# フォーティネット
# グローバル脅威レポート

## FortiGuard Labs による 2021 年下半期レポート

# 目次

# 概説とハイライト

新年を迎えると、過去と決別し、新しい、できればより良い未来に突き進みたいという誘惑に駆られるものです。しかしながら、「歴史を学ばなければ過ちを繰り返す」という戒めに従って、過去の過ちを繰り返さないようにするために、FortiGuard Labs が監視している世界中に配置されたセンサーを通じて、2021 年下半期のサイバー脅威環境を振り返ってみましょう。以下にその概要を紹介します。


## Log4j の重大な影響

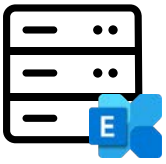
12 月第 2 週に発生したにもかかわらず、エクスプロイト活動が急拡大し、この半期で IPS の検知が最多になりました。過去の注目された脆弱性と比べてみても、Log4j RCE は 1 ヵ月足らずで、ピーク時の 10 日間の平均件数の測定値で、2021 年におけるもう 1 つの代表的ツールである ProxyLogon の 50 倍近く活動しました。


## ELF 形式のマルウェア

脅威アクターは、Linux ベースのマルウェアを強力な武器として自らの攻撃ツールに次々と追加しています。ELF ファイル（Linux のバイナリ形式）の検知数が 2021 年に倍増し、フォーティネットの AV センサー向けに 4 倍のシグネチャが新たに作成されることになり、穏やかな年末を迎えるというわけにはいきませんでした。


## ランサムウェアのトレンドの変化

過去 12 ヵ月間で 10.7 倍に増加したランサムウェアの検知数は、2021 年下半期もフォーティネットのセンサーで高水準を維持しました。全体の検知数は以前のように急増していないかもしれませんが、この脅威の巧妙さ、攻撃性、影響力は衰えませんでした。

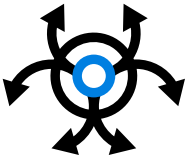



## Exchange Server に対するさらなる攻撃

Microsoft Exchange Server に存在する 4 つの脆弱性を標的にするエクスプロイトが上半期に多くの組織を攻撃し、下半期もいくつもの攻撃が次々と出現し、攻撃が沈静化することはありませんでした。

## ベビーモニターのハッキング

人気のベビーモニターに存在するリモートアクセスの脆弱性が、乳幼児の親だけでなく、多くの人の注目を集めました。この脆弱性が新しいエクスプロイトの上位に入り、家庭に数え切れないほど多く存在する、最も弱い存在を保護する IoT にもリスクがあることを再認識することになりました。



## ATT&CK フレームワークの活用

敵の目標を理解することは、その敵が使用する可能性のある、変化する多数の手法から身を守る上で極めて重要です。いくつかの手法に注目することで、マルウェアが侵入する方法を効果的に遮断できます。地域別と業界別の攻撃手法を理解し、自らの地域や業界に多い手法から確実に保護できるようにしておくことが重要です。

# 2021 年下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毎日観測される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、フォーティネットはセキュリティデバイスの出荷数では業界最多の実績を有しています。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、2021 年下半期のサイバー脅威動向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。最初に、2021 年に首位に躍り出た（あるいは急上昇した）脅威を検証します。

## IPS の検知

FortiGate ファイアウォールで動作する FortiGuard 侵入防止システム（IPS）センサーが捕捉した活動は、脅威アクターがどのように脆弱性を見つけて標的を攻撃し、不正インフラストラクチャを構築するかについて、比類ない情報を提供してくれます。業界で広く利用されている MITRE ATT&CK フレームワークに置き換えると、これらの検知は、偵察、リソース開発、初期アクセスの手法に相当します。図 1 は、2021 年下半期のエクスプロイト活動の月ごとの上位の標的を示しています。

図 1 を見れば、1 年の締めくくりとして、Log4j2 と呼ばれる人気の Java ライブラリに影響する、それほど知られていなかったリモートコード実行（RCE）の脆弱性（CVE-2021-44228、CVE-2021-45046、CVE-2021-45105）から始めないわけにはいかないでしょう。サイバーセキュリティ業界の誰もが Log4j ゼロデイエクスプロイトの存在を知ることとなり、多くの人が睡眠時間を削って残業を強いられることになりました。

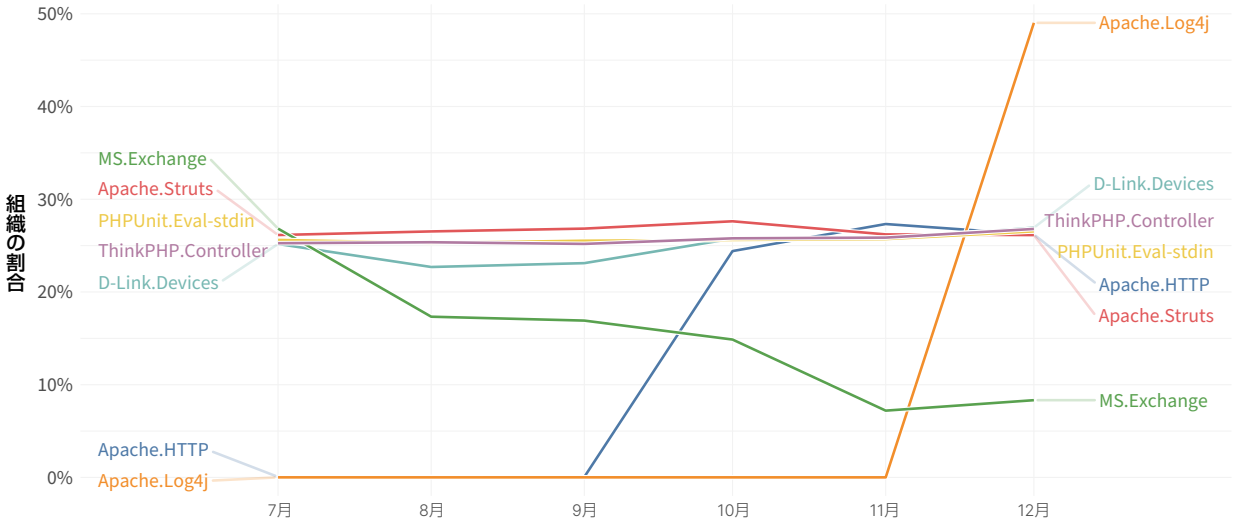



図 1：2021 年下半期の上位の IPS 検知率（テクノロジー別）

12 月の第 2 週に発見されたにもかかわらず、エクスプロイト活動が急拡大し、IPS 検知数がこの半期で最多になりました。これらの検知は、FortiGuard IPS が動作している組織の 50% 近くで記録されました。この点を考慮しながら次点だった別の Apache エクスプロイト（CVE-2021-42013、CVE-2021-41773）に目を移すと、31% の組織で検知されたことがわかります。Log4j については、本レポート後半で詳しく解説します。

もう 1 つの RCE 脆弱性で、Microsoft Exchange Server に影響する悪名高い「ProxyLogon」（CVE-2021-26855）が、この半期の初めにかけて首位に返り咲きました（2021 年上半期レポートの「ProxyLogon フィードの狂乱」を参照）。2021 年には、ProxyShell、ProxyToken、ProxyOracle といった名前の Exchange Server のさらなる脆弱性が次々と明らかになり、エクスプロイトが下半期に急増しました。これらの Microsoft Exchange Server の脆弱性は、別途、本レポートの後半でカバーしてありますので、ご確認ください。

大々的に報道された脆弱性だけでなく、ネットワーキングや IoT のコンシューマー向けの人気のデバイス（Dasan や D-Link など）も攻撃されました。十分に理解している製品であっても、見落とすことなく、注意する必要があります。脅威アクターは、在宅勤務が増えて個人と企業のネットワークの境界が曖昧になっている今のトレンドを悪用しようとしています。このことは、「エッジへの攻撃」が 2022 年に注目すべき 5 つのサイバー脅威に入った大きな理由でもあります。

IPS 検知数が最多だったものだけでなく、新しく上位に入った脅威にも注目したいと考え、図 2 に、過去 6 ヵ月間に検知数が上位になり、その前の 6 ヵ月間に活動が確認されなかったエクスプロイトをまとめました。TP-Link.HTTP のコード実行の脆弱性以外のすべてが、2021 年 7 月以降に作成されたものです。この図には、上位に新たに入ったエクスプロイトの地域別の比較もまとめました。図 2 のいくつかのエクスプロイトについてはすでに説明しましたが、ここではこの図にのみ記載されているいくつかのエクスプロイトを紹介します。

| | アフリカ | アジア | ヨーロッパ | 南米 | 中東 | 北米 | オセアニア |
|---|---|---|---|---|---|---|---|
| Apache.Log4j.Error.Log.Remote.Code.Execution | 45.9% | 48.8% | 49.4% | 49.7% | 44.4% | 47.1% | 45.4% |
| Apache.HTTP.Server.cgi-bin.Path.Traversal | 28.7% | 32.9% | 32.6% | 36.8% | 27.2% | 27.9% | 25.6% |
| Atlassian.Confluence.CVE-2021-26084.Remote.Code.Execution | 24.0% | 28.2% | 27.1% | 31.6% | 22.8% | 20.5% | 21.4% |
| Arcadyan.Routers.images.Path.Authentication.Bypass | 18.6% | 22.5% | 21.2% | 23.8% | 19.2% | 17.0% | 15.8% |
| MS.Exchange.Server.CVE-2021-34473.Remote.Code.Execution | 16.5% | 13.0% | 18.7% | 13.6% | 11.1% | 13.8% | 15.7% |
| Apache.Log4j.Error.Log.Thread.Context.DoS | 12.4% | 13.7% | 12.7% | 12.5% | 11.2% | 11.0% | 10.1% |
| SixApart.Movable.Type.XMLRPC.API.Remote.Code.Execution | 7.9% | 10.8% | 9.7% | 13.4% | 6.7% | 16.0% | 8.9% |
| Atlassian.Confluence.Server.S.Endpoint.Information.Disclosure | 8.5% | 6.9% | 16.6% | 9.6% | 7.2% | 13.9% | 5.2% |
| Hikvision.Product.SDK.WebLanguage.Tag.Command.Injection | 8.3% | 11.2% | 8.8% | 11.7% | 10.4% | 7.6% | 7.5% |
| Zoho.ManageEngine.ADSelfService.Plus.Authentication.Bypass | 6.2% | 6.7% | 5.9% | 6.5% | 5.1% | 15.8% | 14.7% |
| Libxml.CVE-2017-7376.Buffer.Overflow | 9.2% | 6.7% | 10.6% | 6.9% | 5.7% | 12.0% | 9.7% |
| TP-Link.HTTP.Management.Code.Execution | 8.8% | 10.9% | 8.1% | 10.2% | 7.7% | 6.4% | 6.6% |
| WebSVN.Search.php.Command.Injection | 9.1% | 6.4% | 6.6% | 8.5% | 5.5% | 5.9% | 5.9% |
| Lucee.Administrator.imgProcess.cfm.Arbitrary.File.Write | 6.3% | 7.1% | 5.9% | 7.4% | 4.1% | 4.6% | 5.1% |
| Apache.HTTP.Server.mod_proxy.SSRF | 4.0% | 5.2% | 3.6% | 3.4% | 3.3% | 3.8% | 3.0% |
| Sophos.SG.UTM.WebAdmin.PreAuth.Remote.Code.Execution | 4.2% | 3.8% | 3.3% | 4.2% | 4.7% | 3.0% | 2.5% |
| Alibaba.Nacos.ConfigOpsController.Authentication.Bypass | 4.8% | 4.2% | 3.7% | 4.2% | 3.2% | 2.8% | 2.5% |
| VMware.vCenter.Server.Analytics.Arbitrary.File.Upload | 3.4% | 4.3% | 3.6% | 3.8% | 4.7% | 2.8% | 2.5% |
| Motorola.Halo+.Baby.Monitor.Remote.Code.Execution | 3.2% | 3.8% | 3.3% | 3.3% | 2.5% | 2.6% | 2.4% |
| CHIYU.TCP.IP.Converter.Multiple.XSS | 3.4% | 3.1% | 3.4% | 2.8% | 2.9% | 2.4% | 2.3% |

図 2：地域別の新規かつ急増した IPS 検知（組織の割合）

最初に、Atlassian の Web ベースの Wiki である Confluence の脆弱性に注目しましょう。新しい OGNL インジェクションの脆弱性に関連する CVE-2021-26084 が最も深刻で、多くの攻撃者がこのバグが発表された直後に注目し、脅威アクター Atom Silo が間もなく登場して、脆弱な Confluence サーバーを標的にランサムウェアを配信するようになりました。米国の CISA（Cybersecurity and Infrastructure Security Agency）はこれを重視し、アラートを発表して早急な対策を呼びかけました。

Zoho ManageEngine ServiceDesk Plus（CVE-2021-40539）にも触れる必要があるでしょう。CISA と FBI の共同勧告によると、このエクスプロイトが成功すると、攻撃者が実行ファイルをアップロードし、管理者権限の侵害、ラテラルムーブメント、レジストリハイブや Active Directory ファイルの流出などの攻撃後の活動を可能にする Web シェルを送り込むことができます。図 2 からわかるように、北米とオセアニア（主にオーストラリア）で最もエクスプロイト活動が活発です。CISA と FBI は 9 月に、Zoho の別の脆弱性（CVE-2021-44077）に関するアラートを発表しており、この Threat Signal に、脆弱性の評価と対策が解説されています。

VMware の新しい 3 つの脆弱性（CVE-2021-21985、CVE-2021-21980、CVE-2021-22005）により、この仮想化プラットフォームが 2021 年下半期に新たに上位に入ることになりました。1 つ目の CVE を標的にするエクスプロイトの検知数が最も多く、VMware もこの CVE は深刻であるとして、最優先でパッチを適用するように顧客に呼びかけています。活動は世界中にほぼ均等に分散していますが、中東とアジアが最多になりました。

そして最後に、Motorola の Halo+ ビデオベビーモニターを標的にするエクスプロイト活動（CVE-2021-3577）にも注目しないわけにいかないでしょう。ベビーモニターがこれほど上位に入ったことはこれまでになかったはずです。ハッカーが家庭に侵入したのはこれが初めてではありませんが、ベビーベッドに侵入というのは驚きであり、まったく新しい次元の憂慮すべきことです。この新しいレベルのプライバシー侵害については、「ベビーモニターのハッキング」のセクションで詳しく解説します。

## マルウェアの検知

フォーティネットのアンチマルウェアソリューションで検知されたサンプルは、企業の環境に足場を築き、特権を昇格させ、ラテラルムーブメントを可能にする目的で使用されることが多いツールについての実用的なインテリジェンスを提示します。マルウェアは、Execution（実行）から Impact（影響）までの ATT&CK マトリクスの複数の手法を使用できることから、あらゆる種類の脅威アクターにマルチツールとして利用されています。

図 3 に、地域ごとの有力な「新人王」候補を示します。この図に登場しているのは、2021 年のいずれかの時期に作成され、2021 年下半期に各地域のデバイスで最も多く検知された 10 位までに入ったマルウェアシグネチャです。

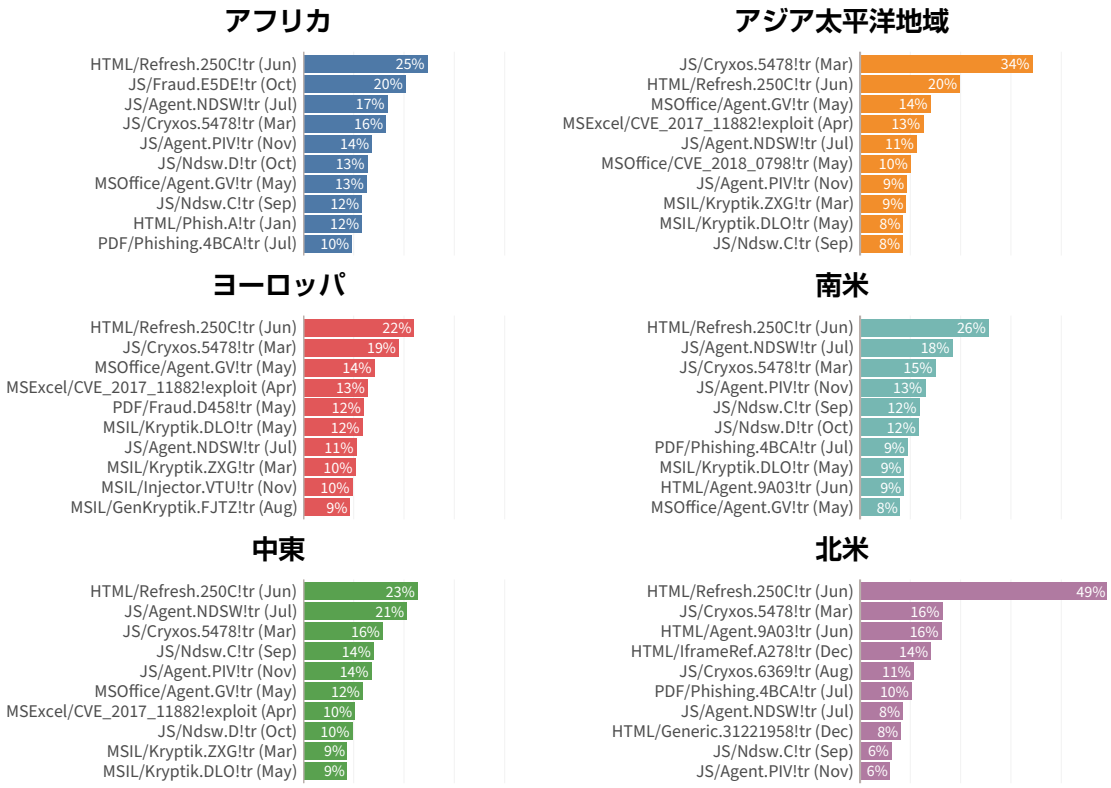



図 3：2021 年下半期の新しいマルウェア亜種の地域別の検知率（組織数の割合）

当然ながら、検知数は地域によって異なりますが、その拡散のメカニズムは、Microsoft Office 実行ファイル（MSExcel/、MSOffice/）、PDF ファイル、ブラウザのスクリプト（HTML/、JS/）の 3 つに大別することができます。また、MSIL（Microsoft Intermediate Language）で保存されたファイルも標的になります。

ブラウザベースのさまざまな形のマルウェアがどの地域でも上位を独占している点にも注目するべきでしょう。多くの場合、マルウェアが埋め込まれたフィッシングやスクリプトという形で送り込まれ、コードをインジェクションしたりユーザーを不正サイトにリダイレクトしたりします。COVID-19、政治、スポーツなどの最新ニュースを知りたいという人間の願望に乗じたこのような手法が広く採用されるようになっています。また、自宅のネットワークからブラウザを利用する人が増えていることから、このようなマルウェアと被害者となる人の間の保護レイヤーが少なくなっています（企業の Web フィルターがないなど）。

## ELF 形式のマルウェア

しかしながら、覚えておくべきは、現在のチャートの上位に入っている脅威だけでなく、小規模や件数が少ない脅威も大きな問題につながる可能性があり、監視する価値が十分にあるということです。このようなトレンドの 1 つとして我々が着目しているのが、Linux システムのエクスプロイトの目的で設計された、多くの場合に ELF（Executable and Linkable Format）バイナリとして送り込まれるマルウェアです。Linux は、多くのネットワークのバックエンドシステム、さらには、IoT デバイスやミッションクリティカルアプリケーションのコンテナベースのソリューションで利用されており、これまで以上に攻撃の標的にされるようになりました。

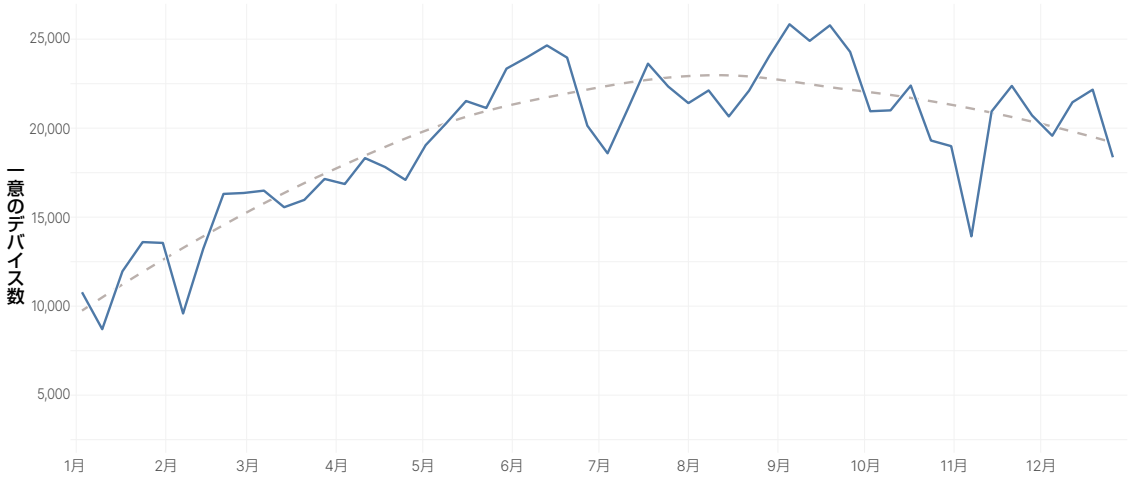



図 4：2021 年に Linux システムを標的とした ELF ファイルが検知された一意のデバイス数

図 4 からわかるように、フォーティネットのセンサーでの ELF をはじめとする Linux マルウェアの検知が 2021 年に 2 倍に増加しました。また、2021 年第 4 四半期にフォーティネットの AV センサーに届いた新しい Linux マルウェアのシグネチャは、第 1 四半期の 4 倍でした。一瞬で急増したとは言えないものの、無視できるものでもありません。このような亜種の増加や拡散は、Linux マルウェアがサイバー犯罪者の重要な武器になりつつあることを示しています。

最も一般的な ELF の亜種は、感染したマシンをボット化し、脆弱性を悪用して増殖する Linux マルウェアとして知られている Muhstik と関連性があります。Muhstik のエクスプロイトの 1 つが、フォーティネットの IPS センサーで大量に検知された Confluence の脆弱性です。詳細については、マルウェアのこちらの分析を参照してください。

Linux システムを標的にしてデータを流出させる、10 月に 10 位以内に入った RedXOR マルウェアの新しい亜種に関連するボットネット活動も観測されました。Cobalt Strike の Beacon 機能の不正目的での実装である Vermilion Strike は、リモートアクセス機能を持った Linux システム用のマルウェアです。Log4j も、Linux バイナリが使用されている最近の攻撃のもう 1 つの例です。

Microsoft が現在、WSL（Windows Subsystem for Linux）の Windows 11 への統合を積極的に進めていることから、マルウェアも間違いなく、これに追随するでしょう。WSL は、Linux バイナリ実行ファイルの Windows でのネイティブ実行に使用される互換レイヤーです。以上のことが、Linux 攻撃の継続的な増加を示す十分な証拠であり、2022 年の予測の上位に入った理由でもあります。

## ボットネットの検知

一般的に、IPS とマルウェアのトレンドが感染前のサイバー脅威の活動を示すものであるのに対し、ボットネットの活動は感染後の活動を表します。システムが感染するとリモートのホストとの通信の試行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。ボットネットのトラフィックを ATT&CK の用語に置き換えると、コマンド & コントロール（C2）TTP に相当します。

このデータから繰り返し得られる教訓の 1 つは、最も成功したボットネットは長期にわたって驚くほど安定して活動していることです。フォーティネットのセンサーで検知が多い脅威が長期にわたって存在し続ける傾向があり、その最大の理由は、サイバー犯罪者は攻撃力を持続することを重要視し、不正インフラストラクチャの維持に多くの労力を傾けているためです。

そのため、通常の検知数指向ではなく、検知されたボットネットトラフィックの件数に基づき、図 5 を作成しました。色付き帯の幅は、上位 10 位のボットネットの C2 通信の総数を表します。ボットネット全体でも個々のボットネットでも、活動の件数は明らかに、時に増加し、時に減少しています。リモートアクセスのトロイの木馬（RAT）である Warzone と RedLine Stealer マルウェアに関連する C2 活動の幅が広い箇所が 2 つ顕著にあらわれています。

ただし、その前に、10 位以下のすべてのボットネットの C2 活動が一番下の狭い「その他すべて」の帯に収まるほど、上位のボットネットに集中している点に注目したいと思います。ほとんどがよく聞く名前であり、フォーティネットだけでなく、多くの企業が、Mirai（デバイスでの検知率が 1 位）、ZeroAccess、Pushdo などの、長期にわたって上位に入っているボットについて、繰り返し解説してきました。そこで今回は、特にコンシューマーや中小規模企業向けのネットワークで活動が活発だった、2021 年下半期に新たに上位に入った注目すべきボットネットを取り上げます。

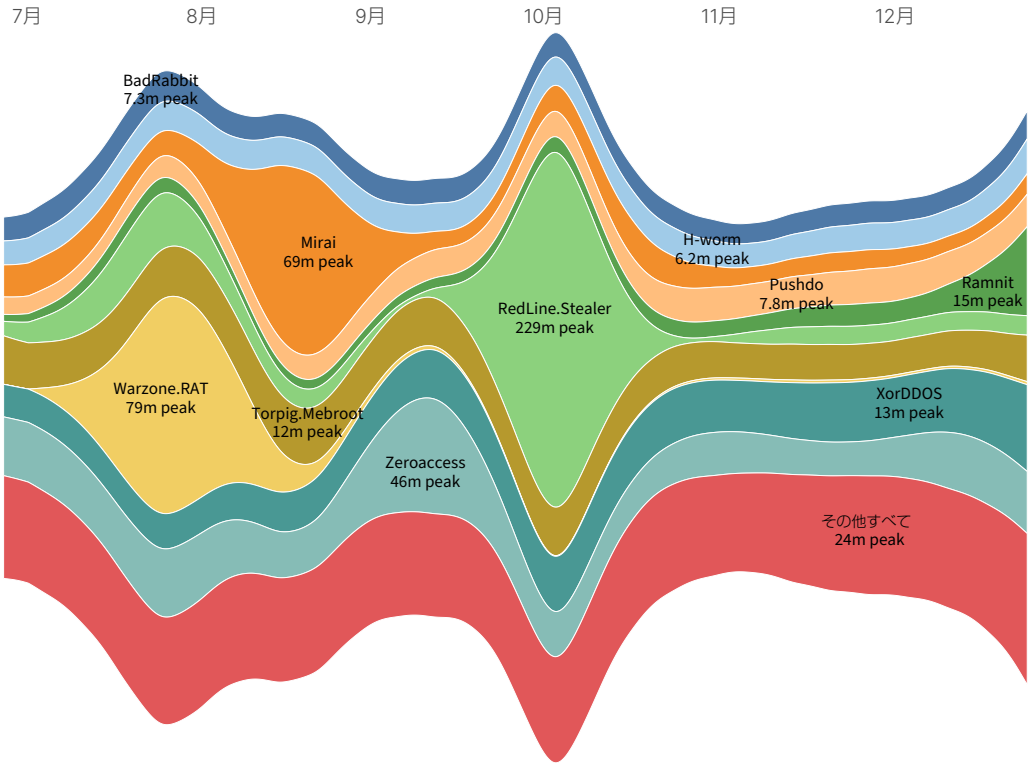



図 5：2021 年下半期に検知された上位のボットネットの週ごとの件数（総検知数）

Warzone RAT は、低価格で高機能の MaaS（Malware-as-a-Service：サービスとしてのマルウェア）ツールとされていることから、BargainZone RAT という呼び名の方がふさわしいのかもしれません。この RAT を低予算で不正を企む犯罪者に最適な選択肢だとする Blackberry による説明は、かなり的を射た表現であると言えます。サイバー犯罪の市場のコモディティ化が進む今、Warzone はビジネスモデルを確立し、成功を収めました。図 5 の Warzone RAT 感染に起因するボットネット活動の大幅な拡大が、その成功の証です。

7 月下旬の Warzone RAT ボットネットの急増は、おそらくはアジア太平洋地域の製造業を標的にしたスピアフィッシング攻撃によるものです。この攻撃は、フォーティネットのデータでも確認でき、アジアでの関連する活動が他の地域の 4 倍になりました（図 6 参照）。フォーティネットのオープンファブリックエコシステムのメンバーである Anomali が、この攻撃で確認された TTP と Aggah 脅威アクターとの関連性を指摘しています。

RedLine Stealer マルウェアは、少なくとも 2020 年の初期から存在し、感染したシステムから認証情報を搾取する目的でサイバー犯罪に使用されています。RedLine Stealer によって盗まれた情報がダークネット市場で、ユーザー認証 1 セットあたり 10 米ドルという低価格で販売されています。COVID-19 の感染が世界中に拡大した時期に登場した RedLine Stealer の開発者は、感染拡大の恐怖と不安に乗じて感染を拡大させることに成功しました。

図 5 での関連するボットネットのトラフィックの 9 月下旬から 10 月上旬にかけての急増は、RedLine Stealer の悪質さを物語っています。図 6 を見ると、中近東とヨーロッパで最も活動が活発であることがわかります。図 5 を見ると、RedLine Stealer は一時的に大流行したものの、現在は収束したという見方もできますが、RedLine の開発者は自らのウイルスと同様に、マルウェアの形を定期的に変えながら、新たな標的を探しています。事実、FortiGuard Labs は最近、COVID に乗じた、「Omicron Stats.exe」というファイルの新しい亜種を発見しており、これで終わりではないはずです。

| | アフリカ | アジア | ヨーロッパ | 南米 | 中東 | 北米 | オセアニア |
|---|---|---|---|---|---|---|---|
| XorDDOS | 6.1k | 7.3k | 53 | 3.1k | 9.2k | 19 | 0 |
| RedLine.Stealer | 2.2k | 2.6k | 4.9k | 1.7k | 5.1k | 3.3k | 1.3k |
| Zeroaccess | 170 | 9k | 3.2k | 905 | 2.5k | 3k | 1.5k |
| Torpig.Mebroot | 1.6k | 8.1k | 832 | 631 | 1.4k | 4.5k | 235 |
| Mirai | 440 | 1.2k | 5k | 689 | 1.9k | 2.2k | 4.9k |
| BadRabbit | 7.7k | 336 | 2.2k | 2.3k | 3k | 0.21 | 0 |
| H-worm | 3.1k | 404 | 1.1k | 944 | 589 | 5.7k | 0.9 |
| Warzone.RAT | 425 | 4.6k | 1.2k | 744 | 614 | 1.2k | 1.7k |
| Pushdo | 1.1k | 3.8k | 1.4k | 495 | 539 | 2.5k | 497 |
| Ramnit | 2.4k | 3.8k | 100 | 812 | 1.8k | 33 | 3 |

図 6：2021 年下半期に地域別で最も活発だったボットネット（組織あたりの件数）

最後に、これまでの図に登場しなかった、Emotet に触れておくことにしましょう。前回のレポートで、このボットネットの解体に向けて複数の法執行機関が協力し、結果として活動が減少したと解説しましたが、解体から 10 ヵ月後に、Emotet は瀕死の状態に追い込まれたものの、完全に死んでしまったわけではなく、下半期に復活の兆しがあることがわかりました。ただし、Emotet の活動はかつての水準よりはるかに低く、世界中で猛威を振るっているわけではありません。例えば、検知数の 3 分の 2 が中南米地域に集中しており、これはヨーロッパや北米の 25 倍に当たります。瀕死の状態に追い込んだことを当面の勝利とすることにしましょう。

# 注目すべき出来事

## Log4j の重大な影響

この数年間で、12 月に明らかになった CVE-2021-44228、すなわち、Java ベースのログフレームワークである Apache Log4j のリモートコード実行（RCE）の重大な脆弱性ほど、業界全体が注目し、問題視した脆弱性はないでしょう。この脆弱性は、Java アプリケーションが存在するほぼすべての環境に影響するだけでなく、エクスプロイトが非常に簡単で、攻撃者は脆弱なシステムを完全に制御する手段を手に入れることができます。さらには、Log4j を使用していることをアプリケーションの何層も下までたどって見つけなければならないこともあるため、その特定が時として非常に困難になるという問題もありました。

Apache Foundation が 12 月 9 日に、CVE-2021-44228、すなわち「Log4Shell」と呼ばれるようになった脆弱性を発表しました。国家が支援する脅威アクターや組織的犯罪集団などの攻撃者がインターネットをスキャンして脆弱なシステムを探し始めたため、この IPS は数日以内に 2021 年下半期に最も多く検知された IPS になりました。複数のセキュリティベンダーが、クリプトマイナー、ランサムウェアツール、Mirai などのボットネットを運用する組織を含む脅威アクターが、Log4j の脆弱性のエクスプロイトを攻撃キットに組み込んでいることを確認したと報告しています。図 7 の Log4j の最初の数日間の活動の累計を見れば、攻撃者がこの脆弱性にどれほど注目したかが十分に理解できます。Log4j RCE の検知数は、わずか 21 日間で、悪名高い Apache Struts の脆弱性（CVE-2017-5638）の年間検知数の 1.4 倍を記録しました。

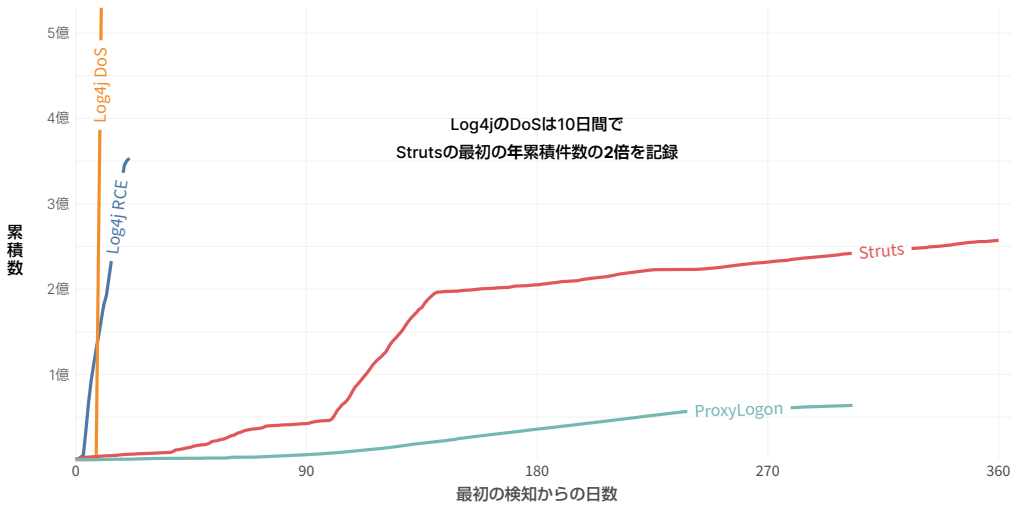



図 7：Log4j の累積数と過去の注目された脆弱性の比較

この活動で、インターネット接続されたサーバーからバックエンドシステム、ネットワークコンポーネント、SCADA システム、クラウドアプリケーションまでのすべてに対する広範囲の攻撃が心配されました。脆弱性が公表されてパッチが提供される少なくとも 1 週間前にはこの脆弱性を標的にするエクスプロイト活動が始まった、というレポートが報告されたことで、恐怖心を煽られることになりました。Log4Shell の公表の翌週には、Apache Foundation が Log4j ロギングフレームワークの他の 2 つのバグ、CVE-2021-45046 と CVE-2021-45105 を報告しました。これらの脆弱性は Log4Shell ほど重大ではなかったものの、多くの組織が 1 週間で 3 度の Log4j バージョンの更新に追われることになりました。

懸念が拡大したにもかかわらず、発見から 1 ヵ月間にこの脆弱性に関連する重大な侵害が報告されることはありませんでした。バグが公開された直後に組織が慌てて防御策を一斉に講じた結果というのが大方の見方ですが、攻撃者はバグを悪用してネットワークに侵入し、攻撃の時期を待っていると推測する人もいます。過去のこのような例の 1 つが、2017 年に Equifax で発生した、Apache Struts の脆弱性（CVE-2017-5638）を悪用した侵害です。約 1 億 5 千万人分の個人情報が流出したことが判明したのは、脆弱性が公表された数ヵ月後で、この脆弱性を標的にした最初の不正活動のほとんどが沈静化してから時間が経過した時期でした。

この Apache Struts の脆弱性は、この数年間で Log4Shell と同様の懸念レベルが喚起された脆弱性の 1 つで、昨年 3 月に明らかになった Exchange Server の「ProxyLogon」の脆弱性（CVE-2021-26855）が、その最も新しい例です。この認証回避の脆弱性を悪用した場合、攻撃者がユーザーになりすまし、オンプレミスの Exchange Server や E メールアカウントにアクセスする手段を手に入れることができます。攻撃者はこの脆弱性を Exchange Server の他の 3 つの脆弱性（CVE-2021-26857、CVE-2021-26858、CVE-2021-27065）と組み合わせることで、数万台のサーバーを Microsoft がパッチを公開する前に侵害しました。この脆弱性を重視した FBI は、感染したシステムから所有者の許可を得ることなく Web シェルを削除するという、前例のない措置を取りました。

これが次の「大規模なデータ漏洩」の入口であったかどうかは、時間の経過と共に明らかになるはずですが、歴史を教訓にすれば、侵害を事前に特定して断絶する、時間的および精神的な備えが不可欠ということになるでしょう。

## Exchange Server に対するさらなる攻撃

Microsoft の Exchange Server テクノロジーは、2021 年下半期も上半期と同様に、企業にとっての大きな痛点となりました。Exchange Server の脆弱性を標的にしたエクスプロイトが、2021 年下半期の件数ベースで、Log4j の脆弱性、Apache Struts の別の脆弱性に次ぐ 3 位になりました。7 月には、Exchange Server を標的にしたエクスプロイトが他のどのテクノロジーよりも多く確認されました（図 1 参照）。下半期の不正活動の多くは、「ProxyShell」、「ProxyToken」、「ProxyOracle」と呼ばれる Exchange Server の複数の異なる脆弱性に関連するものでした。

ProxyShell は、Exchange Server の 3 つの脆弱性（CVE-2021-34473、CVE-2021-34523、CVE-2021-31207）を使用することで脆弱なシステムでの不正コードのリモート実行を可能にするエクスプロイトチェーンです。Microsoft が 2021 年 4 月と 5 月の月例セキュリティアップデートプログラムの一環としてこの脆弱性を修正しましたが、脆弱性に対する攻撃が 1 年を通して止むことはありませんでした。米国の CISA（Cybersecurity and Infrastructure Security Agency）などが 8 月に、脅威アクターが ProxyShell の脆弱性を悪用してインターネット接続された Exchange Server で不正コードを実行していると警告しました。

脅威アクターは多くの攻撃では、侵害されたマシンに、その後の攻撃で使用する目的で、隠された Web シェルをドロップしました。フォーティネットが 9 月に報告した攻撃では、それまでに特定されたことのない脅威アクターが ProxyShell を悪用して偵察活動を実行し、最終的に脆弱な Exchange Server で永続性を確保したことがわかっています。フォーティネットの調査で、攻撃チェーンの一部として使用された、合計 22 個の DLL がメモリに見つかり、その多くが悪意のあるものだとわかりました。また、「Tortillas」という新しい脅威アクターによる攻撃でも ProxyShell が悪用され、Babuk ランサムウェアファミリーの亜種が送り込まれました。複数のセキュリティベンダーから、ProxyShell を悪用した BEC（Business Email Compromise）攻撃も報告されています。ある段階で、米国だけでも 2 万台以上の Exchange Server が ProxyShell の脆弱性を悪用した攻撃を受ける可能性がありました。

昨年 9 月に明らかになった ProxyToken の脆弱性（CVE-2021-33766）は、ProxyShell や ProxyLogon ほど深刻ではないものの、Exchange Server が標的にされやすい環境であることを再認識させるものでした。このセキュリティトークン迂回の脆弱性は、標的のサーバーから攻撃者が制御するサーバーにメールを転送するルールを作成したり、機密情報を流出させたりする手段を攻撃者に提供するものでした。

「ProxyOracle」の場合は、Microsoft Exchange を攻撃する新たな方法を脅威アクターに提供するものであり、この脆弱性は、CVE-2021-31195 として追跡されるクロスサイトスクリプティングの問題と、CVE-2021-31196 として追跡される Padding Oracle 攻撃という 2 つの異なる CVE で構成されていました。これらの脆弱性を組み合わせて悪用すると、ユーザーを誘導して不正リンクにアクセスさせるだけで、パスワードを平文に復元できます。図 8 は、この 1 年が Exchange Server にとっていかに厳しい年であったかを示しており、6 月のピーク時には、プロキシ関連の CVE だけでも、30% を超える組織で検知されました。

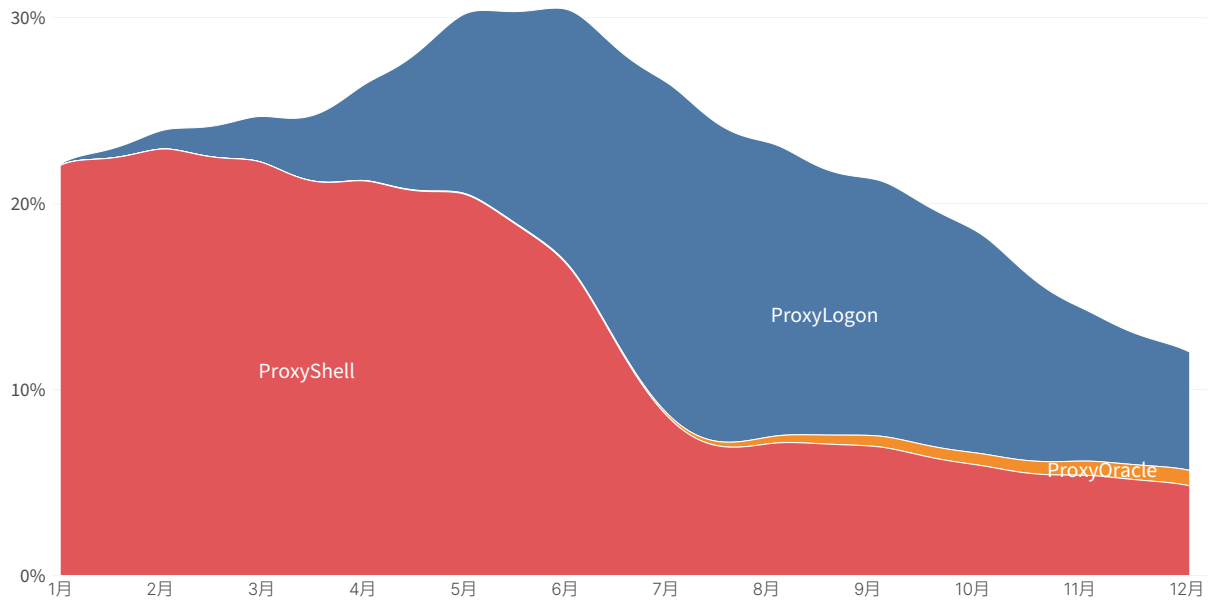



図 8：2021 年のプロキシ関連の CVE の月別の IPS 検知

セキュリティ研究者は、攻撃者とハッカー（ブラックハットとホワイトハットの両方）が、Exchange Server が広く利用され、E メールアカウントやその他の機密データにアクセスできるという単純な理由で、Exchange Server の弱点を今後も探し、悪用し続けると予想しています。

## ランサムウェアのトレンドの変化

2021 年上半期のレポートで特に注目されたのが、ランサムウェア亜種を検知するセンサーの数が 12 ヵ月前の 10.7 倍になったことでした。2021 年の年度末を迎えて、このトレンドが続くかどうか見極めたいと考えましたが、結論から言えば、そうではありませんでした。

以前のレポートのようにランサムウェアが急増したわけではないものの、図 9 を見ると、2021 年下半期もフォーティネットのセンサーでのランサムウェアの検知数が高水準を維持しているのがわかります。ランサムウェア検知の頻度は全体として減少傾向にあるものの、この脅威が高度化し、攻撃力や影響が拡大する勢いが衰えることはないでしょう。

脅威アクターは、新種や既知のさまざまなランサムウェア亜種で組織を攻撃し続け（週あたり約 150,000 件の検知数）、多くの場合に大きな爪痕を残しました。ランサムウェア攻撃でデータを盗み、流出させると脅して身代金を要求する二重恐喝が、かつてのように稀ではなく、当たり前のことになりました。

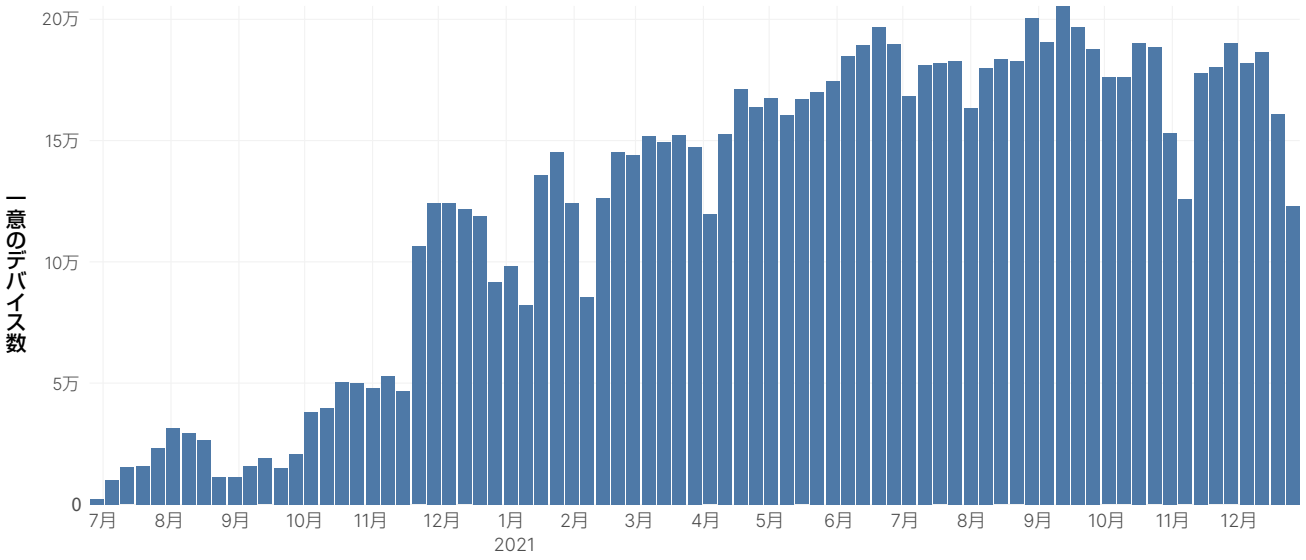



図 9：過去 18 ヵ月（2020 年 7 月～ 2021 年 12 月）の週別のランサムウェア検知数

2021 年下半期の Kaseya のリモート監視 / 管理テクノロジーである VSA に対する攻撃は、影響が広範囲に及んだことで、大きく注目されました。ある脅威アクターが VSA の古い脆弱性を悪用して、Kaseya のマネージドサービスプロバイダの 50 ～ 60 社の顧客が利用していたシステムにランサムウェアを送り込み、下流の顧客にまで感染が拡大しました。Kaseya に対する攻撃の影響を受けた組織の正確な数は不明ですが、世界中で数千社が被害を受けたとも言われています。このインシデントは、ソフトウェアサプライチェーン攻撃の「一度の侵害が複数の被害を引き起こす」特性を再認識させるものであり、頂点であるホワイトハウスに至るまでのあらゆる米国政府機関の関係者が直ちに対策に乗り出しました。このような攻撃が将来的に増加すると予想されています。

Phobos、Yanluowang、BlackMatter の新しいバージョンを始めとする複数のランサムウェア亜種や RaaS（Ransomware-as-a-Service：サービスとしてのランサムウェア）モデルで販売されているランサムウェアファミリーが関係する活動が 2021 年下半期に常に一定のレベルで観測されました。BlackMatter は、コロニアルパイプラインを攻撃した DarkSide の活動が沈静化した直後に登場しましたが、DarkSide が名前を変えただけの犯罪集団であると考えられています。BlackMatter を運用する集団は、医療機関やその他の重要インフラストラクチャを攻撃しないとしていたにもかかわらず、実際には攻撃を実行しました。FBI と CISA は 10 月の共同勧告で、BlackMatter ランサムウェアが食品や農業の分野の 2 社を含む、米国の複数の重要インフラストラクチャ組織に対する攻撃に使用されているとアラートを発表しました。

2017 年に初めて登場した Phobos ランサムウェアの更新や、新しい亜種の開発が 2021 年下半期も活発であることがわかりました。また、昨年 8 月頃に登場した Yanluowang ランサムウェアが米国の複数の組織、特に金融サービス、エンジニアリング、製造、IT サービスの分野の組織を攻撃していることもわかりました。このマルウェアを運用する犯罪者は以前に、ThiefLock と呼ばれる別のランサムウェアファミリーを配布していたことがあります。あるセキュリティベンダーによると、Yanluowang を運用する犯罪者が今後は RaaS（Ransomware-as-a-Service）モデルを採用するようになる恐れがあり、そうなると、複数の脅威アクターが Yanluowang ランサムウェアを配布する目的で利用するようになるでしょう。

VMware ESXi ハイパーバイザーテクノロジーを標的とした攻撃も 2021 年下半期にいくつも確認されています。例えば、ビデオゲーム会社の CD Projekt RED を Hello Kitty というランサムウェア集団が攻撃して同社のソースコードを盗んで流出させた例や、名前は特定されていないある企業に対する攻撃で、結果的に同社のすべての VM が極めて短時間でオフラインになってしまった例などが挙げられます。これらの攻撃では、ESXi の 2 つの脆弱性（CVE-2019-5544 と CVE-2020-3992）が悪用されましたが、いずれも、組織が攻撃された段階ですでにパッチが提供されていた古い脆弱性です。

## ベビーモニターのハッキング

2021 年 9 月に、モトローラ製の Halo+ ベビーモニターのリモートコード実行の脆弱性を悪用しようとする攻撃が確認されました。その後の攻撃で、このベビーモニターのディスプレイ、カメラ、付属のアプリ、デバイス間で共有しているデータへの完全アクセスにより、脅威アクターが一般家庭の最も奥にある場所の 1 つに侵入しました。気持ちの悪い出来事ではあるものの、IoT デバイスが急増し、入手しやすくなったために、個々のデバイスの攻撃対象領域の規模と複雑さが拡大しているという事実を浮き彫りにしています。

優れたスマートガジェットはとても便利であり、IoT デバイスは人間と環境との関わり方に革命をもたらしましたが、新しい IoT デバイスが増えるたびに、インターネット接続が 1 つ増え、ハッカーの侵入口が 1 つ増えることを意味します。多くの IoT デバイスでセキュリティパフォーマンスの低さが度々問題視されている中で、これはユーザーにとってありがたいニュースではありません。

2021 年下半期に不正アクセスを可能にする脆弱性が存在したデバイスは、ベビーモニターだけではありません。2021 年 8 月、何百万台もの家庭用ルーターがマルウェア攻撃の標的になりました。この攻撃で、Arcadyan ルーターの認証回避の脆弱性を悪用しようとしていたことがわかっています。数ヵ月後の 10 月に、FreakOut ボットネットが Linux ディストリビューションの ZeroShell のリモートコード実行の CVE を含む複数の異なる脆弱性を悪用して DVR に感染し、Monero マイニングに使用したことが確認されました。

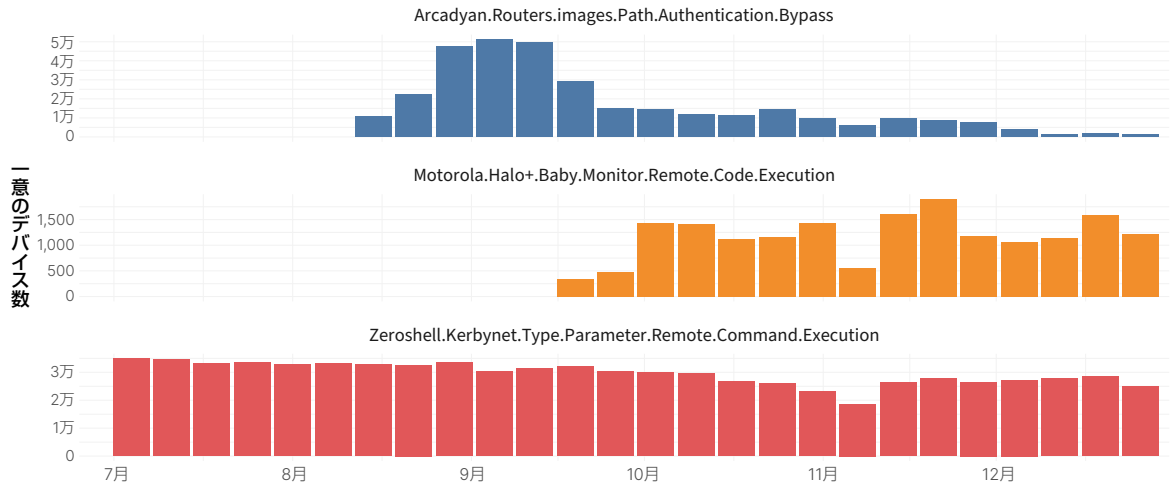



図 10：2021 年下半期の一部の IoT デバイスの週別の IPS 検知数

ベビーモニターをはじめとする多くのガジェットがインターネット接続されるようになったことで、過去最高となる 20,000 件の脆弱性が 2021 年に CVE リストに公開されることになりましたが、この記録が塗り替えられる日もそれほど遠くないでしょう。新しい脆弱性の件数の多さから、CISA は、運用指令 22-01 を発表し、関係機関に対して、攻撃される可能性が最も高い脆弱性の修正に最優先で取り組むよう要求することになりました。

在宅勤務への一斉の移行が進む中で、従業員の自宅に置かれた多数の IoT が個人ネットワークへの侵入口になり、企業の攻撃対象領域に吸収されることになります。多くのサイバー攻撃と同様、この種の攻撃で最も懸念されるのは、デバイスへの初期不正アクセスではなく、侵入してしまえば、ネットワークのラテラルムーブメントによって他のデバイスに移動する機会を攻撃者が得ることです。企業にとって重要なのは、優れたセキュリティ対策を実装することに加えて、サイバーセキュリティに対する意識と責任の文化を育成することであり、それは、従業員の職業人としての生活だけでなく、個人としての生活にも及ぶことになります。

## ATT&CK フレームワークの活用

防御を専門とする方やこのグローバル脅威レポートを長くお読みいただいている方は、個々のマルウェア亜種が入れ替わっていることにお気付きのはずです。MITRE の ATT&CK フレームワークなどの取り組みは、敵の行動を攻撃目標とそれを達成するためのステップ（戦術と手法）をまとめることで、リアクション型を迫られる防御側の不利な立場を解消しようとするものです。FortiGuard Labs は MITRE と共同で、防衛側の意識と能力の向上を目的とするさまざまなプロジェクトを推進しており、特に、MITRE の Center for Threat-Informed Defense には積極的に貢献しています。

特定の一時的なマルウェアの機能を永続的な手法に照らして理解することで、次の攻撃からの保護に必要なコンテキストが明らかになりますが、個々の手法の増減 / 検知率についてはどうでしょうか？ 2021 年下半期に FortiSandbox Cloud で活性化したマルウェアサンプルのテレメトリを使用し、攻撃される可能性が高い環境で発生したはずである出来事を調査しました。

図 11 に、3 つの戦術、すなわち実行、永続化、防御の回避の手法の検知率を示します。実行には、不正コードの実行を試行する手法が該当しますが、分析したサンプルの機能の 82% を上位 3 つの手法が占めることがわかります。永続化の手法については、偏りがさらに大きく、確認された機能の 95% 近くを上位 2 つの足場を築く手法が占めました。

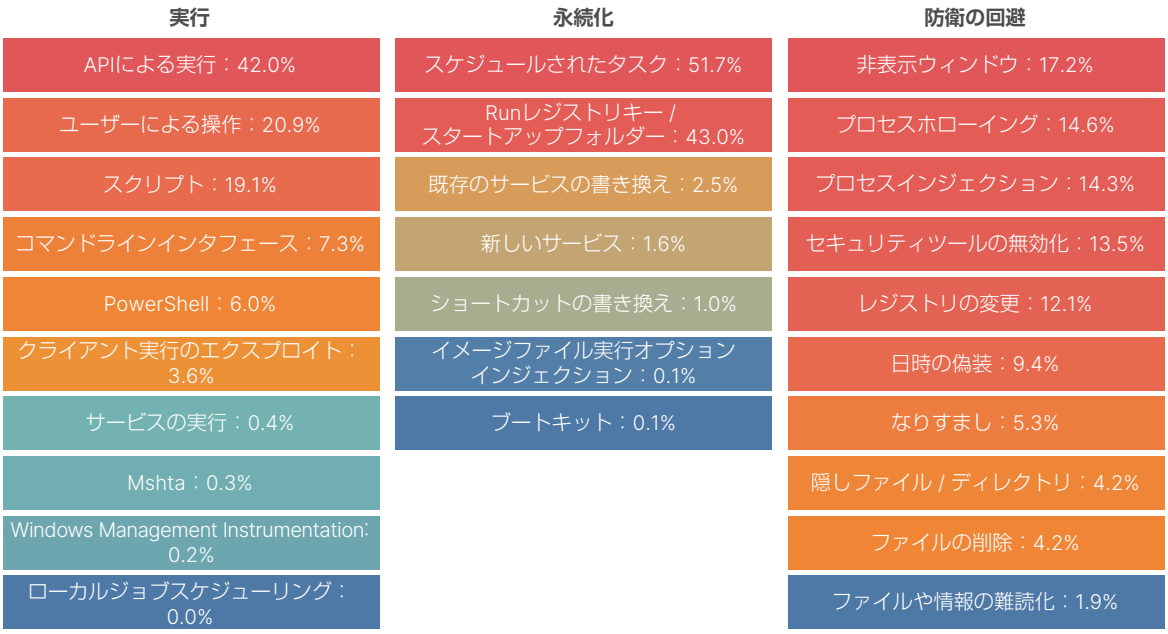



図 11：2021 年下半期のいくつかの戦術の手法の検知率

防御の回避のさまざまな手法から判断すると、攻撃者の行動をできるだけ早く停止すること、すなわち、攻撃者が足場を築き、防御側の能力を知る機会を得る前に停止することが重要です。

図 12 の永続化の手法の地域別の分類を見ると、アジアで観測されたサンプル以外は、図 11 と同様の手法に集中しているのがわかります。この地域での防御では、新規や変更されたサービスのレビューを標準の運用に組み込むべきでしょう。

| | アフリカ | アジア | ヨーロッパ | 北米 | オセアニア | 南米 |
|---|---|---|---|---|---|---|
| スケジュールされたタスク | 55.9% | 42.7% | 56.5% | 51.4% | 55.8% | 50.5% |
| Runレジストリキー / スタートアップフォルダー | 40.4% | 44.7% | 40.9% | 44.6% | 40.9% | 46.4% |
| 既存のサービスの変更 | 1.9% | 5.1% | 1.7% | 2.2% | 3.2% | 1.1% |
| 新しいサービス | 0.1% | 6.6% | | | 0.2% | 0.5% |
| ショートカットの書き換え | 1.7% | | 0.5% | 1.3% | | 1.5% |
| その他 | | 1.0% | 0.4% | 0.5% | | |

図 12：2021 年下半期の永続化の手法の地域別の検知率

図 13 を見ると、API による実行、すなわち、マルウェアがアプリケーションと直接やりとりしてアプリケーションを侵害する手法が全業種で最も一般的な実行手法だとわかります。ユーザーによる操作とは、サイバー犯罪者が被害者を特定の行動に誘導することですが、教育分野が突出しています。教育分野のユーザーが大きな侵入ベクトルであることに疑いの余地はほとんどないものの、攻撃者もマルウェアで優先する機能としてこれを考慮しているようであるのは興味深いことです。また、ユーザーにリンクをクリックさせたりファイルを開かせたりする、ユーザーによる操作に該当するマルウェアの割合が教育分野で高い（32%）のに対し、エネルギー / 公益事業分野では、スクリプトを使用してシステムに直接アクセスするマルウェアの割合が 2 倍近いのも興味深いことです。

| | 航空／防衛 | 農業 | 自動車 | 銀行／金融／保険 | 建設 | コンサルティング | 教育 | エネルギー／公共事業 | 環境 | 食品／飲料 | 政府機関 | 医療 | 法務 | 製造 | メディア／通信 | MSSP | 非営利団体 | 小売業／観光／宿泊業 | テクノロジー | 通信事業者 | 運輸／物流 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| APIによる実行 | 42% | 44% | 42% | 41% | 43% | 38% | 38% | 39% | 38% | 47% | 41% | 40% | 44% | 46% | 45% | 45% | 47% | 42% | 42% | 41% | 38% |
| ユーザーによる操作 | 25% | 17% | 24% | 20% | 22% | 23% | 32% | 13% | 22% | 19% | 22% | 19% | 18% | 21% | 20% | 18% | 18% | 20% | 22% | 18% | 23% |
| スクリプト | 18% | 18% | 18% | 22% | 20% | 16% | 15% | 24% | 18% | 17% | 18% | 20% | 21% | 19% | 19% | 20% | 19% | 22% | 18% | 20% | 20% |
| その他 | 15% | 21% | 16% | 17% | 15% | 23% | 16% | 24% | 21% | 17% | 18% | 21% | 17% | 14% | 15% | 16% | 16% | 17% | 18% | 21% | 20% |

図 13：2021 年下半期の実行の手法の業界別の検知率

# まとめ

フォーティネットは、世界経済フォーラムのサイバーセキュリティセンター（C4C：Centre for Cybersecurity）の創設時からのパートナーです。C4C は、官民が参加するサイバーセキュリティコミュニティの国際的な対話と協力を促進する目的で創設された、公平で独立したグローバルプラットフォームです。フォーティネットは現在、C4C プラットフォームの一部である Partnership against Cybercrime に基づき、サイバー犯罪エコシステムのマップ作成と相互の関係やビジネスオペレーションの理解によって、本レポートで解説しているような活動を中断させるための支援を行うプロジェクトにリーダーとして参加しています。

サイバー犯罪をコストのかかる行為にし、サイバー犯罪者のリスクを高くするための方法の詳細については、フォーティネットが共同執筆したこのレポートをお読みください。このレポートでは、解体作戦に向けたグローバルな能力の強化とサイバー犯罪抑止のための幅広い取り組みの必要性を解説しています。

参考文献

* 本文中のハイパーリンクは、本レポートの電子版（https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ja_jp/TR-21H2.pdf）よりご参照ください。

**フォーティネットジャパン合同会社**

〒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-21H2-202204-R1