KASPERSKY lab

Kaspersky Security Bulletin 2018

2019年サイバー脅威の予測

グローバル調査分析チーム、プリンシパルセキュリティリサーチャー
ヴィセンテ・ディアス（Vicente Diaz）

目次

予測を行うことは非常に難しいことです。しかしながら、ここでは水晶玉をのぞき込む代わりに、最近の出来事や、今後悪用される可能性のあるトレンドをもとに2019年のサイバー脅威を予測していきます。
知りあいの頭脳明晰な人々に意見を聞き、APT攻撃に基づいたシナリオを作成して（セキュリティ侵害といえば、伝統的にこの攻撃が最も時代を先取りしているので）、2019年に起きるかもしれない出来事を「予測」しました。

※　当レポートは、Kaspersky Security Bulletin: Threat Predictions for 2019（英語）に基づき作成したものです。

大規模なAPTの終焉

多数のサイバー攻撃者が日々発見されているこの世界で、最初の予測が真逆の方向を示しているように思われるのではないでしょうか？

この予測の背景には、セキュリティ業界が、政府の支援を受けて何年もかけて準備された極めて高度な活動を、着実に発見していることがあります。攻撃者の立場になって考えれば、このような状況下では、見つかりにくく、攻撃者を特定しにくい、より高度な新技術を研究せざるを得ません。

実際、その方法はたくさんあります。唯一の要件は、セキュリティ業界が利用している、攻撃者像やさまざまな攻撃と痕跡の間の類似性を特定するためのテクニックを理解することです。これはそれほど大きな秘密ではありません。攻撃者は十分なリソースを持っているので、さまざまな活動を同時に実行すれば、同じ攻撃者や活動へ関連づけされるのは非常に難しくなります。リソースに恵まれた攻撃者は、従来の活動をそのまま続けながら、革新的な活動を新たに繰り出すことができます。もちろん、従来の活動が発見される可能性は十分にありますが、新たな活動を発見するのはかなりの難題です。

ごく一部の攻撃者に限定した話になりますが、極めて高度な攻撃を仕掛けるよりも、ISP（インターネットサービスプロバイダー）など、標的が存在するとわかっているインフラストラクチャーや企業を直接狙う方が効率的な場合もあります。場合によっては、マルウェアを必要とせず攻撃者の目的を達成できることもあります。

一部の活動は、異なるツールや技術を使用する別のグループや企業へ外注する場合もあり、攻撃者像の調査を非常に難しくしています。政府が背後にいる活動の場合、このツールやそれを扱う人材が分離していることによって、こういった攻撃活動の今後に影響を与える可能性があることに留意しておくと良いでしょう。このシナリオでは、技術的能力やツールは民間企業が所有していて、誰でも買えるようになっていますが、多くの場合、購入するのは、技術的な詳細やそれがもたらす結果をあまり理解していない人たちです。

これらを総合すると、極めて高度化された新たな活動が発見される可能性は低いことを示しています。潤沢なリソースを持つ攻撃者たちは、ただ単に新しい枠組みへとシフトしていくものと見ています。

ネットワークハードウェアとIoT

あらゆるサイバー攻撃者が、ネットワークハードウェアを標的として設計された機能やツールを使うようになると考えるのは理にかなっています。「VPNFilter」のような攻撃活動は、攻撃者が多目的「ボットネット」を展開するために、どのようにマルウェアを使い始めたのかを示す良い事例です。このケースでは、マルウェアが拡散してしまっている最中でも、攻撃の検知までにある程度の時間がかかったので、さらに標的を絞った攻撃が行われた場合はどうなるかが懸念されます。

事実、豊富なリソースを持つ攻撃者ではさらに過激になり、「1つの組織を標的にして集中攻撃する代わりに、もっと基本的なインフラストラクチャーを直接狙えば良いのではないか」と考える可能性があります。そこまでのレベルの侵害が発生したことは（私たちの知る限りでは）まだありませんが、攻撃者すべてにとって、このレベルのコントロール権の奪取がどのくらい魅力的かは、「Regin」などの過去の事例を見れば明らかです。

ネットワークハードウェアの脆弱性により、攻撃者はさまざまな攻撃方法を取ることができます。攻撃者たちがボットネットを使って大規模な不正アクセスを行い、そのネットワークを将来、別の目的で使用するかもしれません。また、秘密裏に攻撃を仕掛けるため、厳選された標的に近づくかもしれません。後者の場合、通信をミラーまたはリダイレクトするためのVPNトンネルを開くと、必要な情報がすべて攻撃者に提供される、マルウェアレス攻撃も考えられます。

これらのネットワーク要素はすべて巨大なIoTの一部でもあり、そこではどうやら、ボットネットが止められないペースで増殖を続けているようです。たとえば、重要インフラを混乱させ得ることも考慮すると、悪者の手に落ちたボットネットは信じられないほど強力です。ボットネットは豊富なリソースを持つ攻撃者による攻撃グループの偽装や、もしくは何らかのテロ活動に悪用される可能性があります。

このような多目的ボットネットは、破壊的攻撃以外にも使えます。たとえば、短時間の周波数ホッピングを用いて悪意あるコミュニケーションを行ったり、これまで流出に悪用されてきたチャネルを迂回して、監視ツールを回避したりすることができます。

毎年同じことを繰り返し警告しているようですが、日を追うごとに強力になっているため、我々は絶対にIoTボットネットを過小評価してはなりません。

公的な報復

外交や地政学の観点からの最大の課題は、現在進行中のサイバー攻撃にどう対処するかということでした。答えは単純ではありません。検討すべき項目が多々ある中でも、攻撃がどれほど悪質で露骨であったかで対応は大きく変わります。しかし、米民主党全国委員会（DNC）を標的にしたハッキングのような事件の発生後、事態は深刻化したように見受けられます。

Sony Entertainment Networkに対するハッキングやDNCへの攻撃など、近年注目を集めた攻撃の捜査は、多数の容疑者の起訴につながりました。その結果、容疑者が裁判にかけられるだけでなく、その攻撃の背後に誰がいたかが公になります。これは、より深刻な外交的影響をもたらす議論の一端となりかねない世論の醸成に利用される可能性があります。

実際に、民主的なプロセスに介入したとの疑惑により、ロシアがそうした影響を受けるのを私たちは目の当たりにしてきました。これにより、今後この種の活動に対する考えを見直す動きが出てくるかもしれません。

しかし、このようなことが起こるかもしれないという恐怖や、すでに起きたかもしれないという考えを植え付けたことは、攻撃者にとって最大の成果でした。攻撃者たちはこうした恐怖、不確実性、疑念を、より巧妙な別の方法で悪用することができることを、「Shadow Brokers」などの目立った活動からも見て取れます。このような動きは今後さらに出てくると見ています。

将来的にどんなことが起こるのでしょうか。これまでの活動はおそらく、プロパガンダの成り行きをうかがうテストに過ぎなかったと考えられます。事は始まったばかりであり、例えば「Olympic Destroyer」で見た「偽旗（にせはた）」の事例のように、さまざまな方法で悪用されると考えられます。なお、Olympic Destroyerでの偽旗作戦の最終的な目的が何であったのか、どのように展開される可能性があったのかは、いまだに明らかになっていません。

新規参入者の登場

APTの世界を少し単純化すると、豊富なリソースがあり最先端を行く（が、消滅が予測される）古参の攻撃者たちと、この世界に参入しようとしている精力的な新人グループの2つに分けられます。

新規参入の障壁がこれほど低くなったことはありません。非常に効果的なツールが無数に存在し、漏洩したエクスプロイトやあらゆる種類のフレームワークが再利用され、公開されて、誰でも使えるようになっています。さらに、これらは必要であれば簡単にカスタマイズできるうえ、攻撃者像の調査がほとんど不可能になります。

このようなグループが多く見られるようになってきている地域は、東南アジアと中東です。私たちは、これらの地域を拠点にしているとみられるグループが、その地域における標的の防御の不十分さとセキュリティ文化の欠落につけこんで、ソーシャルエンジニアリングを悪用し、急成長していることに気づきました。標的側が保護を強化するにつれ、攻撃者たちも同様に攻撃能力を増強し、ツールの技術レベルを向上させると同時に、ほかの地域にも活動範囲を広げています。スクリプトベースのツールを使ったこの攻撃シナリオでは、OPSECの失敗にかかわらず、活動の改善を続けながら、地域的なサービスを提供する新興企業もみられます。

PowerShellとは対照的に、JavaScriptによる脆弱性攻撃後（Post-Exploitation）ツールの機能を管理者が制限することは難しく、システムログもなく、また古いOSでも実行できることを考えると、このツールが短期間のうちにどのように生まれ変わるかという点も興味深く、より技術的な角度からも考慮に値します。

ネガティブリング

Meltdown、Specter、AMDFlawsや、これらに関連する脆弱性（および今後発見されるもの）で明け暮れた1年、私たちは最も危険なマルウェアはどこにあるかを改めて考えさせられました。リング0未満の脆弱性を実際に濫用しているものはまだ発見されていないとはいえ、私たちが持っているセキュリティメカニズムではほぼそれを感知できないため、わずかな可能性でも非常に恐ろしいものです。

たとえば、システム管理モード（SMM）の場合、2015年以降、PoCが少なくとも1つ公開されています。SMMはCPUの機能で、メモリ空間へアクセスさせることなく、リング0プロセスにコンピューターへの完全なリモートアクセスを効果的に提供します。そう考えると、これを悪用したマルウェアが今のところ見つけられていないのは、単に検出が難しいからか、あるいはそうではない何かがあるのか、と疑ってしまいます。この機能を悪用するチャンスを逃がさず、長年の間、このメカニズムを利用しようと試行錯誤しているグループが存在することは間違いありません。もしかしたら、成功している可能性もあります。

同様の状況は、仮想化/ハイパーバイザー上で動作するマルウェア、またはUEFI上で動作するマルウェアでも見られます。私たちは、どちらのマルウェアについてもPoCで確認しました。また、HackingTeam社は、UEFI永続モジュールも公開しています。これは、少なくとも2014年から利用可能でしたが、こちらも本物のITWサンプルはまだありません。

このようにレアなマルウェアを見つけられるのでしょうか。それとも、まだ悪用されていないのでしょうか。後者の可能性は低いと思います。

典型的な感染経路

このレポートの中では最も意外性のない予測だと思いますが、スピアフィッシングについても触れておきます。これまでに最も成功した感染経路が、近い将来、さらにその重要性を増すと考えています。その成功の鍵となるのは、標的の好奇心を刺激する作用ですが、先日来発生しているさまざまなソーシャルメディアプラットフォームからのデータの大量漏洩を、攻撃者がこのアプローチの改善に役立てた可能性があります。

FacebookやInstagram、LinkedIn、Twitterなどの大手ソーシャルメディアへの攻撃から得られたデータは、市場に出回っており誰でも手に入れることができます。一部のケースでは、攻撃者の本命がどのデータだったのかは不明ですが、個人的なメッセージや認証情報も含まれているでしょう。このデータはソーシャルエンジニアリングにとって宝の山なのです。たとえば、攻撃者が、あるユーザーに近しい友人から窃取した認証情報を使用して、このユーザーが以前、個人的に話したことをソーシャルメディアでシェアすれば、投稿の信憑性が高まり、攻撃の成功確率は劇的に上がります。

攻撃者はこれを昔ながらの偵察技術と組み合わせて、標的が正しいことを二重チェックして確認し、必要な相手にだけマルウェアを配布し、検知される確率も最小限に抑えることができます。添付ファイルについては、悪意ある活動を始める前に、必ず人間による対話型操作をさせることで自動検知システムを回避することがかなり標準的になっています。

機械学習を使用して、フィッシングの効果を向上させようという取り組みもみられます。実際はどのような結果になるかはまだわかっていませんが、これらの要素をすべて組み合わせたスピアフィッシングが今後も、特にソーシャルメディアを経由した効果的な感染経路として、存続することに間違いはないでしょう。

破壊的な破壊者

「Olympic Destroyer」は、2018年の1年間に大きな話題を呼んだ、破壊的なマルウェアの1つですが、多くの攻撃者がこのような機能を定期的に攻撃の中に組み込んでいます。破壊的な攻撃には、攻撃者にとってのメリットがいくつかありますが、特に、相手の注意をそらすことができる、攻撃後にログや証拠をすべて消去できる、という点で有効です。また、ただ単に標的に不愉快な思いをさせたいときにも使えます。

このような破壊的攻撃の中には、ウクライナで見られたような現在進行中の紛争に関連する地理戦略的な目的を持つものや、サウジアラビアの石油会社数社が受けた攻撃のように政治的利権を狙ったものもあります。また、ハクティビズムもしくは、強力な、黒幕に操られた代理グループによる活動の結果と思われるケースもあります。

いずれにしろ、このような攻撃すべてのポイントは、この破壊的な攻撃が「素晴らしすぎて」使わなければもったいないということです。たとえば、政府は「公的な報復」として外交的対応と戦争行為の中間に位置するものとして使うでしょう。事実、それを試している政府もあります。このような攻撃の大半は前もって計画されたもので、偵察と侵入は最初に済ませてあります。攻撃者が、すべての準備を整え、あとは引き金を引くだけであるとか、何らかの武器を構えて突撃命令が出るのを待っている、といった状況にすでに陥っている標的がどのくらい存在するかはわかりません。

ICS環境や重要インフラはこのような攻撃に特に脆弱で、業界や政府が過去数年間、状況の改善を目指して多大な努力をしていたにもかかわらず、現状は理想とはほど遠いものです。来年、このような攻撃が広がりを見せることがなくとも、発生件数は増え、特に政治的判断に対する報復は増加するだろうと予測されるのはこのためです。

高度なサプライチェーン攻撃

これも憂慮される攻撃経路で、過去2年にわたり悪用され続けているため、誰もが、関係している供給元の数と、そのセキュリティのレベルについて気を揉んでいました。このような攻撃への対応策は簡単にはみつかりません。

サプライチェーン攻撃は、（水飲み場型攻撃のように）業界全体や、（「NotPetya」の攻撃で見られるように）国全体を標的にするには最高の攻撃経路ですが、より対象を絞った攻撃となると、検知されるリスクが高まるので、そこまで優れた攻撃とはいえません。また、たとえば、共通ライブラリのパブリックリポジトリに悪意あるコードを注入するといった無差別攻撃も増えています。この方法は、ある特定のプロジェクトでこのようなライブラリが使用される時間を正確に狙った攻撃には効果的でしょう。攻撃終了後には、悪意あるコードがリポジトリから削除されます。

さて、標的を絞りこんで、このような攻撃を仕掛けることができるでしょうか。ソフトウェアの場合、いたるところに痕跡が残り、マルウェアが複数の顧客に配信される可能性があるので難しいと思われます。供給元が特定の顧客とだけ取引しているのであれば実現性は高まります。

ハードウェアへの埋め込みはどうでしょう？現実に起こりうることでしょうか？先日、これに関する議論がありました。スノーデン氏の起こした漏洩事件で、顧客へ配送中のハードウェアを改竄できるということがわかりましたが、よほど強力な組織でもない限り、そう簡単なことではありません。そのような力があったとしても、いろいろな要因で制限されるでしょう。

しかし、ある特定の注文をした購入者がわかっている場合、攻撃者は配送中ではなく、出荷元でハードウェアを改竄すると考えるほうがより現実的です。

どうすれば工場の組み立てラインにある技術管理機能をすべて回避できるのか、またどうすればこのような改竄ができるのかを想像するのは難しいことです。これらの可能性を排除したくはありませんが、おそらく、製造元の協力が必要でしょう。

全体的に見て、サプライチェーン攻撃は効果的な感染経路として、これからも行われるでしょう。ハードウェアへの埋め込みの可能性は極めて低いと思いますし、もし、行われたとしても、おそらく誰も気づかないでしょう。

そしてモバイル

この項目は、毎年予測に登場します。画期的なことは何もありません、ゆっくりとした感染の波に2つの速度があることを考えるのはいつも興味深いことです。PCだけを狙っても意味がないので、すべての攻撃者たちがその攻撃活動にモバイルコンポーネントを組み入れているということは言うまでもありません。実際、Android用の痕跡の例は多数見つかっていますし、iOSへの攻撃も多少の進展が見られました。

iPhoneへの感染を成功させるには、複数のゼロデイを結合する必要がありますが、信じられないほど豊富なリソースを持っている犯罪組織はこのような技術に資金を提供し、重大な攻撃に使用できるということを覚えておいてください。一部の民間企業は、iPhoneが物理的に手元にあればどれにでもアクセスできると主張しています。資金が潤沢ではない犯罪組織でも、このようなデバイスのセキュリティを回避する独創的な方法を見つけています。たとえば、不正なMDMサーバーを設定し、ソーシャルエンジニアリングを通じて、標的にこの偽サーバーの使用を依頼することで、攻撃者による悪意あるアプリケーションのインストールを可能にできます。

2018年の初めに漏洩したiOSのブートコードが、攻撃者にどのような利益をもたらすのか、また攻撃者がこのコードを悪用する新たな方法を発見するかどうかを確認するのは興味深いことです。

とにかく、モバイルを標的にしたマルウェアについては、大規模な感染拡大はないと思いますが、熟練した攻撃者が、標的のデバイスにアクセスする方法の発見を目指して、活動を続けることは予測できます。

そのほかの脅威

攻撃者は今後の将来へ向けてどのようなことを考えているのでしょうか。1つ考えられるのは、特に軍事分野において、脆弱で間違いやすい人間ではなく、より機械的なものの使用へと置き換わるだろうということです。これを念頭に置き、さらに2018年4月、オランダに拠点を置く化学兵器禁止機関（OPCW）のWi-Fiネットワークをハッキングしようとしてオランダから追放されたGRUのエージェントを例に考えて、近距離のハッキングには人間の代わりにドローンを使うというのはどうでしょうか。

また、あまたある仮想通貨プロジェクトにいくつかバックドアを仕掛け、データ収集や、金銭的な利益を得るというのは？
デジタル製品を使ってマネーロンダリング（資金洗浄）するとか？ゲーム内課金を使い、その後、このアカウントを市場で売るのはどうでしょうか。

予測したことが常に期待外れになる可能性はあまたにあります。環境の複雑さを完璧に理解することはもはや不可能で、さまざまな分野でスペシャリストによる攻撃が発生する可能性が高まっています。どうすれば証券取引所の内部にある銀行間システムを詐欺に悪用できるでしょうか？私にはまったくわかりません。そのようなシステムが存在しているかさえ知らないのです。これは、このような活動の背後にいる攻撃者が想像力を駆使していることを示す一つの例に過ぎません。

私たちは、将来の攻撃を予測、理解して、その発生を阻止するために存在しているのです。

株式会社カスペルスキー
PR-1047-201812