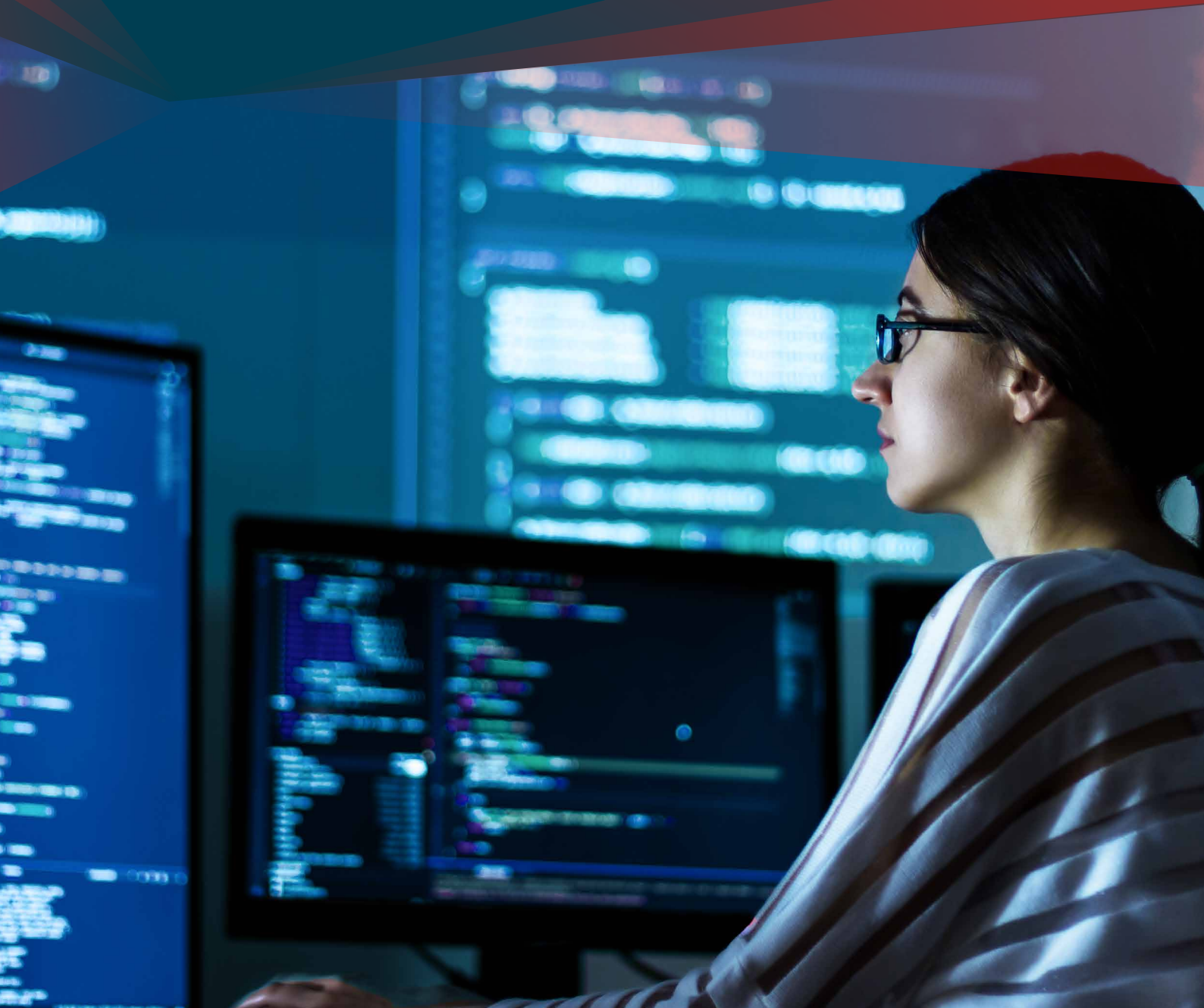
FORTINET

# フォーティネット グローバル脅威レポート

FortiGuard Labs による 2020 年上半期版レポート



# 目次

# 2020 年上半期の概説と発見事項

数年後に 2020 年を振り返ったとき、最も記憶に残っているのは新型コロナウイルス（COVID-19）のパンデミックであり、それがサイバーセキュリティに取って代わられることはないでしょう。このウイルスの世界的大流行は前例のない出来事であり、私たちは今後長い間、その余波に対処していくことになるに違いありません。それでも、2020 年前半の 6 ヵ月でサイバー脅威の状況に大きな進展があったことに変わりはありません。脅威トレンドの中には、新型コロナウイルスに関連するものもあれば、独自の特性を持つものもあります。下半期に向けて準備を整えられるよう、本レポートではこれらのトレンドを整理し、アドバイスを提供します。

### コロナ関連の脅威の拡散

コロナウイルスの感染は急速に広がりましたが、パンデミックをテーマにしたあらゆる種類のサイバー犯罪の手口や詐欺の方が、さらに速く拡散された可能性があります。本レポートでは、コロナの次に来るかもしれない世界的イベントをベースにした攻撃スキームに騙されないようにするための要点を網羅しています。

### ブラウザをめぐる戦い

サイバー犯罪の手口に関して言えば、今年の初めにはフィッシングなどの攻撃で使用される Web ベースのマルウェアが他の拡散手段を上回りました。また、人々がオフィスではなく自宅でインターネットを閲覧していることが原因で、企業の Web トラフィックが減少していることにも注目しました。この 2 つの傾向が重なったということは、企業はブラウザ対策を強化する必要があることを意味しています。

### 個人の領域に食い込む境界線

在宅勤務に関するトピックを、もう 1 つお伝えしましょう。複数の家庭用ルーターおよび IoT デバイスに対するエクスプロイトの試みが、IPS 検知数の上位に入っていました。フォーティネットは、誤った推測で 2 つの事柄を結び付けることをよしとしませんが、この結果は、ネットワーク境界が自宅にまで到達するという「ニューノーマル（新常態）」を攻撃者が利用しようとしていることに起因しているのだと考えずにはいられません。

### 一向にやむ気配のないランサムウェア攻撃

企業組織を標的にした上半期のランサムウェア攻撃の最後を締めくくったのは、6 月に発生したある有名メーカーに対する攻撃です。この攻撃によって業務は妨害され、いくつかの施設では一時的に生産が中断されました。

### Stuxnet 後の OT への脅威

この 6 月で Stuxnet の登場から 10 年が経過しました。Stuxnet は、オペレーショナルテクノロジー（OT）のセキュリティに対する見方を一変させたマルウェアです。この 10 年間に多くのインシデントが発生しましたが、産業界のエアギャップ（物理的に隔離された）環境への侵入を試みる攻撃の最新例となったのが、スパイ活動フレームワークの Ramsay です。これらの脅威から身を守る方法について解説します。

### エクスプロイトの時代

これまでのところ、2020 年は公開された脆弱性の総数の記録を塗り替えるペースが続いています。しかし、2020 年は実際にエクスプロイトを使用する脆弱性の割合が過去最低となっています。高い数値でありながら割合が低いということは、脆弱性管理チームの仕事量は増えるでしょうか、それとも減るのでしょうか。後ほど詳しく解説します。

# 2020 年上半期に上位を占めた脅威

本レポートで紹介する調査結果は、世界中の本番環境で観察された数十億件の脅威イベントを収集しているさまざまなネットワークセンサーから取得された、FortiGuard Labs の脅威インテリジェンスに基づくものです。第三者機関の調査によれば [*1]、フォーティネットはセキュリティデバイス出荷台数において業界最大を達成しています。複数の観点から脅威を概説するフォーティネット独自の本レポートをお読みいただくことで、2020 年上半期のサイバー脅威環境がどのようなものであったかを理解していただけるはずです。

## 脆弱性とエクスプロイト

フォーティネットのセンサーが捉えた IPS のアクティビティから、攻撃者が脆弱なシステムをどのように偵察し、侵入を試みるのかを知ることができます。それらの IPS シグネチャがトリガーされたとしても、それは必ずしも攻撃が成功したことを示すものではありません。しかし、現在どのタイプの脆弱性とシステムが標的になっているのかを知ることはできます。2020 年上半期にエクスプロイトの標的となった上位のプラットフォームとテクノロジーを、月毎に図 1 に示します。ここでは、最大の動きを示しているものを強調表示し、以下でその考察を行っています。

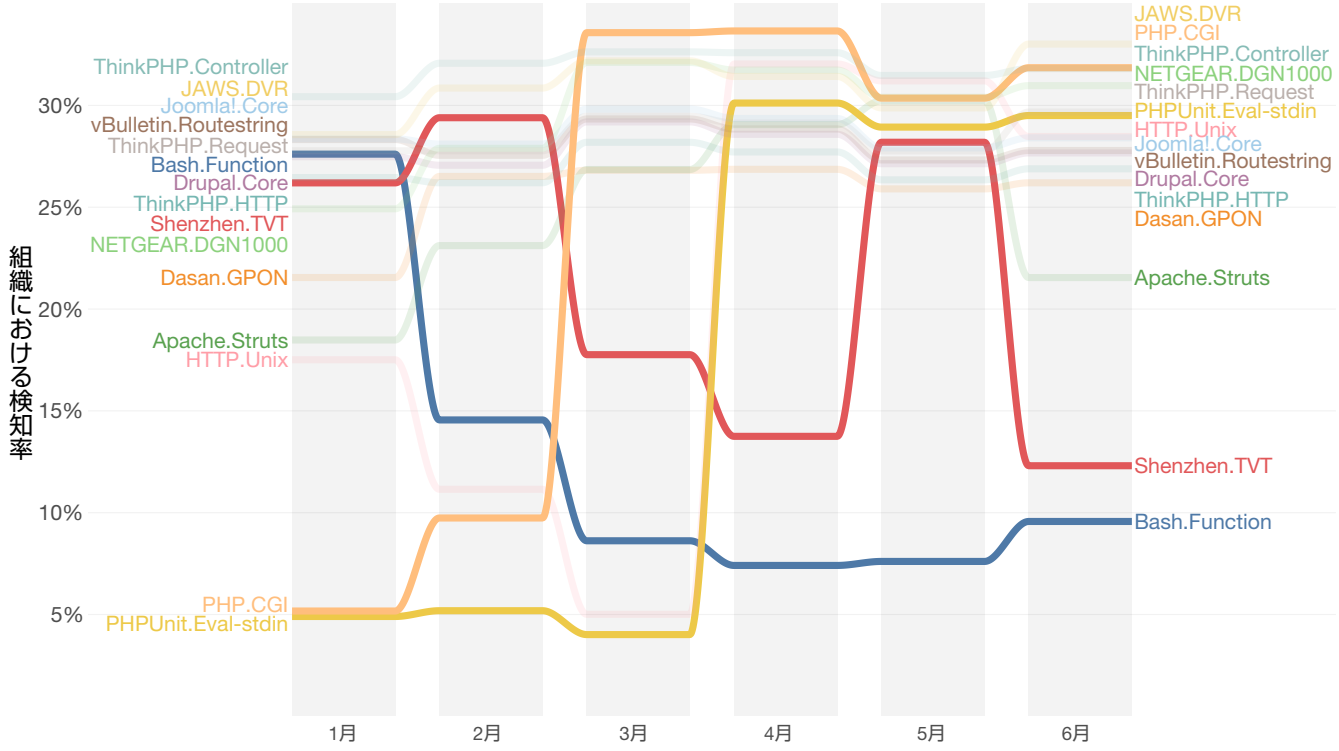



図 1：2020 年上半期に最も多かった IPS 検知数（月別）

月別の推移について説明する前に、検知率上位の構成を確認しておきましょう。1 つの例外（Shenzhen）を除いて、図の左右に記載されているテクノロジーは、過去のレポートと非常に似ています。グラフの上部には、これまで通り ThinkPHP、Joomla、Drupal、vBulletin などのコンテンツ管理システム（CMS）がランクインしており、これらのプラットフォームが大量のサイバー攻撃を受けていることを思い出させてくれます。これらのツールを使用している組織は、ツールの保守を怠らないことが極めて重要です。

2017 年に発生した Equifax の情報漏洩事件と関連がある Apache Struts の脆弱性は別として、他のいくつかのテクノロジーはネットワークデバイスのカテゴリに分類されます。このようなデバイスについては、本レポート後半の特集で解説します。ただし、Shenzhen は IPS 検知の「新顔」であるため、ここで説明することにしましょう。2018 年に初めて発見された Shenzhen は、2019 年後半に急増し、2 月のある週には 2 番目に多く検知されました。この活動は、Shenzhen TVT DVR [*2] および OEM に存在するリモートコード実行の脆弱性を標的にするエクスプロイトと関係があります。このエクスプロイトには、オンラインゲームサービスに対する DDoS 攻撃で知られるグループ Lizard Squad との関連を示唆する指標が含まれています。これは、さまざまなスキームのために消費者向け IoT デバイスから成る大規模ボットネットを構築しようとする犯罪者のもう 1 つの例です。

*1 IDC Worldwide Security Appliance Tracker - 2020 年 4 月（ファイアウォール、UTM および VPN アプライアンスの年間出荷台数に基づく）

*2 「Shenzhen TVT DVR」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/48519/shenzhen-tvt-dvr-remote-code-execution

本レポートで標的の上位をリストアップするだけでなく、このようなグラフを掲載することにしたのは、かなり大きな変化があったためです。Bash のリモートコード実行（RCE）の脆弱性は 1 月に大きな動きを見せ、その後数回下落し、6 月末には検知数上位の中での最下位に落ち着きました。この脆弱性は基本的に、2014 年に発見され、Heartbleed よりも深刻だとされた悪名高い Shellshock RCE です。2 月には、PHP CGI [*3] に存在する引数インジェクションの脆弱性に関連した検知が大幅に急増しました。3 月には別の PHP 関連の検知が急増しました。これは、PHPUnit [*4] に存在する別の RCE の脆弱性を標的としたものでした。Shenzhen は 4 月に再び急増しましたが、5 月には大きく落ち込みました。

ここでは、必ずしもグローバルなチャートの上位には入っていないものの、各地域で有名になったエクスプロイトに焦点を当ててみましょう。図 2 にそれらのエクスプロイトを示します。Zivif [*5]、TrueOnline [*6]、Allegro [*7] もまた、脆弱な IoT デバイスの偵察を試みるエクスプロイトの例です。特定の地域で特定のエクスプロイトが蔓延している理由は必ずしも明確ではありません。その代表的な例が、タイの ISP である TrueOnline です。

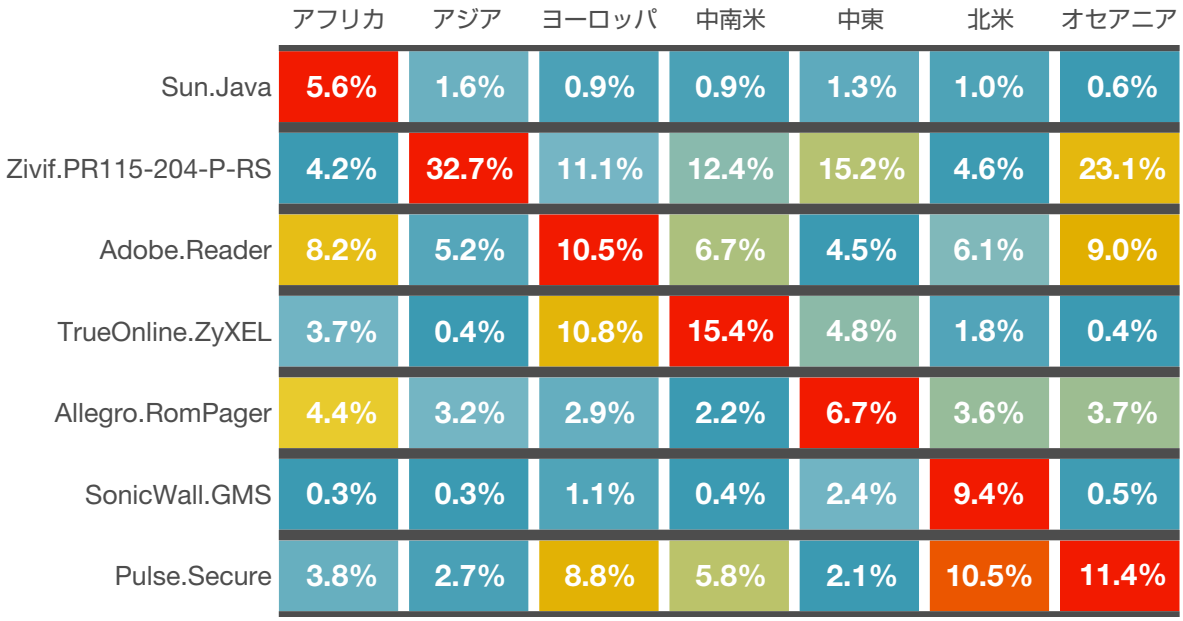



図 2：2020 年上半期に多かった IPS 検知数（組織の割合）

この脆弱性は、TrueOnline が（おそらくタイの）顧客に配布している ZyXEL ルーターの修正済バージョンに影響を与えます。そこで浮かんでくるのは、中南米での検知率がアジアと比較してなぜこれほど高いのかという疑問です。その答えは単純です。このルーターのファームウェアには言語パッケージが含まれており、世界的な販売が可能になっています。ISP が 2016 年頃に ADSL から VDSL に移行した際、ZyXEL ルーターは中南米の国々に広く販売されるようになりました。その経緯が現在の状況に反映しています。

では次に、特定の業種で異常なほど高い検知率を示した IPS 検知を見てみましょう。ここでは、図 3 に基づいて大まかな所見をいくつかお伝えしますが、各分野の詳細を確認するかどうかについては読者に委ねます。これらの一部（TAR-Archive [*8]、FTP.Login [*9] など）は簡単に悪用が可能であり、犯罪者はセキュリティ上のミスにつけ込もうとしているように見えます。

DotNetNuke は .NET ベースの CMS です。DotNetNuke の Web サイトによると [*10]、米国防総省は DotNetNuke を使用して数百の公開 Web サイトを運営しています。これはおそらく、公共機関の検知率の上昇と関係があります。MSSP で観測された PostgreSQL エクスプロイトの増加は、意図せずにデータベースがインターネットからアクセス可能な状態になっていることを示している可能性があります。Shodan で検索すると、数十万個の PostgreSQL データベースが見つかり、その多くは Amazon Web Services（AWS）でホストされています。お使いの MSSP が機密データを漏洩していないか、確認が必要です。

*3 「PHP CGI」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/31752/php-cgi-argument-injection
*4 「PHPUnit」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/45765/phpunit-eval-stdin-php-remote-code-execution
*5 「Zivif」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/45491/zivif-pr115-204-p-rs-web-cameras-hardcoded-password
*6 「TrueOnline」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/43619/trueonline-zyxel-p660hn-v1-unauthenticated-command-injection
*7 「Allegro」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/39849/allegro-rompager-cookie-remote-code-execution
*8 「TAR-Archive」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/13313
*9 「FTP.Login」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/22909/ftp-login-brute-force
*10 「DotNetNuke」、DNN Corp.（英語）：https://www.dnnsoftware.com/

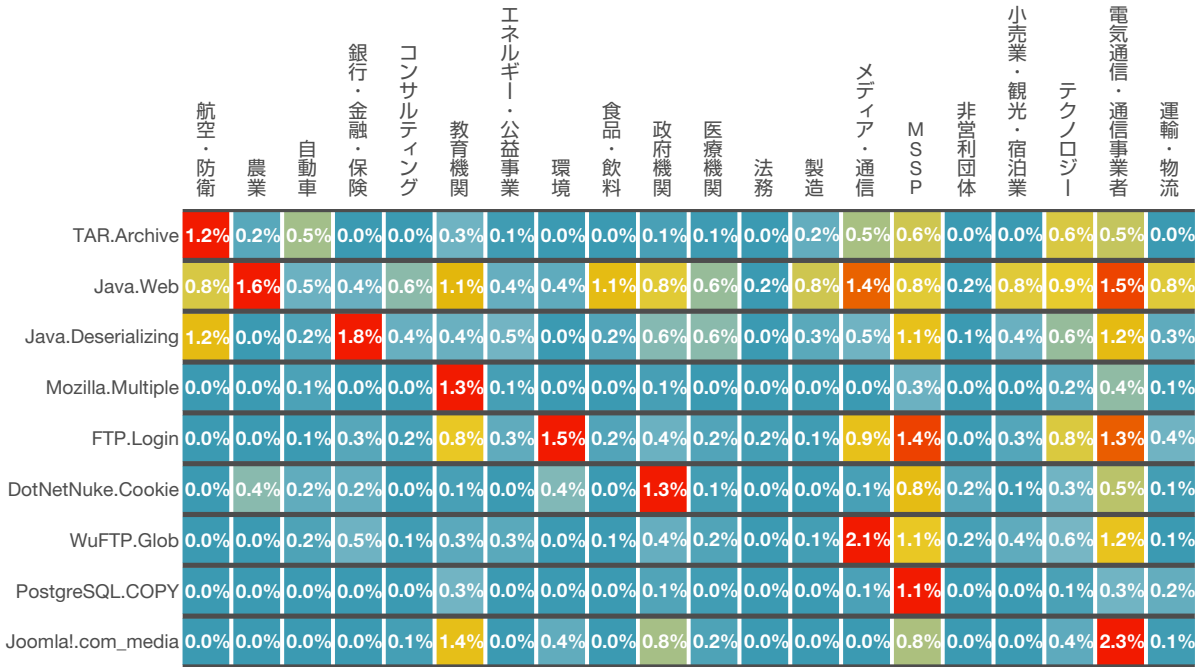



図 3：2020 年上半期の業種別 IPS 検知数（組織の割合）

一般的に、教育機関、メディア企業、MSSP、通信事業者は、他の業種に比べてホットスポット（狙われやすい場所）が多いと言われています。これらの業種に属する企業は、より広範囲の脅威を阻止できるように防御体制を整えておく必要があります。一方、法律事務所や非営利団体は、上から下までブルーグレー一色です。これは、これらの業種では異常に検知数が多い、もしくはその業種特有の脅威が検知されなかったことを示しています。ただし、これらの業種が標的になっていないという意味ではなく、単に上半期は多くの新たなエクスプロイトの標的にならなかったに過ぎません。次のセクションでは、これらの業種もマルウェアからは簡単に逃れられないことがお分かりいただけると思います。

## マルウェアの検知

マルウェアのトレンドには、攻撃者の意図と能力が反映されています。IPS 検知と同様に、フォーティネットのセンサーでマルウェアが検知されたとしても、必ずしもそれは感染が確認されたことを示すものではなく、悪意のあるコードの武器化や拡散を示していると考えられます。ネットワーク、アプリケーション、およびホストのレベルのさまざまなデバイスで、そうした攻撃を検知することができます。

図 4 は、2020 年上半期の月毎に最も検知されたマルウェアの順位を示しています。テクノロジーに焦点を当てるために IPS 検知を省略したケースと同様に、ここではマルウェアを特定の亜種ではなく、ファミリー（カテゴリ）に分類しています。このようにした目的は、多くの場合短命な数多くの亜種を類似点によってグループ化することで、「木を見て森（マルウェア）を見ず」にならないようにするためです。

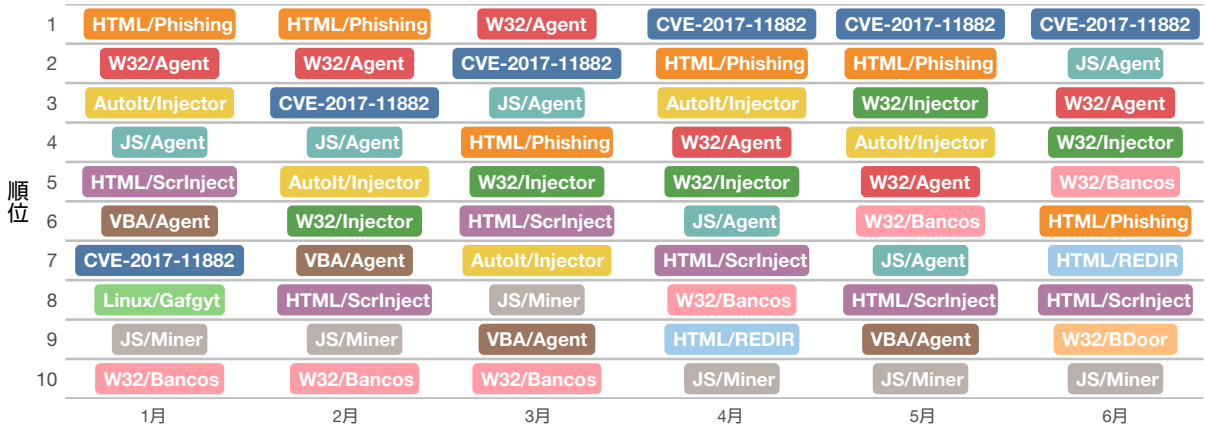



図 4：2020 年上半期に最も検知数が多かったマルウェアのカテゴリ（月別）

ここで言及すべきマルウェアは、Web ベースのフィッシング詐欺のすべての亜種を含む HTML/Phishing ファミリーです。これらのマルウェアは、1 月と 2 月は上位にいましたが、6 月には上位 5 位から脱落しました。/ScrInject（ブラウザスクリプトインジェクション攻撃）や /REDIR（ブラウザリダイレクションスキーム）などの HTML 攻撃と合わせて考えてみると、サイバー犯罪者はユーザーが最も脆弱で騙されやすくなる Web 閲覧へと誘導することに強い関心を寄せていることがわかります。Web ベースのマルウェアは、従来のアンチウィルス製品を難読化したり迂回したりして、感染の可能性を高めています。また、オフィスではなく自宅でインターネットを閲覧している人が多いために、企業の Web トラフィックが著しく減少していることからも、さらに懸念が高まります。確実に防御するには、2020 年の上半期にブラウザがマルウェアの主要な拡散手段であったことに注目し、リモートシステムを一貫して制御できるよう適切な措置を講じる必要があります。

図 5 の中でもう 1 つ注目しておくべきマルウェアは、CVE-2017-11882 [*11] を悪用するマルウェアです。この脆弱性は数年前に公開されたものですが（脆弱性自体はさらに古いものです）、2020 年上半期に検知数が着実に増加し、4 ヵ月連続で首位を維持しました。そして、この増加に注目したのはフォーティネットだけではありませんでした。4 月 1 日（エイプリルフールではありません）、米国シークレットサービス（USSS）は悪意のある添付ファイルを使用した偽の COVID-19 メールについての注意喚起 [*12] を掲載しました。USSS 刑事捜査局の代表者は、このマルウェアを拡散している攻撃者が CVE-2017-11882 を悪用して複数の攻撃キャンペーンを展開しようとしていると、CSO Magazine [*13] に語っています。特に卑劣だと思われるメールは、米国保健福祉省（HHS）を騙って、受信者に「COVID-19 に感染した」と伝えるものです。医療機器メーカーを標的にして、医療機器の提供を求める（マルウェアが埋め込まれた）文書を E メールで送信する攻撃もあります。

図 5 は、図 3 で使用した方法を踏襲して、特定の業種で異常に高い検知率を示したマルウェアファミリーを特定しています。列を見渡してみると、全体がブルーグレーの業種は 1 つもありません。すべての業種に少なくとも 1 つのマルウェアのホットスポットがあり、中には複数のホットスポットが存在している業種もあります。

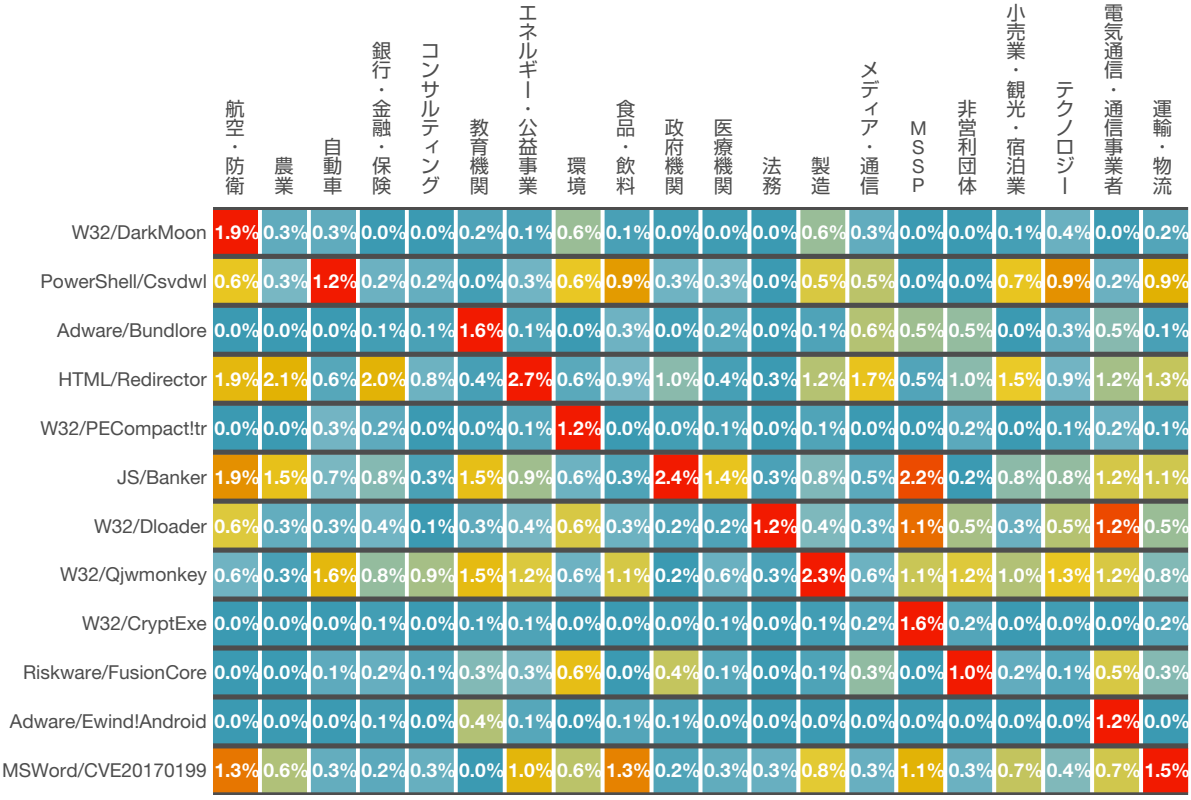



図 5：2020 年上半期の業種別マルウェア検知数（組織の割合）

マルウェアの名前は必ずしもわかりやすくはありませんが、直感で理解できるものもあります。不明なものについては、FortiGuard Labs による用語解説（英語）[*14] をご参照ください。たとえば、通信事業者は Android デバイスでより多くのマルウェアを確認しています。アドウェアは教育機関を標的にしています。JS/Banker は、銀行よりも政府機関や MSSP から頻繁にデータを盗み出します。自動車業界は、PowerShell の影響に眉をひそめています。業種毎の説明はこのくらいにして、次はボットネットの問題について解説します。お客様の組織に最も影響を与える脅威に対するセキュリティ対策を強化する上で、本レポートの詳細な説明が役立つことを願っています。

*11 「CVE-2017-11882」（英語）：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882

*12 「Fraudulent COVID-19 Emails with Malicious Attachments」、米国シークレットサービス（USSS）、2020 年 4 月 1 日（英語）：https://metacurity.com/wp-content/uploads/2020/04/Alert-20-006-I-COVID19-Malicious-Emails-1.pdf

*13 「Beware malware-laden emails offering COVID-19 information, US Secret Service warns」、Cynthia Brumfield 著、CSO Magazine、2020 年 4 月 9 日（英語）：https://www.csoonline.com/article/3536696/us-secret-service-warns-of-malicious-emails-offering-covid-19-information.html

*14 FortiGuard Labs の用語解説（英語）：https://fortiguard.com/encyclopedia

## ボットネットの活動

一般的にエクスプロイトとマルウェアのトレンドは感染前の攻撃の前兆を示すものであるのに対し、ボットネットのアクティビティはすでにそのボットネットに感染した事を示しています。システムが感染するとリモートのホストとの通信が頻繁に発生することから、悪意のある活動の全容を監視する上で、このトラフィックは重要な役割を果たします。

ボットネットのデータを調査する度に、サイバー犯罪者の間では広範で持続的な制御が高く評価されていることがわかります。その副作用として、主要なボットの活動に著しい一貫性があることが挙げられます。図 6 はこのことを完璧に示しています。検知率の月毎のランキングは、IPS 検知やマルウェア検知よりもはるかに一貫性があります。過去のレポートでボットネットの持続性を調査したところ、大規模な企業のセキュリティチームは通常、ボットネットのトラフィックを特定し、合理的な時間内に感染したシステムを一掃することができます。しかし、小規模企業や数百万台の消費者向けデバイスに感染したボットネットは、かなりの期間常駐する傾向があります。今回は、そうした事例が多く確認されています。

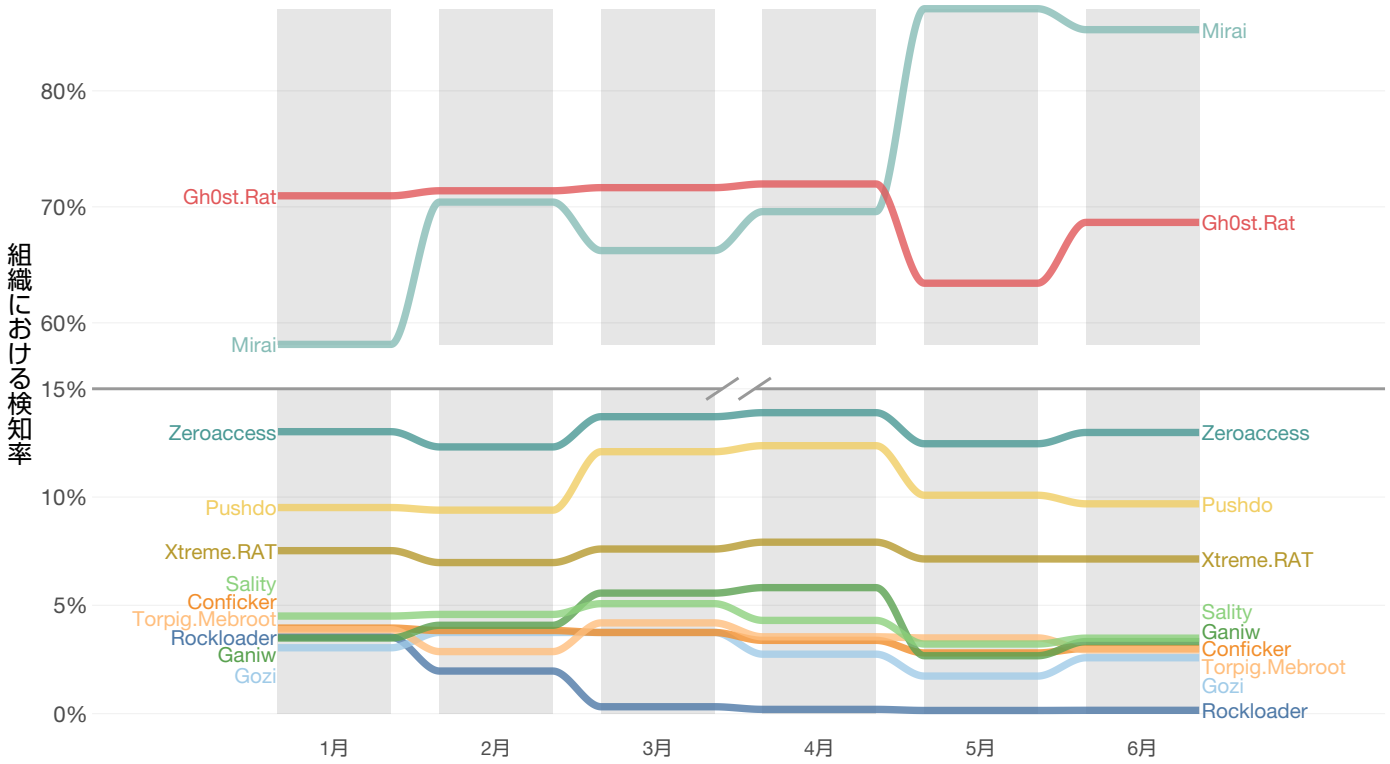



図 6：2020 年上半期に最も検知率の高かったボットネット（縦軸：途中省略）

図 6 の最初の 2 つのボットネットである Mirai と Gh0st が、2019 年下半期と同様にチャートを占めています。消費者向け IoT 製品に存在する新旧の脆弱性を標的にしている攻撃者が強い関心を寄せていることから、Mirai は 5 月初旬にボットネット 1 位に急上昇しました。このトレンドに注目すべき理由として、在宅勤務の従業員が企業ネットワークに接続する際に使用するデバイスをサイバー犯罪者が悪用して、企業ネットワークへの足場を確保しようとしている可能性があることが挙げられます。ある意味、企業ネットワークの境界線が家庭にまで広がっていると言えます。

古いマルウェア / ボットネットファミリーである Gh0st もまた、在宅勤務のユーザーやアプリケーションを標的にした攻撃に利用されていました。Gh0st はリモートアクセスボットネットで、攻撃者による感染システムの完全制御、キー入力の記録、Web カメラやマイクのライブフィード、ファイルのダウンロードやアップロードなどの不正行為を可能にします。

ボットネット間のばらつきをより明確に示すために、図 7 では図 6 の上位を拡大し、地域間で比較しています。Mirai と Gh0st は現在でも拡散を続けていますが、その活動は全世界で同じではないことは明らかです。たとえば、数ある Mirai の亜種のいずれかに関連するトラフィックを検知した組織の割合は、アジアよりもヨーロッパの方が 20% 以上高くなっています。しかし、ヨーロッパは Gh0st の活動では第 3 位です。

| | アフリカ | アジア | ヨーロッパ | 中南米 | 中東 | 北米 | オセアニア |
|---|---|---|---|---|---|---|---|
| Mirai | 70.7% | 63.3% | 85.6% | 78.0% | 68.3% | 84.8% | 85.3% |
| Gh0st.Rat | 62.7% | 59.2% | 66.7% | 60.6% | 58.0% | 72.9% | 72.5% |
| | | | | | | | |
| Pushdo | 14.3% | 17.4% | 20.0% | 19.7% | 14.7% | 21.6% | 19.3% |
| Zeroaccess | 15.0% | 17.4% | 10.8% | 15.9% | 14.1% | 12.4% | 11.4% |
| Ganiw | 10.9% | 13.2% | 9.2% | 10.9% | 9.0% | 8.8% | 10.4% |
| Xtreme.RAT | 10.2% | 12.4% | 7.4% | 10.5% | 11.4% | 6.2% | 8.3% |
| Sality | 12.6% | 12.8% | 2.5% | 6.2% | 16.6% | 2.6% | 2.0% |
| Torpig.Mebroot | 8.1% | 7.6% | 7.3% | 5.3% | 4.6% | 4.9% | 3.5% |
| Mariposa | 6.1% | 9.7% | 4.5% | 6.8% | 5.4% | 3.2% | 3.7% |
| Gozi | 10.4% | 10.0% | 2.7% | 4.4% | 9.5% | 2.4% | 1.9% |
| Necurs | 7.3% | 5.9% | 2.3% | 3.7% | 5.9% | 3.4% | 3.5% |
| FinFisher | 6.5% | 11.7% | 2.4% | 3.3% | 3.4% | 1.9% | 2.2% |
| Conficker | 5.8% | 7.2% | 2.7% | 4.7% | 6.2% | 1.0% | 0.5% |
| Rockloader | 3.8% | 2.4% | 3.5% | 2.2% | 1.2% | 4.3% | 2.2% |
| XorDDOS | 2.5% | 3.4% | 1.2% | 2.6% | 2.7% | 1.6% | 1.2% |
| Zeus | 2.3% | 8.1% | 1.7% | 2.5% | 2.1% | 1.4% | 1.0% |
| Nitol | 2.0% | 4.6% | 1.2% | 2.7% | 2.1% | 1.7% | 1.2% |
| Ramnit | 6.4% | 6.3% | 1.4% | 1.9% | 5.0% | 1.1% | 1.0% |
| njRAT | 3.2% | 3.7% | 1.1% | 2.3% | 3.0% | 0.9% | 2.0% |
| Emotet.Cridex | 3.1% | 2.0% | 0.8% | 3.8% | 1.5% | 0.9% | 1.0% |

図 7：地域別で見る 2020 年上半期に検知数の多かったボットネット（組織の割合）

図 7 を下に移動していくと、さらに大きな地域差があることがわかります。Gozi はアフリカで蔓延しており、FinFisher はアジアで特に活発な活動を見せています。Emotet.Cridex は、中南米で拡散している唯一のボットネットです。Sality は中東の組織で拡散しており、Pushdo が最も検知されているのは北米です。不思議なことに、オセアニアはここに示したボットネットのいずれにおいても 1 位の座を獲得していません（ただし、Mirai は僅差の 2 位）。このような違いは、標的の選択、インフラストラクチャ、テクノロジーの導入、セキュリティ構成、ユーザーの振る舞いなど、無数の要因によるものです。

# 注目の脅威とトレンド

## 世界的パンデミックの悪用

新型コロナウイルスがサイバーセキュリティに与えた甚大な影響について、セキュリティ研究者や他のベンダーがすでに多くの文書を公開していますが、フォーティネットもブログ記事で解説し、3 / 4 号抄訳 [*15]、4 / 2 号抄訳 [*16]、4 / 21 号（英語）[*17]、5 / 1 号（英語）[*18]、6 / 3 号抄訳 [*19]、そしてその他多数 [*20] の記事やレポートなどを多数発表してきました。とはいえ、それを理由に 2020 年上半期の脅威活動をまとめたレポートにおいて新型コロナウイルスのトピックを取り上げなければ、怠慢とのそしりを免れません。

予想されていた通り、便乗型のフィッシング詐欺師から陰謀を企む国家的攻撃者にいたるまで、あらゆる種類のサイバー犯罪者が、自らの利益のために今回のパンデミックにつけ込む方法を見つけました。世界中の組織は、突然に在宅勤務の従業員の大半をサポートしなければならない状況に直面したのです。この変化は、保護が脆弱なホームネットワーク、家庭用デバイス、VPN 接続、ビデオ通信、コラボレーションツールを標的にして、企業ネットワークに侵入する絶好の機会を攻撃者にもたらしました。

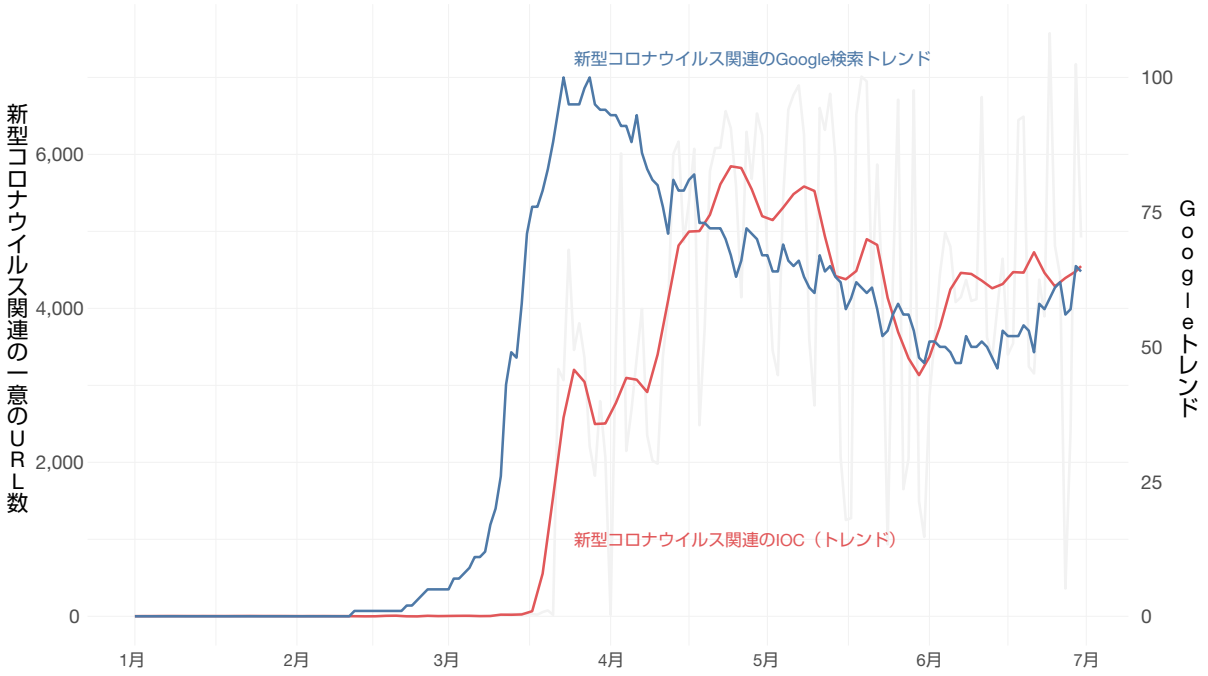



図 8：新型コロナウイルス関連の Google 検索トレンドと、新型コロナウイルスをテーマにした悪意のある URL の比較

脅威活動の痕跡が確認され始めたのは、パンデミックの範囲と影響に対する社会的な認識が高まったのとほぼ同時期でした。図 8 は、コロナウイルスに関連した Google 検索のトレンドと、コロナウイルスをテーマにした悪意のある URL を Web フィルターで検知した結果を比較したものです。これらのドメインの多くは、「コロナウイルス」、「ワクチン」、「クロロキン」、「レムデシビル」などの単語が含まれており、認証情報の収集やマルウェア / スパムの拡散を目的として作成されました。これは、社会に広く影響を与える大きなニュースや出来事を利用するために、いかに攻撃者は迅速に行動するのかを示しています。

また、CDC（疾病対策センター）や WHO（世界保健機関）などの信頼されている情報源を装った、パンデミック関連のガイダンスを含むとされる文書が添付された、悪意のある E メールが急増していることも確認されました。金融機関を標的とするトロイの木馬 Emotet のオペレーターは、いち早くコロナウイルスへの恐怖心につけ込み、この方法でマルウェアを拡散させようとした攻撃者でした。

その後数週間から数ヵ月の間に、新型コロナウイルス関連の手口を使用した悪意のある活動が範囲を広げていることが確認されました。この活動には、フィッシングやビジネスメール詐欺のスキーム、国家が支援する攻撃、ランサムウェア攻撃などが含まれています。フォーティネットが追跡した脅威には、以下のようなものがあります。

*15 「過熱する新型コロナウイルス（COVID-19）報道を悪用した攻撃の増加」、フォーティネット、2020 年 3 月 4 日：
https://www.fortinet.co.jp/blog/threat-research/attackers-taking-advantage-of-the-coronavirus-covid-19-media-frenzy.html

*16 「COVID-19（新型コロナウイルス）に便乗した標的型攻撃で情報を窃取するマルウェア」、フォーティネット、2020 年 4 月 2 日：
https://www.fortinet.co.jp/blog/threat-research/latest-global-covid-19-coronavirus-spearphishing-campaign-drops-infostealer.html

*17 「Deconstructing an Evasive Formbook Campaign Leveraging COVID-19 Themes」、フォーティネット、2020 年 4 月 21 日（英語）：
https://www.fortinet.com/blog/threat-research/deconstructing-an-evasive-formbook-campaign-leveraging-covid-19-themes

*18 「Scammers Using COVID-19/Coronavirus Lure to Target Medical Suppliers」、フォーティネット、2020 年 5 月 1 日（英語）：
https://www.fortinet.com/blog/threat-research/scammers-using-covid-19-coronavirus-lure-to-target-medical-suppliers

*19 「COVID-19（新型コロナウイルス）関連のサイバー攻撃について：FUD（恐怖、不安、疑念）に付け入る手法」、フォーティネット、2020 年 6 月 3 日：
https://www.fortinet.co.jp/blog/industry-trends/covid-19-attacks-explained-an-overview-of-the-current-attacks-exploiting-fud-around-the-pandemic.html

*20 フォーティネットセキュリティブログ：https://www.fortinet.co.jp/blog/

- 偽のコロナウイルス感染拡大マップが掲載された Web サイトを介して拡散される、情報窃取マルウェア AZORult
- Gamaredon APT グループによるウクライナの軍事諜報機関を標的としたフィッシング攻撃
- ベトナム系の APT32 グループによる中国本土への攻撃
- 北朝鮮と関係のある Kimsuky APT グループによる、韓国の組織に対する標的型攻撃

総じて、2020 年上半期にコロナウイルスをテーマにした攻撃の標的として最も多かったのは、米国、中国、ロシアの組織でした。

コロナウイルスをテーマにしたメッセージ、添付ファイル、または文書に隠されたランサムウェアも、もうひとつの脅威となりました。フォーティネットでは、2020 年上半期にこのカテゴリに分類された 3 つのランサムウェア（NetWalker、Ransomware-GVZ、CoViper）を追跡しました。この 3 つのうち、CoViper はデータを暗号化する前にコンピュータのマスターブートレコード（MBR）を書き換えてしまうため、特に悪質です。これまでにも、MBR を消去するツールとランサムウェアを組み合わせて、PC を効果的に機能停止させる攻撃がいくつか確認されています。

また、上半期の最後になって、米国やその他の国で新型コロナウイルス関連の研究に関与している組織を攻撃する、国家レベルの脅威グループによる活動と思われる報告がいくつかありました。

2020 年上半期のパンデミック関連の悪意のある活動が、最終的にどのような影響を与えたのか（あるいは与えなかったのか）は不明です。しかし、多くの組織にとって、今回の攻撃は保護が脆弱なホームネットワークから接続するテレワーカーがもたらす脅威から自社ネットワークを保護するためには、ゼロトラストモデルをはじめとするより良いアプローチが必要であることを浮き彫りにしました。また、防御する側がニュースに目を光らせ、最新の脅威の一歩先を行くことの重要性も明らかになっています。

## DVR から DMZ へ

パンデミックの影響でテレワークが急増していることから、自宅のルーターや DVR、およびその他のインターネット接続デバイスのセキュリティに注目が集まっています。懸念されるのは、これらのシステムのセキュリティが不十分であることを攻撃者が悪用して、企業ネットワークや、在宅勤務の従業員が企業ネットワークに接続する際に使用するデバイスへの侵入の足掛かりにする可能性がある点です。もう 1 つの問題は、攻撃者がこれらのデバイスを悪用すれば、Mirai のような大規模ボットネットを短期間で構築し、DDoS 攻撃やマルウェアの拡散に利用できることです。

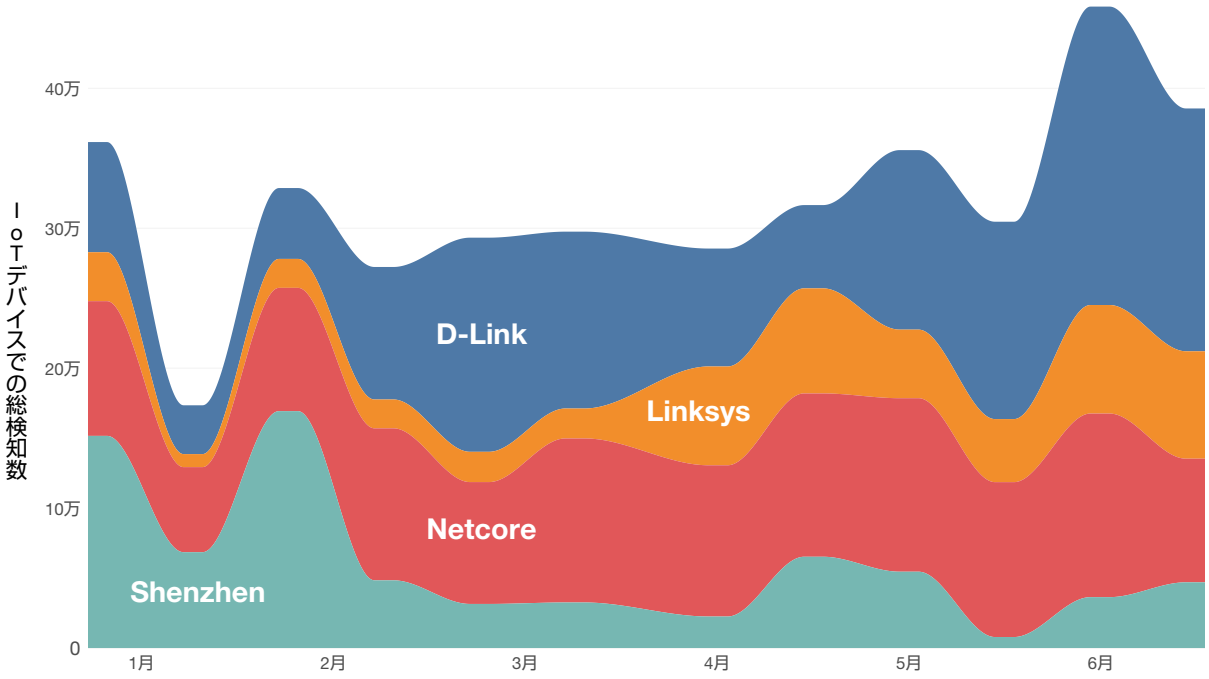



図 9：2020 年上半期に一般的なネットワークデバイスを標的にした IPS 検知数

2020 年上半期には、攻撃者が家庭用 IoT 製品の新旧の脆弱性を引き続き悪用しようとしていることを示す証拠が多数確認されました。Shenzhen TVT DVR の脆弱性を狙う悪意のある活動が急増していることについては前述しましたので、ここでは省略します。2020 年上半期に攻撃者の関心を集めたもう 1 つの脆弱性は、D-Link ルーターに関係するものです。このコマンド実行の脆弱性は D-Link ルーターの複数のモデルに存在しており、攻撃者は脆弱なデバイスを完全に制御することができます。この脆弱性を標的とした悪意のある活動の大半が、5 月と 6 月に発生していたことが確認されました。攻撃の量や標的デバイスの数は、ピーク時で 16 万台と Shenzhen DVR の脆弱性と比較してさらに多くなっており、攻撃者の関心の高さを示唆するには十分でした。

しかし、フォーティネットが観測した中で最も持続性の高かった大規模攻撃は、Netcore/Netis ルーターに影響を与えたものでした。1 月から 6 月末までの間、Netcore/Netis ルーターのハードコードされたパスワードのセキュリティがバイパスされる問題が、執拗な攻撃を受けていました。このバックドアの脆弱性が発見されたのは 2014 年 8 月でしたが、それ以来、フォーティネットが追跡してきた中で最もトリガーされた IPS シグネチャの 1 つとなっています。攻撃のピークとなった 5 月には、このシグネチャから 6,000 万件以上のヒットが収集されました。

また、Linksys ルーターに存在する認証バイパスの脆弱性と、Linksys E シリーズのルーターに存在する別のリモートコマンド実行の脆弱性は、2020 年上半期に攻撃者から大きな注目を集めた、ルーターにおける他の 2 つの脆弱性です。

攻撃者はすでに、これらの脆弱性を悪用して非常に大規模なボットネットの構築に成功しています。たとえば、上半期に出現した IoT ボットネット「Dark Nexus」は、数千台の ASUS ルーターと D-Link ルーターで構成されています。また、2020 年上半期に研究者によって確認された[*21] ピアツーピアボットネットである Mozi は、前述したコマンド実行の脆弱性が存在する D-Link デバイスなどの悪用されたルーターや DVR から成る、別のボットネットです。

このような脆弱なデバイスがホームネットワーク上に存在していると、数多くのテレワーカーを擁する組織では攻撃対象領域が大幅に拡大することになります。したがって、オフィスにいた時と同等の保護レベルで在宅勤務の従業員を保護するために、さまざまな選択肢を評価する必要があります。

## OT への脅威：過去と現在

前のセクションで説明した IT デバイスの正反対に位置するのが、OT（オペレーショナルテクノロジー）です。SCADA（Supervisory Control And Data Acquisition：監視制御・データ取得）システムやその他のタイプの ICS（産業用制御システム）を標的とした脅威が検知される数は、当然ながら IT と比較してはるかに低いですが、その重要性が低いわけではありません。図 10 は、ICS のメーカーやコンポーネントを標的としたエクスプロイト検知の内訳です。

OT 管理の担当者でなければ、この 6 月に重要な記念日があったことに気付かなかったかもしれませんが、2020 年は Stuxnet の発見から 10 年の節目の年です。Stuxnet は、イランの核計画にとって重要な施設を妨害したことで話題を呼んだ、悪意のあるワームです。この重大な出来事以降、世界中で OT システムを標的とした高度なサイバー攻撃が多数[*22] 発生しています。その原因の 1 つとして、OT ネットワークがインターネットに接続されるようになり、攻撃を受けやすくなったことが考えられます。この仮説は、OT 組織の 74% が過去 12 ヵ月間にマルウェアの侵入を経験していることを明らかにした、フォーティネットの「State of Operational Technology and Cybersecurity Report（オペレーショナルテクノロジーの現状とサイバーセキュリティレポート）」[*23] でも裏付けられています。

*21 「New Mozi Malware Family Quietly Amasses IoT Bots」、CenturyLink、2020 年 4 月 13 日（英語）：https://blog.centurylink.com/new-mozi-malware-family-quietly-amasses-iot-bots/

*22 「Evolution of Cyber Threats in OT Environments」、フォーティネット、2020 年 6 月 11 日（英語）：https://www.fortinet.com/blog/industry-trends/evolution-of-cyber-threats-in-ot-environments

*23 「2020 State of Operational Technology and Cybersecurity Report」、フォーティネット、2020 年 6 月（英語）：https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf

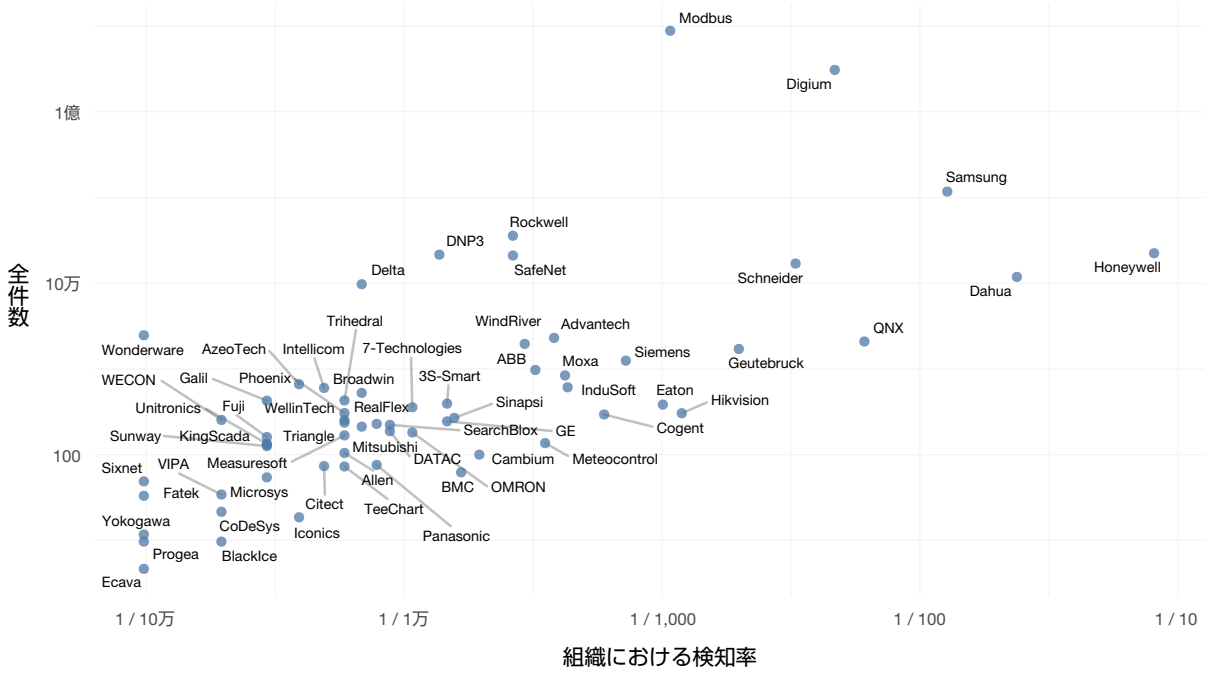



図 10：産業用システムが関係している IPS 検知率と件数

OT 脅威の最近の動向では、2 つの出来事が 2020 年上半期特に注目を集めました。1 月に、米国、ブラジル、ドイツの IPS センサーで、Modbus TCP サーバーとプログラマブルロジックコントローラ（PLC）[*24] が関与する情報漏洩の可能性のある活動が急増しました。そのため、図 10 で示したすべての OT システムの中で、Modbus 関連の検知が最も多くなっています。ただし、このシグネチャのすべてのトリガーが必ずしも悪意のあるものとは限りません。しかし、SCADA ネットワークに侵入した攻撃者が Modbus コントローラにアクセスして問題を引き起こす可能性があるため、監視する価値はあります。

2 つ目の注目すべき出来事は、5 月に研究者が Ramsay を発見したことです [*25]。Ramsay は、隔離されたネットワークやアクセスが厳しく制限されたネットワーク内の機密ファイルを収集し盗み出すために設計された、スパイ活動フレームワークです。ここで Ramsay について言及するのは、OT 環境がまさにそうした特性を持っているからです。Ramsay がいつから活動していたのかは明確ではありませんが、以前から存在する APT グループ「Darkhotel」と関係があります。その名が示すように、Darkhotel は産業施設よりもホテルの Wi-Fi ネットワークを悪用することで知られています。しかし、注目すべきは Ramsay の過去ではなく、その潜在能力です。

フォーティネットは、OT オペレーション、とりわけ重要インフラの一部である OT オペレーションの保護に尽力している数少ないセキュリティベンダーの 1 つです。OT 環境の保護という特有の課題と、その解決にフォーティネットをどのように活用すればよいのかについては、こちらをご覧ください [*26]。

## 活動の場を広げるランサムウェア

企業組織を標的にした上半期のランサムウェア攻撃の最後を締めくくったのは、6 月に発生したある有名メーカーに対する攻撃です。この攻撃によって業務は妨害され、いくつかの施設では一時的に生産が中断されました。

セキュリティ研究者は、攻撃に使用されたマルウェアが EKANS（一般には Snake とも呼ばれます）だと特定しましたが、これは ICS システムを攻撃するためにカスタマイズされた機能を持つランサムウェアです。フォーティネットがこのマルウェアを分析 [*27] したところ、高度に難読化されていること、GO プログラミング言語で書かれていること、OT と ICS システムを標的にしている点を除いては、他のランサムウェアツールと大差がないことが判明しました。この攻撃、そして EKANS が使用されているという事実は、攻撃者がランサムウェア攻撃の対象を OT 環境にまで拡大している可能性を示唆しており、気掛かりです。

2020 年上半期、フォーティネットは前のセクションで説明した新型コロナウイルスをテーマにしたものなど、その他のランサムウェア脅威に特有の活動を分析しました。観測されたトレンドの 1 つは、攻撃者が被害者組織のデータをロックするだけでなく、データを盗み出して大規模に公開すると脅して身代金をゆすり取ろうとする、ランサムウェアのインシデントが増加していることです。

*24 「Modbus TCP サーバーとプログラマブルロジックコントローラ（PLC）」、FortiGuard Labs（英語）：https://fortiguard.com/encyclopedia/ips/11529/modbus-tcp-unauthorized-read-request-plc
*25 「Ramsay: A cyber-espionage toolkit tailored for air-gapped networks」、Ignacio Sanmillan 著、ESET、2020 年 5 月 13 日（英語）：https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/
*26 「重要インフラの保護」、フォーティネット：https://www.fortinet.com/jp/solutions/industries/scada-industrial-control-systems
*27 「OT / ICS を標的にする EKANS ランサムウェアの詳細」、フォーティネット、2020 年 7 月 1 日：https://www.fortinet.co.jp/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems.html

その一例である DoppelPaymer は、自動車や航空宇宙業界向けのカスタムパーツのサプライヤー、NASA の請負業者、カリフォルニア州トーランス市政府に対する攻撃に使用されたランサムウェアです。フォーティネットの分析によると、DoppelPaymer はファイルを暗号化するだけでなく、Web サイトにファイルを転送します。そして、被害者が身代金の支払いを拒否した場合には、この Web サイトにデータが公開されます。

この手口は、1 月に Maze ランサムウェアの攻撃を受けた Medical Diagnostic Laboratories が身代金の支払いを拒否したため、同社が所有する約 10 GB の研究データを Maze のオペレーターが公開した際に初めて使用されました。その後、Sodinokibi や DoppelPaymer のオペレーターもこのハイブリッドモデルを使用するようになっています。このトレンドにより、組織が今後ランサムウェア攻撃で重要な知的財産、企業秘密、機密データなどを失うリスクが著しく高まっています。

RaaS（Ransomware-as-a-Service）は、2020 年上半期も引き続きサイバー犯罪者の間で活用が進んでいます。フォーティネットが追跡した RaaS の脅威の 1 つが、RDP（Remote Desktop Protocol）を攻撃ベクトルに利用してネットワークに対する初期アクセスを実行するランサムウェア「Phobos」です。このマルウェアが、ブルートフォース攻撃によって認証情報を取得したり、盗まれた認証情報を使用したり、ポート 3389 の安全でない接続を利用したりできることをフォーティネットは確認しています。このマルウェアは RaaS モデルで販売されているため、高度な手法を使わない攻撃者でも比較的簡単に利用できるようになっています。

Phobos のようなマルウェアは、組織が RDP サーバーの保護の重要性を再認識するきっかけとなっています。セキュリティが不十分で、インターネットからのアクセスが可能な RDP サーバーは、企業ネットワークに最初にアクセスする手段を探している犯罪者の格好の標的となっています。数多くの地下フォーラム / マーケットプレイスでは、すでにハッキングされた RDP サーバーへのアクセス情報が比較的安価に販売されているため、多くの犯罪者は侵入に向けた最初の作業をする必要さえありません。警告が繰り返し出されているにもかかわらず、何十万ものシステムがアクセス可能であり、インターネット経由での攻撃に対して未だ脆弱な状態が続いています。

他にも、Sodinokibi、Nemty、DeathRansom の 3 種類のランサムウェアが、2020 年上半期に RaaS モデルを介して拡散されていることが確認されました。フォーティネットが分析した DeathRansom の初期バージョンは、実際にはファイルを暗号化していませんでしたが、最近のバージョンはファイルの暗号化を実行していることがわかっています。

図 11 は、「ランサムウェアは我が社のような企業には影響しない」という考えが誤りであることを示しています。この図を見れば、今年前半の 6 ヵ月間にランサムウェアの被害を免れた業種がなかったことは明らかです。最も多く狙われた業種は、通信事業者、MSSP、教育、政府、テクノロジーの 5 つでした。医療機関はランサムウェアの標的になるケースが多いものの、ここでは中間的な位置にあります。

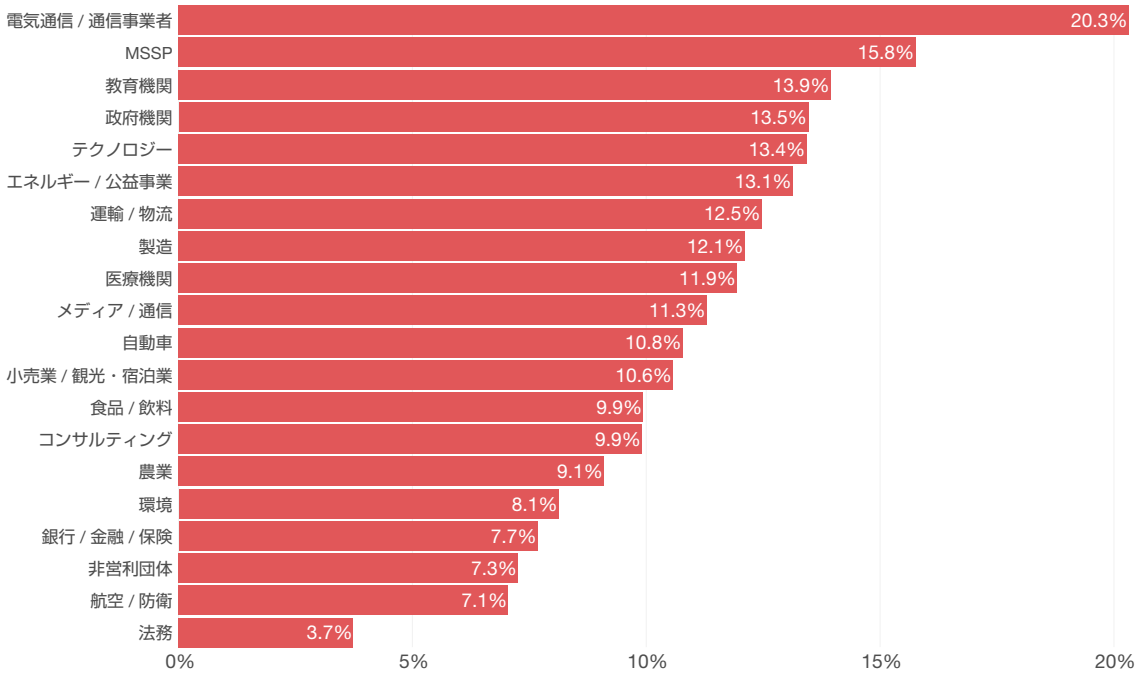



図 11：2020 年上半期にランサムウェアを検知した組織の割合

サイバー犯罪者が一部の被害者から多額の身代金を引き出すことに成功していることから、ランサムウェアの活動は当面衰えないでしょう。実際、ハイブリッド攻撃が増加していることや RaaS が入手しやすくなっていることは、今後の状況が悪化する可能性が高いことを示唆しています。しかし、絶望する必要はありません。ランサムウェアに対抗する効果的な方法はいくつかあります[*28]。

*28 「Steps to Protect Your Organization from Ransomware」、フォーティネット、2020 年 1 月 24 日（英語）：
https://www.fortinet.com/blog/industry-trends/fifteen-steps-to-protect-your-organization-from-ransomware

## エクスプロイトの時代

近年、脆弱性の悪用をモデル化して予測する取り組みに関心が高まっています。これは、最新の脆弱性スキャンで検知されたすべての脆弱性を修正するには、時間もリソースも不足しているという長年の葛藤から始まっています。もう 1 つの理由として、ここ数年で CVE リスト [*29] に追加される公開済み脆弱性の数が急増していることが挙げられます。その主な要因は、脆弱性に CVE を割り当てる権限を持つ組織 [*30] を MITRE が増やしたことにあります。CVE をより容易に、より包括的に追跡できるようになったのは良いことですが、同時に修正の対象が増え続けていることを意味します。そのため、脆弱性の修正に優先順位を付けることがますます重要になってきています。

1 つは、実環境で悪用されている脆弱性に優先順位を付けることです。この場合、どの CVE が悪用されたかを把握するには、その悪用を検知するためのセンサーを広範囲に配備しなければならないという課題があります。この課題については、フォーティネットがすでに対応済です。

図 12 の横軸は、各々の年に公開された CVE のうち、2020 年上半期にフォーティネットがエクスプロイト活動を検知した CVE の割合を示しています。全体での割合は 6% ですが、より新しい CVE（赤みがかった色）の方が悪用される率が低いことがわかります。これまでのところ、2020 年は CVE リストの 20 年以上の歴史の中で、過去最少の悪用率（1% 未満）を記録しています。この現象は、前述した CVE の増加と関連しています。また、エクスプロイトの開発と拡散には時間がかかるという事実も関係しています。

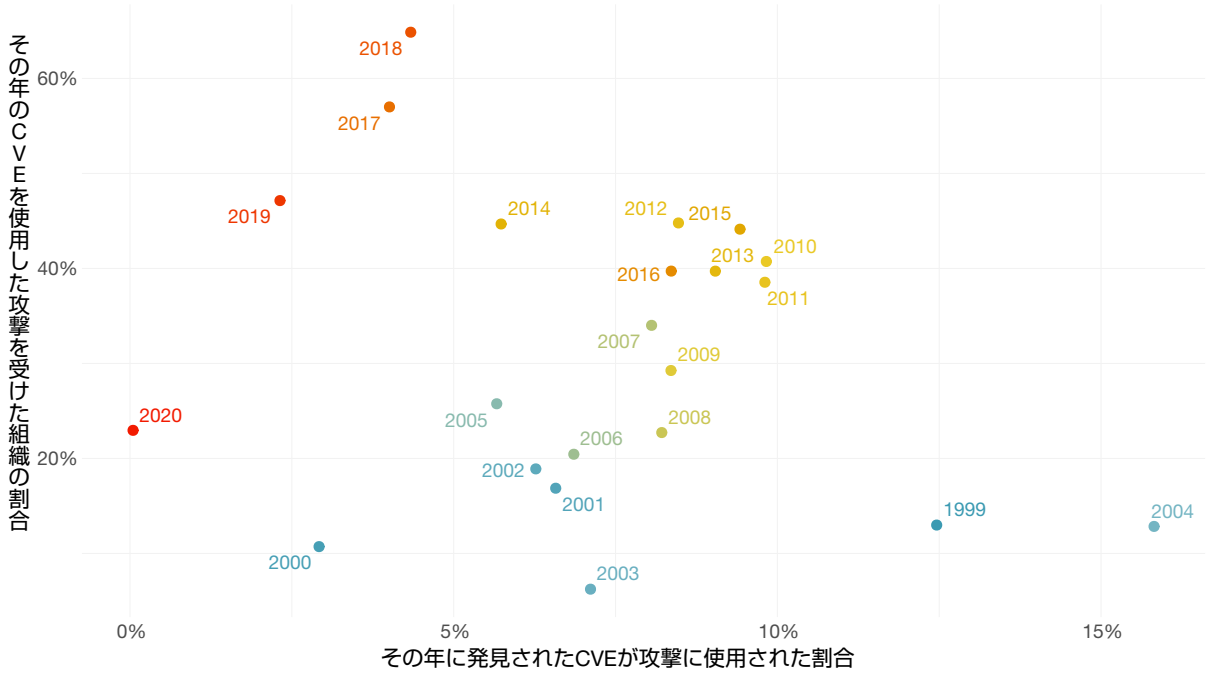



図 12：年別で見る、エクスプロイトが検知された CVE の割合（縦軸）と、エクスプロイトを検知した組織の割合（横軸）

図 12 の縦軸は、別の視点も提供しています。縦軸は、各年に公開された CVE を標的としたエクスプロイト活動を検知した組織の割合です。ここからは、最も高いエクスプロイトの検知率（65%）を示しているのは 2018 年の脆弱性ですが、4 分の 1 以上の企業が 15 年前（2005 年）の CVE を悪用しようする試みを検知したことがわかります。ここで忘れてはならないのは、「古い脆弱性だからといって、新たな問題が発生しないとは限らない」ということです。ただし、一般的には（大規模なエクスプロイトの開発と、正規のハッキングツールや悪意のあるハッキングツールを介した拡散に必要な時間を考慮に入れても）、新しい脆弱性ほど広範囲に悪用される傾向があります。

つまり、防御する側は、ネットワーク全体でより多くの脆弱性に対処するだけではなく、実環境で悪用されている脆弱性にも取り組むようになってきています。最新の脅威に対処し続けることは容易ではありません。本レポートで提示したような分析結果が、少しでも皆さまのお役に立つことを願っています。次回のレポートでは、2020 年下半期にサイバー脅威の状況がどのように変化したかを検証します。

*29 「CVE リスト」（英語）：https://cve.mitre.org/cve/

*30 「CVE Numbering Authorities」（英語）：https://cve.mitre.org/cve/cna.html

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ



TR-20H1-202009-R1