RAMPANT RANSOMWARE

猛威を振るうランサムウェア：
WANNACRYへの
対応と攻撃を防ぐ方法

Accenture Security

ハッキングの最新手口：
WANACRYPTOR

サイバー攻撃の多様化と絶え間ない進化によって、世界中の企業や団体は増大するリスクに直面しています。ランサムウェア（別名クリプトウェア）は、企業のデータを攻撃し、感染したPCをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。相手に支払いをしても復号される保証はありません。警視庁や情報処理推進機構は、今後このような攻撃の発生頻度が高まり、多くの企業が標的となり、身代金の要求額はますます増えると警告しています。この種の攻撃の最新手口がWannaCry（別名WanaCrypt0r）です。

複数の情報源によると、2017年5月12日、セキュリティ研究者やさまざまな組織は、複数の組織を標的とするマルウェアによるセキュリティ脅威が発生し、世界中の国々に感染が広がっていると報告を始めました。その日、WanaCrypt0rと呼ばれるマルウェアは急速に広まり、160カ国以上で混乱を引き起こしました。感染したコンピュータ1台につき300ドルから600ドルに相当する身代金をビットコインで支払うよう要求したのです。

アクセンチュア・セキュリティとiDefense（セキュリティの研究機関。2017年にiDefenseのセキュリティ・インテリジェンス事業をアクセンチュアが買収）による共同チームは、事件発生以前から継続的に情報を収集しており、主要なフィッシング活動とその他のマルウェアファミリーおよび関連のハッカーについて調査し、WanaCrypt0rによって最初に使用されたインフラストラクチャのノード6カ所のうち5カ所をすでに特定していました。以前のマルウェア攻撃でも使われたノードを事前にリスト化したことによりサンプルが特定のTorの出口ノードを使うことに気が付きました。iDefenseはお客様に情報提供を行い、2017年3月の時点でこの攻撃で最初に使われた脅威のインフラストラクチャのいくつかを保護していました。これに加えて、アクセンチュアのサイバーディフェンス・サービス（インシデント・レスポンスとエンドゲーム社のエンドポイント・ディテクション・アンド・レスポンス（EDR）インテグレーションを用いたスレット・ハンティングなど）を活用していたお客様も、脅威が拡散する前にエンドゲーム社の行動解析と機械学習エンジンのおかげで保護されていました。

「WannaCry」感染に関する統計

90,000
以上のシステムが感染

最初に感染したのは
医療業界／通信業界

160
カ国以上で感染

感染した国：ロシア、中国、台湾、ウクライナ、米国、カナダ、韓国、フランス、インド、ブラジル、香港、日本、英国、ドイツ、ポーランド、チリ、メキシコ、スペイン、イタリア

WannaCryに対する現在の評価

この攻撃は組織に対して極めて大きな影響を及ぼし得るもので、感染したらどのような組織でも業務に混乱が生じるほどの脅威であることを認識すべきです。初期のWanaCrypt0r亜種に組み込まれていた“キルスイッチ”のドメインはシンクホールに登録されましたが、まだこのマルウェアは重大な脅威だと考えています。それは、新しい亜種が今後も出現する可能性があり、標的となった組織が効果的なパッチやその他の管理手段を持ち合わせていないと考えられるからです。それに加えて、他のハッカーがより強力な亜種を使って別の組織を攻撃する際、同じ脆弱性を利用するだろうと私たちは考えています。

技術的な詳細情報

初期の報告では、フィッシング活動によってマルウェアに感染するとされていました。しかし、セキュリティ提供会社や感染した組織では攻撃を媒介したＥメールなどを特定できませんでした。セキュリティのコミュニティは数件のＥメールを特定しましたが、それらが送り込んできたのは異なるマルウェアファミリーでした。さらなる調査で、ハッカーによりWindowsのSMBの脆弱性を利用した可能性が明らかになりました。マイクロソフトは2017年3月14日、この脆弱性を解決するセキュリティ更新プログラムMS17-010をリリースしました。しかし、被害を受けた組織では、パッチを適用せずインターネットに直接アクセスしたシステムが悪用され、それらが初期の感染媒体になったと考えられています。

WanaCryptOrの主な特徴

- 感染したシステム上にあるファイルを暗号化するか判断するのにキルスイッチを使用
- キルスイッチは単純なURLチェックのリクエスト
- 3月12日にアクティベートされており、システムがそのURLにアクセスできない場合（プロキシやその他理由で）はファイルを暗号化

感染したコンピュータごとに無作為なパブリックキーとプライベートキーのセットを作成する非対称暗号を使用

シャドーコピーを削除して、エラーを無視するようWindowsのブートメニューを変更する機能

Windowsのファイル共有リソース（IPCを含む）を使ってネットワーク内で横方向に感染を広げるワームとしての機能

セキュリティ情報MS17-010（ETERNALBLUE–CVE-2017-0145）に記載されているSMBの脆弱性を悪用する機能

ユーザーのリモート デスクトップ プロトコル（RDP）セッションを悪用する機能

身代金要求のメッセージを27カ国語で表示

Torクライアントを使用

ビットコインでの支払いを要求

WanaCrypt0rを防ぐ

ランサムウェアWanaCrypt0rから組織を守るために、以下のアクションを推奨します。

- 適切なパッチ管理の実施を導入し、セキュリティ更新プログラムを即座に評価・展開する。優先度が高いのはWanaCrypt0rに悪用された脆弱性を修正するパッチ（MS17-010）
- 厳格なポリシーを課し、個人のノートPCから共有ネットワークリソースへの接続を防止
- 以下のキルスイッチWebサイトへのアクセスを、ブロックはせずに監視する。
  - iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea <.> com
  - ifferfsodp9ifjaposdfjhgosurijfaewrwergwea <.> com
- SMBv1を無効化
- SMBプロトコルでの送受信、または信頼できないネットワークとのRDP接続を無効化
- アンチウイルス製品とエンドポイントソリューションのバージョンを常に最新に保ち、タイムリーな脅威情報と統合
- ストレージデバイスやサーバー、エンドユーザーのコンピュータに保存された情報を定期的かつ安定的にバックアップ
- 業務上の必要性がない限り、Torやピア・ツー・ピア、その他の同様なサービスへのネットワークトラフィックをブロック
- 感染または検知した場合、感染したシステムをネットワークから即座に切断
- 感染したシステムをできる限りイメージ（適切と思われる場合、証拠となるイメージをキャプチャ）した上で、ユーザーのデータをバックアップコピーから復元。細心の注意を払って最初に感染したシステムを発見し、システムが再感染するのを回避する

セキュリティを第一に

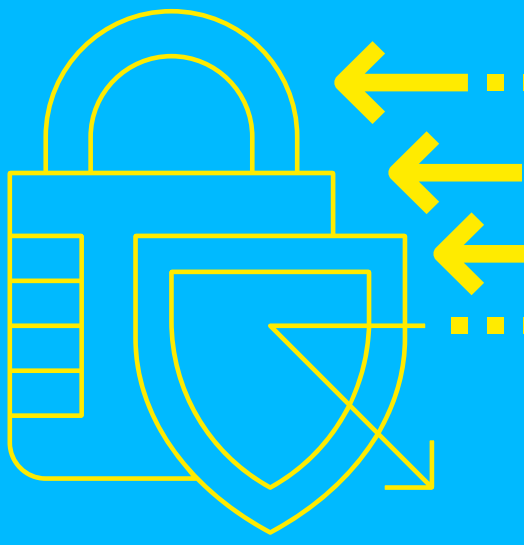
最近のサイバー攻撃の手口は決して想定外のものではありません。しかしその規模、つまり感染した国と組織の数は前代未聞です。結果として多くの組織で業務に重大な影響が生じ、この攻撃は“極端な”マルウェアと認定されました。感染からの復旧だけでなく、似たような脅威や亜種の攻撃を防ぐために、そして究極的には将来のランサムウェア攻撃に備えて組織の安全性を高めるために、一刻も早く適切なステップを踏まなければなりません。

アクセンチュア・セキュリティは2016年に発表したレポート内で、ランサムウェア・アズ・ア・サービス（RaaS）という新しいサイバー犯罪の動きを取り上げています。悪意のあるハッカーが実際に金銭を脅し取るマルウェアをキットにまとめたもので、技術力の低いハッカーでも努力や技術的な知識なしで攻撃できるようになるのです。

2016年前半、インターネット上には新しいランサムウェアの亜種についてのレポートや、公的ならびに民間セクターで幅広い分野のさまざまな組織がランサムウェアに感染したというレポートが拡散していました。よく知られているのはハリウッド長老教会派医療センターが2016年2月に感染した事例です。救急車の受け入れを拒否したことに加え、コンピュータを使えなくなった病院スタッフが手書きで患者情報を記録することを余儀なくされ、最終的に病院は非常事態に陥りました。

現在まで話を進めると、サイバー攻撃のシナリオは英国の国民保健サービス（NHS）やその他多くの世界中の組織で繰り返されています。ランサムウェアは新しいものではありませんが、ユーロポール（EUの警察機構）によれば、WannaCryマルウェアによる今回の攻撃は、前代未聞の大規模なものでした。

次ページ以降では、ランサムウェア攻撃の被害者とならないためにセキュリティ対策の先進的な企業が採用した対策を紹介します。



フィッシング
攻撃

大半のランサムウェア攻撃はフィッシング攻撃から始まります。防止に向けたトレーニングと意識向上プログラムを社員が受講することにより、フィッシング詐欺の明らかな兆候と取り扱い方法が分かるようになります。

＜主な対策・プログラム＞

不正なEメールを見分けて問題を回避するためのトレーニング

ソーシャルエンジニアリング攻撃を受けたと思われる場合の対処方法

指導内容に対する社員の習熟度を評価する定期的なテスト

ランサムウェアと
Eメールの管理

ランサムウェアはＥメール経由で攻撃をすることが多いので、Eメールの管理を強化すると、悪意あるEメールが社員に届くのを防ぐことができます。

＜Eメール環境を保護するためのステップ＞

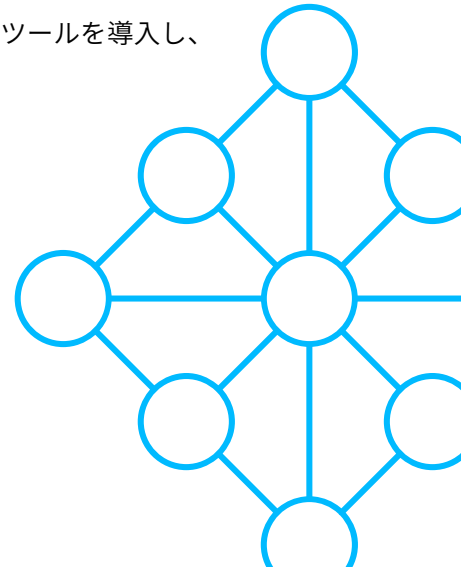
- 強力なスパムフィルターを使い、疑わしいＥメールがエンドユーザーに届くのを防ぐ。
- なりすましを防止するためにセンダー・ポリシー・フレームワークとドメイン・キーズ・アイデンティファイド・メールを使って受信メールを認証。
- 送受信されるEメールをスキャンして脅威を検知し、実行可能なプログラムをフィルターにかける。
- ProofpointやマイクロソフトATPなど、クラウドベースのＥメール解析ソリューションを導入し、悪意のあるＥメールを通じて広がる既知の脅威を特定・隔離。
- 企業の外部から来たＥメールであることが明白に分かるようにＥメールの設定を変更し、社員にさらなる注意を促す。
- ファイルの拡張子を表示するようにし、JavaScriptなど通常は社員に送られることのないファイルタイプを見分けやすくする。
- マクロをサポートせず、文書を開かなくても内容を見ることができるマイクロソフトのOfficeビューアーをインストールする。

インフラストラクチャを
保護する

ハッカーはさらに賢くなり、疑いを持たない社員がミスを犯して悪意のあるEメールを見逃すことも考えられます。

＜インフラストラクチャを守るためのアクション＞

- 社内のPC管理者権限を解除または制限。
- 特徴的な挙動の有無を調べる等の行動分析を含み、頻繁に署名をアップデートするエンドポイント保護を使用。
- PCのセキュリティ準拠プログラムを維持し、すべての関連ツールが備わり動作することを確認。
- サーバーとPCが同じネットワークに属さないようにネットワークを分割。
- セキュリティシステムを見直して設定を適正化／強化（ウイルススキャナー、ファイアウォール、侵入防止システム、Ｅメール/Webゲートウェイ）。
- 実行コマンドを「いいえ」に初期設定。これによって認証済みアプリケーションを特定し、それぞれのプログラムが何を変更・更新できるかを制限でき、サーバーが安全に保たれる。また、ランサムウェアがサーバーを操作したり、悪意のあるソフトウェアをダウンロードしたりするのをブロックする。
- OSとアプリケーションのパッチを定期的に適用し、既知の脆弱性が悪用されないようにする。
- 管理者権限を、本当に必要としている人だけに限定して与える。
- SIEMソリューションを設定し、事案にフラグを立ててクリーンアップの手法を自動化する。
- Webフィルター/URLブロッカーを導入または強化する。社員はフィッシングのＥメールに含まれるリンクをクリックするだけでなく、感染の疑いがあるWebページを開くことでもマルウェアに感染する恐れがある。Webフィルタリングはランサムウェアをホスティングしているサイトをブロックするほか、サーバーの操作をブロックする。
- OpenDNSやフォースポイント、パロアルトなどのクラウドベースの解析ツールを導入し、既知の悪意あるWebサイトからのトラフィックをブロックする。



強力な
事業継続計画

ランサムウェアの攻撃は無作為ではなく、標的を定めた意図的なものです。最善の防御措置を講じても攻撃を受けてしまう恐れはあります。回復のための強力な事業継続計画を策定しておけば、身代金を支払うような事態を回避できます。

＜ランサムウェアに効果のある事業継続計画のポイント＞

重要タスクを容認可能な時間内で終えられるよう回復目標を整合する。

回復計画を定期的に、見直し、更新、テストする。

万が一攻撃を受けた場合もバックアップが暗号化されないよう、PCとファイルサーバーをバックアップ用デバイスに常時接続すべきではありません。

加えて、バックアップ・ソリューションは古いバックアップの上書きではなく、定期的なスナップショットを保存する方法を導入してください。

アクセンチュアはすべての企業・組織が現在のマルウェア対策を見直し、最新の取り組みを導入することを推奨します。このような対策により、ランサムウェア攻撃に対する組織の脆弱性は減少します。しかし進化した脅威には十分な対応ではないため、新たな脅威やそれを防止するための最新手法に関する情報にも常に注意を払うよう、強く推奨しています。

付録
WANACRYPTORのIOC（痕跡）と検知シグネチャ

iDefenseは以下のURLとドメインを含むネットワークトラフィックをブロックするよう推奨します：

gx7ekbenv2riucmf.onion	hxxp://178.16.208.58:443	rddetpruqlmh2.com
57g7spgrzlojinas.onion	hxxp://86.59.21.38:443	gljc5nmgzacv.net
xxlvbrloxvriy2c5.onion	hxxp://91.121.83.108:41962	gjgwfrwmefhyrr2evy.com
76jdd2ir2embyv47.onion	hxxp://104.131.11.214:8080	76ylh2uax.net
cwwnhwhlz52maqm7.onion	czrrumvbl5ck6s3ma.net	w64mek2oznzvkf.com
hxxp://193.23.244.244:443	bnq7nevohqmz45d43n.com	
hxxp://217.79.179.177:9001	b4e6t3df.net	

検知シグネチャ

以下の検知シグネチャを使って感染を検知することができます。

```
rule EQN_SMB1_PatientZero{
    meta:
        description = "Detection of network traffic towards the 1st
sinkholed domain - kill switch"
        author = "Kiran Bandla - iDefense"
    strings:
       $smb1_free_hole = { 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff
fe 00 00 40 00 0c ff 00 00 00 04 11 0a 00 }
        $ipc = "\\\\%s\\IPC$"
        $userid = "__USERID__PLACEHOLDER__"
        $treeid = "__TREEID__PLACEHOLDER__"
        $old_c2 = "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"
    condition:
        $smb1_free_hole and $ipc and $userid and $treeid and $old_c2
}
rule WanaCrypt0r
{
        meta:
            description = "Detects artifacts from WanaCrypt0r Ransomware"
            author = "Leo Fernandes - iDefense"
         strings:
            $a = "WanaDecryptor"
            $b = "Wana Decrypt0r"
            $c = "WanaCrypt0r"
            $d = ".wnry"
            $e = ".WNRY"
            $f = "bitcoin"
            $g = "vssadmin"
            $h = "torproject"
        condition:
            4 of them
}
```

さらにiDefenseは、MS17-010が悪用された可能性を検知するために、セキュリティ識別子によって特定されたエマージング・スレッツ・スノートの規則（https://rules.emergingthreats.net/）を実装するよう推奨します：

2024207	2024213	2024219
2024208	2024217	2024220
2024212	2024218	

iDefense IntelGraphで、WanaCrypt0rインテリジェンス・アラートをチェックして最新情報を入手してください：「WanaCrypt0rのテクニカル分析」https://intelgraph.verisign.com/#/node/ intelligence_alert/view/15bae2ae-8743-4526-ae5e-2e595d572302?source=search

IntelGraphで以下の関連情報を入手できます。

マルウェアファミリー

“WanaCrypt0r,” https://intelgraph.verisign.com/#/node/malware_family/view/e891c945-e821-4158-9d62-c20743e0e292?source=search

検知シグネチャ

“WanaCrypt0r.yara,” https://intelgraph.verisign.com/#/node/detection_signature/view/193089a5-bb97-4a3d-a32f-ccabccf98287?source=search

“WanaCrypt0r_SMB.yara,” https://intelgraph.verisign.com/#/node/detection_signature/view/aeb5f1bc-555d-423f-99c1-bcb582803840?source=search

脅威グループ

“SpamTech,” https://intelgraph.verisign.com/#/node/threat_group/view/7802308f-0d3c-499c-989b-e60f416ceb27?source=search

ファイル

“e333604e0d214d03328a854df130377f,” https://intelgraph.verisign.com/#/node/file/view/71cfa24e-fa8a-4d96-b558-8e53bb15db7f?source=search

“db349b97c37d22f5ea1d1841e3c89eb4,” https://intelgraph.verisign.com/#/node/file/view/13dfa64b-027b-4e37-9ea8-f13b261eac91?source=search

お問い合わせ先

アクセンチュア株式会社
〒107-8672東京都港区赤坂1-11-44
赤坂インターシティ
Tel: 03-3588-3000（代）
Fax: 03-3588-3001（代）
Mail: info.tokyo@accenture.com

アクセンチュアについて

アクセンチュアは「ストラテジー」「コンサルティング」「デジタル」「テクノロジー」「オペレーションズ」の5つの領域で幅広いサービスとソリューションを提供する世界最大級の総合コンサルティング企業です。世界最大の規模を誇るデリバリーネットワークに裏打ちされた、40を超す業界とあらゆる業務に対応可能な豊富な経験と専門スキルなどの強みを生かし、ビジネスとテクノロジーを融合させて、お客様のハイパフォーマンス実現と、持続可能な価値創出を支援しています。世界120カ国以上のお客様にサービスを提供する41万1,000人以上の社員が、イノベーションの創出と世界中の人々のより豊かな生活の実現に取り組んでいます。

アクセンチュアの詳細はwww.accenture.comを、
アクセンチュア株式会社の詳細はwww.accenture.com/jpをご覧ください。