公開レポート

NTT DATA
Global IT Innovator

【緊急レポート】
ランサムウエア「Petya」亜種の大規模感染について v1.1

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6月29日

目次

エグゼクティブサマリ

- 2017年6月27日、欧州やロシアなどでランサムウェア大規模感染が報告された。

- 被害状況（6/28時点）
  - ウクライナ：首都キエフの国際空港や地下鉄、市役所、国営電力会社ウクルエネルゴ、チェルノブイリ原子力発電所の放射線レベル計測システム等で不具合が発生。
  - その他、ロシア、英国、デンマーク、米国、オランダ、フランス、インド等で被害発生。
  - 6/29時点で、身代金約10000米ドルが支払われた。

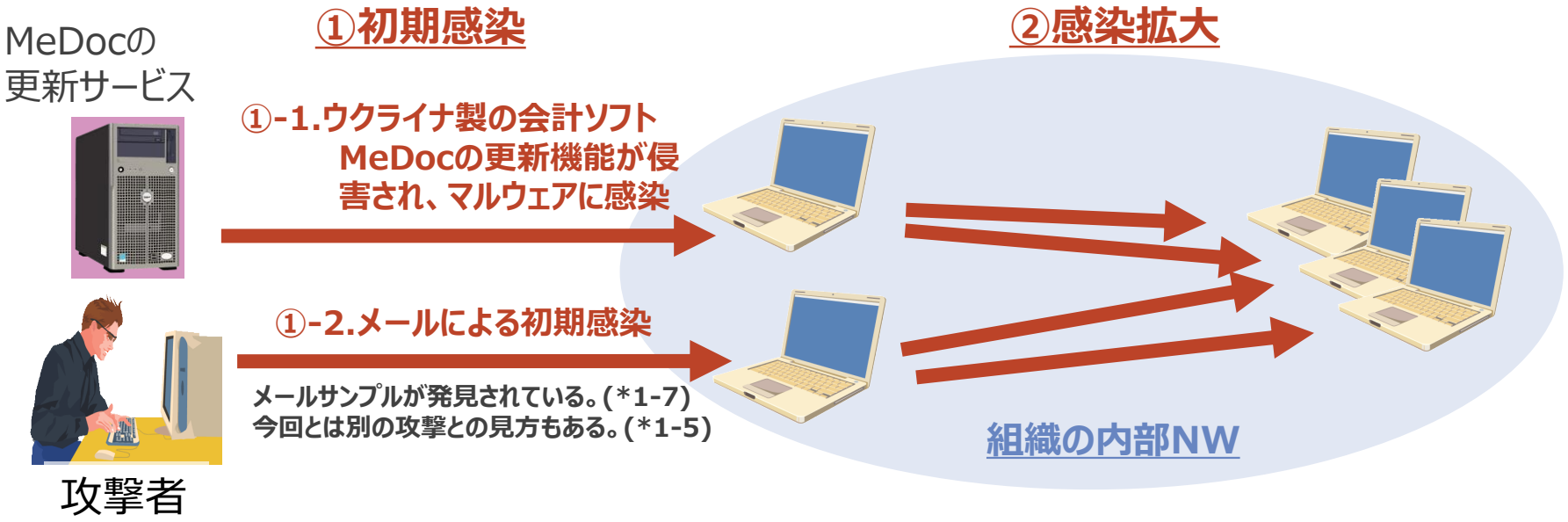
- 攻撃情報
  - ランサムウェア：Petyaの亜種（別名PetrWrap、NotPetya、GoldenEye等）
  - 攻撃手法：ネットワーク経由で感染を広げる。端末上のファイルを使用不能にし、復旧と引き換えに300ドル相当のビットコインの支払いを要求する。
  - 感染拡大には、ハッキングツール「EternalBlue」やWindowsの正規ツールPsExecやWMIコマンドの使用、会計ソフト「MeDoc」のアップデート侵害、ばらまきメールなど、複数の手法が報告されている。各手法の関連は不明。（6/28時点）

- 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
  - SMB関連のポートをインターネットに公開しない（詳細は本資料の「４．」に記載）

1. 本攻撃の全体像と攻撃手法

攻撃対象：Windows XP～10を搭載したコンピュータ

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、全容は不明。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、*1-4、 *1-5、*1-6）



②感染拡大 では、3つのメカニズムが確認されている。

- 内部NWで管理者権限のある共有フォルダをスキャンし、共有フォルダを保有する端末でPsExecを実行する
  - すでに感染した端末が、共有フォルダを保有するシステムのファイル書き込み・実行権限を持つ必要がある。
- 認証情報を取得するツール「mimikatz」「LSADump」等を実行して内部NW上の他端末のID/パスワードを盗み、他端末にログオンしてWindows Management Instrumentation Command-line (WMIC) を使う
- 内部NWにMS17-010を未適用の端末があった場合、SMBの脆弱性を悪用するツール「EternalBlue」を実行する
  - ランサムウェアWannaCryの感染と類似の手法

⇒ SMBの脆弱性が修正済みのコンピュータでも、今回の攻撃の被害が発生する可能性がある。

2．被害状況

(注) 2017/6/29 時点の情報です
情報源：*2-1～*2-7

6/29時点で、身代金として約10000米ドルが支払われた。(*2-8)

国	組織名	被害状況
ウクライナ	政府	政府官房のネットワークがダウン。一部省庁のwebサイトに接続不可。
	中央銀行	※詳細不明
	複数の銀行	業務に支障が発生。
	チェルノブイリ原子力発電所	放射線レベル計測システム等で不具合が発生、手動での計測に切り替え。
	ウクルエネルゴ（国営電力会社）	※詳細不明
	国営航空会社	※詳細不明
	首都キエフの国際空港	航空機の発着に影響が発生。
	首都キエフの地下鉄	決済に支障が発生。
ロシア	ロスネフチ（石油最大手）	公式webサイトに接続不可。生産設備への影響防止で予備システムに切り替え。
	エブラズ（鉄鋼右手）	※詳細不明
英国	WPP（広告大手）	情報システムが影響を受ける。
デンマーク	モラー・マースク（海運大手）	複数の拠点で情報システムがダウン。
米国	モンデリーズ（食品最大手）	オーストラリア・タスマニア島の工場が影響を受ける。
オランダ	TNT（運送大手）	一部システムで復旧対応が必要。
フランス	サンゴバン（建築資材大手）	※詳細不明
インド	ムンバイ近郊の港	積み出し、積み入れができなくなる。同港はモラー・マークスが運営。

3．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（ランサムウェアWannaCryへの対応の再掲）
    - ✓ 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）

- 公的機関による注意喚起
  - 6/27　ベルギーCERT.be、米US-CERTが注意喚起（*3-1、*3-2）
  - 6/28　IPA、JPCERT/CCが注意喚起（*3-3、*3-4）

４．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) （*4-1）

■ 回避策

本格対処が難しい場合、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（*4-1）

(2) ファイアウォール等により、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
- Windowsコンピュータ（端末とサーバの双方とも）のAdministrator権限を最小限のユーザーにのみ付与する
  ※mimikatzが感染拡大に悪用されている場合の対策として
- 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

5．調査を経ての不明点

■ 犯人
- 犯人に関連した情報は不明

■ 感染方法
- 初期感染の経路は、(1)ウクライナ製の会計ソフトMeDocの更新機能、(2)攻撃メールによる感染の2種類が指摘されているが、全容解明には更に正確かつ詳細な情報が必要
- 感染拡大で、カスペルスキーは「mimikatzによって認証情報が窃取されている」と指摘しているが、攻撃者がmimikatzをインタラクティブに操作しているのか、または自動化しているのか、確認が必要

6．攻撃の狙いおよび攻撃者に関するNTTDATA-CERTの分析

■ 攻撃の狙い

- 金銭窃取の可能性は低い
  - ✓ 身代金を支払ったことを電子メールで攻撃者に通知するよう要求していたが、攻撃者の電子メールアドレスはメールサービスにより閉鎖されてしまった。
  - ✓ 他のランサムウェアでは、Torによる連絡が一般的。
  - ✓ 今回の攻撃における身代金の支払い手法は比較的稚拙に見える。
- 社会インフラを破壊し、混乱を招く狙いの可能性がある
  - ✓ 政府機関、金融機関、社会インフラ関連の企業が多数被害を受ける。
- ウクライナを特に標的とした可能性がある
  - ✓ カスペルスキーの観測（6/27時点）で国別感染数の60％がウクライナだった。（*1-1）
  - ✓ 初期感染で悪用された会計ソフトMeDocは、企業がウクライナ政府に納税する際に使用されている。（*6-1）

■ 攻撃者の素性

- 反ウクライナの考えを持った個人または集団の可能性がある
  - ✓ ウクライナ政府の高官は「ウイルスを分析したところ、ロシアが関与した可能性がある」と話した。（*6-2）
  - ✓ クリミア半島併合などでウクライナとロシアは緊張関係にある。
  - ✓ 一方、ロシアが今回の攻撃に関与したとの証拠は公表されていない。
  - ✓ ロシア政府の見解は未確認。

参考情報

(*1-1) SECURELIST “Schroedinger’s Pet(ya)” https://securelist.com/schroedingers-petya/78870/
(*1-2) Ars Technica “A new ransomware outbreak similar to WCry is shutting down computers worldwide“ https://arstechnica.com/security/2017/06/a-new-ransomware-outbreak-similar-to-wcry-is-shutting-down-computers-worldwide/
(*1-3) FireEye “Petya Ransomware Spreading Via EternalBlue Exploit“ https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html
(*1-4) Trend Micro “Large-Scale Ransomware Attack In Progress, Hits Europe Hard” http://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/
(*1-5) Forbes “Another Massive Ransomware Outbreak Is Going Global Fast” https://www.forbes.com/sites/thomasbrewster/2017/06/27/ransomware-spreads-rapidly-hitting-power-companies-banks-airlines-metro/
(*1-6) Palo Alto Networks ”Threat Brief: Petya Ransomware” https://researchcenter.paloaltonetworks.com/2017/06/unit42-threat-brief-petya-ransomware/
(*1-7) NCC Group “June Global Ransomware outbreak” https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2017/june/live-incident-blog-june-global-ransomware-outbreak/
(*2-1) BBC “Global ransomware attack causes turmoil” http://www.bbc.com/news/technology-40416611
(*2-2) 朝日新聞デジタル 「欧州各国に大規模サイバー攻撃　銀行・空港など被害」 http://www.asahi.com/articles/ASK6W7XHMK6WUHBI03C.html
(*2-3) YOMIURI ONLINE 「露・欧で身代金ウイルス攻撃…銀行や空港被害」 http://www.yomiuri.co.jp/world/20170628-OYT1T50001.html
(*2-4) 毎日新聞 「サイバー攻撃　ウクライナ、露、英、印などで大規模被害」 https://mainichi.jp/articles/20170628/k00/00m/030/185000c
(*2-5) 産経ニュース 「ウクライナにサイバー攻撃　政府、銀行など大規模」 http://www.sankei.com/world/news/170627/wor1706270041-n1.html
(*2-6) 産経ニュース 「露・ウクライナにサイバー攻撃　政府や銀行など大規模　世界に被害広がる可能性」 http://www.sankei.com/world/news/170628/wor1706280003-n1.html
(*2-7) ブルームバーグ 「大規模サイバー攻撃がアジアに拡大、インドの港湾施設で被害」 https://www.bloomberg.co.jp/news/articles/2017-06-28/OS8N9Z6TTDS001
(*2-8) BLOCKCHAIN LUXEMBOURG S.A. https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
(*3-1) CERT.be “Global cyber-attack impacts hundreds of companies” https://www.cert.be/docs/global-cyber-attack-impacts-hundreds-companies.html
(*3-2) US-CERT “Multiple Petya Ransomware Infections Reported” https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported
(*3-3) IPA 「感染が拡大中のランサムウェアの対策について」 http://www.ipa.go.jp/security/ciadr/vul/20170628-ransomware.html
(*3-4) JPCERT/CC 「インターネット経由の攻撃を受ける可能性のある PC やサーバに関する注意喚起」 http://www.jpcert.or.jp/at/2017/at170023.html
(*4-1) 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) Recorded Future “Don’t Pay the Ransom: Petya Ransomware Update” https://www.recordedfuture.com/petya-ransomware-analysis/
(*6-2) 日本経済新聞 「欧州で大規模サイバー攻撃　ウクライナ被害集中」http://www.nikkei.com/article/DGXLASGM27H9Z_X20C17A6FF2000/

変更履歴

• 2017/6/28	v1.0	新規作成
• 2017/6/29	V1.1	「１．本攻撃の全体像と攻撃手法」を更新 「２．被害状況」を更新 「６．攻撃の狙いおよび攻撃者に関するNTTDATA-CERTの分析」を追加

NTT DATA

Global IT Innovator