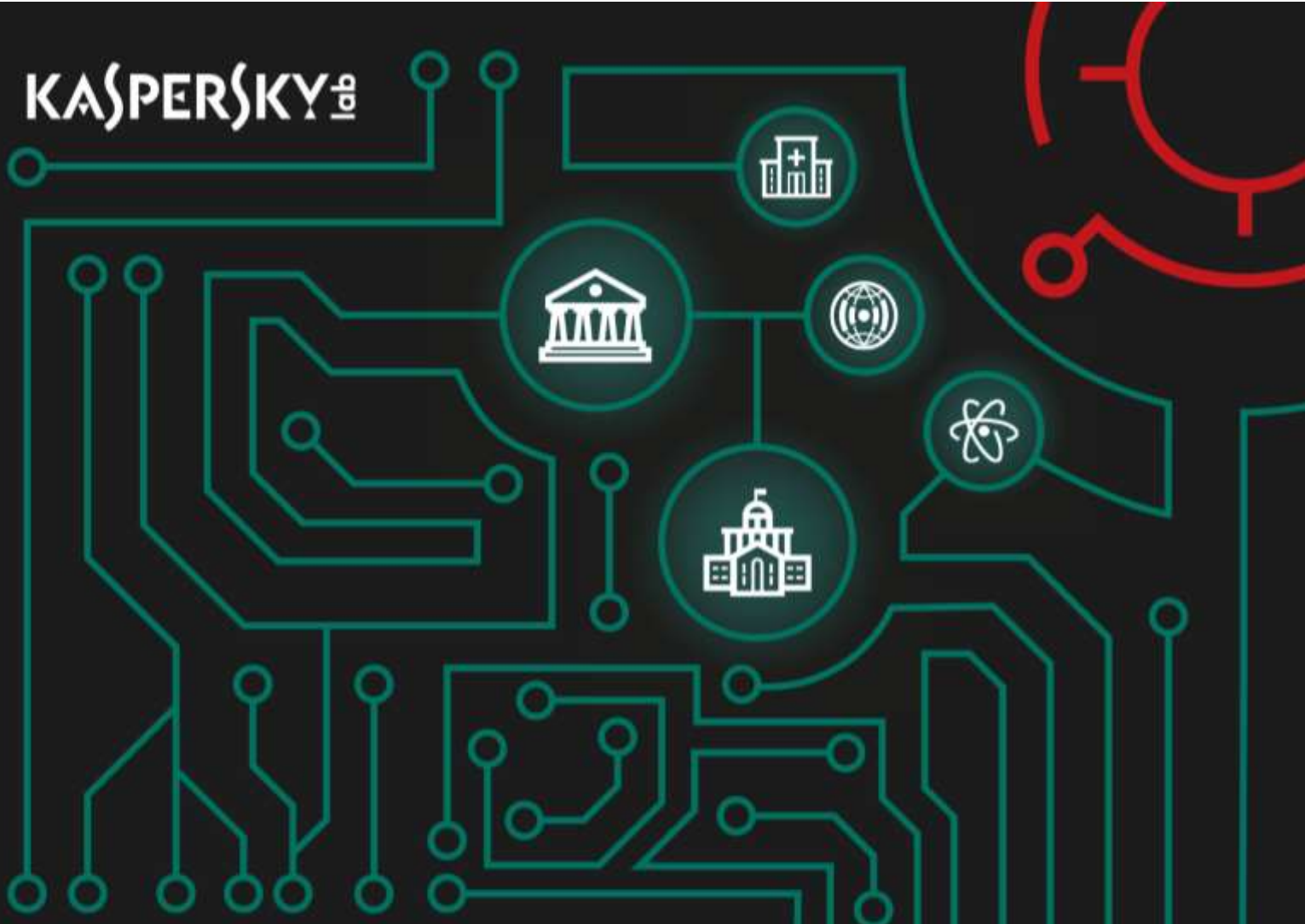


Kaspersky Security Bulletin 2017

2018 年サイバー脅威の予測

Part 1　APT 攻撃の予測

目次

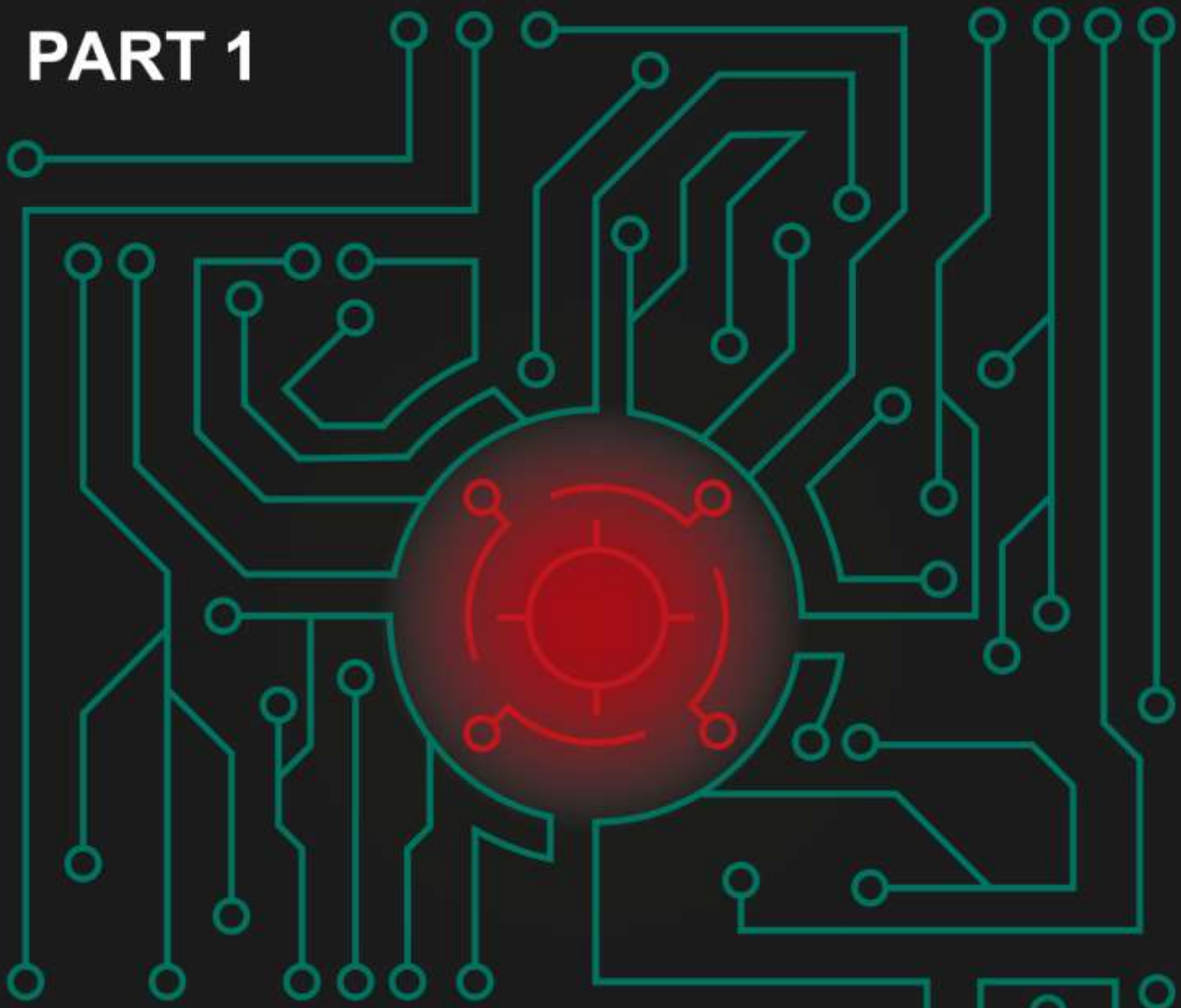
はじめに

2017 年は前年に引き続いて、高度なサイバー犯罪グループによる政治的動機に基づいた大胆な攻撃や大規模な窃盗が報道されましたが、また別のタイプの脅威もメディアの注目を浴びました。あらゆる規模の企業を標的にして、驚異的な速度で拡散するランサムウェアです。5 月と 6 月の一連の破壊型ランサムウェア攻撃によって、ネットワークセキュリティ、ソフトウェアパッチ、あるいは従業員のセキュリティ意識といった分野におけるギャップが改めて露呈しました。

すべての予測は、Kaspersky Lab の専門家が 2017 年を通じて実施した調査と、そこから得られた経験および洞察に基づいています。現在把握している情報をベースに今後の展望を可能な限り正確に予測したものであり、読者の方の注意を喚起し、意識を高め、行動を促進する一助となることを願っています。

＊当レポートは、Kaspersky Security Bulletin: Threat Predictions for 2018（英語）に基づき作成したものです。

PART 1



Part 1

2018 年 APT 攻撃の予測

GREAT

APT 攻撃の予測概要

残念ながら、今年もまた APT の予測を行うことになりました。2017 年一年間を振り返ると、脅威の全体像を把握しなければならないセキュリティリサーチャーであることについて内なる葛藤が生じるものです。しかし観測する事象は刺激的で、当社をさらなるリサーチへ導いています。つまり理論上の予測が実際に形を持って発生しているのです。そのため、実際の攻撃ポイントとそれに対する攻撃者の戦術を理解することで、脅威ハンティングと検知の能力をさらに高め、新しい攻撃に対処することが可能となっています。その一方で、多くのユーザーのセキュリティ対策に懸念を抱く人々が増えているにもかかわらず、発生したそれぞれのセキュリティイベントの被害はさらに壊滅的になっています。当社では、過去の同様の事例の一つとは考えられない新しいイベントが発生しており、一般ユーザー、電子商取引、金融機関、政府機関などが一様に、多様な要素が複合的に作り出す危険な状態に直面していると考えています。

当社の予測は、2017 年を通じた調査の結果を、2018 年にピークを迎えるトレンドという観点で整理する、という方針に基づいています。

2017 年の予測を振り返る

予測は当たったのか？

Kaspersky Lab による 2017 年の予測の内容と、それらに関連する実例を列挙します。

スパイ活動と APT

- 感染の兆候がほとんど見られない、受動的な埋め込み型マルウェアが流行する
  的中– https://securelist.com/unraveling-the-lamberts-toolkit/77990/
- ファイルレス／オンメモリ型マルウェアによる一過性の感染
  的中– https://securelist.com/fileless-attacks-against-enterprise-networks/77403/
- スパイ活動がモバイルを標的に
  的中– https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html

金融システムへの攻撃

- サイバー銀行強盗の増加
  的中– https://securelist.com/lazarus-under-the-hood/77908/

ランサムウェア

- 卑劣で嘘つきなランサムウェア
  的中– https://securelist.com/schroedingers-petya/78870/

産業への脅威

- 的中しなかった（しなくてよかった）- 産業制御システムに対する終末決戦
  が、Industroyer マルウェアによる攻撃を観測 –
  https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

IoT

- 別の名前のレンガ
  的中 - BrickerBot – https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/

情報戦争の増加

- 的中 - 複数の例 – https://citizenlab.ca/2017/05/tainted-leaks-disinformation-phish/

2018 年の予測

1. サプライチェーン攻撃の増加

Kaspersky Lab のグローバル調査分析チーム（GReAT）は、100 を超える APT（Advanced Persistent Threat）グループとその活動を追跡しています。これらのいくつかは想像を超えるほど高度であり、ゼロデイエクスプロイトやファイルレス攻撃ツールなどの幅広いコレクションを使って従来型のハッキング攻撃を行った後に、情報窃取を担当するさらに高度なチームに引き継ぐという組織的な活動を行います。高度なサイバー犯罪者が長期にわたって特定の標的を侵害しようとし、失敗し続けるという事例を多く観測していますが、このような失敗は、標的となった組織が強力なインターネットセキュリティ製品を使用しているか、ソーシャルエンジニアリングの被害に遭わないように従業員を教育しているか、オーストラリア DSD による APT 攻撃に対する 35 の軽減戦略を常に実施しているかのいずれかの理由によるものでした。一般に、高度で持続的と見なされているサイバー犯罪者は、簡単には断念せず、侵入路を見つけ出すまで防御の隙間を探し続けます。

すべてが失敗した場合は、サイバー犯罪者は一歩下がって状況を見直すようです。その際に、標的へ直接の侵害を試みるよりも、サプライチェーン攻撃のほうが有効だと判断する可能性があります。標的となる組織が世界最高レベルの防御をネットワークに適用している場合でも、その組織がサードパーティ製のソフトウェアを使用している場合があります。サードパーティ製品は標的としてよりたやすいと考えられるため、適切に保護された本来の標的組織を攻撃する上で利用される可能性があります。

2017 年には、このような事例がいくつも観測されています。以下はその一例です。

a. Shadowpad
b. CCleaner
c. ExPetr/NotPetya

これらの攻撃は、識別や軽減を行うことは極めて困難です。たとえば、Shadowpad の事例では、攻撃者は、銀行、大企業、そのほかの業界において世界中で広く使用されている Netsarang 社のいくつかのパッケージをトロイの木馬化することに成功しました。クリーンなパッケージと、トロイの木馬化されたパッケージの違いに気付くことは非常に困難です。多くの場合、これらを拡散させているのは、コマンド&コントロール（C&C）トラフィックです。

CCleaner の例では、200 万台を超えるコンピューターが、感染した更新プログラムを受信したと推定されており、この規模ゆえに 2017 年に発生した最大規模の攻撃の 1 つとなっています。Kaspersky Lab では、悪意のある CCleaner コードを分析し、過去に Axiom 傘下の APT グループによって使用された APT17（別名 Aurora）など、ほかのいくつかのバックドアに CCleaner を関連付けることができました。これにより、目的を達成するために APT グループの攻撃範囲が拡大していることが判明しています。

当社では、現時点のサプライチェーン攻撃の量は、認識しているよりもはるかに多いとみていますが、これらの攻撃は今のところ検知されておらず顕在化もしていません。2018 年には、検知と実際の攻撃の両方の観点で多くのサプライチェーン攻撃が観測されるとみています。ある特定のタイプの被害者にたどり着くために、特定の地域や業種用のソフトウェアをトロイの木馬化することが、水飲み場型攻撃に似た戦略となり、これらのソフトウェアが攻撃者にとって非常に魅力的であることが証明されます。

2. モバイルマルウェアのハイエンド化

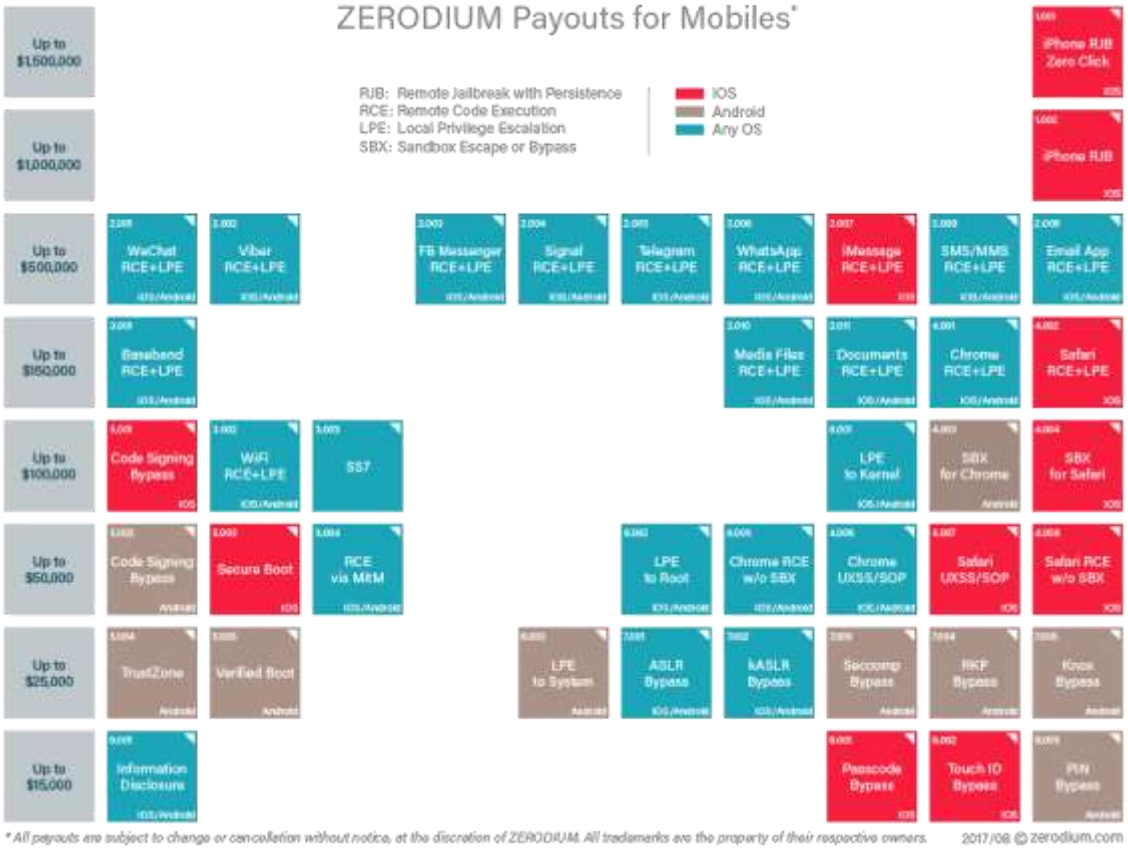
2016 年 8 月に CitizenLab と Lookout が、高度なモバイル用スパイプラットフォーム Pegasus の分析を公表しました。Pegasus はいわゆる「合法的傍受」のソフトウェア群であり、イスラエルの会社 NSO Group によって政府やそのほかの機関に販売されています。iOS など最新のモバイル OS のセキュリティ防御をリモートから回避するゼロデイ機能を組み合わせると、わずかな防御しか備えていないデバイスに対しては極めて強力となります。2017 年 4 月には、Google がスパイウェア Pegasus の Android バージョンである Chrysaor の分析結果を公表しました。Pegasus や Chrysaor などの合法的傍受のスパイウェアに加えて、ほかの数多くの APT グループも独自の埋め込み型のモバイルマルウェアを開発しています。

iOS はイントロスペクションによりロックダウンされる OS であるため、デバイスが感染しているかどうかを確認するためにユーザーができることは殆どありません。Android は脆弱性がさらに深刻化している一方で、デバイスの整合性を確保するために Kaspersky Internet Security for Android などのセキュリティ製品が提供されており、取り巻く状況は良い方向に向かっていると言えます。

モバイルマルウェアについては、テレメトリが十分でないために特定と除去が困難で、Kaspersky Lab では、発生している既存のモバイルマルウェアの総数は現在報告されているよりもはるかに多いとみています。攻撃の増加と、これらマルウェアの捕捉を目的としたセキュリティ技術の改善の結果として、2018 年にはモバイルを標的とする、さらにハイエンド化した APT マルウェアが検出されると予測しています。

3. Web プロファイリングによる、BeEF と似た侵害の増加

より優れたセキュリティ技術と軽減技術が OS に導入されるようになったことから、2016 年と 2017 年はゼロデイエクスプロイトの価格が急騰しました。たとえば、最新の Zerodium の価格表では、持続的攻撃のために、リモートから iPhone（iOS）の脱獄（Jailbreak）が可能なエクスプロイト、つまり「ユーザーと接触することなくリモート感染が可能」なものが最大 150 万ドルとなっています。



驚くべき価格にもかかわらず、これらのエクスプロイトの購入を選択した政府関係者がいたということは、エクスプロイトが偶発的に露見することがないように、ますます多くの注意が払われていることを示しています。攻撃コンポーネントを配布して攻撃を開始する前に、より徹底的な予備調査が行われており、この段階では、たとえば、標的となるユーザーが使用しているブラウザーの正確なバージョン、OS、プラグイン、そのほかサードパーティ製ソフトウェアの特定が重視されています。これらの情報を得たサイバー犯罪者は、より精緻な戦術を立てて、保有している最高レベルのエクスプロイトを使用するのではなく、より重要度の低い「ワンデイ」または「N デイ」エクスプロイトを配布することで目的を達成できるわけです。

これらのプロファイリング手法は、Turla、Sofacy、Newsbeef（別名 Newscaster、Ajax Security Team、または Charming Kitten）などの APT グループにおいて一致していますが、ほかの APT グループでも Scanbox などのカスタムプロファイリングフレームワークを使用しています。Kaspersky Lab では、これらのフレームワークがさらに普及することを考慮し、また高価なツールを温存したいという攻撃者ニーズの増大を考え合わせれば、2018 年にはさらに多くの APT グループが公開されているフレームワークを採用するか独自のフレームワークを開発するようになり、「BeEF（Browser Exploitation Framework）」などのプロファイリングツールキットの使用が増加すると予測しています。

4. 高度な UEFI 攻撃と BIOS 攻撃

Unified Extensible Firmware Interface（UEFI）は、最新の PC 上でファームウェアと OS の仲介として機能するソフトウェアインターフェイスです。2005 年にインテルを代表とする主要なソフトウェアメーカーとハードウェアメーカーが共同で規定し、現在、従来の BIOS 標準の置き換えとして急速に普及しています。UEFI は BIOS にはない多数の高度な機能を備えています。たとえば、実行可能ファイルをインストールして実行する機能や、ネットワーク機能、インターネット機能、暗号化や CPU に依存しないアーキテクチャとドライバーなどが挙げられます。このような非常に高度な機能が UEFI を魅力的なプラットフォームにしていますが、柔軟性に欠ける BIOS の時代には存在しなかった新たな脆弱性への道も開かれています。たとえば、カスタムメイドの実行可能モジュールを実行する機能を利用して、アンチマルウェアソリューション（または OS 自体）が起動する前に、UEFI によって直接動作が始まるマルウェアを作成することが可能になります。

商用レベルの UEFI マルウェアの存在は、Hacking Team の UEFI モジュールが見つかった 2015 年から知られていますが、それを考慮すると重大な UEFI マルウェアが全く見つかっていないことは驚くべきことかもしれません。Kaspersky Lab ではその原因はこれらのマルウェアを信頼できる方法で検知することが困難であるためであると考えています。2018 年には、より多くの UEFI ベースのマルウェアが検出されるでしょう。

5. 破壊型攻撃の継続

2016 年 11 月初旬、Kaspersky Lab は中東の複数の標的に対する新しい一連のワイパー攻撃を観測しました。この攻撃に使用されたマルウェアは、2012 年に Saudi Aramco と Rasgas を標的にした悪名高いワーム Shamoon の亜種で、その後 4 年間活動がありませんでした。Shamoon は Disttrack とも呼ばれており、標的となったユーザーのマシンの中身を効果的に消去する極めて破壊的なマルウェアファミリーです。2012 年の攻撃当日、Cutting Sword of Justice（正義の剣）と名乗るグループが Saudi Aramco への攻撃宣言と、攻撃はサウジアラビアの君主制に対する措置であると Pastebin にメッセージを投稿しました。

Shamoon 2.0 による攻撃は 2016 年 11 月に観測しており、サウジアラビアのさまざまな重要インフラセクターや経済セクターに属する組織を標的にしており、前回の亜種と同様に侵害された組織内のシステムの大量破壊を目的にしていました。当社は当攻撃の調査時に、サウジアラビア内の組織を標的にしたとみられる未知のワイパー型マルウェアも検出しました。当社はこの新しいワイパーを StoneDrill と名付け、高い確度を持って Newsbeef APT グループに関連付けています。

破壊型攻撃に関して言えば 2017 年はタフな一年でした。Shamoon と Stonedrill に加えて、当初はランサムウェアであると見なされていた ExPetr/NotPetya 攻撃も、巧妙に偽装したワイパーであることが判明しました。ExPetr に続いて別の一連の「ランサムウェア」攻撃が発生し、標的となったユーザーがデータを復元できる見込みはほとんどなく、すべてが巧妙に偽装された「ランサムウェア型ワイパー」でした。あまり知られていない事実の 1 つに、2016 年に CloudAtlas APT による同様の一連の攻撃が観測されており、ロシアの金融機関に対して「ランサムウェアに見せかけたワイパー」らしきものが利用されました。

2018 年は引き続き破壊型攻撃が増加し、より明確な形でサイバー戦争が明らかになると予測しています。

6. 暗号の危機

2017 年 3 月、米国国家安全保障局（NSA）が作成した IoT 暗号標準化の提案が、Simon と Speck のバリアントについて問題となり、ISO の承認が得られず 2 度目の遅れとなりました。

2016 年 8 月には、Juniper Networks が自社の NetScreen ファイアウォールで 2 つの不可解なバックドアを検出したことを発表しました。2 つのバックドアで興味深かったのは、攻撃者が NetScreen デバイスの VPN トラフィックの復号の際に使う、乱数ジェネレーターDual_EC に使用される定数がほとんど変更されていなかった点でした。Dual_EC アルゴリズムは、NSA が設計し米国国立標準技術研究所（NIST）が推進したものでした。2013 年のロイターの報道では、NSA が RSA 社に 1,000 万ドルを支払い、製品に欠陥のあるアルゴリズムを組み込ませて暗号の解読を可能にしたとされています。バックドアが理論的に可能であることは 2007 年には明らかになっていましたが、その後も、一部の企業（Juniper を含む）は、論理的にはセキュアな異なる定数セットを用いて Dual_EC を使い続けています。一部の APT 犯罪者にとっては、Juniper をハッキングしてこの異なる定数セットを自らが制御可能でかつ VPN 接続を復号することに利用できるものに変更するには十分なメリットがないと思われます。

2017 年 9 月に、暗号化の専門家による国際グループによって、NSA は標準化を検討していたこの 2 つの新しい暗号化アルゴリズムを撤回せざるを得なくなりました。

2017 年 10 月には、Infineon Technologies 製のハードウェアチップで使用されている RSA 暗号化ライブラリの不具合が報じられました。この不具合は意図的ではなかったようですが、スマートカード、無線ネットワーク、暗号化された Web トラフィックといった、日常生活で使用されている基盤となる暗号化技術は安全なのかという疑問が生じました。2018 年には、より深刻な暗号化の脆弱性が検出され（願わくば）パッチが適用され、それらは標準として含まれるか個別に実装されると予測しています。

7. 電子商取引の ID が危機的状況に

ここ数年、ますます壊滅的になる個人特定情報（PII; Personally Identifiable Information）の大規模な侵害が目立っています。最近では、米国 1 億 4,550 万人に影響を及ぼしたと報じられた消費者信用情報会社 Equifax への侵害があります。これら侵害の重要性に対して多くの人々は次第に鈍感になっていますが、PII の大規模な公開により、電子商取引の基盤や、重要書類の処理にインターネットを採用するという事務作業上の利便性が脅かされることについて理解することが重要です。もちろん、詐欺や ID の盗用は長期にわたって問題となっていますが、基本的な ID 情報の盗用が急増するとどうなるでしょうか。商取引と政府機関（特に米国）は、業務にインターネットを採用するという現代社会の快適さの範囲を狭めるのか、あるいはほかの多要素ソリューションの採用に賭けるのかの選択を迫られることになります。そのため恐らく、ApplePay などの高い耐性を持つ代替の選択肢が ID と商取引を保護する事実上の手段として台頭してきますが、その一方で、煩雑な事務処理を効率化して業務コストを削減するインターネットの重要性や役割が後退する可能性があります。

8. ルーターとモデムのハッキングが増加

脆弱性の存在は知られていても、見落とされている領域には、ルーターとモデムがあります。自宅であれ会社であれ、これらのハードウェアはいたる所にあり、日々の活動には非常に重要です。パッチが適用されず、注意も払われないままに、専用のソフトウェア類が実行されている傾向があります。インターネットに接続されるこれら小型コンピューターは、長期にわたって気づかれることなくネットワークにアクセスしようとする攻撃者にとって重要な結節点となります。さらに、最近の非常に興味深い調査結果では、攻撃者が別のインターネットユーザーに成りすまして、痕跡を別の接続アドレスに完全に紐づけることが可能だと示されています。通信先を欺くミスディレクションや偽旗（にせはた）作戦への関心が高まった今日、この手法は大きな役割を果たすことになります。これらのハードウェアの詳細な調査によって、興味深い結論が得られることが予想できます。

9. 社会的混乱の媒介物

昨年新たに発生した、リークや政治劇といった情報戦争の域を超えて、ソーシャルメディア自体が想像以上に政治色の強い役割を果たしています。政界の情報通の動きにしろ、South Park の作家による Facebook CEO に対する面白おかしいジャブにしろ、人々はソーシャルメディアを運営する大企業に、一定の事実確認と、社会に偏った影響を与えようとするフェイクユーザーやボットを特定することを求めています。残念ながら、これらのネットワーク（たとえば成功を「一日のアクティブユーザー数」などの定量化されたメトリクスで評価する）には、ボットユーザーベースを完全に取り除くだけの動機はほとんどないということが明らかになってきています。これらのボットが明白に問題を呈している場合や、独立系のリサーチャーがこれらのボットを突きとめることができる場合においてもです。明らかな悪用が継続して行われ、政治的に好ましくないさらに多くの人々が大規模なボットネットワークにアクセスできるようになるにつれ、ソーシャルメディア自体に対してさらに大きな反感が向けられます。反感を覚えたユーザーが収益とクリックの悪用による恩恵を享受する、この慣れ親しんだ大企業の代わりを探すようになると予測しています。

APT の予測 - 結論

2017 年に、Kaspersky Lab は脅威存在痕跡の信頼性の低下を発表しました。2018 年には、高度なサイバー犯罪者は前述した多くのツールや恐ろしい攻撃の切り口に磨きをかけて、さらに強力な攻撃を行うとみています。毎年のテーマと傾向は切り離すべきではありません。これらが相互に積み重なることで、個人、企業、政府といったあらゆるタイプのユーザーが直面する、ますます高まる脅威状況が生み出されます。これらの到来を確実に一時軽減する方法は、知識や経験の共有と、信頼できる脅威インテリジェンスを、洞察力をもって適用することです。

Part 1 では APT の傾向を予測しましたが、各業界は固有の課題に直面することになります。2018 年には、これらの課題のいくつかにも注目したいと考えています。