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 年上半期レポート

目次

概説とハイライト

サイバーセキュリティの世界では業界の総意として、その年のキーワードを決める習わしがあります。1 年の半ばを過ぎた段階ではあるものの、2021 年はほぼ確実に、アウトブレイクの年というキーワードで呼ばれることになるでしょう。物理世界の現実に仮想世界が 1 年遅れでようやく追いついたとも言えますが、いずれにしても、2021 年上半期は、多くの組織や数え切れないほどの個人を巻き込む大規模攻撃が次々と発生しました。このような状況でも次の攻撃に一歩先行して備えるため、以下にこの上半期のトレンドを振り返り、解説します。

ProxyLogon フィードの狂乱

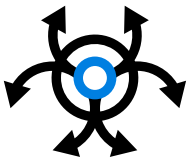
中国を拠点に活動する脅威集団「Hafnium」が、Microsoft Exchange Server の 4 つの脆弱性を悪用し、パッチが提供されるまでの数ヵ月間に数万の組織を攻撃したとされています。この攻撃に目をつけた他の集団もこれらのバグを集中して標的にするようになり、フォーティネットのセンサーでも関連する大量の活動が確認されました。詳細を、最初の注目すべき出来事で解説します。

ランサムウェアの不穏な動き

昨年は間違いなく激動の年でしたが、この 1 年でランサムウェアがさらに 10.7 倍に増加し、検知率が高くなっただけでなく、さらに邪悪なものになりました。コロニアルパイプラインや JBS などのサプライチェーンを停止に追い込んだ攻撃は、ランサムウェア攻撃がさらにレベルアップして、これまで以上に日常生活に影響を及ぼすようになる前兆のようです。その意味と今後の予想を、こちらのセクションで解説します。

OT は IT の影の存在ではなくなった

オペレーショナルテクノロジー（OT）は、注目度という点ではおそらく IT ほどではないものの、物理世界に直結するものであるため、日常生活にも影響を及ぼします。2021 年の産業環境を標的にしたランサムウェアやその他の攻撃で、この結び付きを何度も再認識することになりました。産業用制御システム（ICS）を標的として検知されたエクスプロイトの分析で、想像以上に多くの OT が攻撃者に見つかってしまうことがわかりました。



Emotet の解体と法執行機関による その他の取締り

サイバーセキュリティは長期戦であり、長期にわたって有効で即効性のある対策はほとんどありません。だからこそ、小さな勝利の積み重ねが次の日の戦力になるのです。最も活動が活発だったマルウェアの 1 つの Emotet が法執行機関の連携で解体され、Egregor、NetWalker、Cl0p などのランサムウェアの活動も同様に停止に追い込まれたことは、サイバー犯罪を抑え込もうとする世界中の政府や法執行機関が勝利を収めたことを意味します。このような活動への参加でフォーティネットが得た教訓については、こちらをご覧ください。

2021 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毎日観察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。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。最初に、2021 年上半期に上位に入った脅威を紹介します。

IPS の検知

MITRE ATT&CK は、攻撃者の戦術、技術、手順（TTP）を研究するフレームワークとして、広く利用されるようになっています。ATT&CK の TTP の最初の 3 つのグループである、偵察、リソース開発、初期アクセスは、基本的には攻撃者による脆弱性の発見、不正インフラストラクチャの構築、標的のエクスプロイトの方法を表します。FortiGate ファイアウォールで動作する FortiGuard 侵入防止システム（IPS）センサーは、外部からの侵入口を探すサイバー犯罪者との最初の接点となることが多いため、世界中のこの種の活動に対する優れた可視性を提供してくれます。

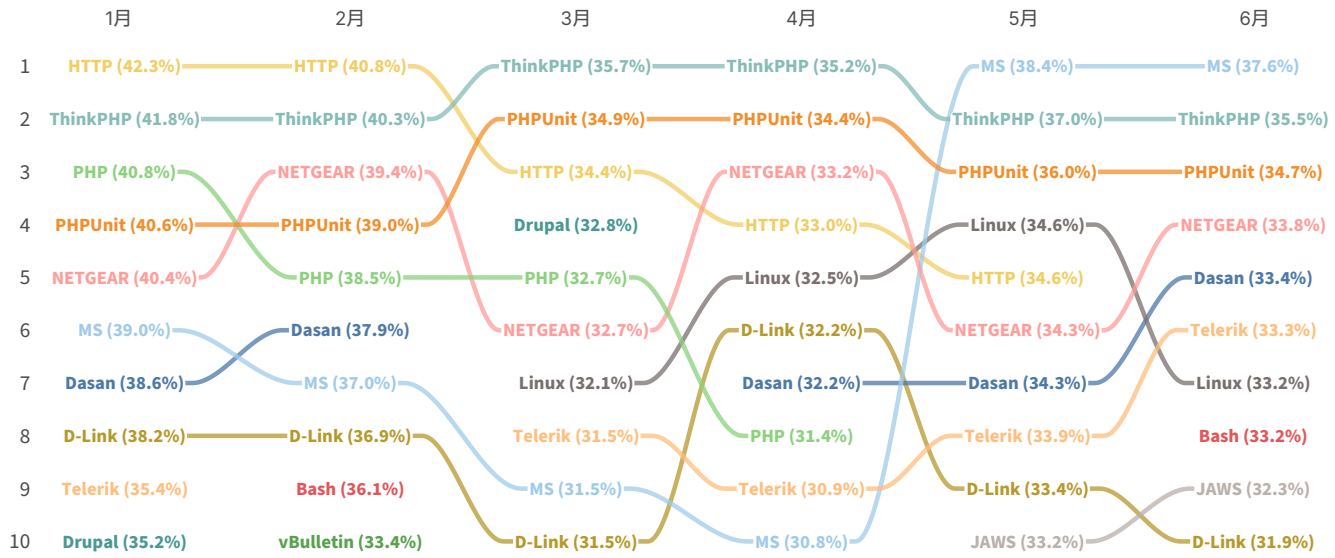


図 1：2021 年上半期の上位の IPS 検知率（テクノロジー別）

図 1 に、2021 年上半期にエクスプロイトの標的になった上位のテクノロジーを示します。ここに示した IPS 検知数には、Web サーバー、コンテンツ管理システム（CMS）、IoT デバイスなどでこれまでに確認された、いくつかの一般的なトレンドが反映されています。これ以降の段落で、この検知数を掘り下げて説明します。1 月と 2 月に 1 位だった HTTP シグネチャヘッダーには、Web サーバーを標的にするさまざまなエクスプロイトが含まれます。IPS で検知された数が最も多かったのは HTTP.Server.Authorization.Buffer.Overflow と HTTP.URI.Java.Code.Injection、検知された組織の数が最も多かったのは HTTP.Header.SQL.Injection と HTTP.URI.SQL インジェクションです。

Web サーバーを始めとする企業サーバーを標的にするエクスプロイトと深い関係がある Microsoft（MS）と Linux は、いずれの月も図 1 に登場しますが、これらのプラットフォームがあらゆる場所で利用されていることを考えれば、大きな驚きはありません。3 月以降の Linux ベースの検知数の増加の背後にある 1 つ目のシグネチャは、リモートの攻撃者がカーネルパニックをシステムで発生させて可用性を低下させる目的で悪用できる脆弱性に関係するものです。Microsoft が 5 月と 6 月に首位に立った背景には、さまざまなシグネチャが存在しますが、最も一般的なものの 1 つが、Microsoft Exchange Server のリモートコード実行の脆弱性のエクスプロイト試行を検知するシグネチャです。詳細は、注目すべき出来事で解説します。

PHP ベースの CMS である ThinkPHP を標的にするエクスプロイトが、上半期のいずれの月も 2 位以内に入りました。他の CMS（Drupal、vBulletin）や関連する開発フレームワーク（PHPUnit）も、月ごとの 10 位以内に何度か入りました。CMS が日和見主義のサイバー犯罪者の格好の標的であるのは、目の前にぶら下がった手の届く果実であるためです。CMS は Web コンテンツ管理を容易にすることを目的としていますが、その容易さを犯罪者も悪用するようになりました。CMS を利用している場合は、CMS やプラグインのセキュリティ修正を確実に適用することをお勧めします。

IPS 検知数の上位に、Netgear、D-Link、Dasan、JAWS など、標的にされることの多いネットワークや IoT デバイスが入っています。これらのほとんどは、2021 年のサイバー脅威予測ホワイトペーパーでトレンドを指摘した、中小規模企業や一般ユーザー向けのテクノロジーです。リモートワークや在宅勤務への移行に伴い、こうした環境のデバイスがサイバー脅威の標的となっています。これらのデバイスが標的にされるのは、攻撃者が詐欺やソーシャルエンジニアリングに悪用できる、ユーザーやユーザーのオンライン活動に関する情報がたくさん存在するためです。

しかしながら、企業のセキュリティプログラムにとってさらに重大な問題は、在宅勤務者の自宅のネットワークから攻撃が開始される可能性があることです。在宅勤務者と仕事に必要な会社のアプリケーションやデータとの間に、どれほど多くのデバイスが存在し、攻撃者がそのようなデバイスを手に入れると、何が可能になるでしょうか。攻撃者も当然ながら、同じことを考えるはずです。

図 1 に示したエクスプロイトの多くは新しいものではありません。一般的に、ある程度の時間が経過した後に上位に入ります。新しく登場したエクスプロイトに注目するため、図 2 に、IPS シグネチャが開発されてから 1 年以内の「新人賞」候補のエクスプロイトをまとめ、検知されたアクティビティを業種別で比較できるようにしました。

	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／公益事業	環境	食品／飲料	政府機関	医療	法務	製造	メディア／通信	MSSP	NPO	小売業／観光／宿泊業	テクノロジー	通信事業者	運輸／物流
vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	21%	26%	20%	24%	19%	20%	39%	23%	21%	20%	36%	23%	17%	22%	29%	32%	21%	21%	27%	40%	26%
MS.Exchange.Server.ProxyRequestHandler.Remote.Code.Execution	16%	18%	15%	19%	14%	14%	23%	19%	16%	16%	24%	17%	15%	17%	20%	25%	14%	14%	20%	28%	20%
F5.BIG.IP.TMM.URI.Normalization.Buffer.Overflow	14%	19%	14%	16%	12%	13%	30%	17%	15%	13%	26%	16%	12%	15%	21%	27%	15%	14%	20%	31%	18%
Netis.WF2419.Router.Remote.Command.Execution	15%	18%	14%	16%	13%	13%	28%	15%	13%	13%	24%	16%	11%	16%	18%	21%	15%	14%	18%	26%	18%
Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	13%	17%	13%	15%	12%	13%	28%	14%	13%	12%	24%	15%	11%	14%	19%	23%	14%	13%	18%	28%	17%
Oracle.WebLogic.Fusion.Middleware.Authentication.Bypass	12%	13%	10%	15%	9%	11%	25%	12%	13%	11%	24%	13%	8%	11%	15%	22%	11%	11%	16%	26%	14%
F5.iControl.REST.Interface.Remote.Command.Execution	10%	8%	6%	11%	5%	7%	18%	8%	9%	6%	18%	10%	6%	7%	10%	16%	8%	7%	12%	22%	9%
F5.BIG.IP.Traffic.Management.User.Interface.Directory.Traversal	8%	7%	5%	11%	4%	5%	14%	8%	5%	5%	16%	8%	5%	6%	10%	15%	7%	7%	11%	19%	8%
MobileIron.MDM.Unauthenticated.Remote.Code.Execution	6%	6%	5%	11%	4%	6%	12%	7%	7%	5%	16%	8%	3%	5%	9%	15%	6%	5%	10%	18%	7%
Spring.Boot.Actuator.Unauthorized.Access	3%	5%	4%	8%	3%	4%	14%	5%	4%	3%	15%	6%	2%	4%	8%	12%	6%	4%	9%	17%	5%
Nette.Framework.Callback.Parameter.Remote.Code.Execution	6%	5%	4%	6%	3%	5%	9%	6%	5%	3%	11%	5%	4%	4%	7%	10%	5%	3%	7%	13%	6%
Cisco.ASA.Web.Interface.Directory.Traversal	4%	4%	3%	9%	2%	3%	8%	4%	4%	3%	11%	5%	3%	3%	6%	10%	4%	4%	7%	14%	4%
Cisco.HyperFlex.HX.storfs-asup.Handling.Command.Injection	5%	6%	4%	5%	3%	3%	8%	4%	3%	3%	8%	5%	4%	4%	6%	12%	4%	4%	6%	14%	5%
VMware.vRealize.Operations.SSRF	3%	3%	2%	6%	1%	3%	6%	4%	4%	2%	10%	4%	2%	2%	5%	10%	3%	3%	6%	11%	4%
CraftCMS.SEOmatic.Template.Remote.Code.Injection	3%	4%	3%	5%	2%	3%	9%	2%	3%	2%	11%	4%	2%	2%	5%	8%	4%	3%	6%	10%	3%
Apache.Flink.JobManager.Arbitrary.Path.Traversal	3%	4%	2%	4%	2%	3%	8%	3%	3%	2%	11%	3%	1%	3%	4%	7%	3%	2%	6%	10%	3%
Apache.Struts.OGNL.BeanMap.Remote.Code.Execution	3%	4%	2%	4%	2%	3%	8%	3%	3%	3%	11%	4%	2%	2%	4%	7%	2%	2%	5%	10%	4%
FreePBX.Remote.Admin.Authentication.Bypass	2%	3%	2%	3%	2%	3%	9%	3%	3%	2%	6%	3%	2%	3%	5%	9%	3%	2%	5%	11%	4%
Citrix.XenMobile.Server.sbFileName.Arbitrary.Path.Traversal	2%	4%	2%	5%	2%	3%	7%	2%	2%	2%	11%	3%	2%	2%	5%	6%	3%	2%	5%	10%	3%

図 2：2021 年上半期の新しい（12 ヵ月未満の）IPS の検知率

IPS シグネチャ命名規則は、直感的にすぐに理解できるものではおそらくありませんが、Threat Encyclopedia を使用して図 2 のシグネチャを検索する際の手掛かりになります。この図の目的は、類似する組織で検知されている新しいエクスプロイトを知ることです。そのため、詳細の解釈についてはお読みいただく皆様にお任せし、観察された結果の概要のみを説明します。

図 2 を見ると、特定の業種では、問題となる特定のエクスプロイトに関係なく、より高レベルの活動が検知されていることがよくわかります。教育、政府機関、マネージドセキュリティサービスプロバイダ（MSSP）、通信事業者は、他の業種より明らかに暖色が多く、多くの場合に検知率が他の業種の 2 ～ 3 倍になっています。これらの業種の組織では多数のデバイスが利用され、多くの関連会社（政府機関の関連団体や MSSP / 通信事業者など）が存在する傾向があります。また、教育機関などは、古くからデバイスのセキュリティや使用方法の管理が厳格ではない分野とされており、金融、メディア、テクノロジーなどの標的になりやすい業種は、予想通りの検知率を示しています。農業での検知率は意外に思えますが、この分野でテクノロジーへの依存度が高くなっていることを考えれば、この調査結果は妥当なものと言えるでしょう。昨今の農場や農業施設には膨大な数の IoT デバイスが配備されていて、それぞれが独自の方法で接続され、外部に公開されています。サイバー犯罪者はそこにつけこみ、あらゆる機会に乗じて攻撃します。

マルウェアの検知

フォーティネットのさまざまなアンチマルウェアソリューションによって検知されたサンプルから、企業の環境に足場を築くための一般的な手法を知ることができます。ATT&CK のコンテキストにおけるこの活動は、攻撃者が標的システムでの不正コードの展開と実行を仕掛ける、実行フェーズに該当します。

図 3 は、マルウェア亜種ではなく、マルウェアファミリーで分類したもので、目的は多くの場合に短命な数多くの亜種を類似点によってまとめることで、大局的な視点も失わないようにするためです。図 4 は、詳細ビューを世界の地域に分け、新しいマルウェアの分布を把握できるようにしたものです。

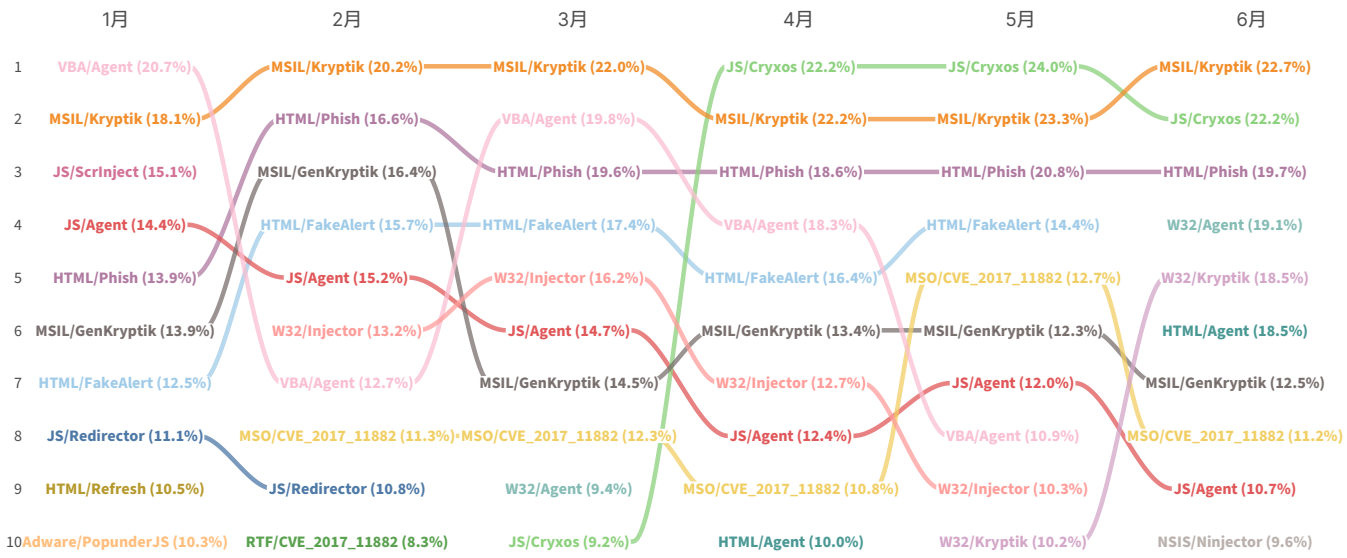


図 3：2021 年上半期の上位のマルウェアの検知率（ファミリー別）

両方の図のファミリーと亜種を攻撃ベクトルで分類すると、2 つの拡散方法、すなわち、Microsoft プラットフォームと Web ブラウザに大別されます。最初のグループ（Microsoft プラットフォーム）に該当するのは、32 ビットの Windows 実行ファイル（W32）、Office、または Visual Basic（VBA）の不正ファイル、さらには、.NET や Microsoft Intermediate Language（MSIL）のパッカーを使用するマルウェアです。Web ブラウザを悪用するマルウェアファミリーには、先頭に HTML や Javascript（JS）が付く場合が多く、これには、マルウェアが埋め込まれたフィッシングやスクリプトによって、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するものが含まれます。このような手法が広く使われるようになったのは、COVID-19 の感染が拡大する中でニュースや情報を熱心に追いかける人々が増え、それと同時に企業の Web フィルターの外で働く在宅勤務への移行が進んでいるためです。

検知率が高いマルウェアをマルウェアファミリー別に並べると、ソーシャルエンジニアリングを悪用する JavaScript ベースのマルバタイジングやスケアウェア（Cryxos など）が増加していることがわかります。このような手口は、Microsoft のテクニカルサポートチームを装う偽の通知によく見られます。デバイスが感染あるいはハッキングされたというメッセージを何らかの形（ブラウザのポップアップなど）でユーザーに知らせ、サポート担当者に連絡して金銭を支払ったり、リモートアクセスを許可したりするように指示されます。全体では、4 分の 1 以上の組織で、2021 年上半期にマルバタイジングやスケアウェアの試行が検知されました。

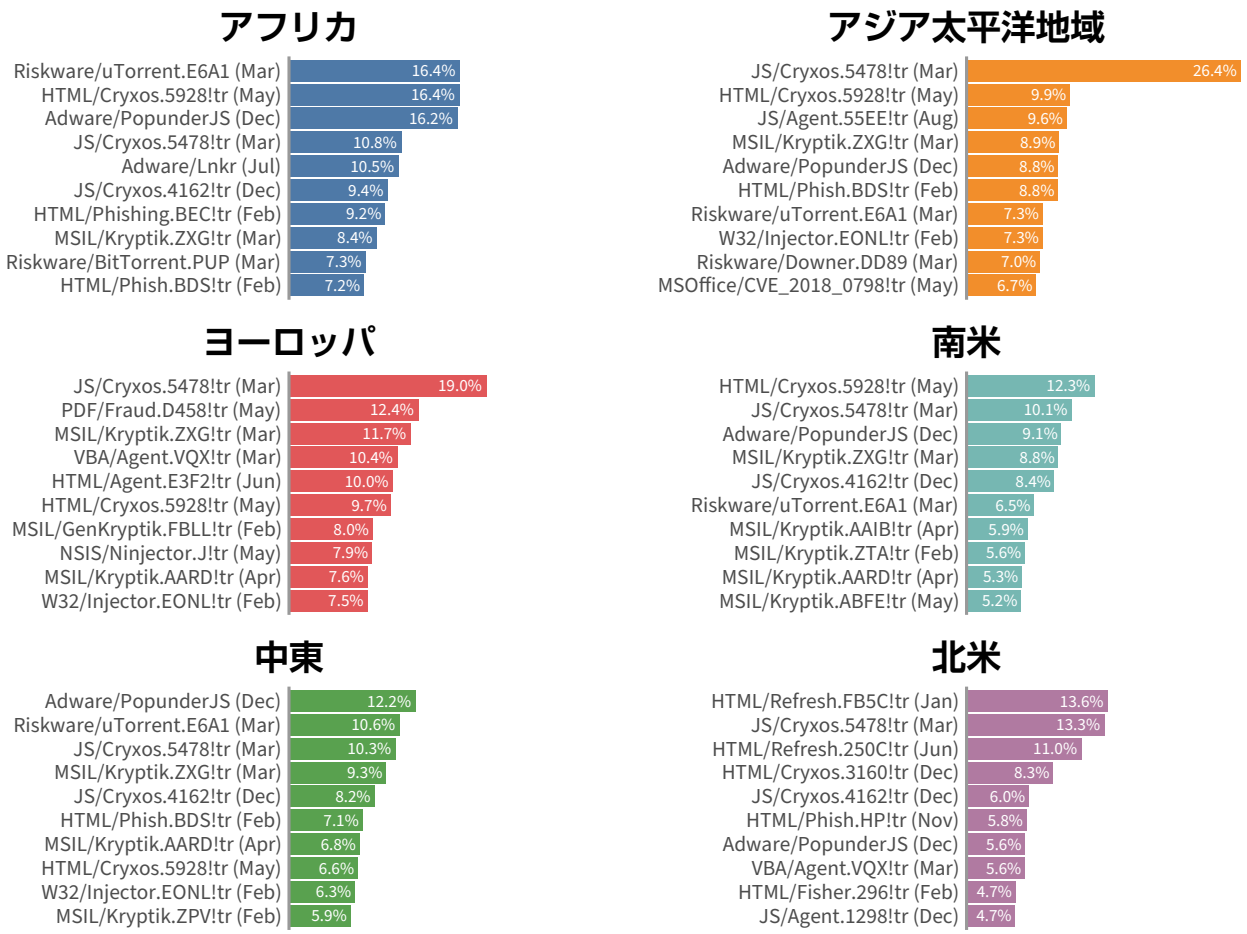


図 4：2021 年上半期の新しい（12 ヵ月未満の）マルウェア亜種の検知率（地域別）

マルバタイジングは、新しい戦術でも、マルウェアの最も危険な形 / 機能でもなく、リモートワークのトレンドがマルバタイジングの増加に貢献しているのは間違いありません。安全性が高いとされてきた企業の境界の外で働く人々が急増し、IT 担当者と同じオフィスで働くことによる利便性が失われたことから、従業員は、以前にも増して自らの判断で行動するようになりました。このことからも、サイバー犯罪者が変動する状況に合わせて既存のツールを変えていることがわかります。

観察されたマルウェアのTTP

過去 6 ヵ月間に検知されたマルウェアサンプルを列挙するだけでなく、それらのサンプルに内在する具体的な機能を調査したいと考えましたが、そのための最良の方法は、マルウェアを活動させて、実際の行動を観察することです。そして、その結果をまとめたのが、図 5 です。

図 5 に、FortiSandbox Cloud サービスで分析したマルウェアに関連する複数の ATT&CK TTP を示します。マルウェアサンプルが標的とする環境でペイロードの実行に成功した場合、ここに記載したような行動に出る可能性があります。すなわち、特権を昇格する、防御を回避する、内部システムを水平移動（ラテラルムーブメント）する、コマンド & コントロールを確立する、不正取得したデータを持ち出す、あらゆる形で影響を与えるといった行動です。

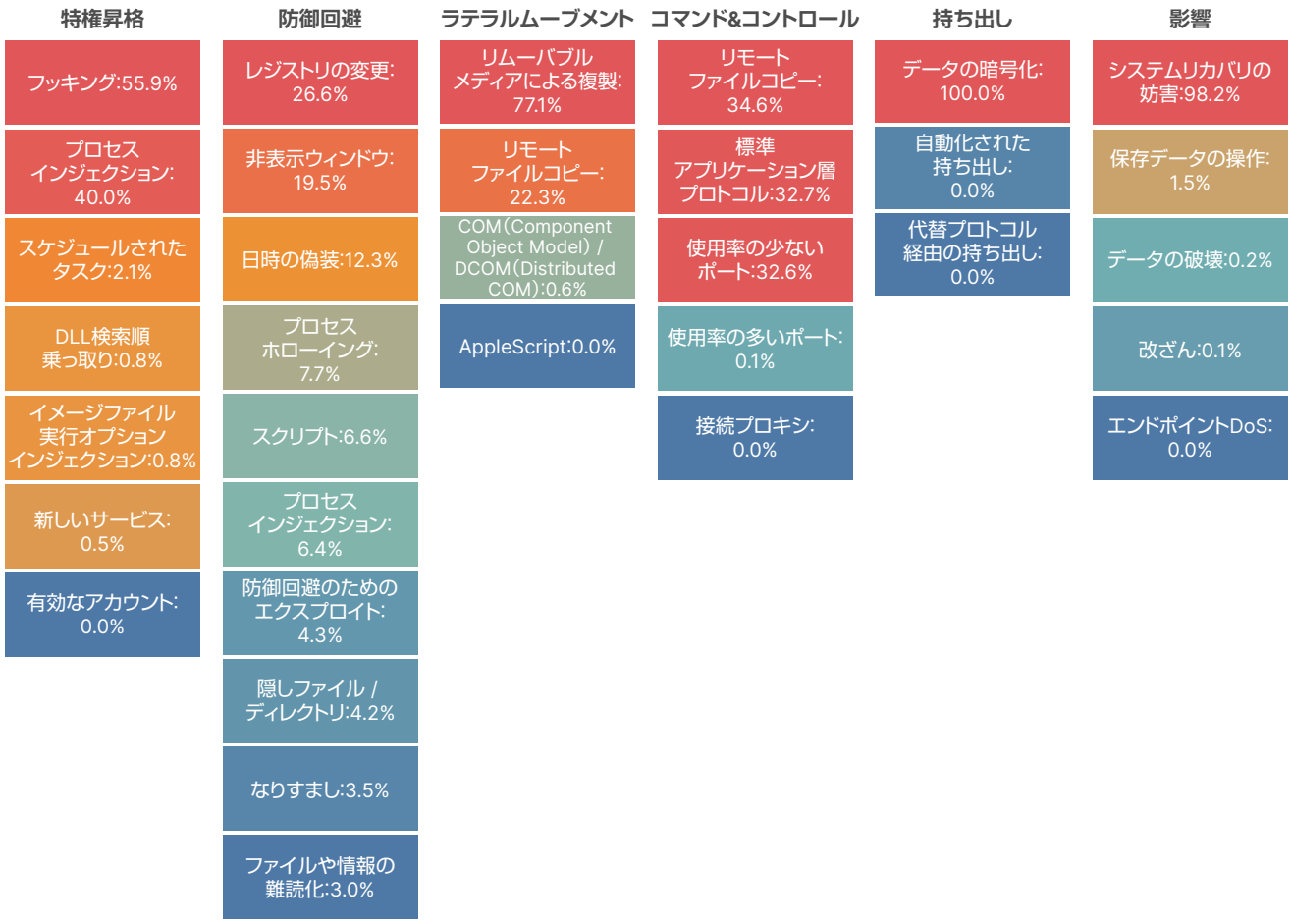


図 5：2021 年上半期にフォーティネットが確認したマルウェアの TTP の相対的な頻度

グラフに示したパーセンテージは、最上位の戦術での各手法の頻度に基づきます。つまり、観測された特権昇格の機能の 55% でフッキングが、そして 40% でプロセスインジェクションが利用されていました。このことから、防御回避と特権昇格の戦術に重点を置いていることがわかります。いずれも新しい手法ではありませんが、不正プロセスがオペレーティングシステムのコアとどのようにやり取りしてリソースを要求するかを理解するために、カーネルレベルでの高度な仕組みが必要になるものもあります。従来の防御をすり抜ける可能性のある（ProxyLogon などの攻撃のような）高度な脅威を阻止する上で最も重要なことは、これらのやり取りの間にインスペクションポイントを置くことです。

APT 犯罪者は、ネットワークに侵入する手段としてゼロデイを好んで悪用するようになってきています。そのため、本番システムに実際に影響する前にこの機能を観察し、ファブリックの統合を活用して減災し、キルチェーンの次の段階に進むのを阻害することが、これまで以上に重要になります。サイバー犯罪者が使用する手法を明らかにし、その情報をもとに脅威に基づく防御を構築できれば、成功率が高くなります。

脅威インテリジェンスに基づく防御の構築に貢献するため、FortiGuard Labs は、MITRE の Center for Threat-Informed Defense に、Sightings Ecosystem などのプロジェクトを通じて参加しています。フォーティネットはこのようなさまざまな方法で業界のパートナーと協力し、情報に基づく強力なセキュリティの実現を支援しています。

ボットネットの検知

IPS とマルウェアのトレンドが「ブームの左」（侵害前）の出来事を明らかにするのに対し、ボットネットは、重要な「ブームの右」（侵害後）に発生する不正活動を明らかにします。ATT&CK の観点からは、感染したシステムがリモートの不正ホストと通信する、コマンド & コントロールの戦術に分類される手法と最も密接に関係しています。図 6 に、2021 年上半期の上位のボットを示します。

図 6 で追跡したボットの説明に入る前に、図の見方を説明します。色別の波線の高さは、それぞれのボットネットに関連する活動が検知された組織の数に対応しています。この図に名前が記載されていないボットネットの検知は、1 番下の比較的細い「その他」の帯に合算しました。このことから、活動の 80% が 10 位までのボットネットに関連するという、パレートの法則が存在することがわかります。そのため、有名なボットネットの解体は、サイバー脅威に対する有効な戦略となるはずです。そのような作戦の 1 つである Emotet ボットネットの解体については、注目すべき出来事で紹介します。

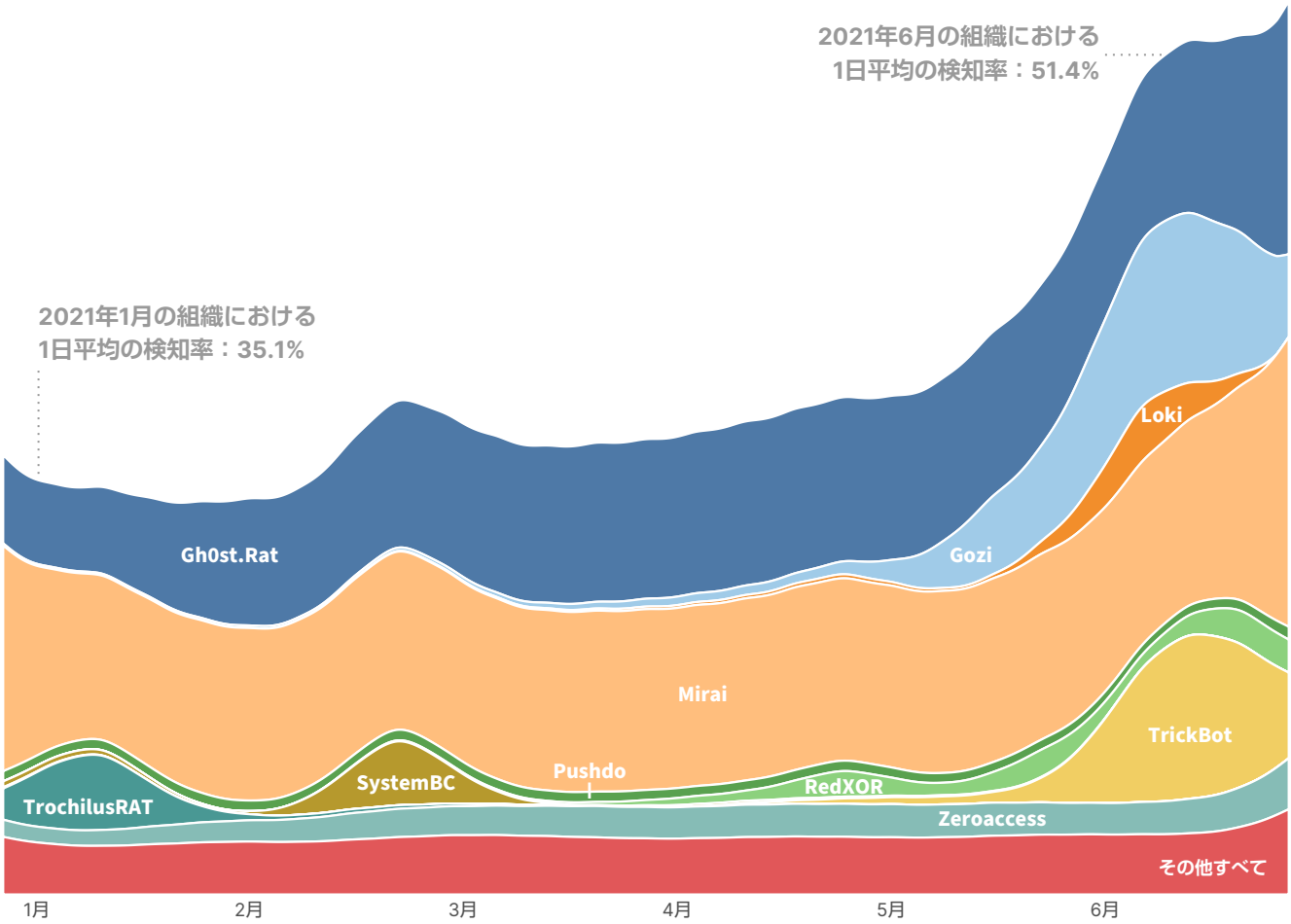


図 6：2021 年上半期のボットネットの検知率

図 6 を見るとわかるように、上半期の後半に活動が大きく上昇し、年初は 35% の組織で何らかのボットネット活動が検知されましたが、半年後にその割合が 51% になりました。この急増の背景を考えてみることにしましょう（ボットネットの集団行動としては異例なことです）。

Mirai は最も太い帯なので、最も検知率が高く、2020 年初めに Gh0st から奪った首位を守り続けています。Mirai は、数年前に IoT ベースの大規模 DDoS 攻撃でその名を知られるようになって以来、新たなサイバー兵器を追加し続けることで優位性を保ってきました（1 や 2 など）。繰り返しになりますが、Mirai が優位性を保ち続けている要因の少なくとも 1 つは、在宅勤務で使用する（または近くにある）IoT デバイスを悪用しようとする犯罪者の増加だと思われます。

Gh0st は期間を問わず（何年も前から）活発に活動している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、ウェブカメラやマイクのライブフィードへのアクセス、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。

非常に珍しいことですが、図 6 のこれ以外のボットネットのほとんどは、これまで 10 位以内に入ったことがないものです。同じような顔ぶれが繰り返し並ぶため、新しいボットネットがここに登場するのは新鮮なことです。上半期の終盤にかけてのこのような急増は、これらの新しいボットネットが、ボットネット全体の活動を新たなレベルへと押し上げたことを示しています。

Trochilus ボットネットとの通信が、オセアニアや東南アジアを中心に、今年の初めに急増しました。過去には、Trochilus という RAT（リモートアクセスのトロイの木馬）が、中国のスパイ集団によって同じ地域を標的とする作戦に使用されたとされています（図 7 参照）。

	アフリカ	アジア	ヨーロッパ	南米	中東	北米	オセアニア
TrickBot	50.0%	41.3%	66.8%	48.6%	40.9%	64.1%	66.4%
Gh0st.Rat	61.8%	61.4%	65.2%	61.4%	56.6%	71.9%	70.5%
TrochilusRAT	41.0%	38.7%	46.4%	42.5%	38.7%	51.5%	54.4%
Necurs	6.2%	4.0%	2.5%	2.9%	4.1%	3.8%	3.8%
Sality	12.9%	13.7%	3.0%	6.2%	18.2%	3.1%	3.3%
RedXOR	11.6%	12.3%	10.8%	20.5%	11.1%	7.9%	8.6%
Nymaim	0.4%	5.7%	0.3%	0.1%	0.1%	0.2%	0.4%

図 7：2021 年上半期のボットネットの検知率（地域別）

2 月に 3 位に躍り出た SystemBC（図 6）は、極めて多くのランサムウェア攻撃で最近利用されている RAT です。TLS で暗号化した永続的なバックドアと C2 の機能を攻撃者が利用できることが、人気の一因です。ランサムウェアの提供者は、E メールで誘導するペイロードから「アクセスファシリテーター」（初期アクセスを手に入れて販売するサイバー犯罪者の響きの良い呼び方）を活用する戦略に移行しており、SystemBC はそのトレンドを支えるツールの 1 つです。

図 6 の上半期後半の TrickBot の活動の大幅な増加が、6 月のボットネット活動全体の急増にも大きく影響しています。TrickBot は、金融機関を標的にするトロイの木馬としてサイバー犯罪シーンに登場しましたが、さまざまな不正活動を支援する、高度にモジュール化された多段階ツールキットへと発展しました。米国の CISA（Cybersecurity and Infrastructure Security Agency）が 5 月に、TrickBot を利用したスピアフィッシング攻撃が急増しているというアラートを発表しました。TrickBot の最初の開発者が 6 月に複数の容疑で召喚されたことは、サイバー犯罪者も処罰の対象になるという戒めになりました。

6 月にボットネットでもう 1 つ大きく変化したのが、Loki の活動です（図 6）。CISA が 2020 年後半に、この情報を不正取得するマルウェアファミリーの検知が急増しているというアラートを発表しました。この急増が新たな攻撃や特定の大規模攻撃によるものだという情報はありませんが、これらの結果は間違いなく、警戒を強めるきっかけとなりました。そこで、この半年間の特に注目すべき出来事を次に解説することにしましょう。

注目すべき出来事

ProxyLogon フィードの狂乱

Microsoft Exchange Server の 4 つの脆弱性は、影響を受けるシステムが多く、3 月 2 日に Microsoft がパッチを公開する前にこれらの脆弱性を悪用する攻撃が活発だったことから、重大な問題として広く知られることになりました。ProxyLogon とも呼ばれるこの脆弱性は、インターネットに接続した Exchange Server が外部からの信頼できない接続を受け入れている組織にとって大きな脅威であり、2021 年春に検知されたインシデントの 30% 以上が、これらの Exchange Server の脆弱性に関連していると報告するベンダーもいます。

これらの脆弱性は具体的には、CVE-2021-26855（認証の回避に使用される可能性のある、サーバーサイドリクエストフォージェリ（SSRF）の問題）、CVE-2021-26857 および CVE-2021-26858（攻撃者による SYSTEM への特権の昇格を可能にする恐れがある、安全ではないデシリアライゼーションの脆弱性）、CVE-2021-27065（認証後の任意ファイルの書き込みを可能にする恐れがある脆弱性）です。この 4 つの脆弱性を併用することで、攻撃者がリモートで不正コードを Exchange Server で実行したり、バックドアをインストールしたりできるようになります。

中国を拠点とする「Hafnium」と呼ばれる APT（高度な持続的脅威）集団がこの脆弱性を悪用し、Microsoft による修正プログラムが公開されるまでに少なくとも 3 万の米国の組織を攻撃したとされています。この脆弱性に対する最初の攻撃は、パッチが提供される 2 ヵ月以上前である 1 月に始まったとされており、米国のシンクタンク、防衛関連企業、法律事務所、NGO、感染症の研究機関などが攻撃されました。Microsoft がこれらの脆弱性を公開したことで、他の多くの犯罪集団、国家が支援する組織、日和見主義のハッカーたちもこれらの脆弱性を次々と標的にするようになりました。その 1 つが、Barium（APT41）と呼ばれる、中国を拠点とするサイバー犯罪集団で、フォーティネットが過去にサプライチェーンの侵害や大手ソフトウェアベンダーに対する攻撃への関与を指摘したこともあります。

この攻撃を受けて、CISA、Microsoft、その他多くのセキュリティベンダーが緊急のアラートを発表しました。この脅威が非常に重大であることから、FBI が 4 月に裁判所の許可を得て前例のない作戦を実行し、システムの所有者に事前通告することなく、米国内の数百台の Exchange Server にインストールされた不正 Web シェルを削除しました。

フォーティネットは、Lemon Duck コインマイナー、BlackKingdom ランサムウェア、Prometei ボットネット、China Chopper（少なくとも 2012 年には開発され、侵害後に脆弱なシステムへの永続的なバックドアアクセスを提供する軽量の Web シェル）などのさまざまなマルウェアツールを使用してこれらの脆弱性を攻撃する犯罪者を追跡しています。フォーティネットの IPS が検知した Exchange Server の脆弱性に関連する活動（図 8 参照）を見ると、ヨーロッパを中心に、この脆弱性を標的にする攻撃が確認されており、複数の報告で、トルコ、米国、イタリアが最も攻撃された 3 ヵ国として挙げられています。活動が特に活発だったのは、CVE-2021-26855 という SSRF の脆弱性で、これを悪用することで、脆弱な Exchange Server への初期アクセスが可能になります。

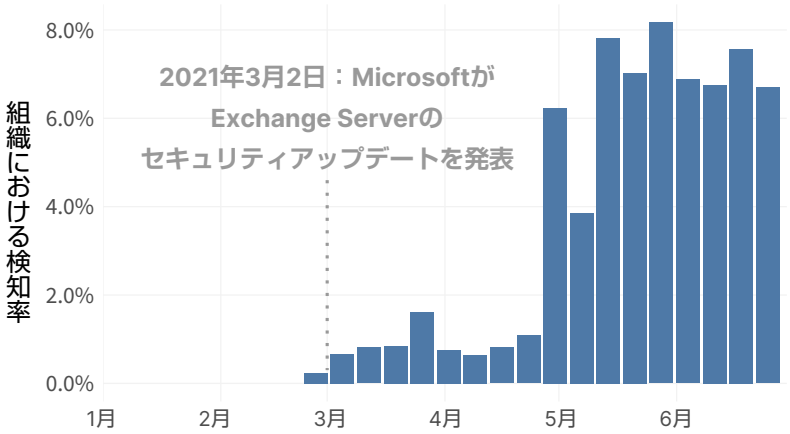


図 8：2021 年上半期の Exchange Server の ProxyLogon 脆弱性を標的とするエクスプロイト活動

セキュリティチームはこれらの攻撃で、E メールなどの広く利用されているテクノロジーの脆弱性がサイバー犯罪者の格好の標的になることを再認識することになりました。これらの脆弱性を最初に悪用したのは、サイバー空間で諜報活動を進めていた、国家が支援する高度な APT でしたが、パッチが利用できるようになると、サイバー犯罪者はすぐにそれをリバースエンジニアリングし、さまざまな攻撃に悪用するようになり、迅速なパッチの適用と多層型防御の必要性が浮き彫りになりました。

ランサムウェアの不穏な動き

ランサムウェアは、今年の第 1 四半期と第 2 四半期も過去数四半期と同様に、世界中の組織にとって不吉な脅威であり続けました。2020 年後半ほどの攻撃の急増ではなかったものの、ランサムウェアの水準は依然として高く、通年で着実に増加しました。2021 年 6 月のランサムウェアの週の平均の活動が、1 年前の水準の 10.7 倍に達しました（図 9）。さらには、一般の認識とは異なり、ランサムウェアは、医療、政府機関、教育だけでなく、はるかに多くの業種の脅威になっています（図 10）。

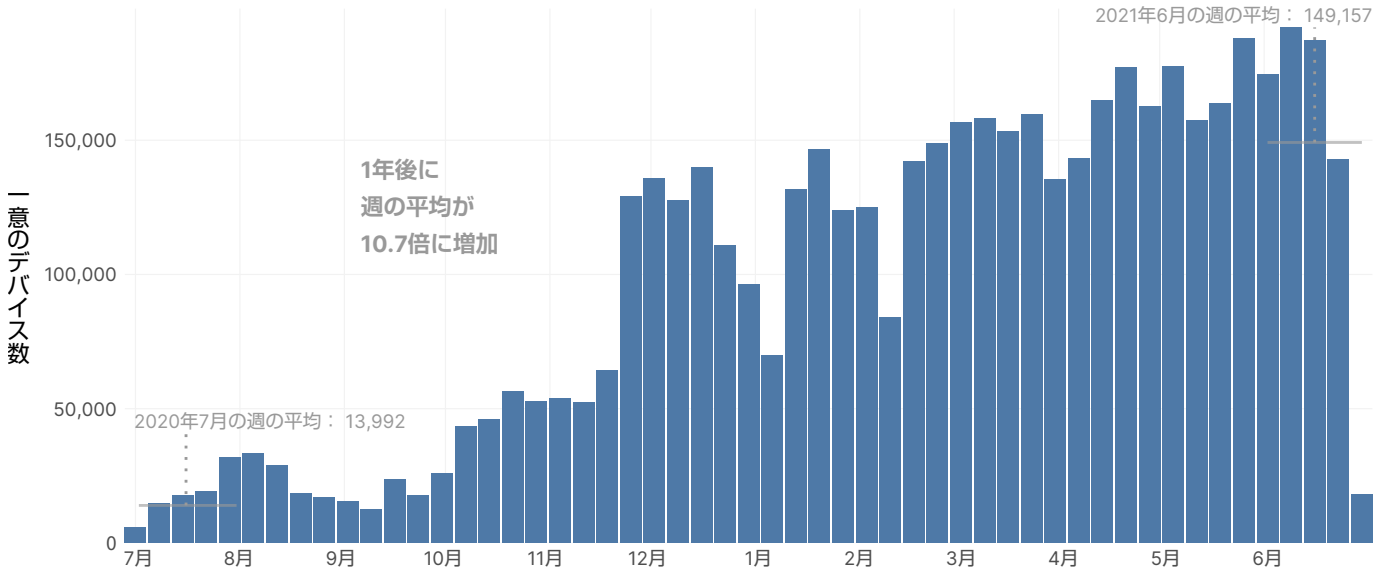


図 9：過去 12 ヵ月（2020 年 7 月～ 2021 年 6 月）のランサムウェア検知数の増加

今年の深刻で注目すべき問題点として、重要分野における OT ネットワークや組織に対する攻撃を挙げることができます。例えば、5 月のコロニアルパイプラインに対する攻撃で、米国東海岸の大部分で燃料供給が一時的ではあるものの大規模停止に追い込まれました。コロニアルパイプラインは、攻撃の背後にいるロシアの脅威集団である DarkSide に 440 万ドルを支払うことで、パイプラインの制御を取り戻しました。5 月には、世界最大の食肉加工業者である JBS が攻撃され、米国内の食肉供給に同様の混乱が生じるのではないかと心配されました。JBS はこの問題を解決するために、1,100 万ドルを攻撃者に支払いました。

この 2 つのインシデントで、ランサムウェアは国家安全保障の問題にまで発展し、報道によると、米国司法省は、ランサムウェアの優先度をテロ攻撃と同等にまで引き上げることを検討しているとのことです。これらの攻撃が最高レベルで米国政府に注目されたことで、DarkSide、Avaddon、Ziggy などの少なくとも一部のランサムウェア提供者が事業を停止すると発表しました。

フォーティネットが 1 月に、DarkWorld と呼ばれる新しいランサムウェア亜種を発見しました。.NET で記述されているこのランサムウェアは、10 種類の暗号化スレッドを生成し、Rijndael 暗号化アルゴリズム（AES）を使用して被害者のファイルをロックすることが確認されています。このランサムウェア亜種に関連する活動のほとんどはインドで確認されており、コロンビア、フランス、チリ、米国がそれに続きました。

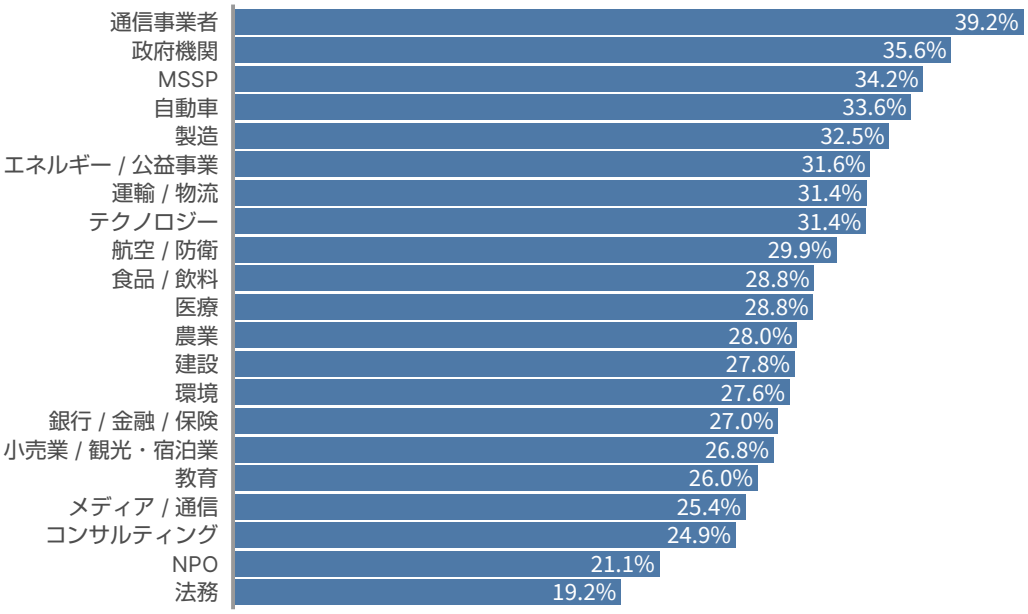


図 10：2021 年上半期のランサムウェアの検知率（業種別）

図 10 を見ると、ランサムウェアがすべての業界に共通の脅威であることがわかります。通信業界の組織が最も多く標的にされており、政府機関、マネージドセキュリティサービスプロバイダー、自動車、製造の順に続きます。最も攻撃の標的になると一般的に考えられている医療と教育の分野でのランサムウェアの検知率は、全業種と比較すると低いことがわかります。企業が認識しておくべきは、業種や規模にかかわらず、ランサムウェアは間違いなく現存する脅威だということです。

OT は IT の影の存在ではなくなった

オペレーショナルテクノロジー（OT）は、注目度という点ではおそらく IT ほどではないものの、物理世界に直結するものであるため、日常生活にまで影響します。OT ネットワークは最近まで、エアギャップで分離された環境として動作していたため、サイバーセキュリティは最優先事項ではありませんでした。SCADA や ICS（産業用制御システム）に対するエクスプロイトは、高度な標的型攻撃で占める割合が極めて低く、ほとんどの組織にとって無関係であると考えられていました。しかしながら、その認識は現代の脅威においても正しいのでしょうか？その証拠をお見せしましょう。

図 11 に、IPS の検知率と検知数を示します。グレーの点は IT に対する攻撃、赤の点は OT システムに対する攻撃の検知率と検知数をそれぞれ表します（1 番右上のテクノロジーの例は図 1 を参照）。IT 関連のエクスプロイトの方が検知率も検知数も間違いなく多いのですが、OT を標的にするエクスプロイトが比較的多いことは、多くの人にとって驚きかもしれません。少なくとも図 11 を見れば、ICS エクスプロイトがサイバー脅威で目立たない特異な存在だという認識は崩れ去るでしょう。

新たなビジネスニーズの登場やインフラストラクチャの老朽化で OT と IT を隔ててきた壁が消滅し、両者のネットワークの融合が進んでいることを考えると、このように認識を改めることは非常に重要です。より柔軟なセキュリティインフラストラクチャへのニーズへの対応の詳細と方法については、産業環境での動向に焦点を当てた 3 月の業界の視点をお読みください。

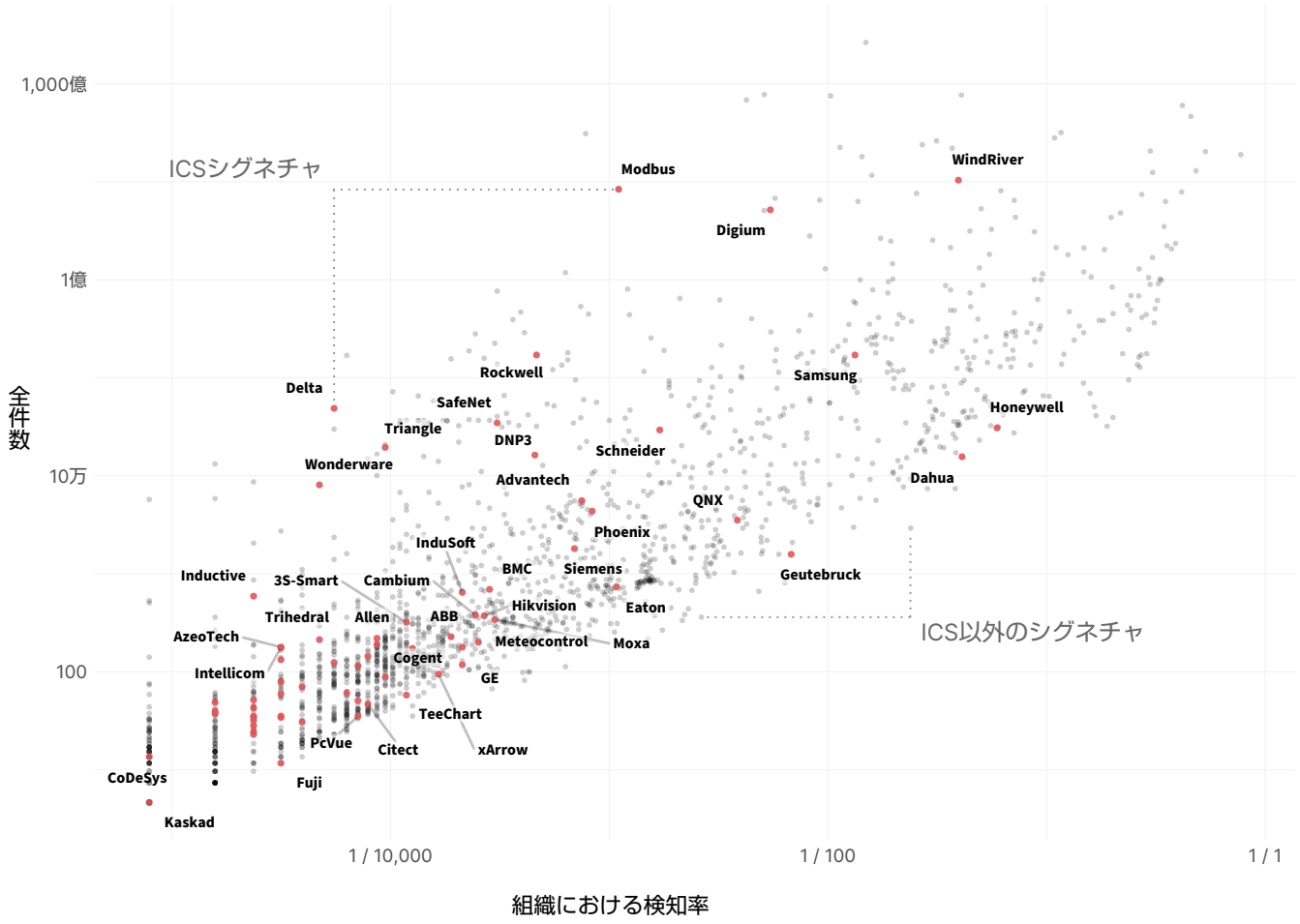


図 11：2021 年上半期の OT（赤）と IT（グレー）を標的にしたエクスプロイトの検知率と検知数

図 11 の特定の ICS の位置を見ると、1 年前の同様のチャートで観察された結果と驚くほど一致しています。これは、OT の脆弱性を特定しようとするサイバー犯罪者の関心の高さと攻撃コストを下げる目的で利用されるさまざまなエクスプロイトツールにそのような脆弱性が組み込まれるようになっていることの表れです。そのため、スクリプトキディと呼ばれる初心者も APT 集団と同じように、外部に公開されている OT を発見する可能性があります。

上半期に ICS の検知が安定して推移する中で、例外的に、WindRiver VxWorks システムを標的とするエクスプロイトの検知率と検知数が増加しました。VxWorks は、世界で最も広く利用されていると言われるリアルタイムオペレーティングシステム（RTOS）であるため、潜在的な攻撃対象領域は広くなります。RTOS には古くから、2010 年に Rapid7 が発見した脆弱性から最近では 2019 年に Armis Labs が発表した「Urgent/11」までの有名な脆弱性が数多く存在します。

Armis は URGENT/11 のアップデートを 2020 年の 12 月中旬に公開し、URGENT/11 の影響を受けた OT デバイスの 97% にパッチが適用されていなかったと主張しました。攻撃の機会を狙う犯罪者がこの発表に注目し、結果としてこれらの脆弱性に対する偵察活動が急増した可能性があります。この仮説を裏付けるように、最も高い検知率の 1 つは、VxWorks のバージョン番号を取得するために試行されたスキャンに対応するものです。このスキャンそのものは大きな脅威ではないものの、この偵察が VxWorks TCP/IP スタックの既知の脆弱性を標的にしている可能性は高く、そのいくつかは RCE を可能にする恐れがあるものです。

ここでの全体としてのメッセージは、OT エクスプロイトは想像より一般的で、攻撃者が注目するようになっていることから、無視してはならないということです。もちろん、ICS を保護する最善の方法は、犯罪者に攻撃される前に脆弱性を発見して修正することです。これを支援するため、FortiGuard Labs は、ゼロデイを特定して公開する取り組みを強化しています。この半期だけでも、複数の脆弱性レポートを Schneider Electric に提出し、お客様の環境の保護に共同で取り組んでいます。

Emotet の解体と法執行機関によるその他の取締り

1 月に、米国、オランダ、英国、ドイツを含む複数の国の法執行機関が共同で、近年で最も活発に活動してきたマルウェアの 1 つである Emotet ボットネットのインフラストラクチャを解体に追い込みました。この作戦では、コマンド&コントロールサーバーとして使用されていた世界中の数百台のサーバーをほぼ同時に乗っ取り、感染システムからのトラフィックを法執行機関が管理するインフラストラクチャにリダイレクトしました。

Emotet ボットネットは、情報の不正取得、トロイの木馬、ランサムウェアなどのさまざまなマルウェアの拡散に広く利用されていました。Ryuk や Qakbot といった活発だったランサムウェアや金融機関を標的にするトロイの木馬である Trickbot などの提供者もこのボットネットを利用していたため、この解体は、このボットネットを利用してマルウェアを拡散させていた犯罪者にとって大打撃となりました。

さまざまな国での単独あるいは共同の同様の解体作戦で、Egregor、NetWalker、Cl0p を始めとする有名な犯罪組織が 2021 年上半期に解体に追い込まれました。これらの作戦で、サイバー犯罪抑止のための政府や法執行機関による取締りが大きく前進しました。法執行機関によるこれらの作戦では、国家が支援する、SolarWinds、コロニアルパイプライン、JBS などへの攻撃を仕掛けた APT 集団に対して米国政府や同盟国がこの数ヵ月間に発表した制裁や起訴も追い風になりました。DarkSide、Avaddon、Ziggy などの一部のサイバー犯罪集団が自ら姿を消したことや、コロニアルパイプライン攻撃の後に一部の地下フォーラムがランサムウェアの取引を拒否するようになったことも、朗報と言えるでしょう。このような行動は、少なくとも一部のサイバー犯罪集団が法執行機関の動きを警戒するようになったことを示唆しています。

しかしながら、善良な人々の成功は称賛に値しますが、法執行機関の行動や自主的な撤退の効果はいずれも一時的である可能性が高く、例えば、フォーティネットのデータを見ると、Emotet の活動は解体後に鈍化したものの、完全になくなったわけではありません（図 12 参照）。TrickBot や Ryuk の亜種に関連する活動は、Emotet ボットネットがオフラインになった後も、件数は減少したものの継続しました。また、解体の直後にマルウェアの検知が一時的に減少したものの、マルウェアの配布元が変更されたため、徐々に元の検知数に戻りつつあると報告しているベンダーもいます。

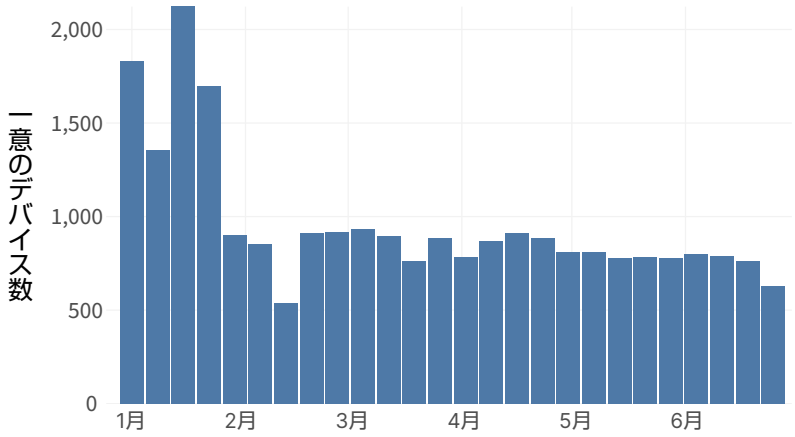


図 12：2021 年上半期の Emotet ボットネット通信の検知数

今回のデータは、サイバー脅威の根絶がいかに困難かを示すものであり、法執行機関の勝利や一部のサイバー犯罪集団による不正活動の自主的な停止といったニュースを理由に警戒を緩めてはならないことを企業に警告するものでもあります。このような行動は確かに価値あるものですが、サイバー犯罪エコシステムを一掃するためには、多くの組織による長期間にわたる多大な努力が必要です。こうした取り組みにささやかながらも貢献する本レポートが、2021 年後半の脅威への備えの一助となることを願っています。

ご存じでしたか？

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サイバー犯罪活動の戦術的な解体を目指す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-21H1.pdf）よりご参照ください。

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-21H1-202109-R1