2017年5月15日

Lastline, Inc.

WannaCry ランサムウェアによる攻撃でわかったこととその対策

インターネットから断絶した場所にいない限り、2017年5月12日金曜日の世界中をターゲットに攻撃したランサムウェアの存在を、日本時間の週末にニュースやメディアなどで知ったことでしょう。この攻撃は週末にかけて新しいバージョンへと更に進化し続けていました。

ここでは、我々ラストライン社がこの WannaCry ランサムウェアの何を知り、対策として何ができるのかを整理したいと思います。

Figure 1 - 2017 年5月11日にラストラインが観測した WannaCry Ransomware Version2 のスクリーンショット

何が起こっていたのか？

米国太平洋標準時間の 2017 年 5 月 14 日(日)時点で、WannaCry ランサムウェア(別の名を「WannaCrypt」や「WannaCrypt0r」などとも呼ばれる。以下、「WannaCry」と云う)は 150 以上の国に攻撃を行い、20 万以上のシステムに影響を与えたと言われています。WannaCry ランサムウェアはそれぞれのシステムのファイルを暗号化し、被害者は3日以内に身代金(英語で「ransom」)300米国ドル(1ドル 110 円換算で約 33,000 円)またはその2倍の金額を要求されました。そして感染から 7 日後、このランサムウェアは暗号化したファイルの削除を行うことになります。このランサムウェアは、28 カ国の言語に対応し、179 種類のファイルタイプの暗号化を実行します。

その攻撃とは

この攻撃は、2016 年あたりからサイバー攻撃に利用されてきたランサムウェアファミリーの新しいバージョンが利用され、直近では 2017 年 3 月にラストライン ラボにて、このランサムウェアファミリーを観測しています。

WannaCry の拡散方法は、ユーザーが URL リンクをクリックしたり、ファイルを開いたりすることなくネットワーク内で自動的に拡散する Old-School ワームを流用しています。(今日の攻撃者はセキュリティ製品による検知を避け、内密に攻撃を成功させる手法に移行しており、ワームはこの数年サイバー攻撃で多用されるがありませんでした。)

そして、ウインドウズの SMB(Server Message Block)サービスの脆弱性を突く攻撃を実行します。一般的に利用されるこの通信プロトコルは、過去 15 年でほとんどのウインドウズで利用され、非常に多くの攻撃の対象となり影響を受けました。

ランサムウェアに関する更に詳細な情報については、2017 年 3 月と 4 月にそれぞれ公開したラストライン ラボのブログ Part 1: Ransomware Delivery Mechanisms と Part 2: Too Overt to Hide をご覧ください。(英語版のみ)

ランサムウェアの進化

現状、WannaCry の進化の中でいくつかのバージョンが確認されています。5 月 12 日の攻撃で利用された最初の WannaCry は、登録されていないドメインへのアクセスを発見した敏感な研究者によって調査が始まり、その研究者はそのドメインを 10.69 米国ドル(1ドル110円換算で約 1,200 円)で購入し世界のインターネットを救いました。ドメインを購入することで、WannaCry の「キル・スイッチ」を押し、活動を止めることに成功しています。

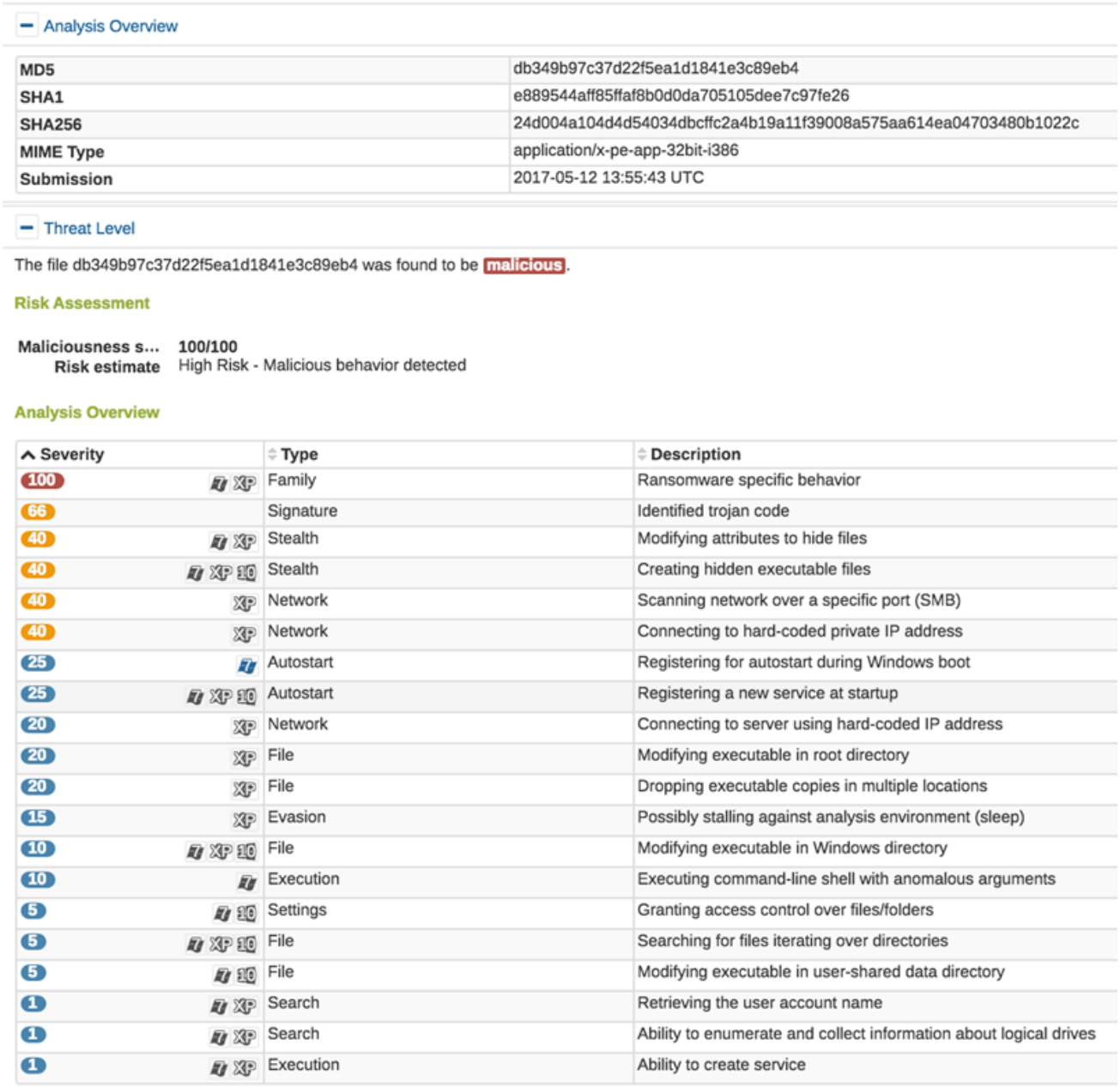
ドメイン名を登録するマルウェアは、シンクホールという技術を利用することで知られており、一般的にマルウェアをゆっくりと拡散されることで使用されます。この研究者によるドメインの購入と登録は、ドメインがインターネット上に伝搬した後に動作するマルウェアには有効でしたが、一部例外があったことは想定外でした。それは WannaCry がプロキシに対応しておらず、プロキシによって守られた組織内では、その該当するドメイン名がプロキシ内で利用している DNS サーバへ伝搬する前に、WannaCry による第一波攻撃が成功してしまいました。

不運にも、UTC 国際標準時で 2017 年 5 月 13 日土曜日の早朝、最初の WannaCry で押した「キル・スイッチ」が既に無効化された新しいバージョンの WannaCry が確認され、この攻撃の拡散が継続して拡大する結果となりました。

Lastline Enterprise のディープ・コンテンツ・インスペクションと驚異の分類

私たちラストラインでは、この WannaCry のディープ・コンテンツ・インスペクションを行い、Global Threat Intelligence Network とネットワークトラフィック解析など、攻撃全体の広範囲な解析が可能な技術によって検出していました。

以下の Figure 2 は、この WannaCry を、ラストラインの技術で解析した結果のスクリーンショットです。ここでは、検知した活動一覧の中で、ランサムウェアの分類やウインドウズの SMB プロトコルを介して拡散していることがわかります。



Analysis Overview

MD5	db349b97c37d22f5ea1d1841e3c89eb4
SHA1	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
MIME Type	application/x-pe-app-32bit-i386
Submission	2017-05-12 13:55:43 UTC

Threat Level

The file db349b97c37d22f5ea1d1841e3c89eb4 was found to be malicious.

Risk Assessment

Maliciousness s... 100/100
Risk estimate High Risk - Malicious behavior detected

Analysis Overview

Severity	Type	Description
100	Family	Ransomware specific behavior
66	Signature	Identified trojan code
40	Stealth	Modifying attributes to hide files
40	Stealth	Creating hidden executable files
40	Network	Scanning network over a specific port (SMB)
40	Network	Connecting to hard-coded private IP address
25	Autostart	Registering for autostart during Windows boot
25	Autostart	Registering a new service at startup
20	Network	Connecting to server using hard-coded IP address
20	File	Modifying executable in root directory
20	File	Dropping executable copies in multiple locations
15	Evasion	Possibly stalling against analysis environment (sleep)
10	File	Modifying executable in Windows directory
10	Execution	Executing command-line shell with anomalous arguments
5	Settings	Granting access control over files/folders
5	File	Searching for files iterating over directories
5	File	Modifying executable in user-shared data directory
1	Search	Retrieving the user account name
1	Search	Ability to enumerate and collect information about logical drives
1	Execution	Ability to create service

Figure 2 - Lastline Enterprise による WannaCry ランサムウェアの解析結果

ランサム（身代金）

身代金支払いにビットコインを使うことは、不法な取引に有効です。UTC 国際標準時の 2017 年 5 月 15 日月曜日時点で、おおよそ 170 回もの支払いを確認し、その金額はおおよそ 48,000 米国ドル(1 ドル 110 円換算で約 528 万円)でした。この金額は、週明けの平日になると仕事も始まるため、被害を受けた組織は身代金支払いを決定し、これからもっと増え続けると想定されます。これらの支払い行為は、以下のサイトでご確認いただけます。

https://blockchain.info/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://blockchain.info/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

https://blockchain.info/address/115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

もちろん、ランサムウェアによる実際のダメージは、支払い金額よりも更に重要かつ大きな問題です。

ランサムウェアによる身代金支払いでの注意点：WannaCry は被害者だけでなく、ランサムウェアの製作者自身による復号化が非常に困難な方法で暗号化されます。そのため、ファイルを復号化して回復する可能性は非常に低いです。身代金を支払ってファイルの復号化と回復ができたと云う公表は、今のところ例がありません。

何ができるのか？

ウインドウズアップデートでパッチを当てる

ウインドウズアップデートで最新のパッチが適用されていることを確認します。マイクロソフト社は、2017 年 3 月 14 日に、緊急のセキュリティアップデートを Security Bulletin MS17-010 として公開しています。マイクロソフト・ウインドウズの SMB サーバ(4013389)のパッチを提供しており、アップデートしていない場合は、今回の脅威に対するリスクが伴います。

マイクロソフト社はこれまで、2017 年 3 月 12 日に Windows XP (高価なサポート契約の締結組織のみ対象)と Windows 2003 Server を含むウインドウズの追加のバージョン向け緊急アップデートとしてパッチ emergency patch (KB4012598)の提供を行なっています。

改善

もしなんらかの理由によって、ウインドウズアップデートのパッチが適用できない場合、WannaCry が拡散時に利用する脆弱性を、以下の方法によって避けることが可能です。

- SMBv1 プロトコルの無効化
- ファイアウィールなどの境界セキュリティ製品でのインターネットアクセスや VPN、その他のアクセスポリシーの見直し
- それぞれのネットワーク境界上で、SMB トラフィックの制御の見直し

- イン方向、アウト方向に対する、445/tcp、137-138/udp、139/tcp の制限を設ける
- ウインドウズアップデートのパッチが適用できないレガシーなシステムのネットワーク分離による拡散の防止又は拡散のスローダウン

調査

ラストライン製品のご利用のお客様は、以下の情報で WannaCry ランサムウェアの調査を行うことが可能です。

- ファイルハッシュ値
- ビットコインサイトのアドレス
- 攻撃に利用されるドメイン名
- レジストリキー
- IP アドレス
- ランサムウェアのファイル情報　など

sha1 のファイルハッシュは以下が含まれます。

- 50049556b3406e07347411767d6d01a704b6fee6
- 51e4307093f8ca8854359c0ac882ddca427a813c
- 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
- 87420a2791d18dad3f18be436045280a4cc16fc4
- 8897c658c0373be54eeac23bbd4264687a141ae1
- af7db69cbaa6ab3e4730af8763ae4bf7b7c0c9b2
- c5e6c97e27331b6d38717e156ba89df1387d94f7
- df815d6a5fbfc135d588bf8f7e9d71319aef2a8d
- e889544aff85ffaf8b0d0da705105dee7c97fe26
- eba84b75362fa0b1486e9458b6a2f2bdc25d19fb
- 45356a9dd616ed7161a3b9192e2f318d0ab5ad10

ビットコインアドレス

- 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
- 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
- 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

以下の活動内容で検索を実行

Lastline Network Analysis の Network Activity で SMB のスキャン活動を検索すると以下のスクリーンショットのように検索可能です。

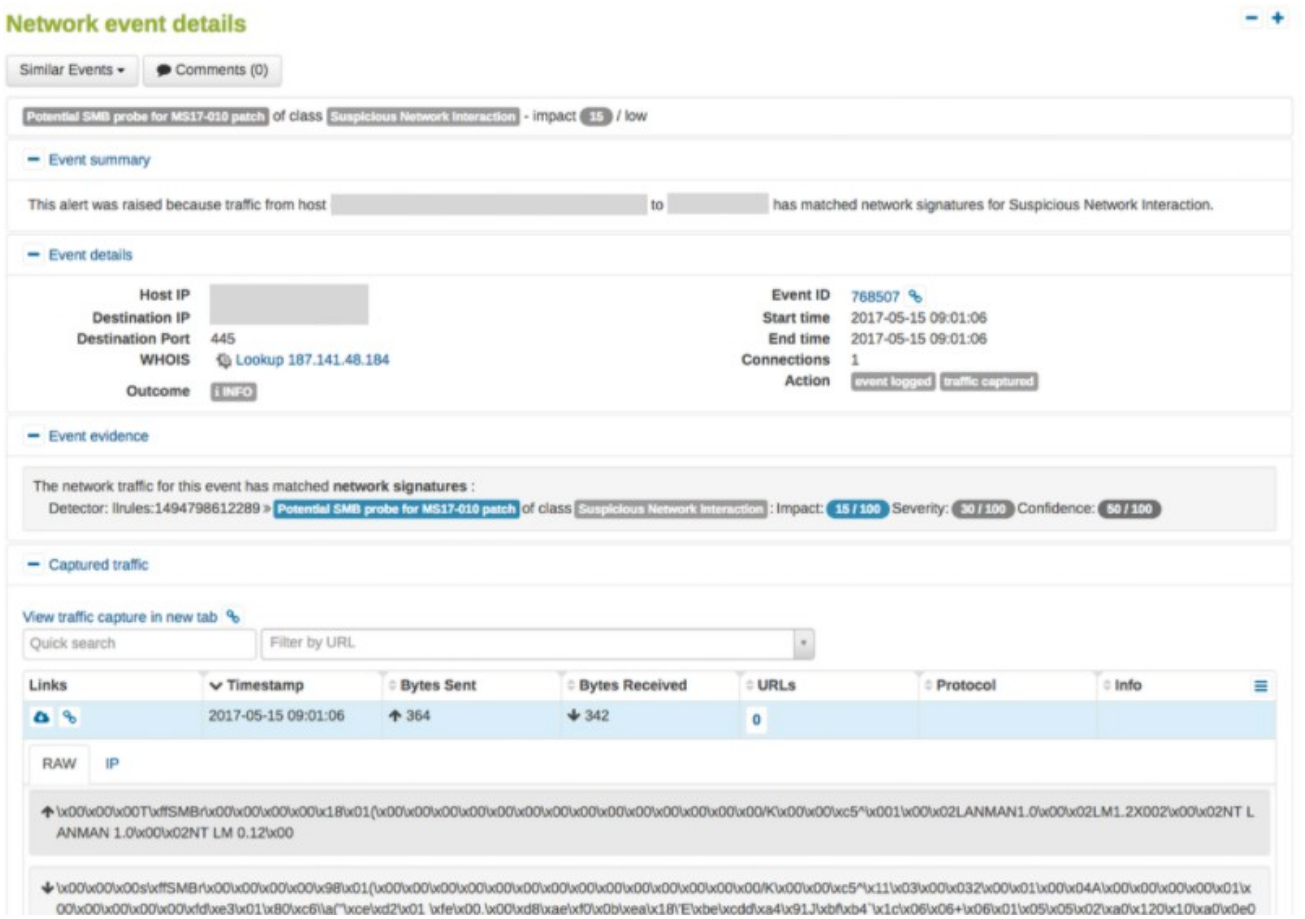


Figure 3 - SMB トラフィックの検知情報①

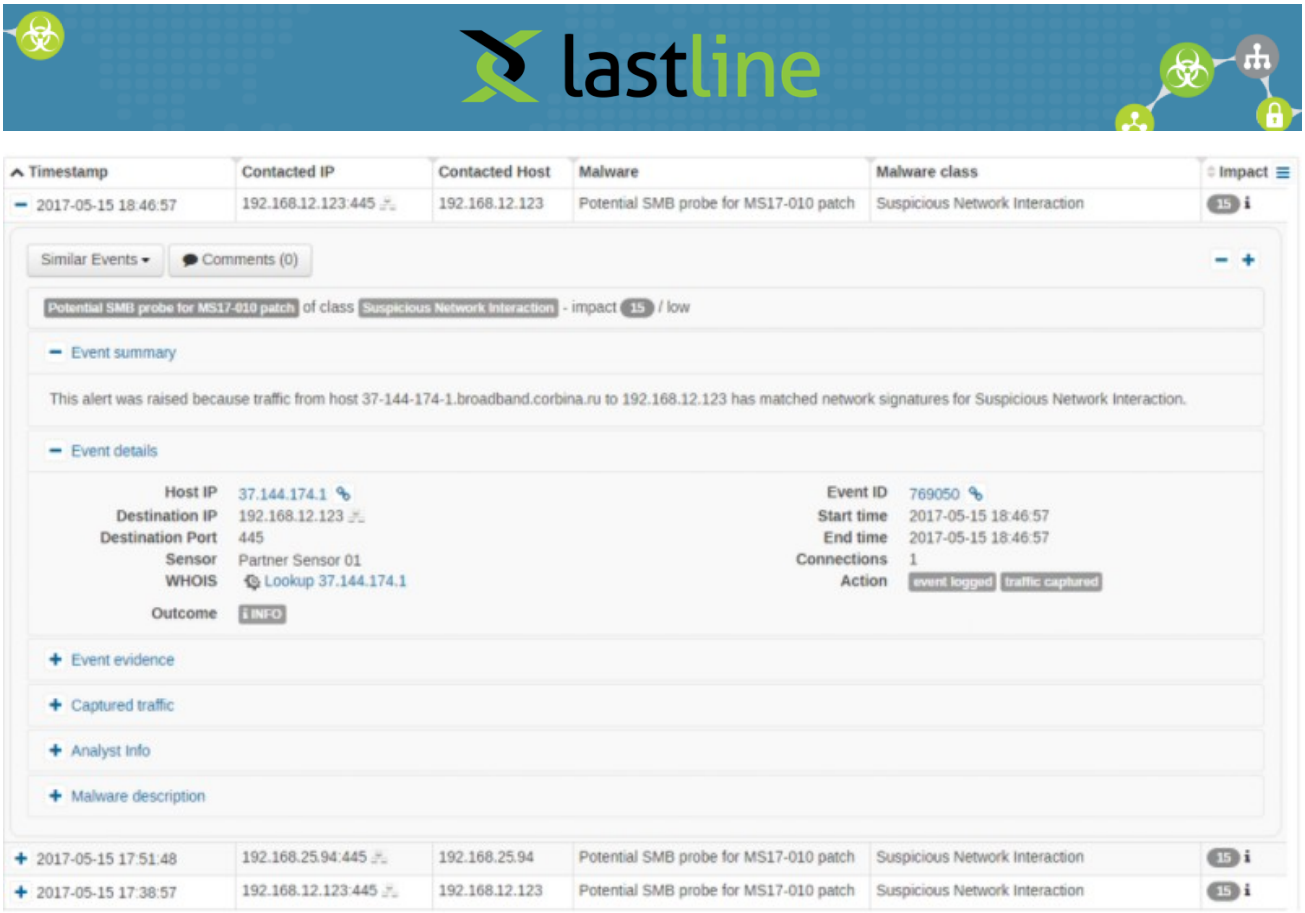


Figure 4 - SMB トラフィックの検知情報②

Knowledge Base License をご購入のお客様は、Intelligence タブで WannaCry から生成された Mutex を以下の名前で検索することで、すでに感染した装置検索やその再感染を防ぐことが可能です。

MsWinZonesCacheCounterMutexA

また、このランサムウェアによって生成されたファイルを、以下のキーワードで検索可能です。

@WanaDecryptor@.exe

以下のサイトへのアクセスを制限、または DNS での名前解決を実行させないようにすることで、拡散を軽減できます。

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- ifferfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb.com
- iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com

以下の IP アドレスへのアクセスは、WannaCry への感染が疑われます。これらの IP アドレスへのアクセス制限することで被害を最小限に抑えることが可能です。ただし、これらの IP アドレスは他の脅威を監視することにも利用されるシンクホールでも利用されます。よって、組織内からアクセスがあったとしても、WannaCry への感染が確実というわけではありませんのでご注意ください。

- 144.217.254.3
- 144.217.74.156
- 184.168.221.43
- 217.182.141.137
- 217.182.172.139
- 52.57.88.48
- 54.153.0.145
- 79.137.66.14

WannaCry Version2 では、以下の場所にレジストリキーを生成することがわかっています。

- HKLM¥SOFTWARE¥WANACRYPT0R

組織内への教育

組織内のユーザーに、改めて面識のない人からのメールに添付されているファイルを開かないこと、面識があっても添付ファイルを開く際には、サブジェクトや本文、署名、添付ファイル、メールヘッダーなど、注意深くチェックをすることなどの注意喚起を行いましょう。

また、今回のような大規模な攻撃の後には、悪意ある攻撃者は、IT 部門やマイクロソフト社、セキュリティ企業、サポート部門を名乗って、フィッシングメールや OS やアプリケーションなどのアップデートを促すメールを送信することがあります。添付ファイルだけでなく、本文の URL リンクなどをクリックする際にも最新の注意が必要です。

セキュリティ制御の適用

組織内ネットワークとインターネットなどの外部やリモート接続などとの境界において、Lastline Enterprise のように、ランサムウェアを含む未知のマルウェアを検出する技術の導入は有効です。Lastline の技術はソフトウェアライセンス及びサービスを含んでおり、販売店からの Lastline 製品の購入に加え、OEM やテクノロジーアライアンスパートナーからも提供させていただいております。

※ 本記事は、2017 年 5 月 15 日に米国 Lastline, Inc.より公表された以下のブログの翻訳版です。
情報は全て以下のブログ公表時の情報です。
https://www.lastline.com/blog/wannacry-ransomware/

※ ランサムウェア関連の以下の記事も併せてご覧ください。
https://www.lastline.com/labsblog/ransomware-delivery-mechanisms/
https://www.lastline.com/labsblog/ransomware-overt-hide-part-2/

Lastline, Inc.について　https://www.lastline.com

米国 Lastline 社は、多くのセキュリティ研究機関やセキュリティベンダーに利用されているバイナリファイル分析「Anubis（アヌビス）」、Web サイト脅威分析「Wepawet（ウェパウェット）」の開発者により、2011 年に設立されました。設立メンバーは、カリフォルニア大学サンタバーバラ校とノースイースタン大学の教授および研究者で、15 年以上の研究開発成果を基に次世代サンドボックス技術を製品化し、APT（Advanced Persistent Threat）を含む標的型攻撃とゼロデイ攻撃に特化した、高検知かつ低誤検知率のマルウェア防御ソリューションを提供しており、OEM 提供も含めて世界で三万社以上の導入実績があります。

本記事の連絡先：

Lastline, Inc.

Senior Systems Engineer, North Asia

橋本　賢一郎　khashimoto@lastline.com

〒100-0005

東京都千代田区丸の内 1-8-3　丸の内トラストタワー本館　20F

TEL：03-5288-5386　FAX：03-5288-5686