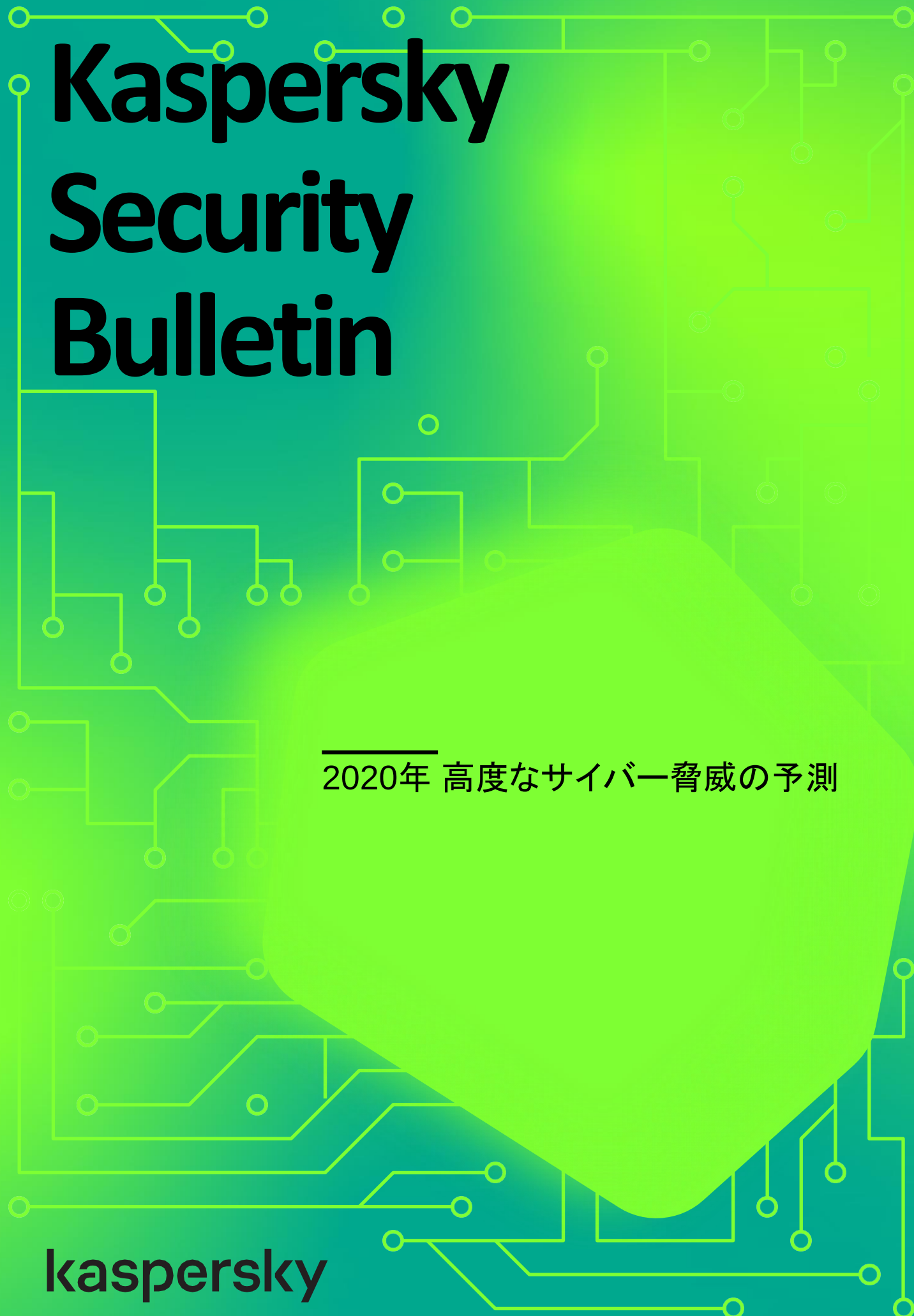




Kaspersky Security Bulletin

2020年 高度なサイバー脅威の予測

kaspersky

目次

2020年:高度なサイバー脅威の予測.....	3
偽旗作戦が次のレベルへ.....	3
汎用的なランサムウェアから標的型ランサムウェアへ	4
オンラインバンキングと決済における新たな攻撃経路	4
インフラストラクチャへの攻撃と、PC以外を標的とする攻撃の増加	5
アジアと欧州間の貿易ルート地域で攻撃が増加	6
攻撃方法の高度化.....	6
モバイルへの攻撃にフォーカスする傾向	7
個人情報の悪用:ディープフェイクからDNA情報の漏洩まで.....	8

* 当レポートは、[Kaspersky Security Bulletin 2019. Advanced threat predictions for 2020](#) (英語)に基づき作成したものです。

2020年: 高度なサイバー脅威の予測

予測ほど難しいことはありません。近い将来悪用される可能性のある傾向を見極めるために、過去12か月に起きたことを根拠に、当社の知識に基づき2020年の高度なサイバー脅威を予測します。

これから述べる予測は、今後数か月に起こりうると考えていることです。APT攻撃のサイバー犯罪グループは、これまでイノベーションの中心となってきたことから、この分野の当社エキスパートの知識とAPT攻撃を観測してきた結果に基づいた予測になっています。

偽旗作戦が次のレベルへ

何よりも考慮すべきことは、サイバー犯罪グループが攻撃とその後のラテラルムーブメント(水平展開)において、売買されているマルウェア、スクリプト、公開されているセキュリティツールや管理者用ソフトウェアを継続的に使用し、特定をますます困難にしていることです。



偽旗(にせはた)作戦は、複数のAPT攻撃グループのシナリオにおいて、重要な要素になりました。これまでの偽旗は、第三者に関連する痕跡を意図的に入れることで、セキュリティリサーチャーたちの注意をその攻撃者からそらすために使われてきました。たとえば、Lazarusグループのマルウェアではロシア語が使用され、WildNeutronではルーマニア語が使用されています。非常にわかりやすい例は、[Olympic Destroyer](#)攻撃でAPTグループのHadesが、単に攻撃元の特定を混乱させただけでなく、攻撃の要素を捏造し別のサイバー犯罪グループの仕業に見せかけ、攻撃元の特定をさらに困難にしたことがあげられます。サイバー犯罪グループは特定されることを回避するだけでなく、積極的にほかのグループにその罪をかぶせようとしており、このような方法はさらに発展するとみられます。

たとえば、無関係な別のAPTグループが使用していた既存のバックドア、コードの盗用や再利用(最近の例は、[英国のNCSCおよびNSAによって概要が公表された、未知のイランのグループのコードを再利用するTurla](#))、意図的に漏洩させたソースコードをほかのグループが使い、攻撃者の特定がさらに困難になることなども含まれます。

何よりも考慮すべきことは、サイバー犯罪グループが攻撃とその後のラテラルムーブメント(水平展開)において、売買されているマルウェア、スクリプト、公開されているセキュリティツールや管理者用ソフトウェアを継続的に使用し、特定をますます困難にしていることです。セキュリティ調査チームはどんな小さな手がかりでも貪欲に求めているため、これらの要素にいくつかの偽旗を組み合わせれば、攻撃元がほかのグループであると思わせるには十分かもしれません。

残念ながら、ランサムウェアは被害者から金銭を搾り取るためのもっとも効果的な手段となっています。



汎用的なランサムウェアから標的型ランサムウェアへ

ここ2年ほど、サイバー犯罪者は暗号化されたデータを元に戻すために相当な金銭を支払う可能性がある企業や組織に的を絞り、この種のマルウェアを使用するようになっており、広範囲におよぶ汎用的なランサムウェア攻撃の数は減少しています。当社では、企業や組織を狙うランサムウェアを「標的型ランサムウェア」と呼んでいます。昨年、標的型ランサムウェアによる事例は複数発生しましたが、今後は、金銭の強要がより顕著になると考えられます。意外な展開としては、サイバー犯罪グループが暗号化したファイルを復元不可能にするのではなく、窃取したデータを公開すると脅すかもしれません。

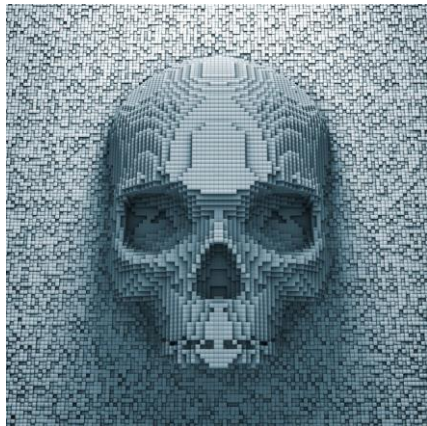
標的型ランサムウェアに加えて、サイバー犯罪者が攻撃を多様化させ、PCやサーバー以外の種類のデバイスを攻撃対象にすることは避けられないでしょう。スマートテレビ、スマートウォッチ、スマートカー、スマートハウスやスマートシティなど、消費者向け製品を狙うランサムウェアがその例です。より多くのデバイスがインターネットに接続されることに伴い、サイバー犯罪者は、それらのデバイスへアクセスし収益化する方法を模索しています。残念ながら、ランサムウェアは被害者から金銭を搾り取るためのもっとも効果的な手段となっています。

オンラインバンキングと決済における新たな攻撃経路

最近、EU全域で新しい銀行規則が施行されたことで、サイバー犯罪者が新たな攻撃経路を開発する可能性があります。このPSD2(Payments Services Directive II: 決済サービス指令)は、決済サービスを提供する企業に規制要件を課しています。確立された銀行業界には属さない、新規のフィンテック企業による個人データの使用も対象となります。モバイルを含むオンライン決済のセキュリティが、この指令の重要な側面です。それに関わらず、銀行は自らの顧客にサービスを提供しようとするサードパーティーに対して、インフラストラクチャとデータに関する情報を開示しなければならないため、攻撃者は新たに詐欺の手法を編み出して、この仕組みを悪用すると考えられます。



インフラストラクチャへの攻撃と、PC以外を標的とする攻撃の増加



攻撃に執着するサイバー犯罪グループは、WindowsやPCシステム以外のネットワーク機器に対しても[VPNFilter](#)や[Slingshot](#)などのマルウェアを使用しています。当然ながら、一度そういったデバイスの不正アクセスに成功すれば、攻撃者はフレキシビリティを手に入れます。ボットネットにより大規模な不正アクセスを行い、そのネットワークを将来、別の目的に使用することもできます。または、厳選した標的に秘密裡に攻撃を仕掛けるかもしれません。当社の[2019年版サイバー脅威の予測](#)では、VPNトンネルを開いてトラフィックをミラーリングまたはリダイレクトさせ、情報を窃取する「マルウェアを使わない」攻撃について考察しました。6月には、サイバー犯罪者が[世界中の少なくとも携帯電話通信事業者10社のネットワークに侵入し](#)、数年間そこに潜んでいたことが明らかになりました。場合によっては、通信事業者のインフラストラクチャに独自のVPNサービスを実装していたかも知れません。多数のIoTデバイスによってもたらされた実世界とサイバー世界の融合によって、サイバー犯罪グループの攻撃機会は増大し、また、犯罪者たちがその可能性を認識していることも明白です。昨年、[未知の攻撃者がRaspberry Piを使用して、NASAのジェット推進研究所から500 MBのデータを窃取したことが報告されました](#)。12月には、英国の[ガトウィック空港で、滑走路の1つで少なくとも1台のドローンが上空にいることが目撃され、衝突の懸念から空港が閉鎖に追い込まれました](#)。趣味でドローンを所有している者によるものか、DDoS攻撃を試みようとした者によるものなのかは不明ですが、ドローンによって国の重要なインフラストラクチャの一部が閉鎖に追い込まれたことは事実です。このような攻撃は間違いなく増加するでしょう。

近年、重要インフラに対する目立った攻撃が数多く行われていますが、広く地政学的な目的に沿ったものとみえています。[産業用施設におけるほとんどの感染は、依然として「主流の」マルウェアによるものですが](#)、この事実は、このような施設がいかに脆弱になり得るかを浮き彫りにしています。重要インフラへの標的型攻撃が、今後のサイバー犯罪活動の主流となる可能性は低いものの、その数は増加することが予想できます。実世界とサイバー世界の融合がますます進む中、地政学的な対立が起きています。これまで観測してきたように、このような攻撃は、外交と戦争に介入する報復の形を政府に提供しています。

「戦争は別の手段による政治の継続である」



アジアと欧州間の貿易ルート地域で攻撃が増加

サイバー攻撃が広範に実世界の緊張や争いを反映していることを考えると、カール・フォン・クラウゼヴィッツの格言「戦争は別の手段による政治の継続である」は、サイバー空間における衝突も含められると解釈できます。これまでも数多くの攻撃が発生しており、たとえば、米国の選挙にロシアが介入したとされたことが、2020年の選挙準備期間に再燃するおそれがあります。また米国は、疑わしい中国のサイバー犯罪グループを起訴によって「公表して非難」しました。別の例としては、「容疑者」を監視下に置くために密かにモバイルデバイスにインストールされるスパイウェアの普及もあげられます。

このような展開には複数の方法が存在します。たとえば、政府が国内外で自国の利益を確保するための政治的なスパイ活動の増加が含まれます。つまり、国内の「望ましくない」個人活動や運動、国外の潜在的な敵の活動を監視しています。また、経済危機に続いて情勢不安が起きる可能性がある、または現実には起きているような状況下では、テクノロジー面でのスパイ活動も予測できます。その結果、トルコ、東欧、南欧、東アフリカなど、アジアと欧州間の貿易ルートに位置する地域で、新たな攻撃が発生する可能性があります。

政府は何が許可され、何が許可されないかをより明確に定義しようとしているため、法律や政策の変更の可能性は十分にあります。一方で、疑惑の矛先が特定の状況から別の状況に向けられるのであれば、これがもっともらしい反証となり、制裁を回避する方法になることも考えられます。また、複数の司法省は、さまざまな種類の「法的傍受」を可能にして、コンピューター上の証拠の収集を切望しているようにみえることから、テクノロジーをより攻撃的に使用できるようになる可能性があります。これに対して、犯罪グループは活動を隠すために、暗号化とダークネットの使用を増やすおそれがあります。

攻撃方法の高度化

トップクラスの攻撃者たちが、実際にどのくらい高度な攻撃能力と、どのようなリソースを持っているかを正確に把握するのは困難です。もちろん、当社はその状況を把握するように努めています。数年前、豊富なリソースを持ち、支払いが可能な攻撃者に対して、ゼロデイ脆弱性が無数に供給されていることを観測しました。昨年も複数の例を目にしましたが、もっとも興味深いのは、[Googleが8月に公表した、iOSを標的としたエクスプロイトがここ2年間で少なくとも14存在すること](#)でしょう。

また、これまでスパフィッシング攻撃の標的となっていたMicrosoft Wordとほかのソフトウェアに対して適用された新しい分離方法は、マルウェアの配信手法に著しい影響を与え、高度な知識を備えていない犯罪グループはマルウェアの拡散方法を変更せざるを得なくなる可能性があります。



数年前、Quantum Insertと呼ばれる攻撃が話題になりましたが、それに類似した、さらに追加の傍受機能がすでに使用されている可能性が高いと考えています。当社では、そのいくつかを発見できると考えています。

物理的なインプラント(おそらく見落とされている)を使用している場合は特に、信号データやWi-Fi/4Gの利用など従来とは異なる方法でデータを窃取する可能性があります。同様に、活動を隠し検知をさらに困難にするために、DoH(DNS over HTTPS)を使用する攻撃者が増加するでしょう。そのようなシステムを検知する当社の能力は向上しているため、数か月の内には、より多くのUEFI(Unified Extensible Firmware Interface)マルウェアや感染を発見できる可能性があります。

サプライチェーンの悪用は、対処が非常に難しい攻撃方法として続くでしょう。攻撃者は改竄したソフトウェアコンテナ、パッケージやライブラリによって、この方法を使用していくものと思われます。

モバイルへの攻撃にフォーカスする傾向

過去10年間の重要な変化は、私たちのデジタルライフにおける主なストレージが、PCからモバイルになったことです。



過去10年間の重要な変化は、私たちのデジタルライフにおける主なストレージが、PCからモバイルになったことです。一部のサイバー犯罪グループはすぐにこのことに気付き、モバイルを標的とする攻撃ツールの開発に重点を置き始めました。当社はこれまでも、モバイルを標的とする攻撃の増大について予測してきましたが、この分野の観測結果に、その推測を常に反映してきたわけではありません。しかしながら、現象の観測不足が、必ずしもそれが起きていないことを意味するわけではありません。

少なくとも14件のiOSのゼロデイ脆弱性を悪用し、アジアの特定の少数派を攻撃した事例は前述しました。また最近、Facebookは自社サーバーがユーザーデータを傍受するマルウェアの実装に悪用されたとして、イスラエル企業のNSOを訴えました。さらに、Zerodiumの価格表によると、Android向けの極めて執拗なゼロクリック(クリックせずとも感染する)のエクспロイトは、現在はiPhone向けのものよりも高額になっています。

これらが物語るのは、攻撃者がこういったテクノロジーにいかにも多額の投資をしているかということです。ほとんどの人が携帯電話を持ち利用していることから、そのデバイスが持つ情報の価値が高いことは明らかです。毎年、モバイルを狙う攻撃には新たな傾向がみられますが、可視性やアクセシビリティが十分でないことから、セキュリティリサーチャーにとっては、攻撃の技術的な詳細情報を多く得ることが複雑になっています。

モバイルを狙う攻撃が、近いうちに無くなる合理的な理由はありません。しかし、この問題についてセキュリティコミュニティの注目が高まっていることから、攻撃が特定され、詳細に分析される数の増加が見込めます。

個人情報の悪用: ディープフェイクからDNA情報の漏洩まで

データの漏洩が攻撃者のソーシャルエンジニアリングの助けになることは、これまでも述べてきました。すべての攻撃者が、悪用される可能性のある被害者の完全なプロフィールを持っているわけではないため、増加し続ける漏洩データの価値は高まります。これは、ランサムウェアのパートで触れた、「ターゲットを絞らない」ランサムウェアの場合にも当てはまります。

記録されたデータが増え続ける世界では、たとえば生体認証データのように、とりわけ機密性が高い情報が漏洩した場合は危険です。また、広く議論されているディープフェイクの技術は、特に動画や音声といったあまり明確ではない攻撃経路と組み合わせることで、そういった攻撃を可能にします。このようなテクノロジーは自動化が可能であり、AIがプロフィールリングや詐欺手法の作成に役立つことを忘れてはなりません。

確かにこれらのテクノロジーはすべて近未来的ではありますが、過去、ソーシャルメディアによる選挙広告の活動で議論されたことと非常に似通っています。このテクノロジーはすでに使われており、攻撃者の利用も時間の問題でしょう。

未来には数多くの可能性があり、当社の予測に含まれていないことが起きるかもしれません。攻撃が展開される環境は広く複雑であるため、さまざまな可能性が存在します。加えて、APTグループの活動を完全に把握している脅威調査チームは1つ也没有。当社は、攻撃者の活動とその影響に関する知見を提供しながら、引き続きAPTグループの活動を予測し、どのような攻撃方法が採られるかを把握できるよう尽力していきます。

