NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2017年6月版 (第21号)＞ (選り抜き版)

2017年6月26日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

世界規模のランサムウェア「WannaCry」の急速な感染拡大と終息の理由
世界規模で被害が確認されたランサムウェア「WannaCry」。攻撃キャンペーンが行われてから当日の内に感染を急拡大したものの、数日で終息に向かった、その背景と企業が取るべき対策を解説します。

世界規模のランサムウェア
「WannaCry」の急速な感染拡大と終息

1. WannaCryの概要

WannaCryとは、ランサムウェアに分類されるマルウェアの一種です。
本マルウェアは感染したホスト上のファイルを暗号化すると共に、SMBv1の脆弱性であるCVE-2017-0144を悪用し、主に内部ネットワークで感染を拡大します。CVE-2017-0144に関するパッチ(MS17-010)は、2017年3月にMicrosoft社より提供されていましたが、同年5月12日に感染キャンペーンが開始されたことに伴い、パッチ未適用及びサポート切れOSの環境において急速に感染が拡大しました。

公開された脆弱性	CVE-2017-0144
影響を受けるバージョン	Windows10を除く、すべてのWindowsサーバ、クライアント
マルウェア種別	ランサムウェア
感染経路	[初期感染] 不明 [感染拡大] ワーム機能 (SMBv1の脆弱性を悪用)
被害状況	- 世界150か国、20万台以上のコンピュータが感染 - 日本国内でも2000件以上のコンピュータが感染
対策	- パッチ(MS17-010)の適用 - SMBv1の無効化 - インターネットアクセス(特定ドメインへのDNSクエリが発行できること)

※ランサムウェア
金銭を要求する類のマルウェアの一種であり、「ファイルを暗号化し、復号のために金銭を要求する」「ウィルススキャンを行った風を装い、マルウェア駆除のために金銭を要求する」など複数の種類が存在する。
本レポートでも「2015.2Q：ファイルサーバにランサムウェア対策を」、「2016.3Q：ランサムウェアの身代金支払い要求への対応と応じた場合の違法性について」など複数回にわたり取り上げている。

2. 事象のタイムライン

WannaCryに関する各組織の動きを以下に記します。

日付	内容
2016年9月16日	Microsoftが、公式ブログでセキュリティの問題を理由にSMBv1の利用停止を推奨
2017年3月14日	Microsoftが、SMBv1の脆弱性を修正するセキュリティパッチ(MS17-010)を公開
2017年4月14日	ハッカー集団(Shadow Brorkers)が、SMBｖ1の脆弱性を悪用するバックドアツール「Doublepulsar」を公開
2017年5月12日	US-CERTが、WannaCryの攻撃キャンペーンに関して注意喚起
	Microsoftが、サポートが終了したOS(WindowsXPなど)向けにセキュリティパッチ(MS17-010)を配布
	複数のセキュリティベンダが、ロシアを中心に、欧州やアジアなど100ヶ国以上で攻撃を観測したことを発表
	WannaCryをベースとした日本国内企業の被害を確認
	イギリスで、WannaCryの拡大を止める最初のキルスイッチが発見される
	有志により、最初のキルスイッチのドメインが登録される
2017年5月14日	IPA及びJPCERT/CCが、週明けの就業前に対策を取るよう注意喚起
	2番目のキルスイッチが発見され、ドメイン登録される

3. WannaCryの動作イメージ

WannaCryの動作イメージを以下に記します。

SMBv1脆弱性を利用して侵入

サービスプロセスとして動作しマルウェア(tasksche.exe)を作成

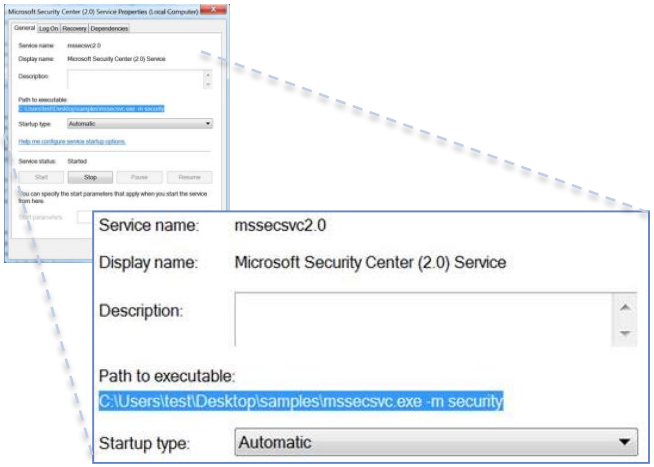
mssecsvc.exe

- 暗号化用S/Wの生成
- 感染の拡大

ファイルを暗号化し脅迫文を表示

tasksche.exe

- ファイルの暗号化
- 脅迫文の表示



2017年6月現在初期の感染経路は明確になっていない

予めバックドアツール「Doublepulsar」に感染していた事が原因ではないかとされている。ただし「Double pulsar」の感染原因も不明

4. WannaCryに感染した場合

　ファイルを暗号化された場合、復号するために金銭(BitCoin)の振り込みを要求されます。ただし現状復号報告はなく、さらに通常ランサムウェアは振込者を特定するために被害者毎に異なるビットコインアドレスを示しますが、WannaCryではコードはあるものの動作せず、3つの固定アドレスを示しており被害者を特定することができないとされています。そのため、仮に金銭を支払っても実際に復号できる可能性は低いと見られています。
　またセキュリティベンダなどから復号用のツールが提供されていますが、「暗号化後、再起動を行っていない」など条件があり、必ずしも復号できるわけではありません。

暗号化されたファイルの拡張子	.WNCRY / .WCRY	
復号に求められる金額	感染から3日以内	$300相当のBitCoin要求
	感染から7日以内	$600相当のBitCoin要求
	感染から7日経過後	復号不可

※BitCoin
2009年ごろより運用が開始された最もメジャーな仮想通貨で、2017年4月時点で時価総額2兆円を超えたとされている。
日本国内においても、コンビニエンスストアや大手家電量販店での採用事例が増加している。

※ビットコインアドレス
2の256乗からなるランダムな文字列であり、BitCoinの預金口座兼振込口座を示す値となる。

5. 早期終息の理由 (1/3)

WannaCryは2017年5月12日に攻撃キャンペーンが開始され、急速に被害が拡大しましたが、その後数日で終息を迎えました。

古いNASやサポート終了OSなどの互換性維持のため未だ企業で稼働し続けているSMBv1の脆弱性を悪用され、かつサポート終了OSが影響対象に含まれているため攻撃が長期にわたることが予想されている中、早期終息を迎えた大きな理由に「キルスイッチ」の存在があります。

キルスイッチ

緊急停止装置を意味し、WannaCryにもキルスイッチが存在することが確認された。
WannaCryのキルスイッチは、特定ドメインへのアクセス可否がポイントとなっており、ファイルの暗号化処理を行う前に判定され、特定ドメインへアクセスできた場合は感染の拡大や暗号化用S/Wの生成は行われない。

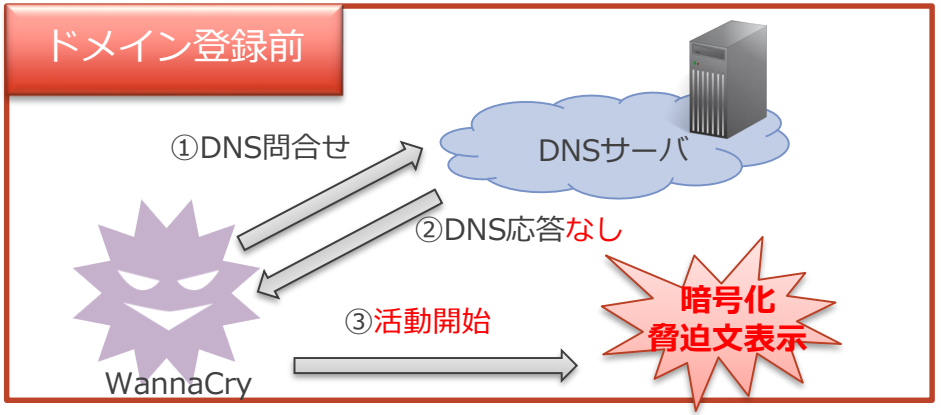
5. 早期終息の理由 (2/3)

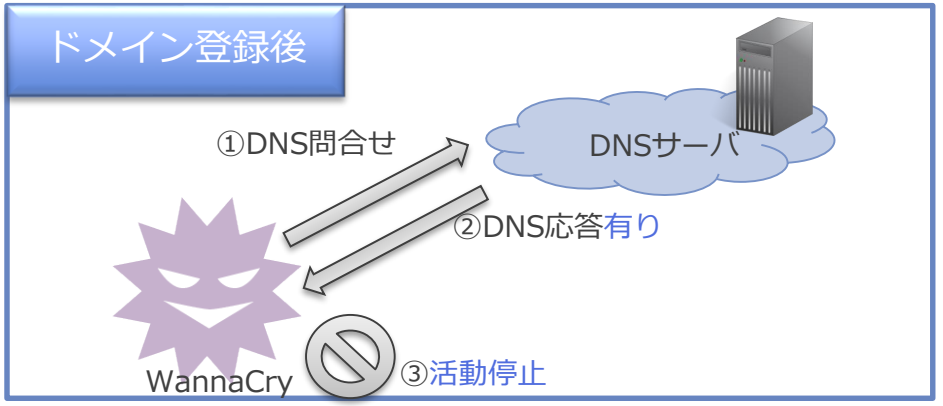
WannaCryにおいては、キルスイッチとして2つのドメインが確認されており、当初は両ドメインとも未登録であったため、アクセスできず、WannaCryが動作する状況にありました。

ただし攻撃キャンペーンの開始から間もなくして、有志により当該ドメインが登録されたことで、インターネットに接続されたシステムは当該ドメインにアクセスできるようになり、WannaCryは活動停止に追い込まれました。

WannaCry キルスイッチドメイン (亜種関連含む)	登録日	オリジナル/亜種
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com	2017/5/12 15:08:04 UTC	オリジナル
ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com	2017/5/14 12:18:03 UTC	オリジナル
Ayylmaotjhsstasdfasdfasdfasdfasdfasdf[.]com	2017/5/15 11:02:03 UTC	亜種
iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com	2017/5/15 11:25:03 UTC	亜種
iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb[.]com	2017/5/16 07:25:21 UTC	亜種

※不用意にアクセスしないよう、一部加工してあります
※6月16日時点で確認されているドメイン情報を示しています
※Proxy環境には非対応であるため、Proxyを導入している場合は各社のDNSでダミーサイトに誘導する等の対応が必要です

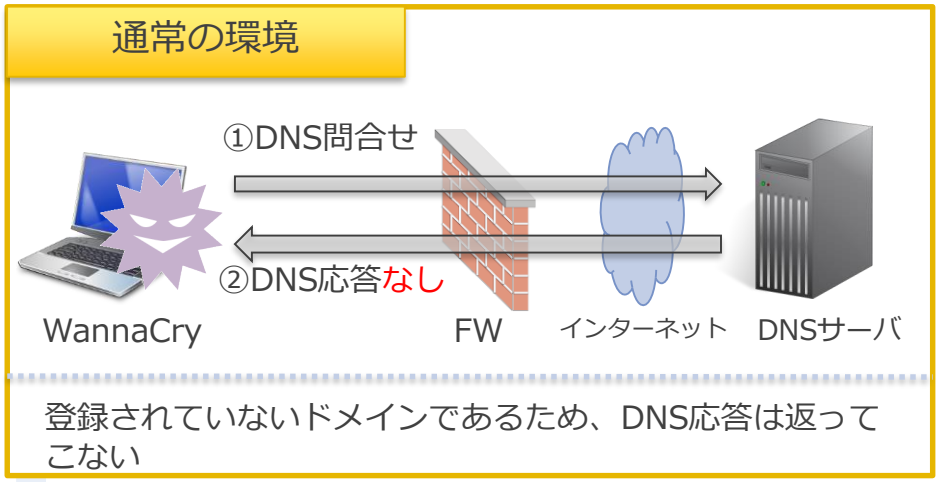


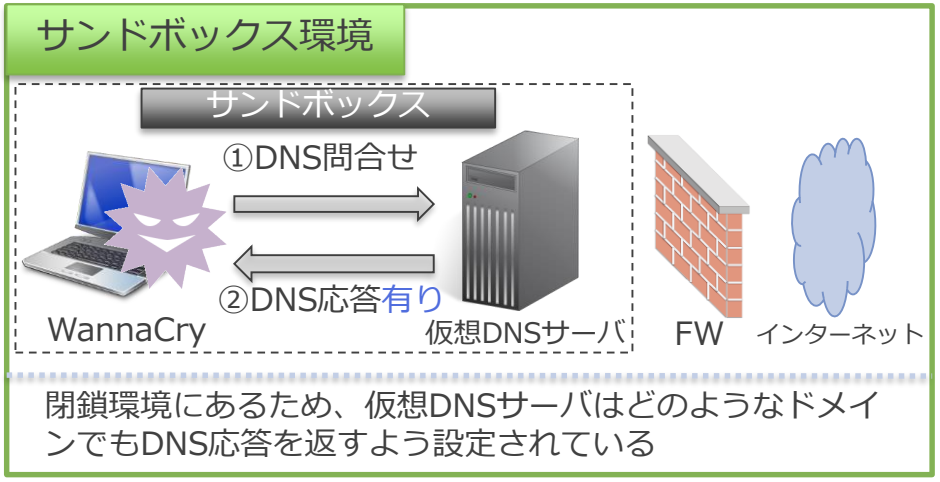


※開発環境などインターネットに接続できない環境では、動作する可能性があります
※WannaCryの亜種が確認されており、「上記以外のドメインがキルスイッチとなっている」「キルスイッチが用意されていない」ケースもあるため、過信は禁物です

5. 早期終息の理由 (3/3)

　ではなぜ攻撃者はWannaCry(暗号化処理)を停止させてしまうリスクを負ってまでキルスイッチを用意したのでしょうか？
　それはマルウェアの挙動解析から逃れるためであると考えられます。通常ウィルス対策ソフトベンダなどがマルウェアの挙動を解析する際は、サンドボックスと呼ばれる周囲のシステムに影響を及ぼさない仮想空間で動作させ、挙動を確認します。一般的にサンドボックス内の仮想DNSサーバは、マルウェアからのDNS問合せに対して、実際の存在の有無に関わらず必ず何らかの応答を返します。本来未登録ドメインであるため返ってこないはずの応答が返ってくることから、サンドボックス内で動作していると判断し、解析をさせまいと活動を停止したわけです。
　このようにマルウェアの挙動解析から逃れるために用意されたと推測されるキルスイッチが、今回の騒動を早期に終息させる一因となりました。





6. まとめ

初期感染経路は不明なものの、セキュリティパッチが配布されてから攻撃キャンペーンが開始されるまで2か月もの期間がありました。適切にパッチ適用の運用が行われていれば、最初の1台目の感染は免れないものの、感染拡大は防げたものとされています。

なお今回は影響を鑑みて、Microsoft社よりサポート期限切れのOSに対してもセキュリティパッチが提供されましたが、これは極めて異例の対応です。

またWannaCryにおいては確実な復号方法がなく、バックアップの重要性を改めて認識させられる一件となりました。適切な対象のバックアップを、適切な場所と周期で取得しておくことで、万が一の事態に備えることができます。

システムのサポート期限(End of Life)を意識した更改計画の立案や、定期的なパッチ適用、バックアップの取得が行われる運用を検討することも各企業には求められています。

7. 参考URL

- ランサムウェア「WannaCry／Wcry」による国内への攻撃を 16,436件確認
  http://blog.trendmicro.co.jp/archives/14906
- 大規模な暗号化型ランサムウェア「WannaCry／Wcry」の攻撃、世界各国で影響
  http://blog.trendmicro.co.jp/archives/14873
- WannaCry ランサムウェアキャンペーンの 脅威の詳細とリスク対策について
  https://www.fireeye.jp/company/press-releases/2017/wannacry-ransomware-campaign.html
- US-CERT “Alert (TA17-132A) Indicators Associated With WannaCryRansomware”
  https://www.us-cert.gov/ncas/alerts/TA17-132A
- Microsoft “Security Bulletin MS17-010”
  https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- 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
- 国際サイバー攻撃、ランサムウエア拡散防ぐ「キルスイッチ」発見と専門家
  http://www.afpbb.com/articles/-/3128112
- 話題のランサムウェア「WannaCry」、MicrosoftがWindows XP向けに異例のパッチを公開
  http://spotry.me/2017/microsoft-sends-out-a-windows-xp-patch-to-block-new-ransomware/
- NSAから流出のバックドア「DOUBLEPULSAR」、世界で感染急増
  https://japan.zdnet.com/article/35100240/
- 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/
- Customer Guidance for WannaCrypt attacks
  https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
- MalwareHunterTeam
  https://twitter.com/malwrhunterteam/status/863332111742365696

NTT DATA

Trusted Global Innovator