CYLANCE

2017 年
脅威レポート

目次

エグゼクティブサマリー 3

2017 年脅威解析の主要な調査結果 3

概要 4

1 回だけ利用される標的型マルウェアの増加 6

N デイエクスプロイト 7

Big Ten 8

- WannaCry 9
- Upatre 10
- Cerber 10
- Emotet 11
- Locky 12
- Petya 13
- Ramnit 13
- Fareit 14
- PolyRansom 15
- Terdot/Zloader 16

マルウェアファミリー以外のトレンド 17

- リンクの脆弱性
  サプライチェーンへの攻撃 18
- 速度と勢い：
  猛烈なスピードのランサムウェア 20
- 存在し続ける低レベルのサイバー犯罪と
  隠れた不正行為 21
- マネーロンダリング 22
- ウォレットを利用したトロイの木馬 22
- 多面的な攻撃 23
- ファームウェアとハードウェアの脆弱性の攻撃 23
- 徹底的な破壊 - 回復不能 24
- アトリビューション：
  重要な領域／重点の移行 25

結論 26

エグゼクティブサマリー

2017 年のサイバー攻撃は、前年よりも数が多く、高度で、容赦がなかったことが判明しました。CIA から盗んだ知識と、NSA から奪ったツールで武装した脅威アクターは、熟達度が高まっていることを示しました。2017 年の 2 つの顕著な脅威である WannaCry と NotPetya では、世界中のシステムへの攻撃で、これらの盗難されたアセットが利用されました。

2017 年には、サービスとしてのランサムウェア（RaaS）で新たな好機が生じ、誰もがマルウェアを作成して、利益を得ることができる可能性が生じました。ファイルレス攻撃の進展によって、これまで信頼性の高かった検出方法から脅威を隠すための新たな手段が提供されました。多様性などのマルウェアの特徴は、従来の防御を回避するために引き続き強力な役割を果たしています。

サイバー犯罪の被害を受ける対象は、民間企業から選挙まで広範囲にわたっています。フランスと米国では、最近の大統領選挙中に、大規模なデータ漏洩が生じました。複数の有名企業では、サイバー攻撃によって顧客の個人情報が漏洩し、ブランドの信用が低下し、業務の復旧に膨大なコストがかかりました。

本レポートには、2017 年にサイランスの顧客が直面した脅威のトレンドとマルウェアファミリーの概要を示します。この情報は、新たに発生し、発展しているサイバー脅威に対して共に戦うため、セキュリティ担当者、研究者、個人を支援することを目標として提供されます。

調査方法

サイランス® は、マルウェア、不正なスクリプト、ファイルレス攻撃、その他の高度な脅威によるセキュリティ侵害からエンドポイントとサーバーを保護することに重点を置いたセキュリティソリューションを提供しています。軽量エンドポイントエージェントと暗号化通信チャネルを通じて脅威が検出されたときに、テレメトリーデータを含むイベントに関する情報が、サイランスクラウド内の顧客のプライベートテナントに送信されます。本レポートの大部分は、2016 年 1 月 1 日～ 2017 年 12 月 31 日の間に収集された匿名脅威データに基づいています。

2017 年脅威解析の主要な調査結果

- サイランスは、2017 年に企業 1 社あたり平均 3,918 件の攻撃を防御しました。これは、前年比およそ 13.4% の増加に当たります。
- 当社の顧客ベース内では、食品業界とサービス業界が、最も多く攻撃を受けました。
- ランサムウェア攻撃は 2017 年中に 3 倍に増加し、すべての業界に影響を及ぼしていますが、最も影響を受けたのは医療業界です。
- トップ 2 の感染ベクターは、依然として電子メールと自動ダウンロードです。
- 企業環境内で実行される脅威による上位のリスクは、システムの損害とデータの破損です。

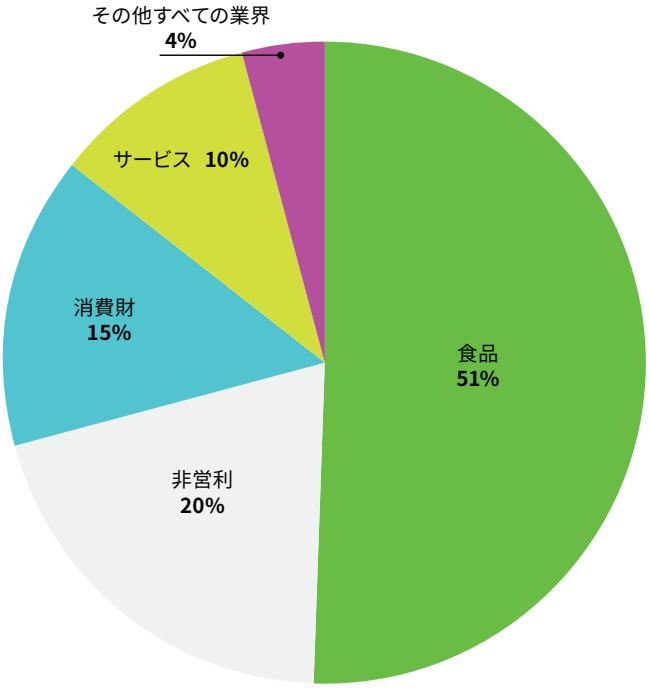
サイランス脅威レポート

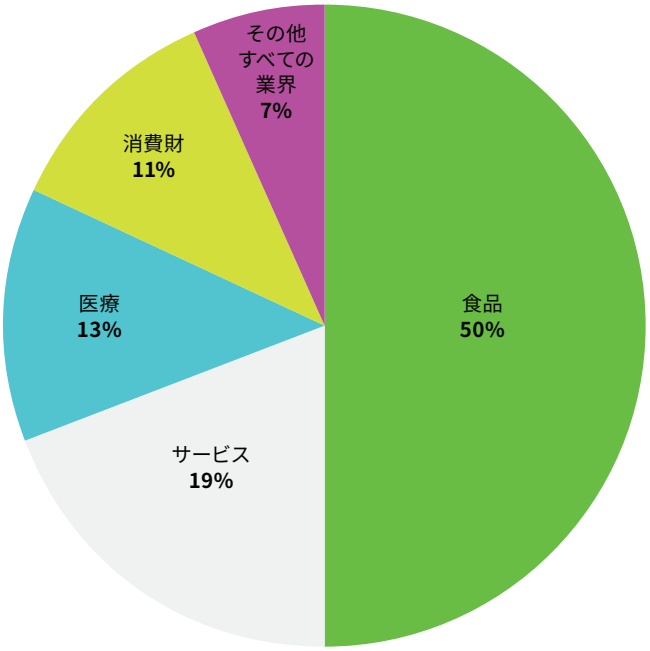
概要

概要

前年と同様に、当社の顧客ベース全体で脅威活動の増加が確認されました。コモディティ化したマルウェア、不正なスクリプト、新たに利用可能になった攻撃の配布方法により、現在、最低限の攻撃スキルを有する者が、標的型攻撃を仕掛けることが、これまでになく容易になっています。

2017 年に、サイランスは 160 を超える国において、世界中の企業 1 社あたり **3,900** 件（同一攻撃を除く実数）の攻撃を防御しました。サイランスエコシステム内で確認された攻撃数は、2016 年と比較して、約 **13.4%** 増加しました。また、当社は、2017 年に食品業界がさまざまなタイプのマルウェアによって最も攻撃を受けたことを確認しました。2 番目に多く攻撃を受けた業界は、サービス業界でした。**サイランスエコシステムでの偏りを減らすため、業界ごとに調査結果の平均値を求めました。**食品業界は、2016 年にもマルウェア攻撃を最も多く受け、この年に 2 番目に多く攻撃を受けたのは、非営利組織でした。





2016 年のマルウェア調査結果

影響を受けた業界

食品	51%
非営利	20%
消費財	15%
サービス	10%
その他すべての業界	4%

2017 年のマルウェア調査結果

影響を受けた業界

食品	50%
サービス	19%
医療	13%
消費財	11%
その他すべての業界	7%

1 回だけ利用される標的型マルウェアの増加

マルウェアの指数的な増加とさまざまな業界に対する大量の攻撃の一因は、1 回だけ利用される多様な形態のマルウェアです。サイランスの顧客コミュニティ内で、ブロックされた脅威の 70% 超は、サイランス以外のいかなる者によっても確認されたことのない脅威でした。次のセクションでは、当社が「Big Ten」と呼んでいる脅威について説明します。これらのトップの脅威・マルウェアが多く使われてきたのは、便乗的な攻撃に利用されることが多かったためでしょう。

公開されているマルウェアシグネチャのリポジトリは、実際のマルウェアの網羅的なカタログであると誤解されることが多くあります。こういった誤った認識があるがゆえに、ユーザーがあるファイルが脅威であるかどうか判断するために、マルウェアのシグネチャの公開情報源を使ってハッシュを調べたり、バイナリを検証したりしてしまうのです。実際、シグネチャの公開リポジトリは、実際の攻撃に使われるすべてのマルウェアの包括的、完全、最新、または信頼性の高い記録では決してありません。これは、共通脆弱性識別子（CVE）にやや似ています[1]。

CVE は、ソフトウェアとハードウェアの脆弱性をカタログ化し、文書化している網羅的な標準に最も近いものです。議論の余地はありますが、CVE は、カタログ化と文書化をきわめて適切に実施しています。しかし、これが完全であり、すべてのソフトウェアとハードウェアの脆弱性を網羅していると言うのは正しくありません。また、CVE の割り当てには時間がかかることが多く、脆弱性が明らかになった後に、脆弱性に CVE が割り当てられるまでに数日以上かかることがあります。したがって、脆弱性に CVE が割り当てられていないからといって、その脆弱性が危険ではないと想定してはなりません。同様に、公開リポジトリに含まれていないマルウェアも、危険なマルウェアです。**悪意ある攻撃者は、自ら作成した脅威が公開マルウェアリスト（またはその他の普及しているリスト）に登録されることを望まず、これを防ぐために特定の対策を講じる場合が多いことも考慮に入れなければなりません。**

悪意ある攻撃者のバイナリが公開リポジトリに登録された場合、攻撃者は監視され、関連するアクティビティに反応し、対処を行い、無効化しなければならなくなります。

多くの場合、攻撃者は、見つかることなく継続的に活動するために、一度だけ利用されるバイナリ、またはホストや攻撃に固有なバイナリを利用します。Project Sauron や Poseidon などの標的型攻撃では、過去数年間にこのアプローチのバリエーションが確認されました。ターゲット環境内におけるファイルの場所を厳密に制御し、きわめて規則正しく管理すると、パブリックハッシュ／チェックサム／ IOC ルックアップに依存している脆弱なセキュリティ対策ではこれらの脅威が検知されなくなります。成功した悪意ある攻撃は、その構成要素が確認されるまで、しばしば数ヶ月さらには数年間にわたって発見されることなく、活動することがあります。発見された時点でさえも、ファイルが公開リポジトリにアップロードされ、他のアナリストがそのファイルを選択し、対処を行い、その内容を明らかにする一連のイベントが生じるためには幸運が必要なことも多くあります。攻撃者が、発見された場合のために、作成する脅威を複雑化し、解析を阻止するための対策を講じていることも多く確認されています。仮想マシン（VM）を無効化する技法、ハードコーディングされた時間制約、ホスト／環境固有のロジックはすべて、難読化と解析の複雑化につながります。

この 1 回だけ利用し、発見を回避するアプローチは、高度な標的型攻撃のみに限られるわけではないという事実はとても重要です。毎日のように発生するコモディティ化したマルウェアを使った攻撃でも、このアプローチが確認されます。これには、ホストに固有な鍵を持つランサムウェアや、一般的なリモートアクセス型のトロイの木馬をはじめとした多数のトロイの木馬などがあります。このような回避技法の一部は、安価／無償のパッカーおよびクリプターに組み込まれていることさえあります。

要するに、すべての脅威に対する情報源として公開リポジトリを信頼することはできません。**高レベルなコモディティ化コードから高度な標的型攻撃まで、最も懸念されるマルウェアは、決して公開リポジトリに登録されません。**

「実際、シグネチャの公開リポジトリは、実際の攻撃に使われるすべてのマルウェアの包括的、完全、最新、または信頼性の高い記録では決してありません。」

N デイエクスプロイト

攻撃の数の増加に加えて、エクスプロイトなどの従来の攻撃ベクターは依然として多く利用されています。攻撃者は、企業や組織への攻撃を試みるために、引き続き既知の脆弱性を悪用しています。**実際、2017 年に確認された多くの攻撃は、攻撃が検出され、ブロックされる 9 ヶ月以上前に報告された脆弱性が悪用されていました。**この手法は、メディアで報道される比較的大規模な標的型攻撃の一部で顕著に用いられました。たとえば、Patchwork と Confucius の攻撃では、アクティビティの後半の段階でさえ、その時点で 1 年（以上）前に報告された 2015 年と 2016 年の脆弱性 [1] が悪用されていました。

仮想通貨を無断でマイニングするマルウェアの感染には、比較的古い脆弱性がよく使われています。公開サーバー（Web サーバーなど）へのフルアクセスを可能にする脆弱性は、攻撃者にとって格好の餌食です。たとえば、2018 年第 1 四半期に、Web サーバーへのアクセスを可能にする CVE-2017-10271 の悪用が顕著に増加しました。これは、悪意あるアクターがマルウェアを感染し実行する必要がある場合に、迅速で確実なアクセスを可能にする脆弱性の一例（Oracle WebLogic）にすぎません。この脆弱性の悪用と概念実証コードが 2017 年末から 2018 年初頭にかけて十分認識されるようになった後でも、その攻撃は引き続き成功していました。このトレンドは続いており、仮想通貨のマイニングを行うマルウェアの感染に EternalBlue が使われていました。これは、非常に拡散しやすく、収益を生む可能性のある組み合わせです。SMB の脆弱性である CVE-2017-0144（および関連 CVE）については 2017 年 3 月にパッチがリリースされているにもかかわらず、2018 年第 1 四半期の時点で未だ多く悪用されています。

企業のシステムには、オンサイトデバイス、リモートデバイス、インフラストラクチャにめったに接続しないデバイスなど、さまざまなデバイスが混在しています。そのため、企業全体のシステムに対するセキュリティ対策は、IT 管理者にとってすでに負担の大きい作業になっています。パッチの適用されていないシステムに対する脆弱性攻撃があることや、1 回だけ利用される変化の著しいポリモーフィックな脅威による攻撃が多数ある中、こうしたシステムに対するセキュリティ保護はますます困難になり、対策コストが高くなっています。この状況により、クラウドへの継続的な接続が不要で、定期的なシグネチャとルールの更新を必要としない、ゼロデイペイロードを検出しブロックすることができるソリューションなど、既知の脆弱性を悪用した攻撃の影響を軽減する方法が、多くの企業や組織で需要が高まりました。

NotPetya と WannaCry の急速な広まりは、多様な形態の脅威およびパッチ管理に対する懸念を高め、世界中の企業や組織に対して警鐘を鳴らしました。本レポートで後に詳述するこうした攻撃によって、多くの企業や組織は、自社のセキュリティ戦略を見直し、急速に広まる脅威に対処する新たな方法を再び探すようになりました。Microsoft は漏洩した NSA ツールに関連する多くの脆弱性にその後パッチを適用してきましたが、単独犯や国家などの攻撃者が、すでに次の攻撃を計画しているのは確かです。したがって、今はセキュリティチームがリラックスできる時間ではありません。セキュリティチームは、脅威の突発的な拡散が一時的に収まっているこの時期を利用して、自社の防御を強化すべきです。

ケーススタディー：業務用電子メールのセキュリティ侵害

このケースの状況は、映画「トワイライト・ゾーン」の一場面のようでした。企業は、自社に対して不正行為を行い、誰もその理由を説明できませんでした。電子メールは、適切な当事者が、不正な小口決済システム（ACH）の各取引を承認したことを示していました。しかし、いずれの承認者も、同意したことを思い出せず、自分の名前が記載されているその電子メールを見たことさえありませんでした。

サイランスはこのインシデントを調査し、真相を究明するよう依頼されました。当社の調査員は、手がかりを得るため電子メールシステムを調査しました。調査員は、複数の電子メールクライアントに、一部の従業員の電子メールを迷惑メールフォルダに振り分ける不審な電子メール処理ルールがあることを発見しました。

攻撃者は、不正な支出の承認のために迷惑メールフォルダを利用することによって、最初の要求者から承認者の CFO まで、すべての者になりすましていました。サイランスによるさらなる解析により、電子メールシステムは攻撃によるセキュリティ侵害を受けていなかったことが示されました。攻撃者は、正当な認証情報を使用して Outlook Web Access(OWA) サーバーにログインし、その窃盗計画を実行しました。

このケースの調査終了時に、サイランスは以下のことを推奨しました。

- 特に特権アカウントや管理アカウントでリモートにアクセス可能なリソースとユーザーに対して、できる限り幅広く多要素認証を実装する。
- 環境内で発生しているアクティビティについて常に通知を受けるため、Office 365 で監査を有効にする。
- 監査ログを一元化し、不審なアクティビティに対してアラートを生成する。
- 複雑さよりも長さを優先した強力なパスワードポリシーを利用する。

[1] confucius - CVE-2016-7193、CVE-2015-1641、CVE-2017-11882、CVE-2015-1641
Patchwork - CVE-2012-1856、CVE-2014-4114、CVE-2017-0199、CVE-2015-1641

Big Ten

2017 年にサイランス顧客コミュニティ内で最も広まった脅威。このセクションでは、攻撃者の間で以下の攻撃の人気が高まった理由を検討します。

WannaCry

ビジネスへの影響：

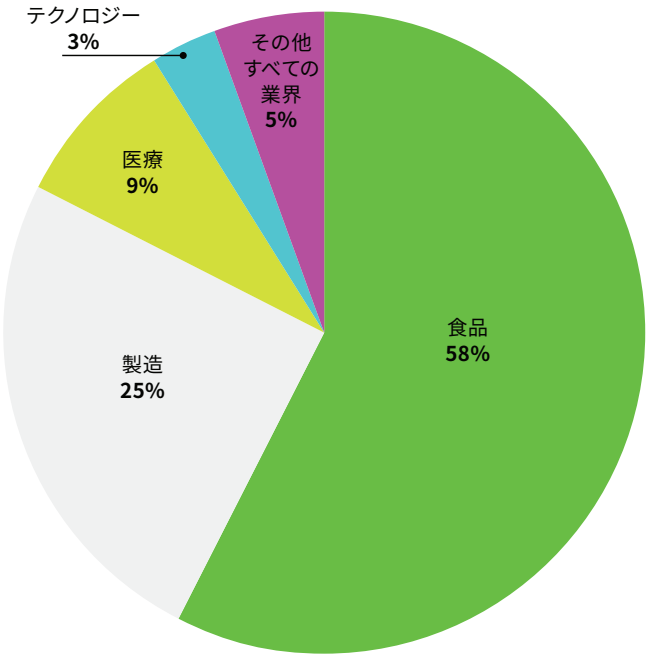
コンピューターのデータが暗号化され企業側で復号できないと、永続的なデータの損失につながります。多くの企業がWannaCry攻撃に直接起因する収益への著しい影響を報告しました。

多くの人々は、感染したコンピューターを深夜に再構成しなければならなかったり、不安感が高まったりするなど、WannaCryのさまざまな影響を感じていました。WannaCryは、多くの企業を警戒させました。残念ながら、WannaCryが発見されたのはこれが最初ではなく、これが最後になることもありません。複雑なソフトウェアシステムにバグはつきものです。しかし、こうしたバグを見つけて悪用するには、きわめて高い知識やスキルが必要になってきており、悪用するには時間もかかるようになっています。WannaCryの出現で、このような破壊的なエクスプロイトを危険な兵器と同じように扱ってしっかり防御しないとどうなるかを目の当たりにしました。

私たちはチームとして、WannaCryの新しい亜種がサイランス製品で確実に検知できるようWannaCryの動向を追跡してきました。その結果、驚くほど多くの亜種に手を焼くことになりました。私たちは、攻撃に使われた亜種の全貌をより鮮明に把握したいと考えました。攻撃者がWannaCryのワーム機能を変更する可能性はいろいろありましたが、実際にはこのワームのペイロードを置き換えたりその機能を大幅に変更したりという試みは見られませんでした。このパッケージ化されたランサムウェアの主な目的は、広まっているワームに大規模ではないけどもほどほどの変動性を持たせ、単純なハッシュベースのブラックリストによって検知される感染が鈍化するのを防ぐことのように思われます。

幸い、WannaCryの広がりは、キルスイッチドメインの発見と有効化によって、大幅に抑制されました。また、Adylkuzzと呼ばれる別の系統のマルウェアで、拡散のために同じSMBエクスプロイトを利用したビットコインマイナーがWannaCryの少し前に発生したことにも、WannaCryの広がりを抑制する効果が多少ありました。Adylkuzzは、感染システムでポート445を閉じるようWindowsファイアウォール設定を変更します。このことは、WannaCryの拡散能力に影響を及ぼした可能性があります。

「Adylkuzzは、感染システムでポート445を閉じるようWindowsファイアウォール設定を変更します。このことは、WannaCryの拡散能力に影響を及ぼした可能性があります。」



WannaCryによる業界別の影響

食品	58%
製造	25%
医療	9%
テクノロジー	3%
その他すべての業界	5%

WannaCryのモジュール的な性質について言うと、WannaCryのモジュール的な性質について言うと、公開リポジトリからのSMB悪用コードが再利用されているだけでなく、他の場所のコードが再利用された強力な証拠があるように思われます。このため、単純なコード解析の観点からアトリビューション作業を行うことは非常に困難になります。個々の構成要素も複雑性が多様であり、大部分は難読化があまり使用されていない分かりやすいものですが、このこともコードの再利用の可能性と、複数の作成者の関与を示唆しているように思われます。

最後に、数百もの亜種が出回っていることが判明したと広く報告されました。このような報告にはある程度の信頼性がありますが、明らかに過半数は、キルスイッチ領域を変更するために主に研究者によって修正されたオリジナルコードの加工バージョンであるか、ディスク上またはメモリ内のイメージから抽出／キャプチャされ、ハッシュ値は異なりますが、機能は同じであるサブコンポーネントのいずれかであると思われます。

Upatre

ビジネスへの影響：

従業員と顧客のデータが失われ、個人情報の盗難のリスクが高まります。

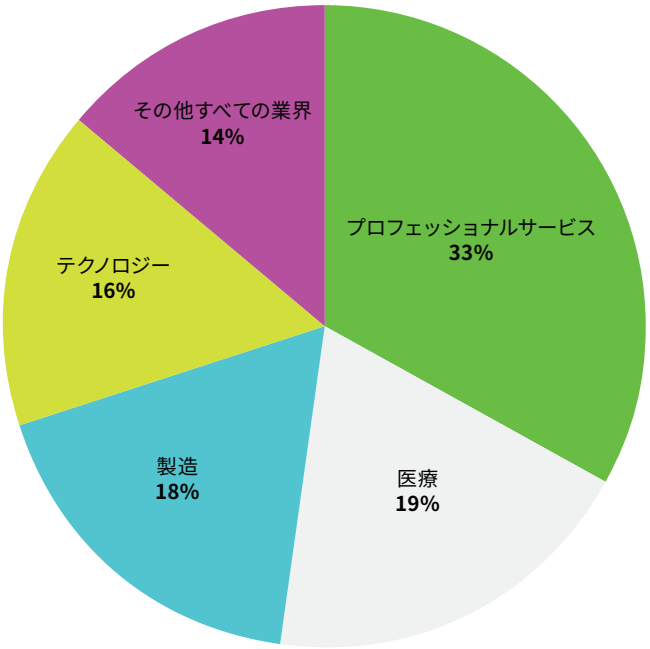
Upatre は、金融機関を標的にしたトロイの木馬、Dyre/Gozi に関連する亜種の多いドロッパー／ダウンローダーです。一般に、zip ファイルを添付した不正なスパム攻撃を通じて配布されます。エクスプロイトキットを通じた配布も確認されました。不正なスパムを利用した攻撃において、多くの場合、zip ファイルには不正な .scr ファイルや .exe ファイルが格納されています。ユーザーがこれを実行した場合、クローンが %TEMP% に配置され、起動されます。次に、金融機関を標的とするトロイの木馬の主要なペイロードが、通常 HTTP を通じて、コマンドアンドコントロール（C2）サーバーからダウンロードされます。C2 サーバのドメインまたは IP アドレスはこのマルウェア本体に埋め込まれています。金融機関を標的とするトロイの木馬は、金融情報や個人情報を盗み、闇市場での取引のためにその情報を提供します。この脅威は、個人と企業に対して同様に影響を及ぼし、個人情報やクレジットカードデータの意図しない漏洩によって、明らかに金融および法律上の被害を受けます。

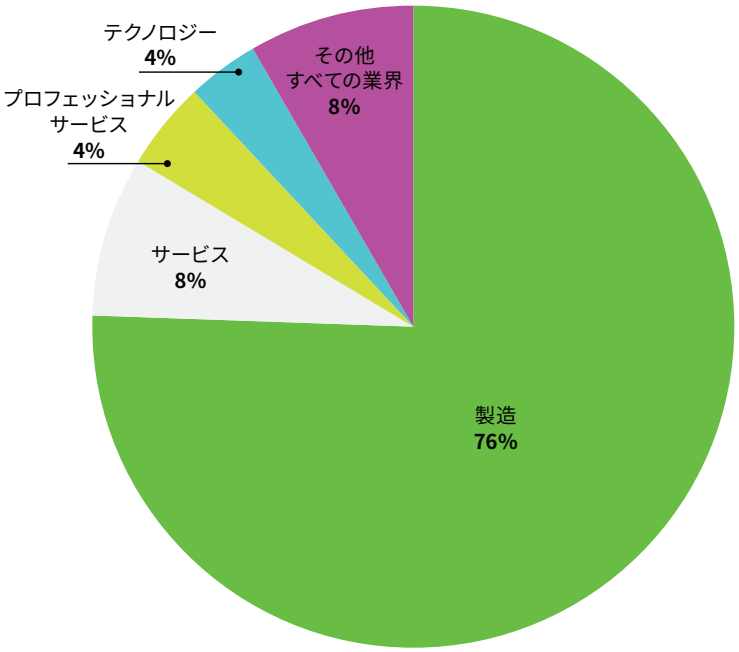
Cerber

ビジネスへの影響：

企業や組織がデータを復号できないようコンピューターに影響を及ぼすため、データの永続的な損失につながります。

Cerber は、不正なマルウェアによって配布されるサービス拒否ボットです。これは、オーディオデバイスにフックして、シャドーコピーを削除し、RC4 と RSA のアルゴリズムを使用してファイルを暗号化し、データベースを暗号化した後に、被害者に音声で脅迫します。過去に、Cerber は、被害者の地域に応じてフィンガープリントを適用し、被害者が以下のいずれかの国に属するかどうかを特定していました。アルメニア、アゼルバイジャン、ベラルーシ、ジョージア、キルギスタン、カザフスタン、モルドバ、ロシア、トルクメニスタン、タジキスタン、ウクライナ、ウズベキスタン。いずれの国にも属さない場合、Cerber は攻撃を続けました。





Upatre による業界別の影響

プロフェッショナルサービス	33%
医療	19%
製造	18%
テクノロジー	16%
その他すべての業界	14%

Cerber による業界別の影響

製造	76%
サービス	8%
プロフェッショナルサービス	4%
テクノロジー	4%
その他すべての業界	8%

「数年を経て、Cerber は Hash Factory サーバーの採用など、アンチウイルス回避技法を組み込みました」

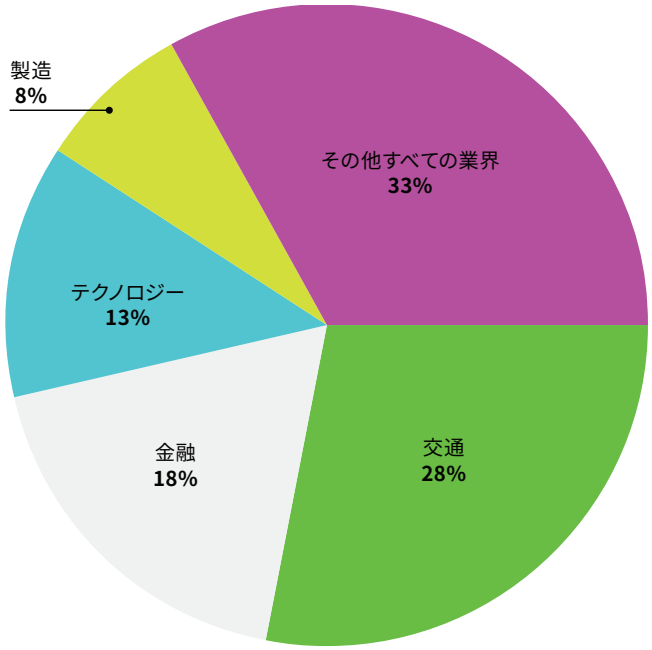
数年を経て、Cerber は Hash Factory サーバーの採用など、アンチウイルス回避技法を組み込みました。このサーバーでは、15 秒ごとにハッシュが無作為に生成され、暗号化されたファイルに隠され、system.dll という名前の NSIS プラグインを使用してメモリに自らをロードするか、カスタム DLL デコーダを使用して、その内容をメモリにロードし、復号します。Cerber に含まれるもう 1 つの新しい特徴は、オフラインで動作する機能です。Cerber は、ファイルレス攻撃の例に含まれることがあります。これは部分的にしか正しくなく、少なくとも言及する攻撃の段階によります。より最近の攻撃では、JavaScript と PowerShell の複数のレイヤーを利用して、ペイロードを直接ダウンロードして実行するか、実行とダウンロードを遅らせ、所定の時間または状態でペイロード全体を実行します。難読化された JavaScript コマンドと PowerShell コマンドのレイヤーにわたって最終ペイロードを埋め込むことにより、検知回避能力と永続性を向上させることができます。しかし、結局のところ、ファイルレスといっても、依然として、感染に使われるファイルやスクリプト／コマンドがあるので、最終ペイロードが実行される前に複数のポイントで防御できるわけです。

Emotet

ビジネスへの影響：

機密性の高い従業員データと顧客データが失われます。

Emotet は、Feodo トロイの木馬ファミリーの亜種です。これは、銀行の認証情報およびその他の機密性の高い情報を盗むことを目的とするトロイの木馬として、2014 年に最初に現れました。ほとんどの場合、これは不正な文書または URL を含むフィッシング電子メールによって拡散されます。この攻撃の最初のステップは、ターゲットに手動で機能を有効にすることを要求するマクロを含む、不正な Microsoft Word ファイルの形式を取ります。スクリプトにはさまざまな難読化技法が使用されていることがありますが、実質的に基本コードは同じです。この難読化されたコードは、プロパティのコメントセクションに保存され、マクロには多数のガベージコードの中に ActiveDocument.BuiltInDocumentProperties 命令があります。このスクリプトは、PowerShell を利用して、certproc.exe として Emotet マルウェアをダウンロードし、実行します。この脅威は、フォルダ \%AppData%\local\microsoft\windows\certproc.exe にコピーを作成した後、レジストリに存続します。Emotet マルウェアは、感染したシステムで機密性の高い情報を探し始めます。攻撃者が関心を持つ情報を見つけた場合、このマルウェアは、C2 サーバーにデータを流失させ始めます。



Emotet による業界別の影響

交通	28%
金融	18%
テクノロジー	13%
製造	8%
その他すべての業界	33%

Locky

ビジネスへの影響：

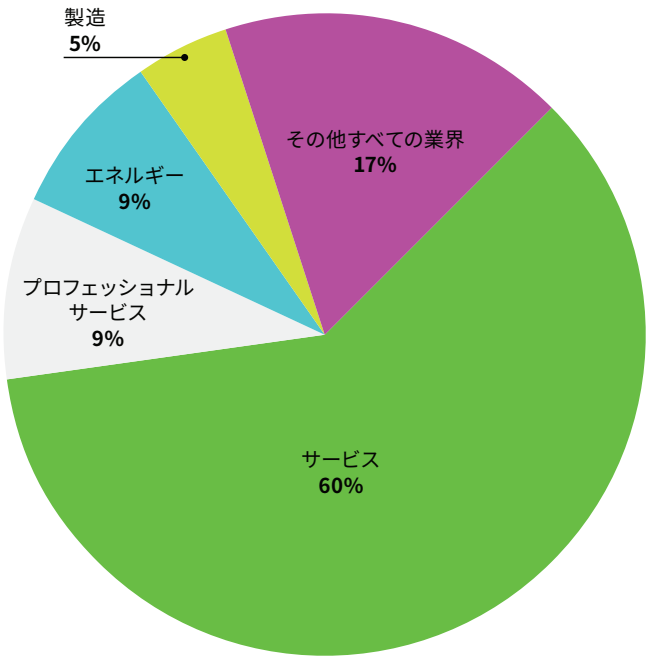
暗号化されたコンピューターが使用不可能になり、機密性の高いデータが失われ、従業員の生産性が低下します。

Locky ランサムウェアは、検出された最初の 1 週間に、40 万を超える被害者に影響を及ぼしました。Locky は、Hollywood Presbyterian Medical Center を攻撃することによって、2016 年 2 月に特に医療業界で顕著な問題を発生させました。この医療機関は、公開された最大の身代金額である 17,000 ドルをビットコインで支払いました。多数の他の大規模な病院も、この攻撃の拡散中に多額の身代金を支払いました。その後、Zepto、Thor、Osiris、Diablo6 など、Locky ランサムウェアの多数の亜種が確認されました。この古いマルウェアは、新しいアプローチを採用する必要がありませんでした。Locky の作成者は、決して修正されることのないプロセスの一部（エンドユーザー）を少しいじるだけですみました。

2016 年の Locky 攻撃の一部は、配信／配布において Dridex マルウェアの手法を使い、最終ペイロードのダウンロードと実行の両方で、PowerShell スクリプトを多く利用するようになりました。Locky の最近の変化は、マルウェアを拡散させるための特に一般的な方法の 1 つである、スピアフィッシング電子メールが利用されたことです。この攻撃は、2 段階で実行されます。最初の段階は、zip アーカイブが添付されたスピアフィッシング電子メールです。このアーカイブには、アーカイブと同じ名前の VBS ファイルが含まれています。

「この古いマルウェアは、新しいアプローチを採用する必要がありませんでした。Locky の作成者は、プロセスにおいて決して修正することのできない唯一の部分であるエンドユーザーの部分を少しいじるだけですみました。」

被害者がアーカイブを展開し、ファイルをクリックすると、VBS スクリプトの実行が開始されます。このスクリプトは、C2 サーバーに接続し、ファイル y872ff2f のダウンロードを試みます。このスクリプトは、異なる名前（GlNPcFUJR.exe）で %AppData%/Local/Temp フォルダにこの第 2 段階のペイロードを保存してから、マルウェアを実行します。2017 年 8 月 1 日にドメイン dbr663dnbssfrodison[dot] net が登録者の電子メール、jenniemarc(at)mail(dot)com を使用して作成されました。このアカウントに対する WhoIs の逆引き検索によって、2016 年から最近では 2017 年 10 月まで、この電子メールアドレスで 333 のドメインが登録されたことが示されます。一部のドメインは、ランサムウェアの他のファミリーに利用されたことが確認されています。



Locky による業界別の影響

サービス	60%
エネルギー	9%
プロフェッショナルサービス	9%
製造	5%
その他すべての業界	17%

Petya

ビジネスへの影響：

機密性の高いデータが破損されます。最近、復号ツールが提供されました。

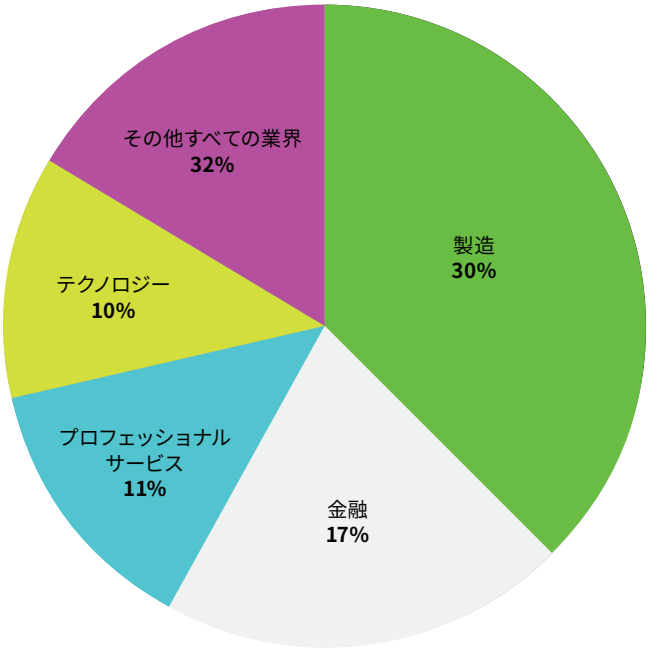
Petya は、複数の亜種と高度な攻撃ベクターを有する非常に強力なランサムウェアであり、2016 年 3 月に初めて出現しました。その感染は、ウクライナの有名組織をターゲットとした攻撃と、このマルウェアによって表示されるトレードマークの点滅する頭蓋骨により、広く知られるようになりました。基本的な亜種は、MFT を暗号化するブートローダー、そのブートローダーをインストールするドロッパー、身代金要求の前に表示される点滅する赤い頭蓋骨で知られています。MFT の暗号化により、特定のファイルだけでなく、ディスク全体が危険にさらされます。Mischa と呼ばれる亜種は、より従来型のランサムウェアとして機能し、Petya が管理者特権を拒否された場合はユーザーモードでファイルおよび実行可能ファイルを暗号化します。Goldeneye と呼ばれるさらに改良された亜種によって、暗号化とディスクロックルーチンが高度化されました。Petya と Mischa のデクリプターは作成されましたが、Goldeneye は復号不能であると思われます。さらに、ワイパー亜種の NotPetya では、暗号化に使用される公開鍵が消去されるため、ユーザーのデータが永久に消去されます。2017 年 7 月時点で、作成者は感染者に対して復号ツールを利用可能にするために使用される秘密鍵を公開しました。

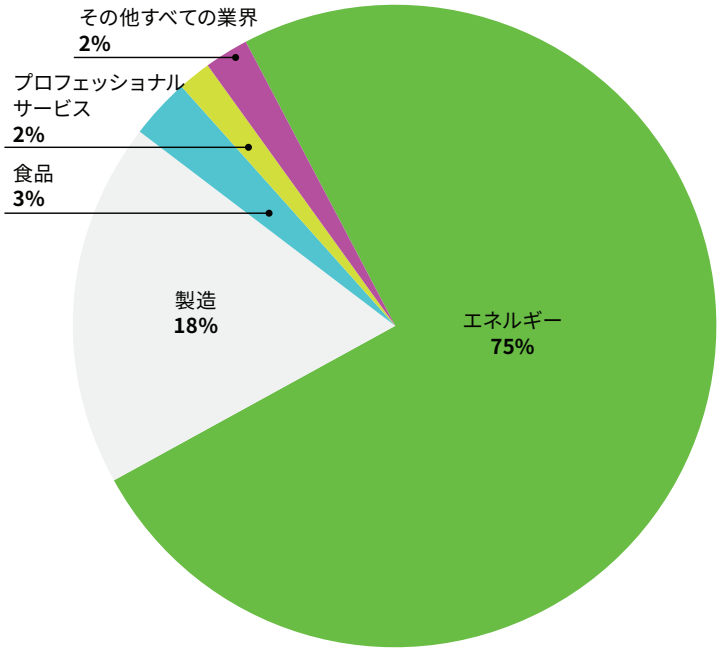
Ramnit

ビジネスへの影響：

機密性の高い顧客情報と従業員情報が失われます。

Ramnit は、Windows PE の実行可能ファイルに感染する寄生ウイルスです。これは、マルウェアへのショートカットファイルを使ったリムーバブルメディアに拡散するワーム機能も備えています。Ramnit は、VBS コードを注入することによって、HTML ファイルにも感染します。この HTML ファイルにアクセスしたユーザーは、このウイルスに感染します。Ramnit は、リモートアクセス型トロイの木馬および金融機関を標的とするトロイの木馬として機能するよう設計されています。2015 年 2 月に、欧州の当局は、320 万台のコンピューターに感染した Ramnit ボットネットを閉鎖しました。しかし、この閉鎖にもかかわらず、Ramnit は、2015 年 12 月に再び出現しました。Ramnit の新しい亜種は、2016 年に英国の大手銀行をターゲットとしました。一部の Ramnit 攻撃は、真のファイルレス方式であり、Power Shell や JavaScript のコードを直接実行せずに動作します。Ramnit は、SSL を通じて取得したレジストリに、XOR で暗号化したペイロードデータを保存することが確認されています。次に、Ramnit のローダースレッドは、レジストリから BLOB を解析し、復号して、この段階で注入を実行できます。





Petya による業界別の影響

製造	30%
金融	17%
プロフェッショナルサービス	11%
テクノロジー	10%
その他すべての業界	32%

Ramnit による業界別の影響

エネルギー	75%
製造	18%
食品	3%
プロフェッショナルサービス	2%
その他すべての業界	2%

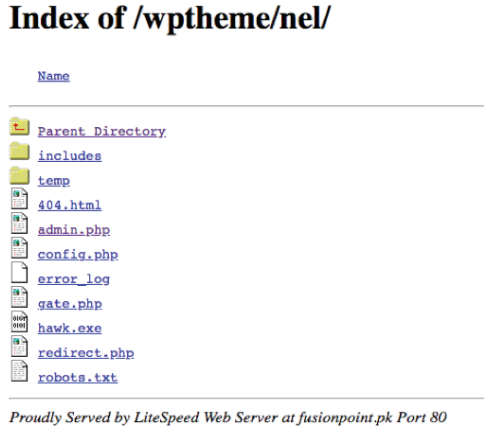
Fareit

ビジネスへの影響：

ユーザー認証情報が漏洩します。

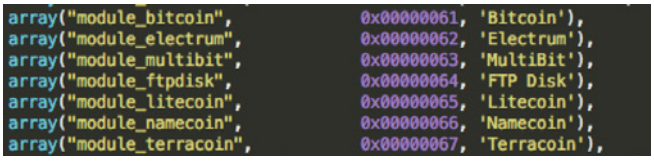
Fareit（別名：Pony/Pony Loader）は、非常に広まっている認証情報収集マルウェアです。これは、他のトリックもいくつか隠し持っています。Fareit は、2011 年以降、さまざまな形式で利用されました。その主な目的は、定義された一連のアプリケーションとプロトコルから認証情報（ユーザー名／パスワードデータ）を収集することです。Chrome、Firefox、Thunderbird などの特に人気のあるアプリケーションから、bisonFTP、Incredimail、Flock などのあまり知られていないレガシーアプリケーションまで、Fareit は、ほとんどすべてのクライアントアプリケーションをサポートしています。

貴重なログインデータの収集に加えて、Fareit は追加のマルウェアを呼び出し、起動するために使用することもできます。このシンプルなツールがまだ多く利用されていることには複数の理由があります。主な要因は使いやすさと、無償で利用できることです。Fareit は、Panel と Builder のシンプルな組み合わせであるため、そのセットアップにはほとんど専門知識が必要ありません。選択した Web サーバーに関連する構成ファイルを置くだけで、これを利用する準備が整います（MySQL、PHP、その他の標準システムが導入されていることを条件とします）。Fareit は、主に不正侵入された正規のサーバー上でホスティングおよび管理されていることが確認されています。そのため、必要なアプリケーションは予め準備されていることが多いのです。



つまり、攻撃者は、インターネットに接続されている Web サーバーのファイルシステムへの書き込みアクセスを取得する方法（エクスプロイトなど）を見つけ、ホストの実際の所有者に気づかれることなく、できる限り長くそのサーバーを悪用します。専用の Fareit/Pony ホストが存在しないことは言うまでもなく、通常はクリーンで安全なホストが侵入により悪用されるほうがはるかに一般的です。設置と管理の容易さに加えて、Fareit は実質的に無償であり、数年間にわたって利用されてきました。さまざまな脆弱性とソースコードの漏洩を通じて、悪意あるユーザーは、数年にわたり Fareit のすべてのバージョンを入手する方法を見つけてきました。最も広まっているバージョンはポスト 2.0（2.2/2.3）であり、悪意あるアクターが、TrojanForge や Fudtool などから非常に古い脆弱性を利用し続けていることが多く確認されています。

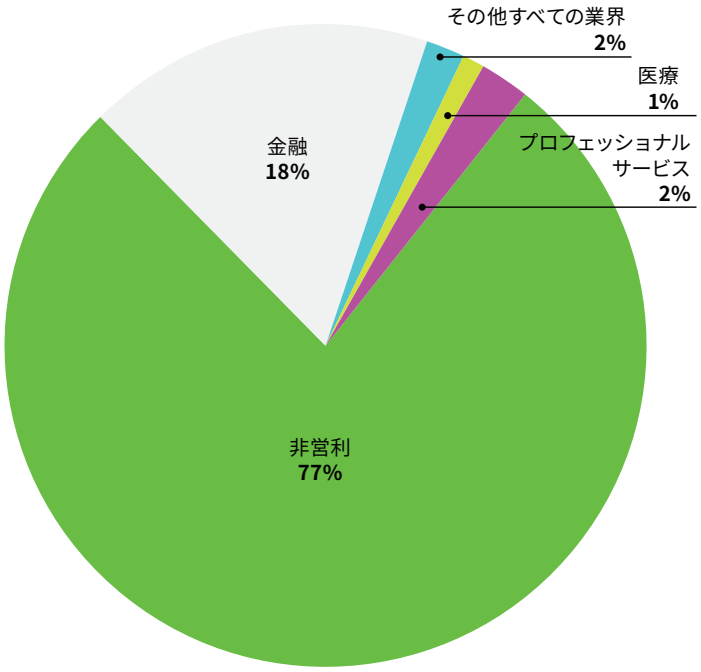
機能に関して、Fareit は認証情報を収集し、悪意あるアクターに送信するという主要な目的において卓越しています。後のバージョンでは、暗号通貨ウォレットサービスと為替取引のログインデータを収集する機能も追加されました。これは、NovaCoin、Primecoin、Frankocoin などのあまり知られていない暗号通貨だけでなく、ビットコインや Litecoin などの非常に人気の高い暗号通貨にも当てはまります。



areit は、早期の攻撃段階で有用なツールであることが実証されました。後の攻撃フェーズで使用する資格情報を収集する手段として、フィッシング攻撃とスピアフィッシング攻撃を通じて Fareit が配布されていることが多く確認されています。

長期的な Fareit 攻撃は、一般に中レベルのスキルの高くないアクターによって管理され、操作されています。開発／スクリプティング言語／サーバー内部のスキルなどを持たない者でも、手動操作をほとんど必要とせずに、サーバーの設置／セットアップおよび初期構成を処理できるよう、セットアップと構成を自動化することができます。Fareit の複数のインスタンスが同じホストで管理され、作業ディレクトリで分けられているケースも非常に多く確認されます。同じホストで他のすぐに使用可能な類似ツールを実行することも、非常に一般的です。Lokibot、Azorult、さまざまなフィッシングキット／ページとともに、Fareit のインスタンスを実行している 1 台のサーバー／ホストが頻繁に確認されます。次のページの画像は、すぐに使用可能なフィッシングキットとともに Fareit がホストされ、一般的な複数の脅威を含むセットアップを示しています。

発見されてから期間が経っているにもかかわらず、Fareit/Pony は、さまざまなレベルの悪意あるアクター間で、人気のある現行のツールであり続けています。このレベルには、一般的なエクスプロイトキット（RIG など）を通じた取り込み／配布が含まれます。起動し、実行するための侵入に対して、ほとんどいかなる障壁もありません。



Fareit による業界別の影響

非営利	77%
金融	18%
プロフェッショナルサービス	2%
医療	1%
その他すべての業界	2%

PolyRansom

ビジネスへの影響：

コンピューターの暗号化によって、ビジネスに不可欠なデータを利用できなくなります。

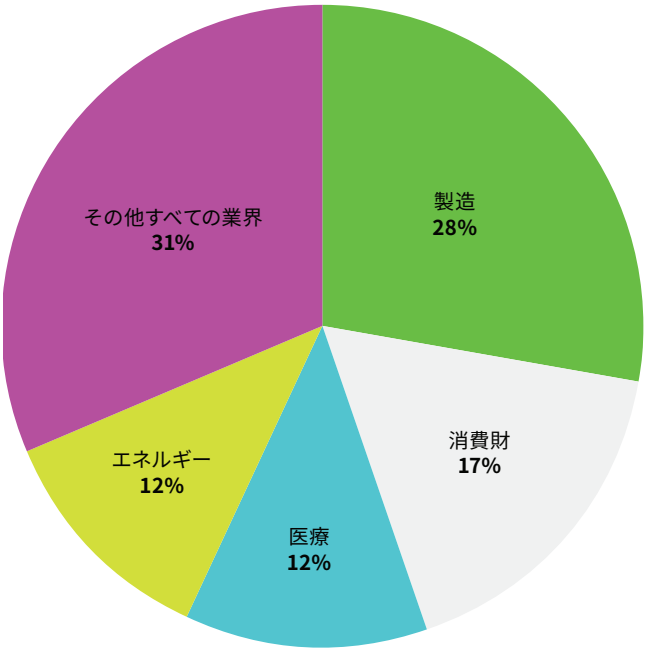
PolyRansom（別名 Virlock/Nabucur）は、非常に亜種が多く、成功しているランサムウェアファミリーの 1 つであるだけでなく、非常に複雑であることも実証し続けています。2014 年に最初に発見された Virlock は、画面ロック機能を備えた寄生感染源でもあるランサムウェアの最初の例です。

PolyRansom は、新たな自己複製を生成し続けることができるため、その解析／リバースエンジニアリングのプロセスがきわめて複雑になります。このマルウェアの寄生的側面を考慮に入れなければならないため、復号ツールは、可能または実行可能であるとしても、コーディングがさらに複雑です。また、暗号化方式の PolyRansom による実装の品質／精度は一貫していません。暗号化レイヤーを簡単に復号できる例もあります。PolyRansom には、特定の時点で必要なコードの最小限の部分のみを復号し、使用後、ルーチンを継続する前にそのコードチャンクを再暗号化する機能があります。この自己のコードに対する再暗号化によって、元のバイナリイメージが変更されます。多様な形態のシナリオと同様に、特に検出制御が検出を処理するために特定のハッシュ／チェックサム／クラウドルックアップに依存している場合、これによりシンプル／基本的な検出制御（シグネチャベースのアンチウイルスなど）が回避されます。

PolyRansom は、上記のファイルに独自のコード（寄生コンポーネント）を追加することによってファイルを処理してから、多くの場合、直接の実行可能ファイルまたは自己解凍 RAR の形式で、実行可能パッケージ／ラッパーを出力します。ファイルの感染／ラッピング時に、この個々のファイルは、実質的に、武器化された、または有効な感染源のコピーになります。この機能は、PolyRansom が真のワームになることなく拡散することができた一因です。共有のストレージ場所（ファイル共有、クラウドベースサービスなど）にあるファイルが感染した場合、ユーザーが感染に気づかずにファイルを開き、または操作しようとしたときに、その感染は、その共有／サービスを通じて拡散する可能性があります。

標準的なランサムウェアの機能に加えて、PolyRansom には、解析を回避するための堅牢な他のメカニズムが含まれています。これには、アンチ VM 機能、カスタム開発パッカーの利用、後に利用されるパック／暗号化された複数のレイヤーなどがあります。実際のファイル暗号化のための暗号化ルーチンも、通常とは少し異なります。ほとんどの確認された攻撃において、暗号化は 2 つの基本的な段階にわたって処理されています。初めに、ファイルは XOR と ROL（Rotate on Left）を通じて暗号化された後に、追加の XOR レイヤーによって暗号化されます。

Virlock/PolyRansom は、Carbanak とその他の大規模な攻撃に関連付けられますが、大規模な攻撃または標的型攻撃のみに利用されるものではありません。このファミリーは、フィッシングや Web ベース攻撃などの標準的な方法を通じて配布されました。



PolyRansom による業界別の影響

製造	28%
消費財	17%
医療	12%
エネルギー	12%
その他すべての業界	31%

Terdot/Zloader

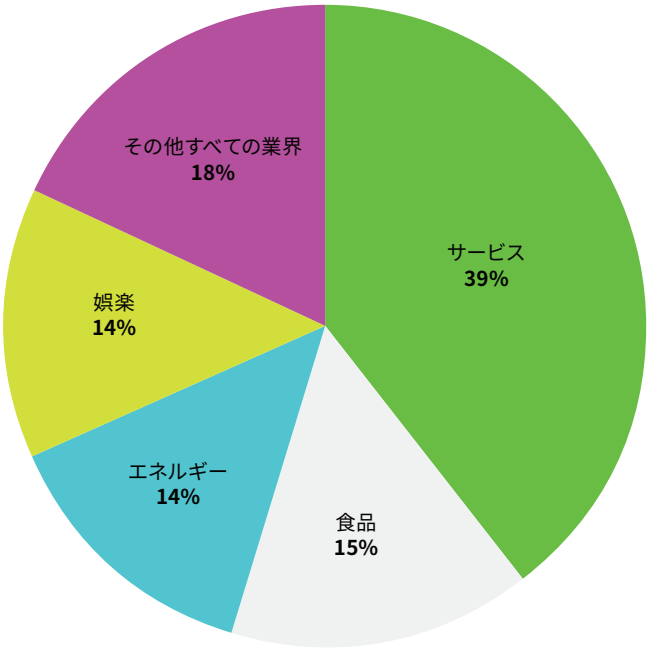
ビジネスへの影響：

機密性の高い銀行および個人のデータが盗まれ、トラフィックデータとページデータが改ざんされます。

Terdot は、2016 年によく知られるようになり、2017 年を通じてさまざまな形式で拡散し続けました。Terdot の起源は、金融機関を標的とする有名なトロイの木馬、Zeus のソースコードにあります。Zeus のソースコードは、2011 年に非常に広く漏洩しました。Terdot/Zloader の主な目的は、Zbot データ盗難コードをダウンロードして拡散することであり、主として銀行およびその他の金融機関を狙うために一般に利用されます。多くの確認された亜種には、バックドア (VNC) 機能も含まれています。Terdot は、Terror や Sundownis などの一般的なエクスプロイトキットに加えて、不正な電子メールメッセージを通じて配布されます。Terdot と Zbot の組み合わせは、SSL 信頼モデルを回避する機能を有するため、特に危険です。このマルウェアは、MITM ブラウザーセッションのために、好みのブラウザーに注入し、独自の偽の SSL 証明書を利用することができます。

```
aData_before    db 'data_before',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1C4ETo
; CHAR aData_inject[]
aData_inject    db 'data_inject',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1554To
; CHAR Str1[]
Str1            db 'data_after',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1335To
; CHAR aData_end[]
aData_end       db 'data_end',0Dh,0Ah,0 ; DATA XREF: sub_1002C43D+1CA3To
; CHAR aWebfakes[]
aWebfakes       db 'webfakes',0         ; DATA XREF: sub_1002F0CF+14CTo
; CHAR aWebfilters[]
aWebfilters     db 'webfilters',0       ; DATA XREF: WebFilters_1002F3A0+14To
```

偽の SSL 証明書の署名を容易にするため、正当な Certutil ツールが利用されます。これにより、機密性の高い銀行／個人のデータを盗むだけでなく、トラフィック／ページデータを変更することもできるようになります。2017 年後半に生じた一部の亜種は、ソーシャルネットワークのアカウントデータを操作してデータを収集し、さらなる拡散を促進するため、自己の実行可能バージョンへのリンクを投稿していることが確認されました。Terdot/Zloader も、攻撃でロシアの被害者を回避する形で、ターゲットを区別していることが示されました（ジオフェンシング）。同様に、ソーシャルネットワークを攻撃する場合、Google+、YouTube、Facebook、Twitter などが格好の攻撃の的となった一方で、ロシアの VK サービスは一般に除外されました。



Terdot/Zloader による業界別の影響

サービス	39%
食品	15%
エネルギー	14%
娯楽	14%
その他すべての業界	18%

マルウェアファミリー以外のトレンド

攻撃に慎重に対処できるように、大量の攻撃がどこで生じているかを把握することは重要ですが、特定の環境に固有な攻撃や、性質上ターゲットが絞られた攻撃に対して計画し、予測することも同様に重要です。

今日のイベントが今後のセキュリティイベントにどのような影響を与えるかを理解するため、以下に、過去 3 年間の混沌としたすべてのセキュリティイベントと攻撃から確認された比較的大きなトレンドをいくつか示します。

リンクの脆弱性
サプライチェーンへの攻撃

長期にわたって信頼されてきたモデルの中核に標的型攻撃が、過去 2 年間に顕著となり、影響が高まりました。安全でセキュアな環境には整合性がきわめて重要であり、高度な攻撃者にとって、データとトランザクションの整合性に対する保証への攻撃がますます利用しやすくなっています。サプライチェーンに対する攻撃は、多様な形を取ることがあります。

特に亜種が多く、損害が大きい攻撃は、正式に思われるチャネルを通じて不正に変更されたコードの形式で配布されてきました。そのプロセス内の 1 つ以上のステップは、悪意あるアクターによって制御されます。多くの場合、攻撃者は、数ヶ月または数年かけて、適切かつ徹底的な調査を実施し、サプライチェーンの脆弱なリンクを苦心して特定します。攻撃者が比較的大規模な最終ターゲットに対して、より小規模なルート（サードパーティ）を特定した場合、攻撃者は次のフェーズの攻撃に進みます。最も抵抗の少ないルートが、常に最も魅力的です。外部コラボレーションシステム、外部更新／パッチ適用メカニズムなどを通じて開発者をターゲットとすることは、ほとんどの場合、ターゲット組織に対するより高速なルートです。

2016 年と 2017 年には、3 件の公開された主要なサプライチェーンのセキュリティ侵害が確認されました（CCleaner、Shadowpad、NotPetya）。サイランスは、こうしたセキュリティ侵害によって、攻撃のレベルが高まるトレンドが生じたと考えています。この 3 つの最近のサプライチェーンに対するセキュリティ侵害は、その前に発生した Kingslayer を初めに検証することによって、分かりやすく説明することができます。

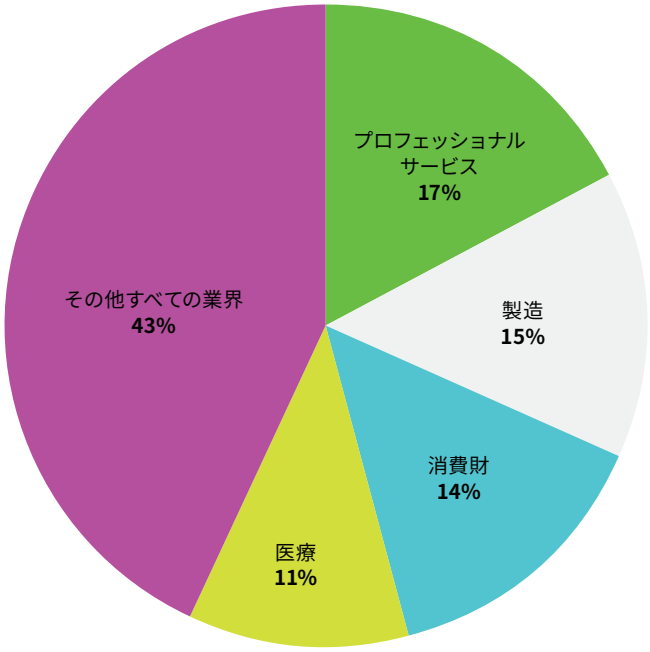
Kingslayer は、2015 年にさかのぼりますが、CCleaner や Shadowpad などの比較的最近のイベントを説明するのに適切な基礎となります。配布された期間は 2015 年 4 月 9 日～25 日と長くありませんが、この攻撃は、最近のモチベーションの高い攻撃者の巧妙さと利用可能なリソースを理解するためのよい例です。Kingslayer バックドアは、トロイの木馬バイナリと、一般的な Windows イベントログ解析ツールのインストーラの形式を取っていました。この攻撃の背後にいるアクターは、比較的短期間に、C2 サーバーをセットアップし、インフラストラクチャを整備しました。この間、正規のアプリケーションをマルウェア化する処理が行われ、正規であるはずというユーザーの信頼は打ち砕かれることになります。トロイの木馬に改変されたバイナリを配布するため、攻撃者は、不正改ざん対象のアプリケーションのソースコードに直接アクセスする必要がありました。このバイナリを配置するにあたって、攻撃者は有効なコード署名鍵でバイナリとインストーラに署名したことも確認されています。これは、攻撃者が、コードのビルドや署名システムだけでなく、ソースコードも制御していたことを示しています。最後に行うことは、正当な配布チャネル（Web サイトなど）にアクセスすることだけです。Kingslayer は、製造企業、政府、金融機関、教育機関、通信企業など、あらゆる業界をターゲットとしました。このレベルの深いセキュリティ侵害と制御、整合性の保証の排除は、2016 年と 2017 年の他の有名な攻撃（CCleaner と Shadowpad）で再現されました。

CCleaner は、被害数でいえば 2017 年の特に大規模な攻撃の 1 つであり、サプライチェーンに対するセキュリティ侵害も発生しました。2017 年 8 月と 9 月の間に、（AVAST/Piriform の）CCleaner と CCleaner Cloud のトロイの木馬バージョンが、正式とみなされたチャネルを通じて配布され、約 250 万台のホストが感染しました。トロイの木馬化された CCleaner のバージョンには、多機能のバックドアが含まれていました。この不正なコードは、感染したホストから機密性の高い情報の収集と漏洩を容易にするだけでなく、追加のマルウェアをダウンロード／インストールすることもできました。全体的な感染範囲は大規模ですが（200 万台超）、特定の感染ホストの 2 次的なペイロードの解析を通じて、攻撃者は特定の情報または特定の企業のデータにも関心を持っていたことを示す兆候が見つかりました。これは、攻撃の背後にいるアクターと思われる存在を考慮に入れれば納得できます。これまで得られた信用できる痕跡を見ると、実績のある有名な中国の APT グループが、この攻撃に関与したことがわかります。このグループ APT17 は、長年にわたって活動し、Operation Aurora、Operation DeputyDog、Operation Ephemeral Hydra など、多数の重大でよく知られた攻撃を実行してきました。CCleaner 攻撃を実行するのに必要な条件を考慮に入れると、APT17 のような確立されたグループによって実行されたことは納得できます。ターゲットを絞った二次的なペイロードの発見時に、AVAST は、以下のような効果的な声明を出しました。

「当社にとって、お客様のコンピューター上の問題を解決することがきわめて重要な事態となりました。当社は、お客様に対して、CCleaner を最新バージョンにアップグレードし（現行バージョンは 5.35 です。影響を受けたバージョンは 5.33 であり、署名に使用された証明書は無効化しています）、Avast Antivirus などの高品質なアンチウイルス製品を利用することをお勧めします。企業ユーザーは、おそらく企業の IT ポリシーに応じて、異なる決定を下すこともできます。攻撃は一部のターゲットのみに絞られていますが、現時点で、当社は企業のコンピューターに感染被害が生じないと表明することはできません」

最終的に、このレベルの攻撃で多くの被害者が生じ、多くの場合、感染ホスト／ユーザー以外に、企業や組織も損害を受けるため、製造、流通、検証のプロセスに対する信頼を立て直さなければなりません。企業が問題を解決できるとしても、露呈された脆弱性を修正し、そのユーザー／パートナー／関連コミュニティ内で信頼を回復し、すべての関連するコストを回収するには、数年かかることがあります。影響を受けたすべての企業が、この規模の被害発生後に回復できるとは限りません。このような事態を防ぐ方法に関して、正式な対話と徹底的な教育の必要性がますます高まっています。

多くの業界が CCleaner の影響を受けましたが、サイランスエコシステム内で、プロフェッショナルサービス、製造、消費財、テクノロジーの業界が特にターゲットとなったことは驚くに当たりません。



CCleaner による業界別の影響

プロフェッショナルサービス	17%
製造	15%
消費財	14%
医療	11%
その他すべての業界	43%

Shadowpad は、CCleaner 攻撃の少し前に配布され、この攻撃には、上述した複数の攻撃と多くの共通する機能的特性がありました。2017 年 7 月に、**NetSarang の Xmanager Enterprise、Xmanager、Xftp、XShell、Xlpd、Xftpd** のダウンロードデータには、トロイの木馬に改変されたライブラリが含まれていました。影響を受けた DLL（nssock2.dll）には、攻撃者が複数レイヤーの複雑な暗号化を通じてリモートに利用できる高度なバックドアが含まれていました。このバックドアは、高度にモジュール化されており、アクティブに組み合わされる C2 サーバーによって、任意のコードのリモート保守／更新、配布、実行をすることができました。また、ペイロードは、レジストリベースの仮想ファイルシステムを通じてコードを生成し、難読化することができました。

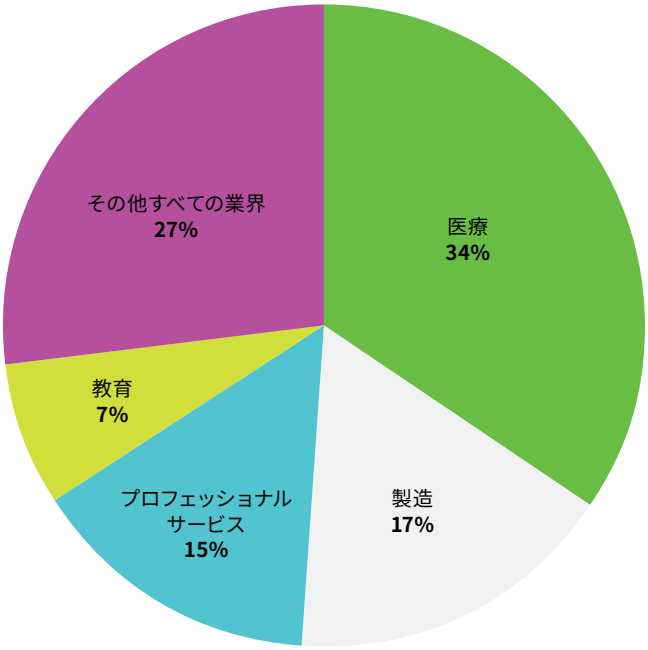
マルウェア化されたバージョンの NetSarang の管理ソフトウェアは、2017 年 7 月 17 日～ 8 月 4 日まで出回っていました。8 月 4 日の時点で、問題が NetSarang に報告され、是正処置が取られました。CCleaner と同様に、Shadowpad の背後にいるアクター（CN グループ、Winnti/Axiom）は、ソースコードと有効な証明書に対するアクセス権を持っていました。マルウェア化されたバイナリは、NetSarang の有効な証明書を使用して署名されました。Shadowpad の背後にある意図は、長期的に、機密性の高いデータ／情報をモニタリングし、盗難することであったことは明らかです。ホストと C2 間の通信は、複数のレイヤーを通じて十分に難読化され、また C2 通信はトランザクションベースであり、また暗号化されています。このことは、標準的な解析方法を通じて不正な通信をモニターすることを一層困難にするため、攻撃の永続性と成功の両方が確実になります。

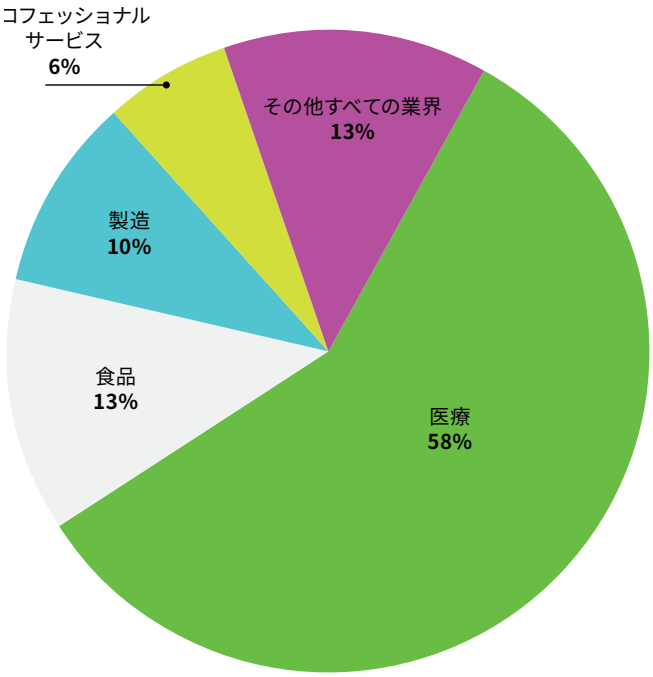
Shadowpad は、医療機関、エネルギー企業および発電企業、金融機関など、さまざまなタイプの業界をターゲットとしました。

NotPetya は 2017 年 7 月に発生し、急速に拡散して、破壊力の高い脅威であることを証明しました。NotPetya は、EternalBlue と DoublePulsar の脆弱性を利用して急速に拡散することができました。また、これは Petya と直接関係していませんが、Petya に似ている MBR の書き換え／上書き機能を備えていました。この特定の脅威では、金銭的な利益ではなく破壊が主な動機でした。しかし、NotPetya はサプライチェーンに対して非常に成功したセキュリティ侵害ともみなされうる点に注意することが重要です。この脅威は、MeDoc と呼ばれるウクライナの会計ソフトウェアパッケージによって初めて配布されました。最初の攻撃において、EternalBlue と DoublePulsar の組み合わせは、感染のさらなる拡大を支援することができました。攻撃者は、NotPetya が出現する数ヶ月前に、MeDoc の更新にバックドアを仕掛け始めました。このような偽の更新によって、攻撃者は、MeDoc インフラストラクチャ内で動き回り、最終的なトロイの木馬を配布／実行することができました。攻撃者は、盗んだ認証情報と Web シェル（PAS）の両方を通じて遅くとも 2017 年 4 月以降から MeDoc 更新サーバーに足掛かりを得ていました。セキュリティ侵害を受けた Web サーバー（NGINX）には、2013 年以降パッチが適用されていなかったことが報告されました。NotPetya から学び、注意すべきことは多くありますが、インターネットに接続している Web サーバーに継続的にパッチを適用し、最新の状態に維持し、適切に構成することを忘れないために、これは重要な教訓となります。

速度と勢い：
猛烈なスピードのランサムウェア

ランサムウェアは、過去になかった現象でも、新奇な現象でもありません。過去 2、3 年に急速に変化したのは、攻撃が増大する速度です。この大幅な増大は、基本的な暗号化機能と感染／拡散のスピードの両方で確認できます。ランサムウェア攻撃は、2017 年に前年比 3 倍に増大しました。サイランスは、ランサムウェア攻撃が 160 ヶ国と 16 種類の業界を超えて広いユーザーに影響を及ぼしていることを確認しました。攻撃を激しく加速させることは、多くの理由で攻撃者にとって非常に魅力的です。第 1 に、感染の拡大が早いほど、当然、獲得できる資金が多くなります。時代遅れの従来型ソリューションを利用してこのような攻撃に対応しようとしても、確実に検出するためにシグネチャの作成を待たなければならないか、または関連ソリューションのスピードが遅すぎて、感染が発生して拡散を続ける前に判断を下すことができない場合があります。これは、特に判断を下すための低速なクラウドベースのルックアップまたは実行前の制御の欠如などに起因することがあります。微妙に異なるどのような推論をするかにかかわらず、犯罪者／マルウェア作成者／攻撃者は、これを十分認識しており、毎日のように報道されている大量のランサムウェア攻撃を成功させるため、これを悪用し続けています。





2016 年のランサムウェア

影響を受けた業界

医療	34%
製造	17%
プロフェッショナルサービス	15%
教育	7%
その他すべての業界	27%

2017 年のランサムウェア

影響を受けた業界

医療	58%
食品	13%
製造	10%
プロフェッショナルサービス	6%
その他すべての業界	13%

ランサムウェアが広まっているのは明らかです。前年に、当社の多数の顧客がランサムウェア攻撃のターゲットとなったことが確認されました。新しい攻撃が生じるたびに、当社は、興味深いトレンドを明らかにするために、特定のペイロードの意図を調査しています。当社の解析によって、いくつかの結論が下されました。

ランサムウェアは、そのイメージとは異なる可能性があります。WannaCry の出現によって、世界中でシステムを利用不可能にするランサムウェアペイロードが配布されました。しかし、ランサムウェア自体は、不正なアクターによる収益の獲得に関して、非常に非効率的でした。感染したユーザーがビットコインで身代金を支払うことができる不正なアクターのランサムウェアサイトが、必要な暗号鍵をユーザーに実際に提供しなかったため、感染したほとんどすべてのコンピューターは、復旧することができませんでした。それでは、WannaCry の目的は、収益の獲得にあったのでしょうか、それともももっと悪意のある何かであったのでしょうか。多くの人は、WannaCry は身代金の支払いではなく、大規模なビジネスの混乱を起こすことを目的としていたと論じました。さらに、WannaCry は、作成者の予想よりも早く拡散した概念検証または気晴らしのための攻撃であったと仮説を立てる者もいます。いずれにしても、ランサムウェアは主流となり、今後の攻撃で顕著な役割を果たすようになります。

存在し続ける低レベルのサイバー犯罪と隠れた不正行為

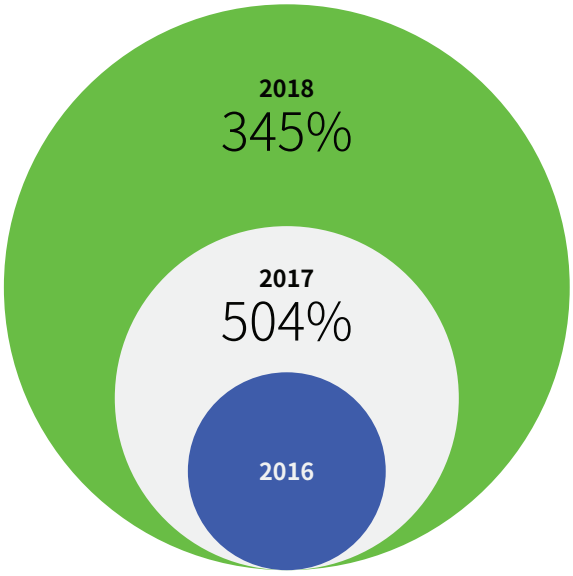
2017 年には低レベル／エントリーレベルのサイバー犯罪活動が大量に生じました。法律の制定によって、特に人気があり取引が盛んであった闇市場の 2 つが差し押さえを受け閉鎖され、犯罪経済は大きな打撃を受けました。民間セクターのパートナーとともに、複数の国際法取締機関は、AlphaBay、Hansa、およびダークウェブ上の、はるかに小規模な複数の市場をターゲットとしました。Bayonette 作戦は、ドラッグ、武器、個人情報、盗難品、デジタルサービスなどの売買を中心に、低レベル経済のかなりの部分に、協調して容赦ない打撃を与えました。AlphaBay と Hansa は、人気と規模においてトップ 2 の市場でした。しかし、他にも生き残り、まだ存続している多くの市場があります。代替的な市場が不足を補い、売り手と買い手がこれに応じて自らの活動を調整するのに、ほとんど時間はかかりませんでした。

今も、複数のダークウェブ市場が繁栄し続けています。このような市場は、犯罪者が市場とサイトに信頼感を持たず、常に警察が潜んでいることを想定している警戒と不審の状況下でも存続しています。Wall Street Market、Dream、Point/T・chka、Berlusconi、および多数の他の市場は、引き続き繁栄し、存続しています。

当社は、闇市場と違法取引一般で暗号通貨が利用される理由と利用される方法の変化も観察し続けています。ビットコインは本質的にセキュアではなく、真の匿名性もありません。暗号通貨を通じた取引の追跡において、標準的な取締手段を補完し、支援するために、1 つの総合的な業界が発生しました。Chainalysis、Blockchain Alliance、BlockSci、Elliptic などの企業は、暗号通貨のアクティビティと取引をモニタリングし、解析することを自社の事業としました。サイバー犯罪者は、自らに対する監視の網が拡大し続けていることを十分に認識し、取引が目立たないよう変化と革新を続けています。暗号通貨は本質的に不正なものではなく、このテクノロジーを支援しているいかなる者も、このように考えることを望んでいません。同様に、暗号通貨とサイバー犯罪は排他的であり、独立しています。しかし、犯罪組織の間での利用と採用率を通じて、暗号通貨に関するイノベーションを追跡できます。

この変化とイノベーションに関して増大している例の 1 つは、Monero、Dash、Ethereum などの代替的な通貨が着実に採用され、少数の他の通貨が選択されていることです。Monero は、真に分散化され、セキュアで、追跡不可能な取引のための唯一の選択肢であることが示されたため、犯罪者の世界では特に魅力的です。まさにこの理由で、閉鎖前の AlphaBay を含む複数の市場が、ビットコインとともに Monero（XMR）をサポートしました。少なくとも、市場に参加している独立の売り手は、Monero のサポートが市場のウォレット／エスクローシステムに含まれていない場合でも、Monero の補足的なサポートを認めています。Libertas など、Monero のみをサポートしている市場もあります。

インフラストラクチャにおけるすべての特別な監視と変化にもかかわらず、これらの市場は繁栄を続け、即時の利益を求めている低レベルの犯罪者に幅広い商品とサービスを提供しています。こうした市場は、必要な武器、ドラッグ、ソフトウェア（マルウェア、クラック、エクスプロイトなど）、および想像しうるあらゆるものに加えて、データ（盗難データ、不正データ、個人データ、金融データなど）の信頼できる入手元であり続けています。



暗号通貨マイナーの増加

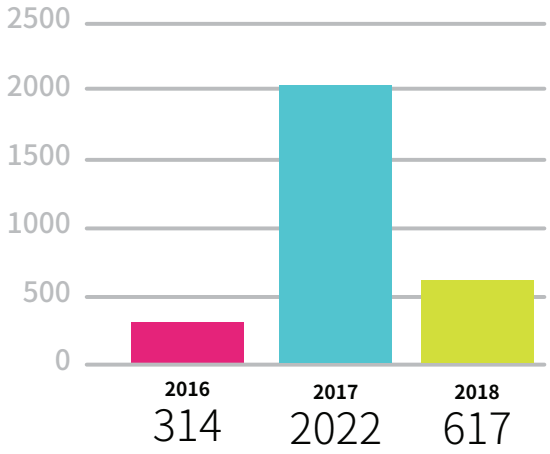
マネーロンダリング

収益全般の現金化とともに、違法活動から生じる資金のマネーロンダリングは、サイバー犯罪世界で非常に重要な問題です。当社は、これに対処するための新たなアプローチを頻繁に確認しています。ビットコイン取引に対する可視性が犯罪者にとって大きな問題となったため、犯罪者は特に昨年、アプローチを変え続けなければなりませんでした。一部の挑戦的な犯罪者は、Apple iTunes エコシステムを通じて利益を洗浄するため、プロミュージシャンになりすますことさえしました[2]。たとえば、個人はオリジナルの音楽を制作し、選択したサービスを通じて、iTunes ストアで購入できるよう音楽を投稿することができます。音楽が購入できるようになると、犯罪者は犯罪活動のビットコインによる利益を iTunes ギフトカードと交換できます。これは、広く利用可能であり、ある程度の疑似的な匿名性が認められますが、ギフトカード自体が不正なものである場合もあります。次に、犯罪者は、ギフトカードを使用して自らの音楽を購入し、Apple から犯罪に無関係な金銭で支払いを受けることができます。この遠回りな方法は、他のオンラインサービスでも利用できます。犯罪者によって作成された現金化ガイドやロンダリングノウハウ文書で、このような方法の説明が増大していることが確認され始めています。言うまでもなく、ある詐欺師が違法に入手した資金を適切にロンダリングする自らの能力に自信がない場合は、ただちに支援を受けることができます。

「暗号通貨とサイバー犯罪経済間の関係は、絶え間ない変化と発展の状態にあります。」

ウォレットを利用したトロイの木馬

暗号通貨とマルウェアのことを考える場合、何よりも先にランサムウェアが連想される傾向があります。しかし、他のタイプの暗号通貨取引に該当するマルウェアのファミリーもあります。Bitswiper や CryptoShuffler などのトロイの木馬は、被害者のクリップボードを監視するよう設計されています。感染ユーザーが支払いまたは送金のために Web フォームに支払先のウォレットをペーストしたときに、ペーストしたデータは攻撃者が選択するウォレットに置き換えられます。このため、被害者は、気づかぬうちに、攻撃者のウォレットに対して直接かつ透過的に資金を送金します。このような脅威と類似の脅威は、犯罪目的の利用のために多くは無償で簡単に入手できます。



通貨泥棒の増加

[2] https://www.consumer.ftc.gov/blog/2016/05/scammers-push-people-pay-itunes-gift-cards
https://www.thedailybeast.com/want-to-launder-bitcoins-how-crooks-are-hacking-itunes-and-getting-paid-by-apple

多面的な攻撃

多面的な攻撃の特徴は、永続性とステルス性を確立し維持するために、複数のツール、方法、戦略が利用されることです。十分な資金と資源を調達した攻撃では、アクティビティの把握がますます難しくなるだけでなく、独自のフォールトトレランスが実現されます。また、設計によって、または注意をそらす文字列やアーティファクトを利用した意図的な欺きや、他のグループによる既知のインフラストラクチャの再利用を通じて、攻撃を調査している組織の資源と重点を分散させる傾向もあります。

攻撃者は、標準の OS ツールおよび機能をあまり改変しなければ、検出されにくくなり、逸脱や追加が多くなるほど、目立ちやすくなります。PowerShell、Netsh、SC、WMI、およびさまざまな自動更新／認証メカニズムはすべて、このモデルに適しています。

イランに拠点を有するとみなされている APT34 Group は、多くの他の攻撃者と同様に、必要に応じて引き続き内部ツールを採用する一方で、外部ツールを多く利用していることで知られています。以下に例を示します。

- 不正な RTF（CVE-2017-11882）で攻撃を開始します。
- RTF が実行され、または開かれたときに、追加のテキストファイル／スクリプトが、（RTF エクスプロイトを通じて）ステージングサーバーからダウンロードされます。
- **ステップ 2 でダウンロードされるスクリプト／テキストは、標準システムユーティリティを利用して、追加のコンポーネント**（エンコードされた PowerShell スクリプト／コマンドなど）をダウンロードし、デコードします。
- **ステップ 3 で実行されるスクリプト／コマンドには、スケジュール設定されたタスクの作成または永続性を確立するためのその他の方法（レジストリなど）が含まれます。**
- ステップ 4 で確立されたコンポーネントは、指定された間隔で実行され、必要なペイロード／コードを起動する最終段階のペイロードであるため、この時点で不正な活動のすべてが実現されます。

一部の定義によると、攻撃を開始するためにシステム機能、Power Shell、RTF 文書のみを扱っているため、上記の攻撃はすべてファイルレスとみなされます。RTF はファイルであり、多くの場合（必ずしも常時ではない）、攻撃者はディスクに対して Power Shell をファイルとして書き込むことが多いため、当社はこれがすべてファイルレスであることに同意しませんが、それでもこの定義は的を射ています。明らかな実行可能形式（PE）のマルウェアバイナリは、この攻撃では出回っていません。

ファームウェアとハードウェアの脆弱性の攻撃

プラットフォームに依存しない攻撃と同様に、もう 1 つの収益性の高い攻撃のターゲットは、デバイスのファームウェア／ BIOS およびハードウェアの脆弱性です。このようなタイプの攻撃は作成にコストがかかりますが、複数のオペレーティングシステムにわたる攻撃に加えて、長期的な永続性を実現できます。複数のクライアントインスタンスをホストしていることがあるコンピューターへの侵入を可能にし、クラウドインフラストラクチャ上にあるデータの漏洩と 2 次汚染につながる可能性があるため、ファームウェアやハードウェアの脆弱性を利用した攻撃は、クラウドサービスプロバイダにとっても懸念事項です。当社は、ファームウェアとハードウェアの脆弱性の報告が増加していることを確認しており、来年このような低レベル攻撃が広まると予想しています。

Intel は、2017 年に複数のファームウェアの脆弱性を公表しました。これらの脆弱性は、マネジメントエンジンや信頼された実行エンジンなどの低レベルファームウェアコンポーネントにあります。一部の脆弱性により、悪意あるアクターは、攻撃に着手し、システムを破壊し、OS の監視外でコードをロードして実行できます。これまでのところ、広まっている既知の攻撃は発見されておらず、更新されたファームウェアをダウンロードできます。しかし、企業環境内のファームウェアパッチ管理は困難であり、採用スピードは速くありません。

ファームウェアの最近の解析によって、最も基本的なファームウェアの保護さえも欠如していることが判明しました。複数のハードウェアベンダーの 3,000 を超えるファームウェアイメージには、ファームウェアの保護が欠けており、攻撃に対して無防備であることが明らかになりました。

また、2017 年 3 月に、Wikileaks は、MAC ファームウェアに対するディスクレスの EFI 持続型攻撃である Der Starke インプラントの説明を公開しました。Der Starke によって、ネットワーク通信を隠すことが可能になります。同様に、テレビなどの IoT デバイスをターゲットとする Weeping Angel 攻撃が、国家アクターによって利用される可能性が生じています。

当社は、2018 年に、攻撃者が永続性を獲得し、データを侵害するために、ファームウェアとハードウェアの脆弱性への感染を検討していることについて、より実際的な証拠が示されると予測しています。

ランサムウェアのケーススタディー

自社の環境がランサムウェアによって暗号化されたある企業は、苦境に陥っていました。機密性の高い情報が、サイバー犯罪者によって乗っ取られました。敵意あるアクターは、「ビットコインで 320 万ドルを支払わなければ、盗難したデータはダークウェブに流出し、会社は破滅するだろう」と容赦なく受け入れがたい要求をしてきました。奪われたデータのバックアップがなく、身代金の要求を満たすための合理的な手段がなかったこの企業は、サイランスに支援を求めました。

サイランスのインシデント対処チームは、この組織の技術環境を評価してから、攻撃者のツール、技法、手順を解析しました。攻撃に成功した方法を特定し、脅威グループのプロセスを調査することによって、サイランスチームは貴重な情報を入手しました。要求に対する回答担当者は、この知識を利用して、身代金の 75% の減額を交渉しました。身代金の減額とともに、サイランスはこの企業のインフラストラクチャに残っている複数の脆弱性に注意を向けました。このランサムウェア攻撃では公開された RDP（リモートデスクトッププロトコル）接続が利用されましたが、システムの完全性を改善する余地は他にもありました。

このケースの調査終了時に、サイランスは以下のことを推奨しました。

- 定期的にスケジュール設定されたバックアップ計画を実施する。
- インターネットからアクセスできるすべての RDP 接続を削除する。
- 社内で年次脅威評価を実施する。

ファイルレス攻撃とスクリプト多用攻撃

ファイルレス攻撃の定義は、過去数年間にやや広くなりました。厳格な観点では、真のファイルレス攻撃（Code Red、SQL Slammer）、疑似ファイルレス攻撃（Ramnit）、および実際にスクリプトを多用し、またはスクリプトに依存している攻撃があります。最近、上記のすべてのサブカテゴリが１つの包括的なファイルレス攻撃にまとめられる傾向があり、誤解につながる可能性が生じています。

すべてメモリに常駐し、追加スクリプトの実行に依存していないマルウェアは、完全なファイルレスです。しかし、回避および永続性を強化するために追加スクリプト（JavaScript、Power Shell など）を利用している攻撃は、スクリプトを多用していると言うべき攻撃との間のグレーゾーンに属します。その一例には、最終ペイロードをダウンロードするために JavaScript/VB を利用し、または追加の PowerShell スクリプトを呼び出してペイロードの実行を遅らせてから、ダウンロードと起動を行う Cerber があります。

Cerber のシナリオにおいて、攻撃の最初の段階では、マルウェアペイロード全体がダウンロードされず、まだファイルが関わっています。マクロ／ VB またはその他の形式のコードが組み込まれた不正な文書を通じて開始された攻撃にも同じことが言えます。ファイルレス攻撃は、検出の回避、内密性、永続性の向上などの理由で、悪意あるアクターにとって魅力的です。しかし、こうした攻撃中に何が実際に発生しているかを正確に記述するために、ファイルレスという用語は慎重に使用する必要があります [3]。

[3] https://www.youtube.com/watch?v=Tiv_-NLZzkc

徹底的な破壊 - 回復不能

2012 年の Shamoon のリリース以降、破壊を目的とした敵意のある攻撃は、一貫して出現し、大きな損害をもたらしてきました。多くの場合、このような攻撃は、政治的な主張を行うためにハクティビストによって利用され、または国家間の対立で利用されます。こうした破壊的攻撃が実行された後、回復への道のりは長く、コストがかかり、しばしばインフラストラクチャの手動による再構築が必要になります。たとえば、Shamoon の場合、Saudi Aramco のシステムは約 5 ヶ月にわたってオフラインになりました。2017 年には、国家に起因するものを含む大規模な破壊的攻撃が確認されました。

2017 年 3 月に、Stonedrill マルウェアは、サウジアラビアをターゲットとするディスク消去機能を備えていると報告されました。この国はたびたび、ディスク消去マルウェアのターゲットにされてきました。その後、2017 年 6 月に、NotPetya が注目を集め、漏洩した EternalBlue エクスプロイトを通じて多くのデバイスに拡散しました。その主要な手口は、MBR への感染により感染システムを起動不可能にして、利益を得ることでした。ウクライナは、この特定のマルウェアによる最大の被害を受けました。

2001 年に初めて発見された Gh0stRAT マルウェアも、EternalBlue エクスプロイトを通じて再配布されたと報告され、ディスク消去機能を備えていました。また、2017 年には、インターネットで Linux ベースのルーターをスキャンし、セキュリティの不十分なデバイスを破壊し、デバイスストレージを破損させ、デバイス上のすべてのファイルを削除するよう設計された Brickerbot のような攻撃も確認されました。

当社は、2018 年に、サービスを中断し、ターゲットに損失を被らせることを目的とした弱体化攻撃が増加すると予測しています。2018 年 2 月には、平昌冬季オリンピック大会の開会式を混乱させることを目的とした Olympic Destroyer と呼ばれる攻撃が確認されました。これには、ネットワーク共有上のファイルを実質的に消去する不正なコンポーネントが含まれていました。この攻撃は、昨年に漏洩した NSA ツールに含まれていた EternalRomance エクスプロイトを通じて配布されました。

アトリビューション：重要な領域／重点の移行

アトリビューションは、セキュリティ業界で常に関心の高い問題です。きわめて頻繁に、アトリビューションは、大きく報道されるために、または手元の重要な問題（攻撃が成功した理由や攻撃が長期間にわたって成功した理由）から話をそらすために利用されます。サイランスは、攻撃者が誰であるかという問題にこだわるよりも、上記の理由に集中するほうがはるかに重要であると考えています。

もちろん、アトリビューションについて議論する必要はありますが、私たちは焦点を絞らなければなりません。アトリビューションには、明確かつ絶対的な学術的価値があります。さまざまな地域／アクターにわたってトレンドとなっている技法、戦術、手順（TTP）に関する網羅的な知識や、そうした知識を経時的にターゲットおよび攻撃と照合することには価値があります。また、アトリビューションには攻撃またはセキュリティ違反に起因する捜査や訴訟に直接関係する警察機関およびその他の組織にとっても価値があります。こうした状況以外では、その価値はそれほど明確ではなくなります。

攻撃者は、実行されうるアトリビューションの取り組みの矛先を変えるため、誤った情報や不信感を故意に植え付けます。たとえば、多くの場合、攻撃者は、他のグループに関連することが知られているツールやインフラストラクチャを再利用します。すなわち、2つの攻撃がサーバーXから実行されたため、いずれも同じグループからの攻撃に違いないとみなされるようにします。これは非常にシンプルなシナリオですが、稀なことではありません。また、攻撃者は、適切と考える任意の方向に公衆のアトリビューション議論の対象を向けるため、インフラストラクチャを難読化または再配置する方法を変えることもあります。

証拠や直接的な知識を持たない公衆のアトリビューションの臆測によって、データ／情報プールの透明度が低下します。証明できない臆測は、実際の捜査を妨げ、上述したアトリビューションの学術的価値も低下させます。

過去数年間にわたって、悪意あるアクターが注意をそらすためのきわめて露骨で顕著な試みが何度かありました。通常、こうした試みは、何よりも注意をそらすことのみを目的としています。WhoIs Team（Dark Seoul）やGuardians of Peace（Sony攻撃）に言及している複数のケースは、数年前から見られる顕著な例です。その多くは、北朝鮮で活動している特定のグループが注意をそらすために採用した比較的平凡な例です。Lazarusと呼ばれるグループは、発生した国に関して誤った結論が導かれるよう、不正なバイナリにさまざまな言語の文字列やコマンド構造を組み込んだことで知られています。2017年には、Lazarusが、さまざまな関連バイナリに組み込まれたロシア語の文字列とロシア語のコマンドセットを使用して、複数のポーランドの銀行を含む金融機関のターゲットを攻撃したことが確認されました。

そのすべては、アトリビューションの試みの方向をそらすことを目的としていました。

より最近では、2018年平昌オリンピックのインフラストラクチャをターゲットとしたOlympic Destroyer マルウェアで、この種類の操作的挙動が確認されました。この攻撃は、今日までのすべての証拠の徹底的な解析に基づいて、ロシアから発生したと思われますが、北朝鮮のLazarusに非難の矛先が向かうよう仕向けていました。Lazarus/DPRKとそれぞれの歴史、TTP、手口について当社が認識しているすべてを考慮に入れた場合、この判断は適切であると思われますが、まだ確定的ではありません。しかし、これは、データがまだ解析され、モニタリングされ、捜査が継続され、不正確な結論を飛躍的に下す（および過度に焦点を当てる）前に、確認されているすべての情報を考慮に入れる必要があることを示す優れた例です。

Hiveまたは類似の戦術の継続的な利用を考慮に入れると、このシナリオ全体は、さらに複雑になることがあります。すでに利用されているこのような方法により、攻撃者は、十分に信頼されたモデル（捏造／偽造されたSSL証明書など）によってサポートされる正当なインフラストラクチャ内に隠れることができます。この隠蔽によって、アトリビューションを判定することがさらに困難になります。

注目に値する攻撃やセキュリティ違反が発生した場合、推測的なアトリビューション情報が世界中に報道される傾向があります。これが発生した場合は、少し時間を取って適切な観点から検討する必要があります。アトリビューションと動機は複雑であるため、発生源にかかわらず、攻撃を防止することに、実際に重点を置くべきです。

Cylanceチーフセキュリティ・トラスト・オフィサーのMalcolm Harkinsは、次のように述べています。「悪意あるアクターにとって攻撃を困難にするために前進し、業界のエネルギーを再び集中させるため、私たちはアトリビューションに取りつかれたように夢中にならないようにする必要があります。『犯人』を見つけることにすべての資源を費やすことによって、私たちは被害者のようにふるまい、自身の責務を最小限にし、責任を限定しようとします。いずれも、セキュリティ侵害を受けた組織や、個人情報をその組織に委託した顧客およびクライアントの役に立ちません。その代わりに、私たちは、侵入の真の発生源についてアトリビューションを行うことができるよう、侵入が成功した『理由』に焦点を当てる必要があります。その発生源こそが、セキュリティ業界が被害者に販売し、結果として攻撃を防ぐのに失敗した要素だからです」

「私たちは、アトリビューションを追求する代わりに、悪意あるアクターにとって攻撃を困難にするため業界のエネルギーを再び集中させる必要があります。」

結論

前年は、世界中の脅威アクターの革新的かつ破壊的な能力を改めて思い知らされた年でした。技術の盗難、独創的なエクスプロイト、創造的な手法に対する不断の取り組みにより、2017 年には大規模な被害が生じました。国家予算の支援を受け、セキュリティ侵害テクノロジーの最新の知識とツールを備えた脅威アクターは、継続的に攻撃を成功させるのに有利な立ち位置を占めています。

2017 年の攻撃に関するサイランスの調査によって、引き続き有効なセキュリティ対策と、もはや適切ではないセキュリティ対策を再評価することが可能になります。以下のような多くの信頼性の高いセキュリティ対策には、引き続ききわめて重要な価値があります。

- ハードウェアとソフトウェアを最新の状態に保つ。
- 環境内のアクセスと権限を適切に管理する。
- リモートアクセスを厳格に制限し、モニタリングする。
- ソーシャルエンジニアリングとフィッシングの試みを特定するため、人員をトレーニングする。
- 攻撃を受けやすいインフラストラクチャに対して強力な物理的セキュリティを維持する。

ファイルレスマルウェアによって利用される多様性や戦術などの脅威の特性により、その他のセキュリティ対策は時代遅れになりました。これには、シグネチャベースのアンチウイルスソリューションやブラックリストが含まれます。

2017 年には長い間尊重されてきたセキュリティアプローチの失墜が明らかに示されましたが、サイバーセキュリティ業界全体では大きな進展が続いています。脅威がファイルレスになる一方で、先見の明のあるセキュリティ企業は、脅威を防御するためにスクリプト制御とメモリ管理を活用し始めています。マルウェアがシグネチャベースの検出を回避しているときに、明確なビジョンを持った企業は、人工知能と機械学習を利用して、セキュリティ侵害を予測し、防御しています。

すべての戦いと同様に、勝利するためには知識が重要な要因となります。2017 年の当社の知識と重要な調査結果を共有することにより、当社は、お客様の組織が 2018 年以降の脅威に対する備えを改善できることを望んでいます。

寄稿者

データアナリスト
Srinivasa Kanamatha
Danny Wu

脅威調査員／作成者
Thom Ables
Steve Barnes
Bronson Boersma
Tom Bonner
Alex Hegyi
Shinsuke Honjo
Marta Janus
Aditya Kapoor
Tom Pace
Carolina Regalado
Jim Walter

編集者
Dan Ballmer
Brigitte Engel
Sally Feller
Anthony Freed
Natasha Rhodes
Steve Salinas
William L. Savastano
Jessica Vose

デザイン
Sheri K. Audette
Drew Hoffman

お問い合わせ

Cylance Japan 株式会社
〒100-6510
東京都千代田区丸の内1-5-1　新丸の内ビルディング10F
www.cylance.co.jp
03-6386-0061 (代表)