS17-010」を、サポート終了済みのWindows XP、8、Server 2003向けに特別に公開（*2-3）
	英公共医療NHSのシステムでランサムウェア感染。20以上の病院で診察や手術のキャンセル、および救急搬送の受け入れ中止が発生（*2-1）
	スペイン政府は同国の通信大手テレフォニカの社内コンピューターの85%が影響を受けていると発表（*2-2）
	AVAST、ランサムウェア「WannaCry」の攻撃を最大で5万2000回検知、被害は99か国、主な標的はロシア、ウクライナ、台湾と発表（*2-3、2-4）
	英BBC、4/14に公開されたDoublepulsarが本攻撃の初期感染に悪用されたと指摘 （*2-3、2-6、2-7、2-8、2-9）
	カスペルスキー、攻撃が７４カ国で４万５千件発生と指摘（*2-4）
	ロシア内務省で約1000台のコンピュータがマルウェアに感染したと発表（*2-9）
2017/5/13	英メディア、日産自動車のサンダーランド工場も影響を受けたと発表（*2-5）
	トレンドマイクロとカスペルスキー、日本に対する攻撃を確認したと発表。（*2-5）
	中国中央テレビ、中国の多数の大学で被害が発生していると伝える。北京大学、上海交通大学等（*2-9）
	仏ルノー、攻撃の影響でフランスやスロベニアの工場が操業を停止したと発表（*2-9）
2017/5/14	欧州警察機関が注意喚起。150カ国で20万件以上の被害が発生と公表（*2-10）
	IPAが注意喚起（*2-11）
	JPCERT/CCが注意喚起（*2-12）
2017/5/15	日立製作所、メールシステムで障害が発生と公表（*2-16）
	JR東日本、社内端末1台でランサムウェア感染が発生と公表（*2-17）

© 2017 NTT DATA Corporation

3. 被害状況

(注) 2017/5/22 時点の情報です

■ 感染件数

＜世界＞

- 150か国で30万件以上の感染報告（米政府） （*3-1）
- WannaCryの感染は、ほぼWindows7で、XPは少ないというセキュリティーベンダからの報告有り(*3-7) (*3-8)

＜日本国内＞

- 5/13午前までの約12時間で、日本国内で600拠点、2000端末で感染判明（JPCERT/CC）(*3-4)
- 5/19までに日本国内では25件の感染報告（警察庁） （*3-2）
  - ✓ 個人ユーザ 18件、企業 5件、行政機関 1件、総合病院 1件

■ 主な被害状況

- 5/22 12時(日本時間)までに、身代金として総額10万1000ドルが支払われた。（*3-3）
- 5/13、英医療機関で手術の中止や緊急搬送の受け入れ停止などの支障が出た。(*2-1)
- 5/15、日立製作所で社内メールシステムでメール送受信ができないなどの障害が発生。（*2-16)(*3-6）
- 5/15、JR東日本で感染が発生。社内ネットワークに接続しておらず、お客様向けサービス等に影響なし。（*2-17）
- 5/16、東急電鉄で感染が発生。社内ネットワークに接続しておらず、お客様向けサービス等に影響なし。（*3-5）

© 2017 NTT DATA Corporation

4. 関連組織による対応

■ マイクロソフトによる対応

- 実施済み
  - ✓ SMB v1の利用停止を推奨(2016/9/16)
  - ✓ SMB v1の脆弱性の修正プログラム「MS17-010」を公開（3/14）
  - ✓ 「MS17-010」をサポート終了済みのWindows XP/8/Server 2003にも公開（5/12）
  - ✓ WannaCrypt注意喚起を公開（5/14）

- 実施予定
  - ✓ 5/15時点で、追加の対応予定はない。

■ 公的機関による注意喚起

- 5/12 スペインCCN-CERT、米US-CERTが注意喚起
- 5/14 欧州警察機関、IPA、JPCERT/CCが注意喚起
- 5/15 総務省が注意喚起
- 5/17 JPCERT/CCが注意喚起を更新

■ 復号について

- Windows XPで、端末を再起動していない等の条件はあるが、復号に成功したと報告有り。（*4-1）

■ その他

- 医療機器メーカーも、独自パッチの準備を進める。（*4-2）

© 2017 NTT DATA Corporation

5. 推奨される対策

■ 本格対処
- Windowsセキュリティパッチの最新化(MS17-010は必須) （*5-1）

■ 回避策

本格対処がむずかしい場合、下記の(1)および(2)を両方実施する。

(1) Microsoftが提供している回避策「SMBv1を無効にする」を実施（*5-1）

(2) FW等により、以下のポートへのアクセスをすべて遮断する
- ✓ 139/tcp
- ✓ 445/tcp
- ✓ 137/udp
- ✓ 138/udp
- ✓ 139/udp

■ その他
- 不審メールを開封しない
- 公式サイト以外のサイトからソフトウェアをダウンロードしない

© 2017 NTT DATA Corporation

6. 初期感染のルートに関するNTTDATA-CERTの見解

■ 大規模攻撃前にDoublepulsarに感染していたコンピュータが、内部ネットワーク上での最初の感染源となった可能性がある。
- 攻撃者は、5/12からの大規模攻撃前に、SMBv1の脆弱性を突いてDoublepulsarに感染させたコンピュータを準備しておき、大規模攻撃開始のきっかけとしたのではないか。

■ 根拠
- Doublepulsarには、設置した攻撃者以外の使用を妨げる機能がある。（*6-1）（*6-2）
- ~~初期感染経路がインターネットに公開されたSMBであれば、通常はインターネットに公開しないサービスのため感染台数が多すぎる~~
  →インターネット上で445番ポートを開放している環境が全世界で50万件以上確認されており、インターネット経由でSMBの脆弱性を突いた攻撃は可能だった。（*1-7）
- 初期感染経路がばらまきメールであれば、数日でサンプルが公開されるはず。
  →感染経路について「電子メール経由の感染ではなかった」とする分析結果もあり。（*6-3）

■ 下記について引き続き情報収集し、仮説を検証する。
- Doublepulsarの感染組織と、本攻撃の被害顕在化組織に相関性があるか
- DoublepulsarがWannacryの感染で果たす役割

© 2017 NTT DATA Corporation

7. 調査を経ての不明点

- 犯人
  - サイバー攻撃集団Lazarusとのつながりが指摘されているが、断定するには至っていない。（*7-1），（*7-2）

- 感染方法
  - 感染経路の全容は不明。
  - Wannacryの感染にDoublepulsarを使用しているという報告有り。（*1-6），（*1-7），（*7-3）

© 2017 NTT DATA Corporation

参考情報

(*1-1) トレンドマイクロ　セキュリティブログ「週明け国内でも要注意－暗号化型ランサムウェア「WannaCry／Wcry　http://blog.trendmicro.co.jp/archives/14884
(*1-2) Microsoft “WannaCrypt ransomware worm targets out-of-date systems” https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/
(*1-3) Cisco's Talos Intelligence Group Blog “Player 3 Has Entered the Game: Say Hello to 'WannaCry' ” http://blog.talosintelligence.com/2017/05/wannacry.html
(*1-4) Microsoft “Customer Guidance for WannaCrypt attacks” https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
(*1-5) JPCERT/CC 注意喚起「ランサムウエア “WannaCrypt” に関する注意喚起」http://www.jpcert.or.jp/at/2017/at170020.html
(*1-6)カスペルスキー ブログ「WannaCry：情報まとめ」https://blog.kaspersky.co.jp/wannacry-faq-what-you-need-to-know-today/15594/
(*1-7)トレンドマイクロ　セキュリティブログ「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
(*2-1) NHKニュース「イギリス各地で国営の病院にサイバー攻撃」http://www3.nhk.or.jp/news/html/20170513/k10010980041000.html
(*2-2) CNN「複数の英病院にランサムウエア攻撃、被害は世界に」https://www.cnn.co.jp/tech/35101103.html
(*2-3) CNET Japan「世界74カ国でランサムウェア攻撃、病院や銀行などに被害」https://japan.cnet.com/article/35101102/
(*2-4) SankeiBiz「世界１００カ国でサイバー攻撃　「身代金」要求型？　７万５千件、日本も被害か」http://www.sankeibiz.jp/macro/news/170513/mcb1705131250021-n1.htm
(*2-5) 朝日新聞「手術を中止、日産工場も影響…サイバー攻撃の被害広がる」http://www.asahi.com/articles/ASK5F5R94K5FUHBI018.html
(*2-6) 毎日新聞「サイバー攻撃　ランサムウエア　ＮＳＡのソフト技術利用か」https://mainichi.jp/articles/20170514/k00/00m/040/039000c
(*2-7) BBC News “Massive ransomware infection hits computers in 99 countries” http://www.bbc.com/news/technology-39901382
(*2-8) 東京新聞「サイバー攻撃　米の情報収集技術を悪用か」http://www.tokyo-np.co.jp/article/world/list/201705/CK2017051402000122.html
(*2-9) NHKニュース「大規模サイバー攻撃　米開発の技術盗まれ悪用か」http://www3.nhk.or.jp/news/html/20170514/k10010980751000.html
(*2-10) 日本経済新聞「サイバー攻撃、150カ国で20万件以上被害　欧州警察機関」http://www.nikkei.com/article/DGXLASGM14H5W_U7A510C1000000/
(*2-11) CNET Japan「週明け、メールを開く前に気をつけたい3つのこと--IPAが呼びかけ、大規模サイバー攻撃で」https://japan.cnet.com/article/35101121/
(*2-12) JPCERT/CC「ランサムウエア "WannaCrypt" に関する注意喚起」http://www.jpcert.or.jp/at/2017/at170020.html
(*2-13) US-CERT “SMB Security Best Practices” https://www.us-cert.gov/ncas/current-activity/2017/01/16/SMB-Security-Best-Practices
(*2-14) Microsoft “Stop using SMB1” https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
(*2-15) Microsoft “Security Bulletin MS17-010” https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
(*2-16) NHKニュース「日立製作所 サイバー攻撃で社内システム一部に障害」http://www3.nhk.or.jp/news/html/20170515/k10010981821000.html
(*2-17) NHKニュース「ＪＲ東日本のＰＣ１台がウイルスに感染」http://www3.nhk.or.jp/news/html/20170515/k10010982011000.html
(*2-18) NSAから流出のバックドア「DOUBLEPULSAR」、世界で感染急増 - ZDNet Japan https://japan.zdnet.com/article/35100240/
(*2-19) US-CERT “Alert (TA17-132A) Indicators Associated With WannaCry Ransomware” https://www.us-cert.gov/ncas/alerts/TA17-132A
(*2-20) CCN-CERT “Identificado ataque de ransomware que afecta a sistemas Windows” https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4464-ataque-masivo-de-ransomware-que-afecta-a-un-elevado-numero-de-organizaciones-espanolas.html
(*3-1) NHKニュース “米高官 サイバー攻撃の被害は約１５０か国で３０万件以上” http://www3.nhk.or.jp/news/html/20170516/k10010983131000.html
(*3-2) 産経ニュース「警察庁把握は計２５件に　ランサムウエア被害」http://www.sankei.com/affairs/news/170519/afr1705190033-n1.html
(*3-3) How Much Wannacry Paid the hacker http://howmuchwannacrypaidthehacker.com/
(*3-4) 毎日新聞 「サイバー攻撃：日立のシステム障害　海外グループ企業でも」https://mainichi.jp/articles/20170515/k00/00e/040/252000c
(*3-5) NHKニュース「サイバー攻撃 東急電鉄でもウイルス感染」http://www3.nhk.or.jp/news/html/20170516/k10010983251000.html
(*3-6) 日立製作所 ニュースリリース「ランサムウェアによる被害および復旧状況について」http://www.hitachi.co.jp/New/cnews/month/2017/05/0517a.html
(*3-7) ITmedia NEWS「「WannaCry」感染の98%は「Windows 7」で「XP」はほぼゼロ」http://www.itmedia.co.jp/news/articles/1705/20/news034.html
(*3-8) REUTERS “Security experts find clues to ransomware worm's lingering risks” http://www.reuters.com/article/us-cyber-attack-failures-idUSKCN18E2SG
(*4-1) マイナビニュース「WannaCryに感染したWindows XP、支払いせずとも復号に成功」http://news.mynavi.jp/news/2017/05/20/110/
(*4-2) ITmedia エンタープライズ「ランサムウェア「WannaCry」、医療機器メーカーも独自パッチを準備」http://www.itmedia.co.jp/enterprise/articles/1705/19/news048.html
(*5-1) 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
(*6-1)threatpost “NSA’S DOUBLEPULSAR KERNEL EXPLOIT IN USE INTERNET-WIDE” https://threatpost.com/nsas-doublepulsar-kernel-exploit-in-use-internet-wide/125165/
(*6-2)@zerosum0x0 “DoublePulsar Initial SMB Backdoor Ring 0 Shellcode Analysis” https://zerosum0x0.blogspot.jp/2017/04/doublepulsar-initial-smb-backdoor-ring.html
(*6-3) ITmedia NEWS「「WannaCry」の拡散、電子メールが原因ではなかった　セキュリティ企業が分析結果公表」http://www.itmedia.co.jp/news/articles/1705/22/news057.html
(*7-1)カスペルスキー ブログ「WannaCryとLazarusグループ － 両者をつなぐもの」https://blog.kaspersky.co.jp/wannacry-and-lazarus-group-the-missing-link/15559/
(*7-2)シマンテック公式ブログ「WannaCry ランサムウェアについて知っておくべきこと」https://www.symantec.com/connect/ja/blogs/wannacry-1
(*7-3)マクニカネットワークス セキュリティ研究センターブログ「マルウェア解析奮闘記 WannaCryの解析」http://blog.macnica.net/blog/2017/05/wanacry-8ff1.html

© 2017 NTT DATA Corporation

変更履歴

- 2017/5/15　v1.0 新規作成
- 2017/5/16　v1.1 更新（エグゼクティブサマリ、３）
- 2017/5/22　v1.2 更新（エグゼクティブサマリ、１、３、４、６、７）

© 2017 NTT DATA Corporation

NTT DATA

Global IT Innovator

© 2017 NTT DATA Corporation