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 年下半期レポート

目次

2020 年下半期の概説と主な発見事項

誰もが同意する出来事はほとんど存在しませんが、2020 年が困難の年だったことには、多くの人が同意するはずです。過ぎ去った昨年のサイバー脅威環境が再現されるよりも、色々な意味で先に進みたいものです。しかしながら、実世界とデジタル環境のどちらにおいても 2020 年の影響が 2021 年に残っているのは事実であり、それを忘れてしまうのは危険なことです。したがって、2020 年後半（2020 年下半期）を振り返ることが、より確かで安全な未来に向かって進むことになります。一緒に振り返っていきましょう。

SolarWinds の大嵐

SolarWinds は、米国ターゲット社の情報漏洩に匹敵する、サプライチェーンのサイバーセキュリティの危機と言えるでしょう。ターゲット社は小売業での最初のハッキングではなかったものの、セキュリティ関係者の多くにとって家族との共通の話題となった最初の事件です。サプライチェーン攻撃にも長い歴史がありますが、SolarWinds で新たな次元へと進んだようです。フォーティネットのセンサーで検知された、この大規模攻撃を詳しく解説します。

継続する APT 集団の活動

2020 年下半期は SolarWinds が大きく注目されましたが、その影で他の多くの APT（高度な持続的脅威）集団による不正活動も続いていました。我々の調査で、2020 年の終盤にかけて最も活動が活発だった集団、活動の目的、主な標的が明らかになりました。

IoT と CMS の危機

IoT（モノのインターネット）デバイスと CMS（コンテンツ管理システム）は、インターネットをめぐる戦いの最前線であり続けています。エクスプロイトの標的となる 10 位までのテクノロジーのうちの 9 つは、このいずれかのカテゴリに分類されます。最重要資産とは言えないまでも、ネットワークでそういった資産と隣合わせである可能性は十分にあるため、攻撃の足場とならないための十分な対策が必要です。

家庭用デバイスの悪用

IoT デバイスが標的にされるようになった背景には、側面からの攻撃という意図が隠されているのかもしれません。自宅とオフィスの境が明確ではなくなった 2020 年、自宅への攻撃成功 Pwn [1] は、企業への侵入に一歩近づいたことを意味します。本レポートで紹介するインテリジェンスを活用して、攻撃の計画を予測し阻止することで、攻撃者を廃絶しなければなりません。

信頼しない事に基づく関係の構築

在宅勤務への移行で多くの人が困難を強いられていますが、プラスの効果として、トラストベースのセキュリティへの移行を迫る決定打になった可能性もあります。境界の消滅によって、セキュリティの監視と適用をすべてのデバイスに移行することが緊急の課題となっています。人間の関係はトラスト（信頼）に基づいて築かれますが、IT は不信感に基づいて関係を築くことで間違いなく健全なものになります。

賭けに出て大きな利益を得る

本レポートで「ランサムウェアの増加」をお伝えしないことはありませんが、今回も例外ではありません。ランサムウェアの活動が下半期の始めから期末までに 7 倍に増加し、再び大きな注目を集めました。RaaS（Ransomware-as-a-Service）の継続的進化、「大物狙い」の傾向、要求を受け入れなければデータを公開するという脅しによって、サイバー犯罪市場が大きく成長し、多額の利益を得られるようになりました。

エクスプロイトが検知される割合の分析

2020 年は、COVID によって「Flatten the curve（曲線を平坦にしよう）」が流行語になりましたが、脆弱性のエクスプロイトにもこれが当てはまります。最後のセクションでは、過去 2 年間の 1,500 件のエクスプロイトの追跡によって明らかになった、エクスプロイトが活動を開始するまでの期間と拡散の範囲について解説します。エクスプロイトが検知される可能性がどの程度あるのか、最後のセクションでご確認ください。

2020 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。第三者機関の調査によれば [2]、フォーティネットはセキュリティデバイス出荷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 年下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、2020 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。

MITRE ATT&CK [3] フレームワークは、攻撃者の TTP（戦術、手法、手順）の分類に基づくサイバー脅威の分析手段として、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 [4]、リソース開発 [5]、初期アクセス [6] 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 侵入防止システム（IPS）[7] のセンサーは、世界中のこの類いの活動の優れた可視性を提供します。優れた可視性を ATT&CK にまで拡大する追加センサーについては後ほど紹介しますが、それに先立ち、2020 年下半期に最も標的にされた 10 位までのテクノロジーを以下に紹介します。

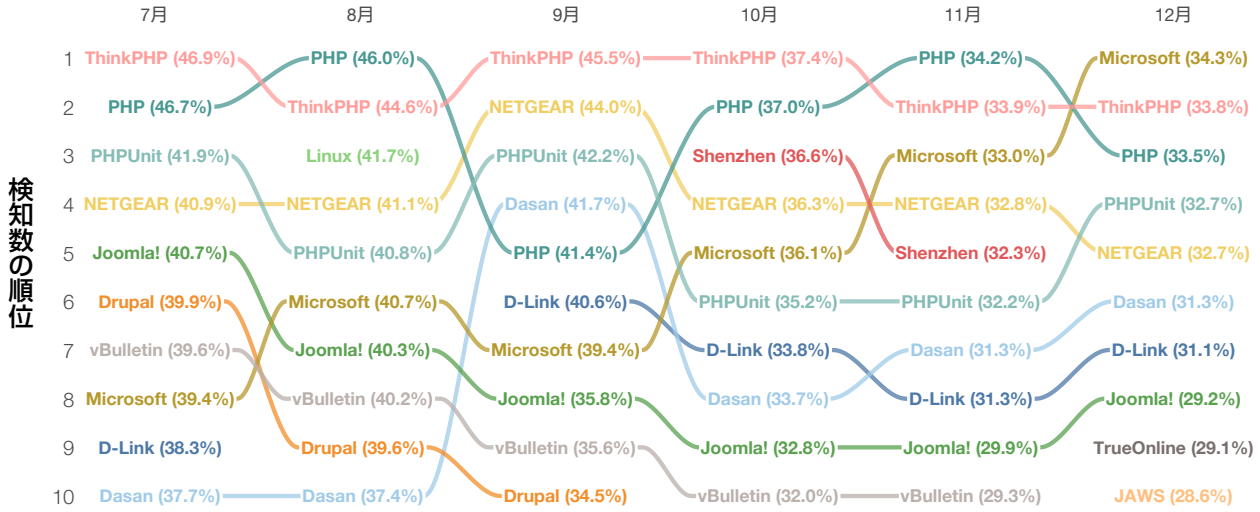

図 1：2020 年下半期に最も多かった IPS 検知数（テクノロジー別）

エクスプロイト検知数の上位は、いずれの月も CMS（コンテンツ管理システム）と IoT（モノのインターネット）に関連するものが占めました。ThinkPHP、Joomla、Drupal、vBulletin などの CMS は、長期にわたりサイバー犯罪者による企業環境へのアクセスを容易にする、狙いやすい標的となってきました。攻撃側に常に狙われる標的であるため、防御側も常に対策を怠らないようする必要があります。

IoT デバイスも、狙いやすい標的の一つです。2020 年上半期のレポートでは、コンシューマー向けのネットワーキングやその他の接続デバイスの脆弱性のエクスプロイト試行の検知が大幅に増加しており、このトレンドが COVID-19 のパンデミックに伴うリモートワークへの移行によるものである可能性があると指摘しました。これらのデバイスの多くが実質的に企業の境界の一部になっていることから、攻撃者がエンタープライズ環境より弱いセキュリティを狙っている可能性があります。つまり、多くの組織にとって不慣れなセキュリティモデルである、感染した環境から従業員が会社のリソースにアクセスしている可能性があります。

ホームオフィスやクラウドなどの新しいエッジ環境が標的にされることは、すでに 2021 年のサイバー脅威予測 [8] の中で予想されていました。このトレンドは、トラストベースのセキュリティへの移行を迫る決定打となる可能性があります。境界の拡大と消滅の進行によって、セキュリティの監視と適用をすべてのデバイスへと移行し、信頼できるデバイスか否かを判断することが緊急の課題となっています。人間の関係はトラストに基づいて築かれますが、IT の関係はゼロトラストに基づくことで間違いなく健全なものになります。フォーティネットによるゼロトラストアクセス [9] の実装によって、ネットワークのあらゆる場所のすべてのデバイスの包括的な可視性と制御が実現します。

最も活発なエクスプロイト活動の追跡は確かに有用ですが、このようなレポートをお読みになっている方にとっては、新たな脅威の監視の方が重要なのかもしれません。図 2 は、2020 年下半期に増加率が最も高かった IPS 検知数をまとめたものです。より正確に言えば、検知したことを報告した組織の割合の観点から、各地域で検知数が大きく増加した上位 5 つを示しています。

	アフリカ	アジア	ヨーロッパ	南米	中東	北米	オセアニア
ELFinder.Connector.Minimal.php.Arbitrary.File.Upload	14.1%	16.5%	17.2%	19.5%	11.8%	13.5%	14.7%
Zpanel.pChart.Information.Disclosure	5.5%					6.5%	6.7%
MS.Windows.CVE-2019-1458.Privilege.Elevation	6.2%	5.6%	5.8%	5.4%	5.9%	4.4%	4.2%
Foxit.Multi.Products.ConvertToPDF.x86.dll.Heap.Buffer.Overflow							5.4%
AlienVault.OSSIM.Framework.Backup.Command.Execution	4.5%			5.6%			4.4%
MS.Windows.TCP.Window.Size.Zero.DoS		3.7%	2.9%	5.1%	4.0%		
Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner		4.2%	2.3%	4.9%	3.8%	2.6%	
OPF.OpenProject.Activities.API.SQL.Injection	4.5%						
ASPXSpy.Webshell		7.9%				3.2%	
AlienVault.OSSIM.av-centerd.Util.pm.Request.Command.Execution			1.7%		1.8%		

図 2：2020 年下半期に各地域で増加率が最大だった IPS 検知

行と列が交差するセルに示した値は、2020 年下半期の検知率です。例えば、ELFinder の任意ファイルアップロードのバグ [10] に対するエクスプロイトは、地域によって異なりますが約 12 ～ 20% の検知率を記録しています。大幅な増加ではないように思えますが、このエクスプロイトは少数の企業での数字です（1% 未満のエクスプロイトでこのレベルに上昇）。増加の要因としては、1）世界中で約 70 万件の導入実績がある WordPress プラグインであること（図 1 の CMS トレンドを参照）、2）リモート攻撃でのエクスプロイトが容易であり、CVSS [11] では満点である 10 点が付けられていることが挙げられます。

もう一つ、世界中で増加率が高かったのは Windows Server と Windows Desktop の複数のバージョンに影響する特権昇格の脆弱性 [12] です。CVE-2019-1458 は、WizardOpium 作戦 [13] や NetWalker ランサムウェア [14] で、北朝鮮のサイバー犯罪者によって 2020 年 1 年間に広範囲で悪用されたことで知られています。図 1 や図 2 の他のエクスプロイトほどの規模ではないものの、このような注目度の高い攻撃に関連していることを考えれば、これらの Windows システムのアップデート [15] が重要であることがわかります。

図 2 のこれ以外で増加率が高かった脆弱性の詳細については、各項に追加されている Threat Encyclopedia [16] のリンクを参考にしてください。このリンクから提供されるコンテキストは、関連する脆弱性を理解し、その脆弱性に対するリスクが自らの組織にあるのか判断する際に役立ちます。多くの場合、影響を受けるデバイスに対してベンダーが推奨しているアクションも記載されています。さらには、フォーティネットをご利用いただいている場合、製品によって保護される範囲や実行されるデフォルトのアクションなどの追加情報も提供しています。

- Zpanel.pChart.Information.Disclosure [17]
- Foxit.Multi.Products.ConvertToPDF.x86.dll.Heap.Buffer.Overflow [18]
- AlienVault.OSSIM.Framework.Backup.Command.Execution [19]
- MS.Windows.TCP.Window.Size.Zero.DoS [20]
- Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner [21]
- OPF.OpenProject.Activities.API.SQL.Injection [22]
- ASPXSpy.Webshell [23]
- AlienVault.OSSIM.av-centerd.Util.pm.Request.Command.Execution [24]

ATT&CK フレームワークの調査を続けたところ、実行 [25] フェーズへと進み、攻撃者が標的とするシステムに不正コードを送り込んで実行しようとすることがわかりました。以上のように、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。図 3 は、2020 年 7 月から 12 月に最も多く検知されたマルウェアの月毎の順位を示しています。

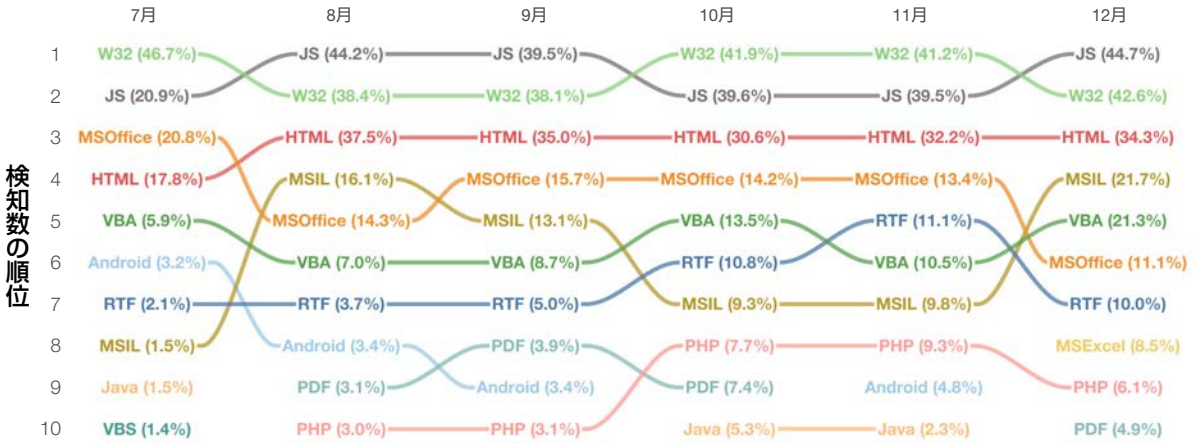

図 3：2020 年下半期に最も検知数が多かったマルウェアのカテゴリ（月別）

図 3 に示すような拡散方法でマルウェアを分類することで、標的のシステムで攻撃者がコードを実行させようとするさまざまな手口に関する実用的インテリジェンスが得られます。具体的な亜種については後ほど説明することにして、ここでは攻撃者が何をどのように標的にするかに注目します。図 3 をこの視点で見ると、いくつかの共通のテーマが見つかります。

マルウェアの作成者が最初に狙うベクトルは、Microsoft プラットフォームです。このプラットフォームには、32 ビット Windows 実行ファイル（W32）、MS Office 製品、Visual Basic（VBA）、Microsoft Intermediate Language（MSIL）が存在します。

図 3 からは、日常業務で作成され利用されることの多い文書を攻撃者が悪用しようとしていることもわかります。これには、前述の MS Office アプリケーションに加えて、RTF や PDF の文書も含まれます。これも以前から指摘されていることですが、一般的なファイル形式や添付ファイルであっても、無条件に信用せずに注意することが重要です。ユーザーの介在やマクロを必要としない脆弱性のエクスプロイトが多い時期には、特に注意が必要です。

図 3 の結果を見ると、Web ブラウザを標的にする攻撃も多いことがわかります。HTML カテゴリには、マルウェアが埋め込まれたフィッシングサイト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。社会不安やグローバルな問題が発生すると、これらの脅威が必然的に増加します。その証拠に、最近の在宅勤務のトレンドによってこれらの脅威が大きな問題になっています。会社のネットワークからブラウザを利用し、Web フィルタリングサービスで保護されていた従業員が保護フィルターの外でブラウザを利用すると、これまで以上に無防備になります。このような保護されない状態を放置すべきではありません。

次に、世界中のセンサーによって検知された具体的なマルウェア亜種について解説します。図 4 は、各地域における、検知された組織の割合が上位のマルウェアの比較です。当然ながら、これらのマルウェアは前述したカテゴリの大部分に分類されます。これらのマルウェアの詳細については、Threat Encyclopedia [26] を参照してください。

	アフリカ	アジア	ヨーロッパ	南米	中東	北米	オセアニア
JS/ScrInject.B!tr	28.0%	15.0%	14.5%	19.1%	21.0%	16.0%	19.1%
JS/Agent.BI!tr	18.9%	8.1%	12.4%	13.1%	11.5%	11.6%	14.4%
MSOffice/CVE_2017_11882.C!exploit	12.3%	12.6%	13.1%	6.7%	12.5%	4.1%	7.5%
HTML/ScrInject.B!tr	14.9%	9.1%	7.4%	5.3%	10.2%	4.3%	8.0%
MSOffice/CVE_2017_11882.B!exploit	8.4%	10.0%	9.9%	5.5%	10.5%	3.3%	6.4%
W32/Agent.OAY!tr	6.8%	12.9%	7.6%	7.2%	5.6%	7.7%	6.6%
MSIL/GenKryptik.EWCI!tr	8.1%	7.7%	8.7%	5.2%	9.2%	3.3%	5.9%
JS/Redirector.IF!tr	7.1%	5.1%	9.2%	4.8%	5.4%	6.9%	9.8%
MSIL/Kryptik.SHS!tr	7.3%	7.6%	6.7%	4.9%	6.9%	2.7%	6.2%
VBA/Agent.SNH!tr.dldr	8.2%	5.0%	8.9%	7.9%	3.4%	3.0%	8.8%
JS/Script.INF!tr	4.8%	4.3%	3.8%	4.8%	6.8%	13.6%	11.4%
JS/Miner.BP!tr	8.8%	5.5%	5.9%	6.9%	5.1%	5.0%	2.9%
VBA/Agent.LXMF!tr	3.8%	4.5%	8.8%	4.5%	3.8%	5.0%	6.7%
RTF/CVE_2017_11882.BX!exploit	4.6%	7.0%	6.7%	4.7%	7.7%	1.8%	4.9%
JS/Agent.79EE!tr	6.9%	9.7%	3.4%	6.5%	4.0%	2.8%	3.2%

図 4：2020 年下半期に最も検知数が多かったマルウェア（地域別）

シグネチャ名の長さと形式からわかるように、CVE-2017-11882 [27] を悪用するマルウェアの 3 つの亜種が上位に入りました。米国のサイバーセキュリティ・インフラストラクチャ庁（CISA）によると、これは国家が支援するサイバー犯罪者が悪用する 10 位までの脆弱性 [28] の一つです。Cobalt Group、Loki、Ursnif、Zbot、Fareit/Pony は、CVE-2017-11882 の悪用で知られているサイバー犯罪者とマルウェアの一例で、COVID に乗じた複数の攻撃 [29] でも使用されました。したがって、これらのマルウェアを考慮して対策を講じることが重要です。

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アクティビティ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感染後のアクティビティを表します。ATT&CK の用語では、ボットネットトラフィックの多くは、感染システムがリモートの不正ホストと通信してさらなる指示を求めるコマンド & コントロール（C2）[30] 活動です。図 5 に、2020 年に最も多く検知されたマルウェアの月毎の検知率を示します。図 5 のパーセンテージは、ボットネットを検知した組織の中での数字であり、これらの組織は全企業の約 1% に過ぎない点に注意してください。つまり、「何らかのボットネットが 12 月に検知された企業は全体の 1% であり、それらの企業の約 75% で Mirai が検知された」ということです。

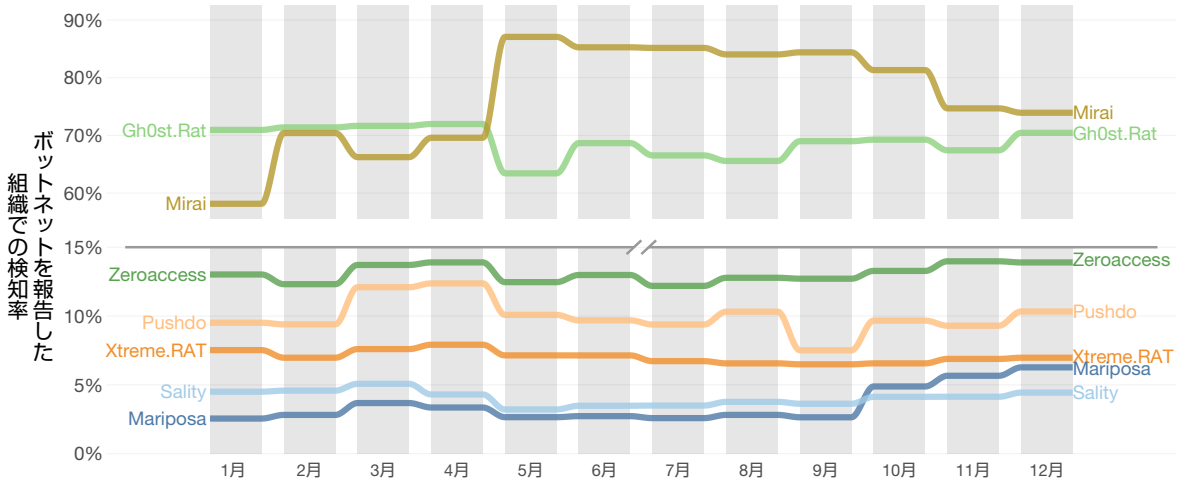

図 5：2020 年に最も多かったボットネット検知数（月別）

2020 年上半期のレポートでは、Mirai ボットネットに関連した活動が急増したとお伝えしました。このトレンドは、COVID-19 のパンデミックをきっかけに在宅勤務の従業員が使用する一般ユーザー向けのネットワークやデバイスをサイバー犯罪者が悪用し、企業の境界を突破するバックドアを探していることを示している可能性があります。Mirai が引き続きボットネットの首位に君臨した一方で、図 1 に示したように IoT 関連の IPS 検知が上位に入ったことは、このトレンドが 2020 年上半期以降も続いていることを示しています。

つまり、5 月のピークを境に Mirai の検知数が低下し始めたのです。この事実から多くを推測するのは危険かもしれませんが、楽観的な見方をすれば、2021 年に入って COVID のピークが過ぎ、「オールドノーマル」に戻る兆しであると言えるのではないでしょうか。「ニューノーマル」が長く続いたことを思えば、これは歓迎すべき変化です。

2020 年下半期の注目すべき出来事

業界を震撼させた SolarWinds

2020 年の最終四半期に大きく報道されたのが、国家が支援する攻撃者が SUNBURST/Solorigate と呼ばれるバックドアを SolarWinds の Orion [31] ネットワーク管理ソフトウェアの正規のアップデートに隠し、世界中の多数の組織に配布していたというニュースです。業界はこのニュースに震撼し、デジタルサプライチェーン [32] を標的とする高度な脅威に対する企業の防御の弱点が露呈しました。その被害者には、複数の米国政府機関に加えて、Microsoft やセキュリティベンダーの FireEye などの大手テクノロジー企業も含まれていました。直接の被害者だけでなく、パートナーやサプライヤーの（長く連なる）チェーンに存在する脆弱なリンクによって、企業の防御が脅かされる可能性があることを肝に銘じる必要があります。

攻撃者は、この攻撃を成功させるために SolarWinds のビルドシステムに侵入し、Orion ネットワーク管理フレームワークのデジタル署名されたコンポーネントにバックドアを挿入しました。このマルウェアは、2 週間の休眠期間の後、特定のデータの収集と転送、偵察の実行、システムサービスの停止などの不正活動のコマンドを受け取っていました。ロシアが関係しているとされる攻撃者は、標的とするシステムでバックドアを使用し、カスタマイズした Cobalt Strike Beacon 攻撃キットなど追加のマルウェアを送り込み、ラテラルムーブメント（水平移動）を可能にしていました。

攻撃を分析した結果、この攻撃者は SolarWinds の最初の侵害から時間をかけて綿密かつ密かに活動を続け、マルウェアの送り込み、第二段階のペイロードの展開、コマンド & コントロール通信を実行することがわかりました。この攻撃者は、信頼できるベンダーが提供する信頼性の高いネットワーク管理ツールにマルウェアを隠すことで、世界最大規模の組織のネットワークで高い特権付きアクセスを取得することに成功したのです。

このマルウェアは、正規の OIP（Orion Improvement Program）プロトコルを利用し、結果を Orion のプラグインファイルに保存することで検知を回避していました。また、少数のマルウェアツールを使用して不正活動を実行していました。不正取得した認証情報をリモートアクセスの手段として利用し、セキュリティ対策として C2 サーバーに被害者の国内にある IP アドレスを使用していました。また、被害者の SAML（Security Assertion Markup Language）[33] トークンで署名した証明書へのアクセスを取得してトークンを偽造し、オンプレミスやクラウドの環境にあるリソースに侵入していたのです。

この攻撃によって、APT（高度な持続的脅威）攻撃者に対する業界の防御のいくつもの弱点が明らかになりました。ほとんどのアンチマルウェアツールや EDR（Endpoint Detection and Response）ツールは、侵害の発見後にシグネチャが開発されて IOC（Indicators of Compromise：侵害指標）が公開されるまで、初期段階のバックドアや不正活動を検知できませんでした。ただし、これらのツールに非があるわけではなく、本来そのように設計されているものなのです。SolarWinds の場合も、数ヵ月にわたり検知されることもなく、世界中の顧客に有害なアップデートを配布していました。

この攻撃は、第 2 段階のペイロードを被害者に合わせてカスタマイズすることで、IOC ベースの検知のメカニズムを回避できることを証明しました。「Golden SAML」と呼ばれる、以前から知られていた手法で SAML 認証トークンを偽造することで、侵害されたネットワークで検知されることなくアクセスを維持できることが実証されました。

この攻撃が明らかになると、Microsoft や FireEye などの被害を受けたセキュリティベンダーから、さまざまな情報が次々と公開されました。FortiGuard Labs は、この新たなインテリジェンスを注意深く監視し、今後の関連する活動を検知する IOC の作成に使用しました。すると予想通り、これらの IOC と一致する接続が**大幅に**増加していることがわかりました。FortiGuard Labs は最終的に、SolarWinds に関連する 300,000 以上のインフラストラクチャへの接続を検知しました。

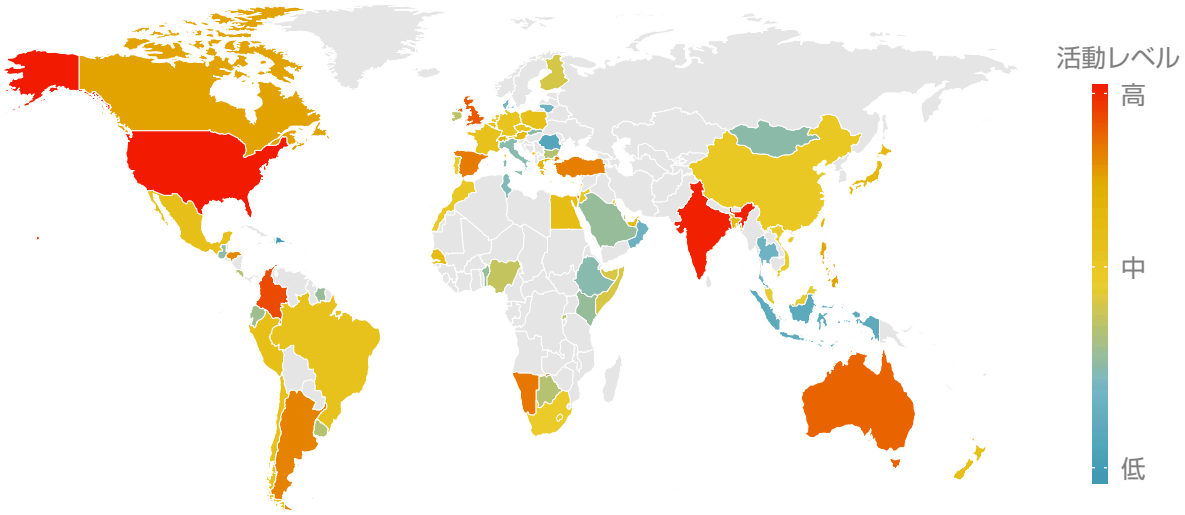

図 6：2020 年 12 月に検知された、SUNBURST に関連するインターネットインフラストラクチャとの通信

インテリジェンスによって多くの活動が明らかになっただけでなく、SolarWinds 攻撃を継続的に追跡することで、この攻撃が世界規模で進行していることが明らかになりました。図 6 に示すように、「ファイブアイズ」[34] における不正 IOC と一致するトラフィックの割合が特に高いことがわかっています。ロシアという例外はあるものの、「間接的影響」あるいは日和見主義的に標的になる可能性を示す証拠によって再認識させられるのは、今日のサプライチェーン攻撃の影響は広範囲に及ぶという事実です。

SolarWinds 攻撃はロシア政府が支援する集団によるものだとする説もありますが、攻撃を分析した複数のセキュリティベンダーは現段階で特定の国への帰属を示す証拠を見つけておらず、その説に同意もしていません。この攻撃の多くの被害者の一つである FireEye は、攻撃はこれまでに特定されたことのない集団によるものであるとし、「UNC2452」という名前で今も追跡を続けています。Volexity はその一方で、SolarWinds 攻撃が「Dark Halo」と呼ばれる集団によるものであることを示す証拠があると述べています。

多くのセキュリティ研究者は、いずれの国が支援しているかに関係なく、UNC2452/Dark Halo とそのキャンペーンを、過去 10 年以上の間に観測された最も重大かつ巧妙な攻撃の一つだと評しています。では、この攻撃をどのように防ぐべきなのでしょうか。FortiGuard Labs の研究者は、最新のインテリジェンスを使用して常にセキュリティ ファブリック [35] のコンポーネントをアップデートしているため、フォーティネットのお客様はこの攻撃に関連する脅威の検知と減災が可能です。

さらには、最初の手順としてサプライチェーンのリスク管理計画を作成し、依存関係と攻撃のリスクに関するポリシーと手順を確立します。この計画では、設計、製造、生産、配布、取得、インストール、運用、保守、廃止を含む、システム開発のライフサイクル全体の主なリスクを文書化することが重要です。より戦術的なレベルでは、アンチウイルスと IPS のシグネチャをアップデートし、既知の SolarWinds の脆弱性がすべて修復されていることを確認するよう、すべての組織に推奨します。

これは、セキュリティ部門のリーダーがタイムリーな脅威インテリジェンスを活用して常に状況を判断することの重要性を認識する良い機会でもあり、そうすることで戦略や防御の優先順位を有事に素早く変更することができます。SolarWinds に類似する次の攻撃を防ぐことのできる保証はありませんが、攻撃を完全に食い止めることの次に有効な方法は、攻撃に直面した際にインテリジェンスをすぐに活用できるようにしておくことです。

SolarWinds 以外の APT 集団

SolarWinds の背後にいる犯罪者が 2020 年下半期の主役だったかもしれませんが、他の犯罪者も眠っていたわけではありません。それらの犯罪集団を以下にまとめて紹介し、防御のヒントを提示します。

多くの APT 集団が、2020 年下半期も COVID-19 の危機をさまざまな方法で悪用し続けました。特に多かったのが、大量の個人情報の収集、知的財産の窃盗、APT 集団にとって国家的に重要なインテリジェンスの取得を目的とする攻撃で、これは米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）が 5 月に発表した勧告で [36] 指摘されたとおりです。ワクチン研究やパンデミック関連の国内外の医療政策の開発など、COVID-19 関連の活動に携わる組織を標的にする APT 活動も増加し、政府機関、製薬会社、大学、医学研究機関などが標的になりました。

2020 年下半期に追跡した犯罪集団の中には、これ以外の活動に関与しているものもありました。その一つである BeagleBoyz [37] は比較的新しい北朝鮮の APT 集団で、米国の法執行機関が「FASTCash 2.0」と名付けた ATM 現金引き出しスキームを使って金融機関を攻撃したことがわかっています。ソーシャルエンジニアリング、スピアフィッシング、水飲み場攻撃などを主な手口とするこの集団は、北朝鮮の悪名高い Lazarus/HIDDEN COBRA APT に関連する活動に関与したとされています。米国の法的機関は、BeagleBoyz が世界中の金融機関から 20 億ドルもの金銭の不正取得を試みたと推定しています。

Lazarus Group [38] については、昨年 8 月に暗号通貨関連の組織を攻撃したことが確認されています。この攻撃では、標的とされた組織の人物の LinkedIn アカウントにフィッシングの文書が送信されました。ブロックチェーン企業の求人広告に見せかけたその文書には、標的とする環境にマルウェアを拡散する仕掛けが組み込まれていました。

MUMMY SPIDER [39] は、大量の Emotet トロイの木馬 [40] を送り出した APT 集団で、2020 年後半にこのマルウェアの別バージョンが確認されたことで再び注目されました。E メール経由で拡散する新バージョンは、E メールアドレスの不正取得、スパムの送信、アカウント認証情報の不正取得、ローカルネットワークへの拡散を目的とするものでした。2020 年下半期、FortiGuard Labs は MUMMY SPIDER と Emotet の新しいバージョンに関連する活動が着実に増加していることを確認しました。おそらくこれが一つのきっかけとなり、ユーロポール（欧州刑事警察機構）が主導する [41] コンソーシアムが 2020 年下半期に Emotet ボットネット解体に乗り出しました。

8 月には、ロシアの有名な Fancy Bear（別名 Sofacy/APT28）[42] が、Drovorub [43] と呼ばれる Linux ベースの厄介なマルウェアを標的のシステムに拡散していることが確認されました。複数のコンポーネントで構成されるこのマルウェアは、ロシアの軍事情報機関が使用する目的で開発されたと言われており、攻撃者はリモートでの感染システムの完全制御や任意コードの実行が可能になります。

2020 年後半に上記以外で確認された APT の多くは、一部を除きこれまでと同様の目的で活動するものでした。図 7 は、FortiGuard Labs が収集したインテリジェンスによって明らかになった、APT 集団に関連する IOC への接続数の変化と国別の内訳を示しています。ここには、最も活動が活発だった 6 つの APT（Turla、Fancy Bear、Lazarus、MuddyWater、TA505、OilRig）に加えて、2020 年下半期に急上昇した 2 つの集団（Kimsuky、Promethium）も含まれています。

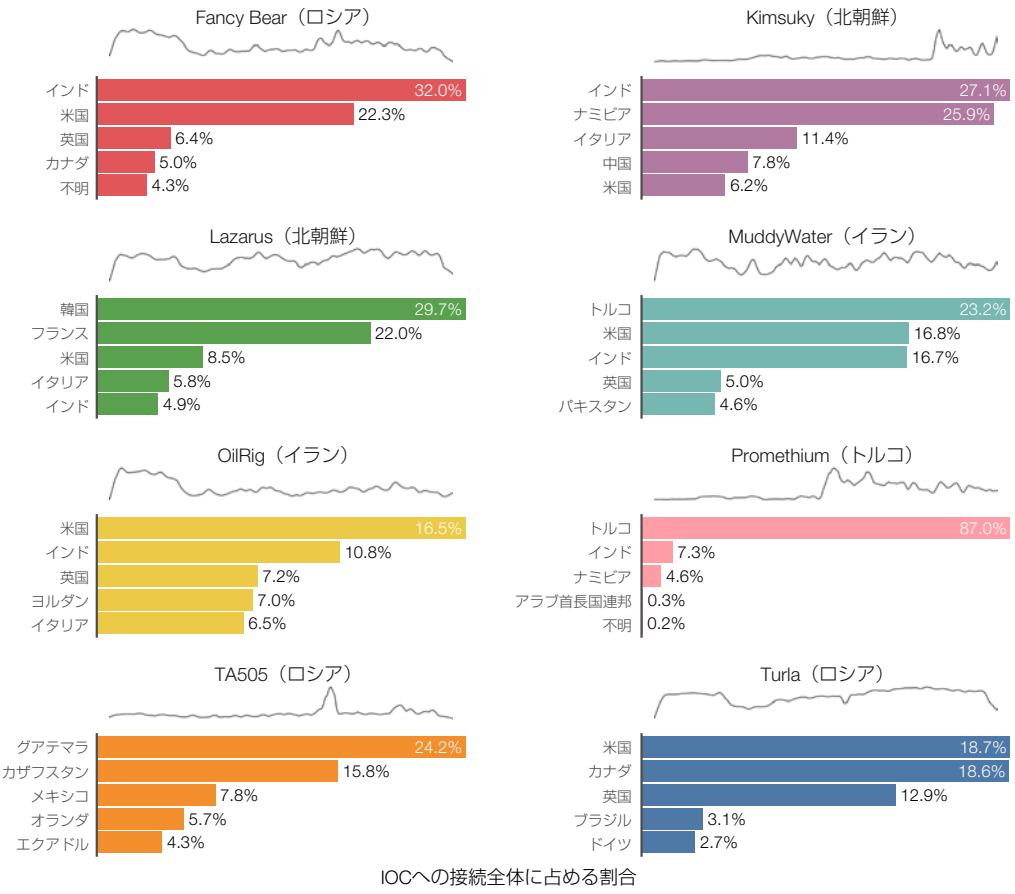

図 7：2020 年下半期に検知された、一部の APT 集団に関連する IOC への接続の起源

図 7 に示した集団の中で、Fancy Bear と Lazarus についてはすでに説明したことがあるため、2020 年下半期の APT の解説では、それ以外の集団をいくつか取り上げます。

Turla（別名 Venomous Bear、Waterbug）[44] は、ロシアを拠点として 20 年以上にわたって活動を続ける集団です。この集団は、主として世界中の政府機関や大使館に対するスパイ活動を行ってきたとされており、2020 年下半期に我々が記録した Turla 関連インフラストラクチャへの接続数は、他のいずれの APT 集団の接続数よりも多くなりました。

MuddyWater [45] は、これまでに中東の通信や公的サービス、石油といった分野を標的にしてきましたが、その以外の分野にも手を広げるようになり、この 1 年ほどで攻撃の範囲と能力が拡大 [46] しました。

TA505 [47] は、スパム攻撃、金融機関を標的にするトロイの木馬（Dridex）、その他の金銭的な動機による攻撃を仕掛ける、ロシアを起源とする集団です。この集団のメンバーとされる 2 名が 2019 年末に起訴された [48] 後、2020 年になって活動を再開 [49] し、マルウェアを拡散したことがわかっています。

Promethium（別名 StrongPity）[50] は、トルコを起源としているとされ 2002 年頃から活動を続けている集団で、政治関連の組織を標的にしてきました。検知数が急増して 7 月にピークを迎えましたが、高い状態が年末まで続きました。他の調査機関 [51] も、2020 年に検知数が急増したと指摘しています。

Kimsuky [52] は、北朝鮮政府と関連性があり 10 年以上も活動を続けている集団です。7 ～ 10 月は活動レベルが低い状態が続きましたが、11 月に入って大幅に増加しました。韓国の組織が主な標的であるため、インドとナミビアでの活動は注目に値します。

OilRig [53] はイランを起源とすると思われる集団で、目標とする標的に侵入する手段として、大規模なサプライチェーンの小規模あるいは脆弱なメンバーを攻撃することで知られています。中東や国外の組織に対するさまざまな攻撃への関与が指摘されており、2020 年下半期には RDAT [54] と呼ばれる革新的なバックドアツールをマルウェアに追加しました。

サイバー犯罪者の新たな手口を知ることは、単なる知識の習得にとどまりません。敵を知り、敵の TTP を深く理解することで、効果的な防御が可能になります。執拗な攻撃者は何らかの方法で侵入を果たしますが、防御に成功する組織は直ちにそれを発見し、一掃することができます。自らの脅威プロファイルを可視化し、関連する最新の TTP を重点的に知ることが重要です。無知は攻撃側の味方であり、防御側の味方ではありません。

悪質化するランサムウェア

ランサムウェアは、2020 年上半期と同様に下半期も世界中の組織を悩ませ続けました。我々のデータからは、ランサムウェア全体の活動が 2020 年上半期よりも大幅に増加していることが明らかになりました。FortiGuard Labs が一度はランサムウェアとして分類したすべてのシグネチャの活動を分析したところ、2020 年 12 月のランサムウェアの活動が 7 月と比べて 7 倍に増加したことがわかりました（図 8 参照）。2020 年下半期に追跡したランサムウェアで最も活発だった亜種としては、Egregor [55]、Ryuk [56]、Conti、Thanos [57]、Ragnar、WastedLocker、Phobos/EKING [58]、BazarLoader が挙げられます。フォーティネットのデバイスにおける検知数に差はあるものの、これらの亜種にはこの期間に活動が増加したという共通のトレンドがあります（図 9 参照）。

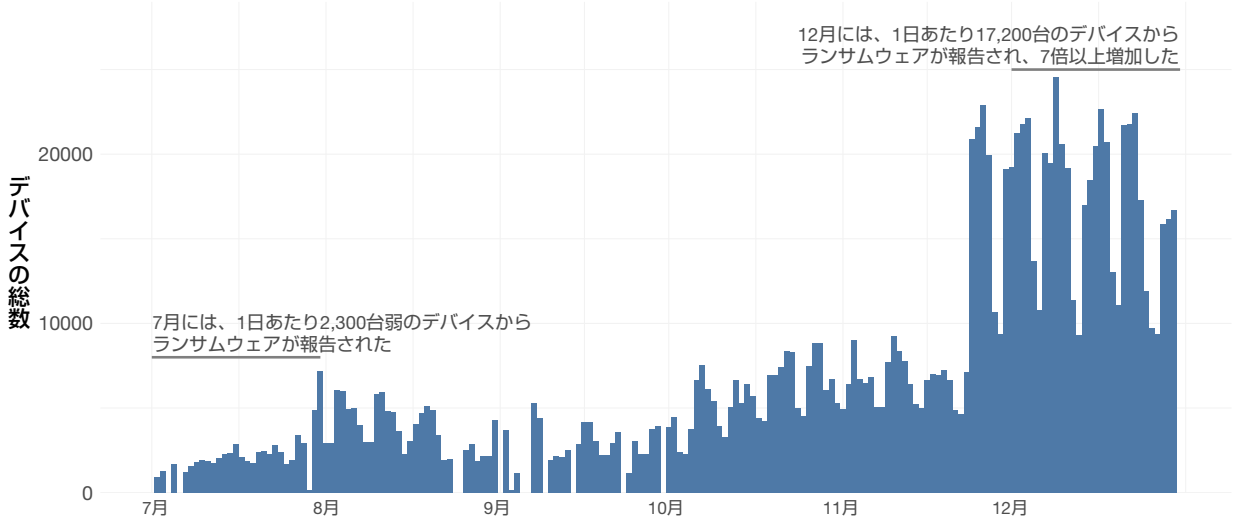

図 8：2020 年下半期にランサムウェア亜種を検知したデバイスの一日あたりの数

今日では極めて重要になっている、ランサムウェアトレンドの追跡を続けるいずれの組織にとっても、この半年間に活動が増加したことに驚きはありません。攻撃者が気付いたのは、クリティカルシステムを暗号化し、復号鍵と引き換えに身代金を要求することが、組織の規模や業種に関係なく金銭を手に入れる比較的簡単な方法だということです。標的を限定し、強引に身代金を要求するこのようなランサムウェア攻撃は、最近では「大物狙い」と呼ばれるようになりました。ランサムウェアを仕掛ける犯罪者が、2020 年を通じてこのような方法で金銭を手に入れるようになったことから考えて、このトレンドがすぐに消滅することはないでしょう。

多くの攻撃者が、COVID-19 パンデミックによる混乱に乗じて医療機関を中心にランサムウェア攻撃を次々と仕掛けました。米国のサイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、保健福祉省、FBI が 10 月に共同で発表した勧告 [59] では、米国の病院や医療サービス機関に対し、2020 年下半期にフォーティネットが追跡してきた TrickBot と BazarLoader [60] マルウェアに関連するランサムウェア活動が増加していると警告されています。2020 年下半期にランサムウェア攻撃の標的となったこれ以外の業種としては、プロフェッショナルサービスやコンシューマー向けサービスの企業、公的機関、金融サービス企業などが挙げられます。

FortiGuard Labs などの団体が 2020 年下半期に観測したランサムウェア活動には、特徴と言えるトレンドがいくつか見つかっています。最も厄介だったのは、データの流出を伴うランサムウェア攻撃が着実に増加し、身代金の支払いに応じなければデータを公開すると脅すようになったことです。ランサムウェア攻撃における追加手段としてデータ不正取得を利用することは、2020 年初めには新しい攻撃戦術の一つに過ぎませんでしたが、年末までには攻撃の大部分を占めるようになりました。

Sodinokibi、Ryuk、Egregor、Conti などの主要なランサムウェア亜種の大半に、昨年には標準機能の一部としてデータを持ち出す機能が組み込まれました。報告されたインシデントの中には、（ときには偽の）攻撃者がデータを手に入れたと主張し、被害者を脅して身代金を要求するものもありました。多くの場合、被害者が盗難されたデータの削除と引き換えに身代金を払うと、攻撃者は約束を反故にしてデータを漏洩したり、販売したりします。このトレンドは、データの確実なバックアップだけではランサムウェアの要求に対する十分な保護とは言えなくなっていることを意味します。

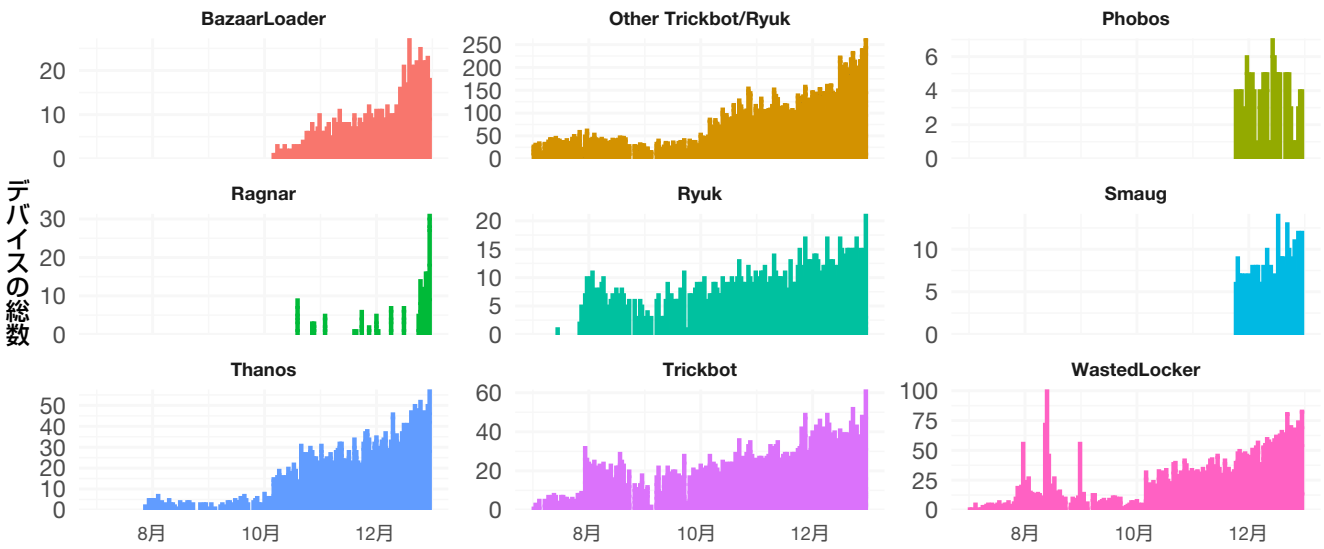

図 9：2020 年下半期に注目された一部のランサムウェア亜種の毎日の検知数

アンダーグラウンドマーケットに出回る RaaS（Ransomware-as-a-Service）オプションの着実な増加も、2020 年下半期の多くのランサムウェア活動の追い風となりました。これらのサービスを利用すれば、スキルやリソースの少ない犯罪者であっても容易に攻撃を開始できます。我々が追跡していた、RaaS を提供するサイバー犯罪者は、Windows、MacOS、Linux のプラットフォームに展開できるランサムウェアを提供する、SMAUG と呼ばれるサービスであることがわかりました。限定された一部のメンバーだけに提供される多くの RaaS とは異なり、昨年春に初めて確認された SMAUG は、年末までには購入を希望する犯罪者に制限なくこのサービスを提供するようになりました。これ以外の有名な RaaS としては、Phobos、Sodinokibi、Conti、Egregor などがあります。

これらの最新のランサムウェアに資金提供したくないのであれば、システムを常にロックしバックアップすることで資金の流れを断ち切ることが重要です。ランサムウェアが使用する主な戦術としては、他の多くの脅威と同様、フィッシングメール、ソフトウェアの脆弱性のエクスプロイト、RDP（Remote Desktop Protocol）などの公開サービスの悪用などが挙げられます。技術的な制御の強化だけでなく、身代金の要求に対する会社としての方針や手順を作成、あるいは見直して、場当たり的な判断を回避することが重要です。ランサムウェアの脅威の減災にあたってのこれ以外の戦略については、こちらの記事で 15 の対策[61] を参照してください。

攻撃までにどの程度の時間がかかるのか

エクスプロイトを企てる多くのサイバー脅威から会社の資産を保護する立場にある方は、このような質問に対する明確な答えが見つからず、フラストレーションを感じた経験があるのではないでしょうか。そのようなフラストレーションは当然のことです。なぜならば、その脆弱性を標的にする次の攻撃の被害が自らの資産に及ぶまでの期間を知らなければ、脆弱性の修復作業に優先度を付けたり、リスクを最小化するための制御を導入することができないからです。すなわち、今すぐその脆弱性を修正すべきか、あるいはすぐに悪用される可能性が高く緊急性の高い他の問題を優先するべきか、その判断は困難です。

なぜなら、正しい判断に必要な規模のデータがある組織は稀であるからです。そのような大量のデータを持つ組織の一つであるフォーティネットの FortiGuard Labs は、他の組織とも協力し、判断に必要な情報を提供しています。フォーティネットは、脆弱性が悪用される時期を予測するためのオープンモデルである ESPP（Exploit Prediction Scoring System）[62] の開発に参画しました。フォーティネットのデータは、Cyentia Institute と Kenna Security による調査にも採用[63] され、脆弱性の修復とエクスプロイトのタイムラインの測定に利用されました。この取り組みの一部を以下に紹介します。

図 10 は、過去 2 年間に活動が検知された 1,500 以上のエクスプロイトの変化を図式化したものです。各ラインは個々のエクスプロイトを表し、X 軸はシグネチャ作成した時点から経過した時間を、Y 軸は組織で検知される可能性を示しています。つまり、それぞれの曲線は、その時点でエクスプロイトが検知される可能性がある事を示しています。少数の例に注目する目的で大半の曲線をグレーで表示しましたが、拡散の時系列的変化がエクスプロイトによって大きく異なるのは明らかです。つまり、このセクションの最初に提議した「攻撃までの時間」に関する質問の答えは、「エクスプロイトによって異なる」ということになります。

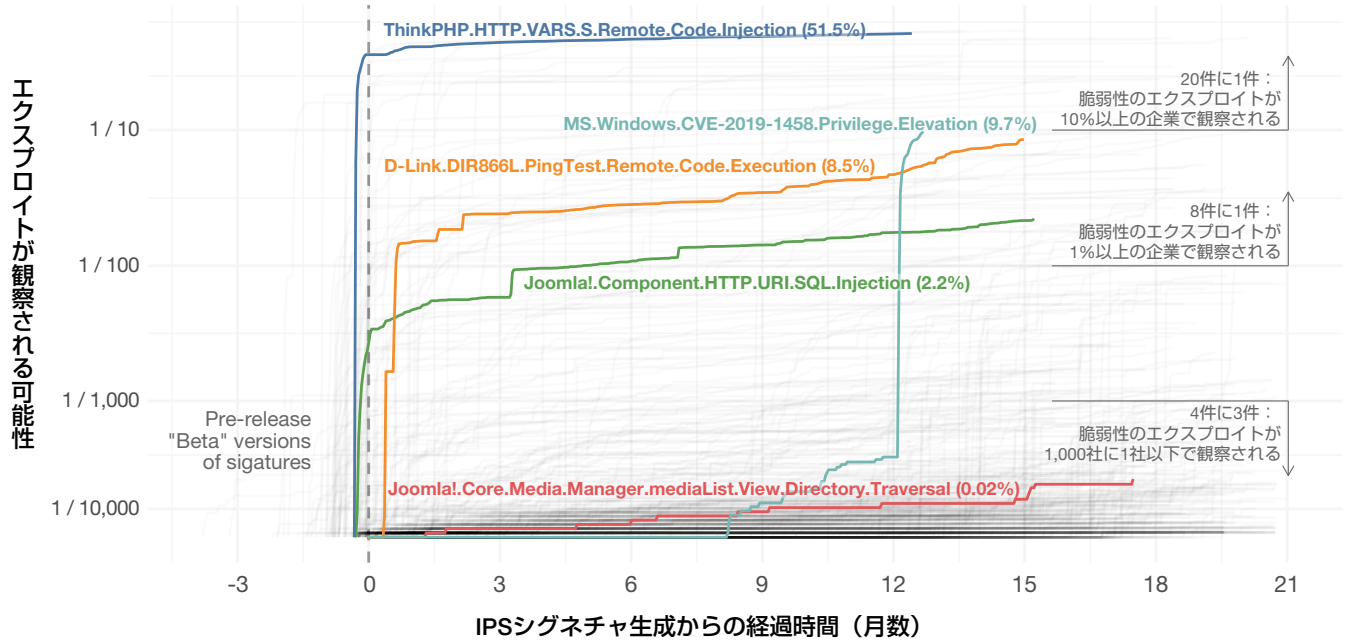

図 10：活動中の 1,500 以上の脆弱性エクスプロイトの検知の可能性

十分納得できる答えとは言えないため、役に立つ統計を図 10 のデータから探してみましょう。これらの大きく異なる複数の曲線から得られる大きなヒントは、ほとんどのエクスプロイトが組織に対して使用される可能性は低いということです（Y 軸）。図 1 に戻って最も標的とされることが多いテクノロジーに注目すると、エクスプロイトは 3 分の 1 以上の組織を繰り返し攻撃すると結論付けられるかもしれません。ただし、これらの IPS 検知によって明らかになったのは、活動中のエクスプロイトが広範囲で観察される脆弱性は極めて少数で、ほとんどが底辺に近い場所で推移していることです。過去 2 年間にフォーティネットのセンサーが記録したすべてのエクスプロイトで 10% 以上の組織で検知されたものは、わずか 5% でした。4 つのうち 3 つのエクスプロイトは、検知された割合が 1,000 社に 1 社以下でした。

図 10 のもう一つの重要なヒントは、攻撃が拡大する速度に大きな差があるということです。ThinkPHP コードインジェクションの脆弱性を標的にする攻撃のように、製品の検知シグネチャが展開された直後（場合によっては展開される前）に検知数が急上昇するものもあれば、Joomla Media Manager に対するエクスプロイトのように、少数の組織に拡散する状態が続くものもあります。さらには、CVE-2019-1458 に対するエクスプロイトのように、最初は停滞しているものの約 12 ヵ月後に突如として急上昇するものもあります。

しかしながら、ThinkPHP や Joomla、あるいは CVE-2019-1458 や図 10 に示した他の曲線のように変化するエクスプロイトが一般的だと言えるのでしょうか？ この質問の答えは、前回のように「エクスプロイトによって異なる」ということにはなりません。図 11 は実際の統計であるため、最初の疑問に対する答えを提示してくれます。

観測の可能性 ...

シグネチャ作成からの経過時間	0.1% 以上の企業	1.0% 以上の企業	10.0% 以上の企業
1 年	17.1% のエクスプロイト	9.1% のエクスプロイト	3.4% のエクスプロイト
1 ヵ月	10.7% のエクスプロイト	5.9% のエクスプロイト	2.2% のエクスプロイト
0 日	8.1% のエクスプロイト	3.4% のエクスプロイト	1.4% のエクスプロイト

図 11：活動中の 1,500 以上の脆弱性エクスプロイトの検知率と拡散の統計

すべての条件が平等で脆弱性を無作為に選んだ場合、どの組織も 1,000 分の 1 の確率で攻撃されるというデータがあると言われています。最初の 1 ヵ月に 1% 以上の企業で観察されたエクスプロイトはわずか 6% で、1 年後も 91% のエクスプロイトはその 1% のしきい値を超えることはありませんでした。論理的に考えれば、その時期にエクスプロイトが全体の 10% で検知されるのはさらに稀なことです。結論として、ほとんどのエクスプロイトはそれほど短時間で拡散するわけではありません。

攻撃の標的になる危険性という点から見れば、この統計が安心材料と言えるかもしれませんが、一般的にサイバーセキュリティでは中間、あるいは平均のシナリオではなく、究極のシナリオを想定します。さらには、前段の冒頭の「すべてが平等」という仮説が自分の組織に当てはまるとも限りません。何らかの理由で、日常的に標的とされる（あるいは不運な）少数の組織の一つになってしまう可能性もあります。そのような場合は、統計は不利に転じるでしょう。

「備えあれば憂いなし」という古いことわざの方が有益だというわけです。そのエクスプロイトが見つからないという確信がない限り、自社は図 10 の曲線の一番上にいると考えた方が安全です。既知のエクスプロイトが存在する脆弱性の修復作業を優先し、その中でも活動が最も活発で短時間で拡散するものを優先します。データによって明らかになるのは、大量に存在する脆弱性のほんの一部です。だからこそ、図 1 や図 2 に示したような情報は、リスク減災にあたって極めて高い価値があるのです。

これらのデータとこの脅威レポートの実用的インテリジェンスを参考にして行動していただくことで、お客様が最も重要な業務に集中できるようになることを願っています。2021 年上半期のレポートでまたお会いしましょう。

1 「What Does 'Pwn' Mean?」、Merriam-Webster（英語）：https://www.merriam-webster.com/words-at-play/pwn-what-it-means-and-how-you-say-it
2 「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）
3 「MITRE ATT&CK」、MITRE ATT&CK（英語）：https://attack.mitre.org/
4 「Reconnaissance」、MITRE ATT&CK（英語）：https://attack.mitre.org/tactics/TA0043/
5 「Resource Development」、MITRE ATT&CK（英語）：https://attack.mitre.org/tactics/TA0042/
6 「Initial Access」、MITRE ATT&CK（英語）：https://attack.mitre.org/tactics/TA0001/
7 「FortiGate 侵入防止システム（IPS）」、フォーティネットジャパン：https://www.fortinet.com/jp/products/ips
8 「2021 年のサイバー脅威予測」、フォーティネットジャパン、2020 年 12 月：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/ja_jp/WP-Cyber-Threat-Predictions-for-2021.pdf
9 「ゼロトラストアクセス」、フォーティネットジャパン：https://www.fortinet.com/jp/solutions/enterprise-midsize-business/network-access
10 「ELFinder.Connector.Minimal.php.Arbitrary.File.Upload」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/43150/elfinder-connector-minimal-php-arbitrary-file-upload
11 「CVSS」、National Institute of Standards and Technology（英語）：https://nvd.nist.gov/vuln-metrics/cvss
12 「MS.Windows.CVE-2019-1458.Privilege.Elevation」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/48581/ms-windows-cve-2019-1458-privilege-elevation
13 「Windows, Chrome Zero-Days Chained in Operation WizardOpium Attacks」、Lawrence Abrams 著、Bleeping Computer、2019 年 12 月 10 日（英語）：https://www.bleepingcomputer.com/news/security/windows-chrome-zero-days-chained-in-operation-wizardopium-attacks/
14 「Arrest, Seizures Tied to Netwalker Ransomware」、Krebs on Security（英語）：https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware/
15 「Win32k Elevation of Privilege Vulnerability」、Microsoft、2019 年 12 月 10 日（英語）：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2019-1458
16 「Threat Encyclopedia」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia
17 「Zpanel.pChart.Information.Disclosure」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/41572/zpanel-pchart-information-disclosure
18 「Foxit.Multi.Products.ConvertToPDF.x86.dll.Heap.Buffer.Overflow」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/41142/foxit-multi-products-converttopdf-x86-dll-heap-buffer-overflow
19 「AlienVault.OSSIM.Framework.Backup.Command.Execution」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/39417/alienvault-ossim-framework-backup-command-execution
20 「MS.Windows.TCP.Window.Size.Zero.DoS」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/17714/ms-windows-tcp-window-size-zero-dos
21 「Wind.River.VxWorks.WDB.Debug.Service.Version.Number.Scanner」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/44135/wind-river-vxworks-wdb-debug-service-version-number-scanner
22 「OPF.OpenProject.Activities.API.SQL.Injection」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/47960/opf-openproject-activities-api-sql-injection
23 「ASPXSpy.Webshell」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/15558/aspxspy-webshell
24 「AlienVault.OSSIM.av-centerd.Util.pm.Request.Command.Execution」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia/ips/38915/alienvault-ossim-av-centerd-util-pm-request-command-execution
25 「Execution」、MITRE ATT&CK（英語）：https://attack.mitre.org/tactics/TA0002/
26 「Threat Encyclopedia」、FortiGuard Labs（英語）：https://www.fortiguard.com/encyclopedia
27 「CVE-2017-11882」、CVE（英語）：https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11882
28 「Top 10 Routinely Exploited Vulnerabilities」、Cybersecurity & Infrastructure Security Agency、2020 年 5 月 12 日（英語）：https://us-cert.cisa.gov/ncas/alerts/aa20-133a
29 「Scammers Using COVID-19/Coronavirus Lure to Target Medical Suppliers」、Val Saengphaibul 著、フォーティネットブログ、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
30 「Command and Control」、MITRE ATT&CK（英語）：https://attack.mitre.org/tactics/TA0011/
31 「Supply Chain Attack on SolarWinds Orion Platform Affecting Multiple Organizations Worldwide (APT29)」、FortiGuard Labs（英語）：https://www.fortiguard.com/threat-signal-report/3770/supply-chain-attack-on-solarwinds-orion-platform-affecting-multiple-organizations-worldwide-apt29
32 「Securing Your Supply Chain: Where Is The Weakest Link?」、Philip Quade 著、Forbes、2019 年 1 月 30 日（英語）：https://www.forbes.com/sites/forbestechcouncil/2019/01/30/securing-your-supply-chain-where-is-the-weakest-link/?sh=1009187b5403
33 「Security Assertion Markup Language」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
34 「Five Eyes」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Five_Eyes
35 「セキュリティ ファブリック」、フォーティネットジャパン：https://www.fortinet.com/jp/solutions/enterprise-midsize-business/security-fabric
36 「Top 10 Routinely Exploited Vulnerabilities」、Cybersecurity & Infrastructure Security Agency、2020 年 5 月 12 日（英語）：https://us-cert.cisa.gov/ncas/alerts/aa20-133a
37 「Joint Technical Alert - "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks"」、Val Saengphaibul 著、フォーティネットブログ、2020 年 8 月 27 日（英語）：https://www.fortinet.com/blog/threat-research/joint-technical-alert-fastcash-2-0-north-koreas-beagleboyz-robbing-banks
38 「FortiGuard Threat Intelligence Brief」、FortiGuard Labs、2020 年 8 月 28 日（英語）：https://www.fortiguard.com/resources/threat-brief/2020/08/28/fortiguard-threat-intelligence-brief-august-28-2020
39 「MUMMY SPIDER」、malpedia（英語）：https://malpedia.caad.fkie.fraunhofer.de/actor/mummy_spider
40 「Malware Threat: Emotet」、FortiGuard Labs（英語）：https://www.fortiguard.com/playbook/malware-family-emotet
41 「WORLD' S MOST DANGEROUS MALWARE EMOTET DISRUPTED THROUGH GLOBAL ACTION」、Europol、2021 年 1 月 27 日（英語）：https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
42 「APT28」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0007/
43 「NSA/FBI Joint Advisory on Previously Undiscovered Malware - "Drovorub"」FortiGuard Labs（英語）：https://www.fortiguard.com/threat-signal-report/3632/nsa-fbi-joint-report-on-previously-undiscovered-malware-drovorub
44 「Turla」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0010/
45 「MuddyWater」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0069/
46 「Iranian state hacker group linked to ransomware deployments」、Catalin Cimpanu 著、ZDNet、2020 年 10 月 15 日（英語）：https://www.zdnet.com/article/iranian-state-hacker-group-linked-to-ransomware-deployments/
47 「TA505」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0092/
48 「Two Russians Indicted Over $100M Dridex Malware Thefts」Jeremy Kirk 著、DataBreachToday、2019 年 12 月 6 日（英語）：https://www.databreachtoday.com/two-russians-indicted-over-100m-dridex-malware-thefts-a-13473
49 「TA505 APT Group Returns With New Techniques: Report」、Ishita Chigilli Palli 著、BankInfoSecurity、2020 年 2 月 3 日（英語）：https://www.bankinfosecurity.com/ta505-apt-group-returns-new-techniques-report-a-13678
50 「PROMETHIUM」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0056/
51 「Promethium APT attacks surge, new Trojanized installers uncovered」、Charlie Osborne 著、ZDNet、2020 年 6 月 30 日（英語）：https://www.zdnet.com/article/promethium-apt-attacks-surge-government-sponsorship-suspected/
52 「Kimsuky」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0094/
53 「OilRig」、MITRE ATT&CK（英語）：https://attack.mitre.org/groups/G0049/
54 「OilRig APT Drills into Malware Innovation with Unique Backdoor」、Tara Seals 著、Threatpost、2020 年 7 月 22 日（英語）：https://threatpost.com/oilrig-apt-unique-backdoor/157646/
55 「Egregor Ransomware Attacks on the Rise - Multiple Organizations Victimized」、FortiGuard Labs（英語）：https://www.fortiguard.com/threat-signal-report/3762/egregor-ransomware-attacks-on-the-rise-vancouver-metro-and-other-organization-victimized
56 「Ryuk Threat Actors Exploiting Windows Zerologon Vulnerability (CVE-2020-1472)」、FortiGuard Labs（英語）：https://www.fortiguard.com/threat-signal-report/3711/ryuk-threat-actors-incorporating-windows-zerologon-vulnerability-cve-2020-1472
57 「Analysis of .NET Thanos Ransomware Supporting Safeboot with Networking Mode」、Kai Lu 著、フォーティネットブログ、2020 年 7 月 16 日（英語）：https://www.fortinet.com/blog/threat-research/analysis-of-net-thanos-ransomware-supporting-safeboot-with-networking-mode
58 「Deep Analysis – The EKING Variant of Phobos Ransomware」、Xiaopeng Zhang 著、フォーティネットブログ、2020 年 10 月 13 日（英語）：https://www.fortinet.com/blog/threat-research/deep-analysis-the-eking-variant-of-phobos-ransomware
59 「JOINT CYBERSECURITY ADVISORY」、CISA, FBI, HHS: The United States Government、2020 年 10 月 28 日（英語）：https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
60 「Trickbot/Ryuk Campaign Targeting Healthcare and Public Health Sectors」、FortiGuard Labs（英語）：https://www.fortiguard.com/threat-signal-report/3721/latest-trickbot-ryuk-campaign-targeting-healthcare-and-public-health-sectors
61 「Steps to Protect Your Organization from Ransomware」、Derek Manky 著、フォーティネットブログ、2020 年 1 月 24 日（英語）：https://www.fortinet.com/blog/industry-trends/fifteen-steps-to-protect-your-organization-from-ransomware
62 「Exploit Prediction Scoring System (EPSS)」、FIRST（英語）：https://www.first.org/epss/
63 「Prioritization to Prediction Volume 6: The Attacker-Defender Divide」、Kenna Security（英語）：https://www.kennasecurity.com/resources/prioritization-to-prediction-report-volume-six/

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-20H2-202103-R1