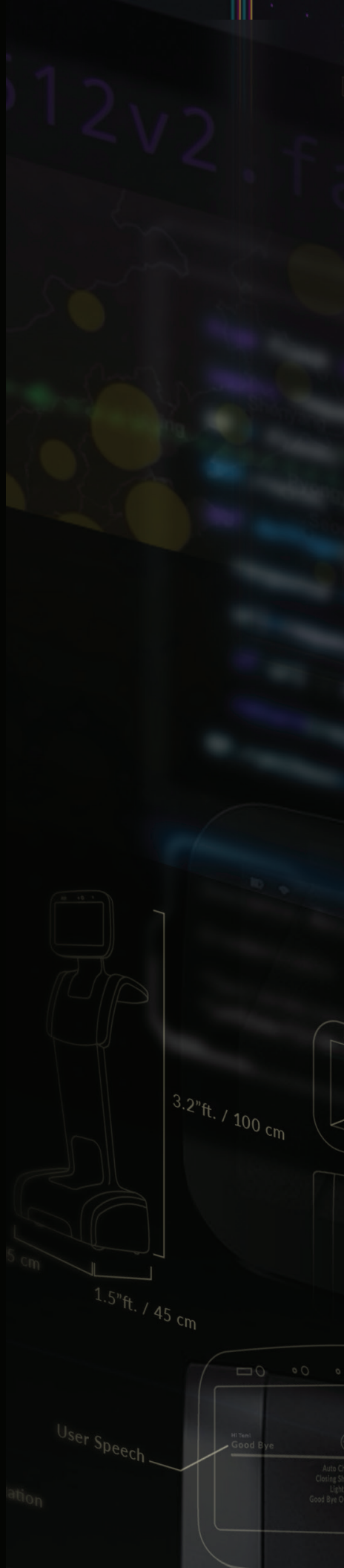

McAfee
MCAFEE
LABS 脅威
レポート
06.21

目次



このレポートでは、この 1 年の大きな流れを踏まえて新しい情報をご紹介します。この流れの中で最も顕著なものは、最近のランサムウェア攻撃です。トピック自体は目新しいものではありませんが、この脅威が現在の主流になっていることは明らかです。

レポートおよびリサーチ

Christiaan Beek
Mo Cashman
John Fokker
Melissa Gaffney
Steve Grobman
Tim Hux
Niamh Minihane
Lee Munson
Chris Palm
Tim Polzer
Thomas Roccia
Raj Samani
Craig Schmugar

弊社チーフ サイエンティストからのご挨拶

2021 年のここまでの状況を振り返ってみましょう。このレポートでは、この 1 年の大きな流れを踏まえて新しい情報をご紹介します。この流れの中で最も顕著なものは、最近のランサムウェア攻撃です。トピック自体は目新しいものではありませんが、この脅威が現在の主流になっていることは明らかです。

この脅威レポートでは、ランサムウェア、特に DarkSide について詳しく説明します。このランサムウェア攻撃は、米国のバイデン大統領とロシアのプーチン大統領との会談でも議題にのぼるほど注目を集めています。ここで政治情勢に踏み込むつもりはありませんが、このランサムウェアが私たちの生活に不可欠なサービスを停止させるほどの脅威であることは十分に認識しておく必要があるでしょう。また、特定の地域からデジタル証拠を収集することは、法的な障壁によりほぼ不可能な状態です。このような環境は攻撃者にとって都合のよいものとなっています。

しかしながら、最近のキャンペーンの情報はすべてマカフィーの製品に組み込まれています。もちろん、MVISION Insights プレビューダッシュボードで追跡できます。

このダッシュボードを見ると、実際には、報道よりも多くの国でこのような攻撃が発生していることが分かります。ここには表示されていませんが、被害者が身代金を支払っているため、結果として RaaS（サービスとしてのランサムウェア）攻撃が増加しています。No More Ransom イニシアチブを立ち上げて 5 年目になりますが、この脅威と戦うためには、よりグローバルなイニシアチブが必要であることは間違いないでしょう。

この脅威レポートが皆様の保護対策のお役に立てば幸いです。

—Raj Samani
McAfee フェロー兼チーフ サイエンティスト

Twitter @Raj_Samani

ランサムウェア : Babuk から DarkSide まで

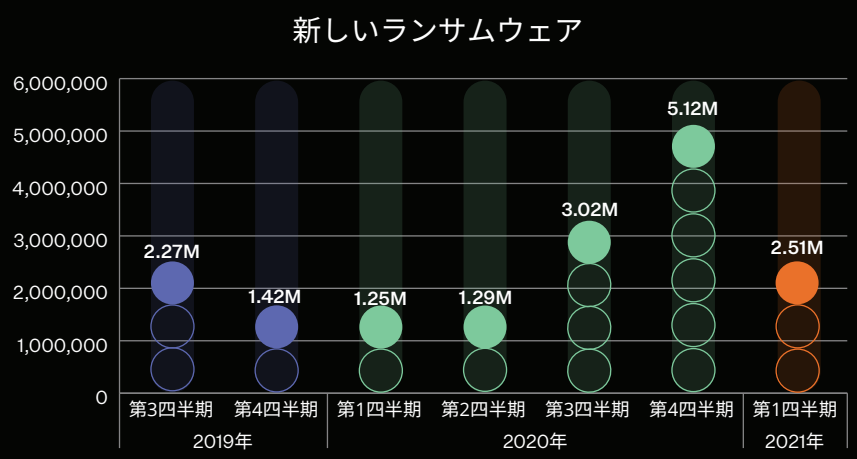
2021 年第 2 四半期は、最近の Colonial Pipeline に対する DarkSide RaaS（サービスとしてのランサムウェア）による攻撃が注目を集めていますが、このランサムウェアの活動はすでに今年の第 1 四半期から始まっています。

2021 年のランサムウェアの動向を見ると、DarkSide の前に Babuk、Conti、Ryuk、REvil が活発な動きを示していました。

第 1 四半期の結果を見ると、小規模なランサムウェアによるキャンペーンは減少していますが、大規模な組織や企業を狙った RaaS による攻撃が発生し、被害を発生させています。第 1 四半期のサンプル数は減少していますが、これは、多くの攻撃者が大規模なキャンペーンではなく、少数の魅力的なターゲットに標的をシフトしたことが影響しています。こうした攻撃を受けた組織の大半は、カスタマイズされたランサムウェア ファミリーの亜種を受信していますが、その量は決して多くありません。

以下に、2021 年第 1 四半期のランサムウェアに対する McAfee Labs の調査結果を示します。

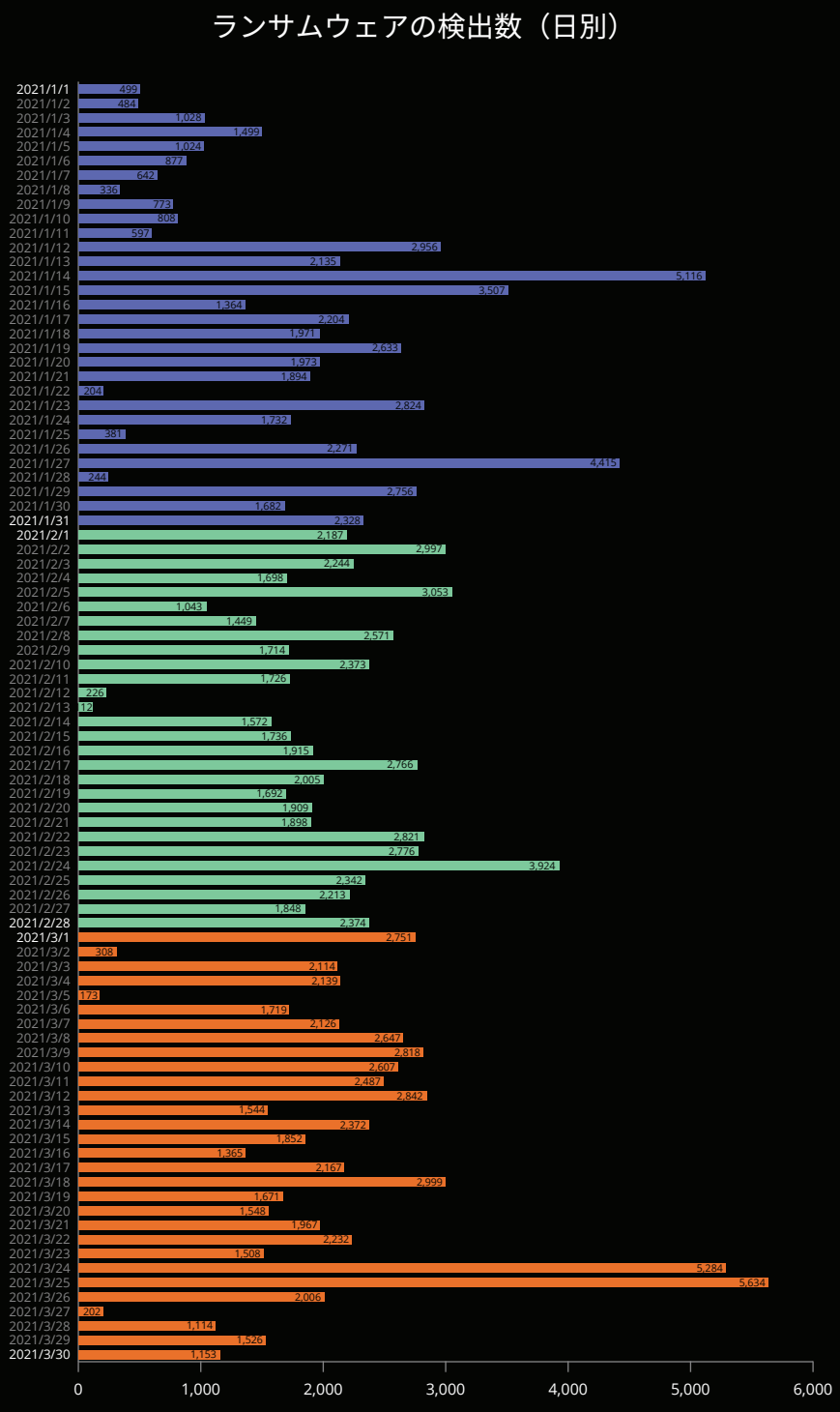
2021 年第 1 四半期に新たに確認されたランサムウェア



出典: McAfee Labs, 2021.

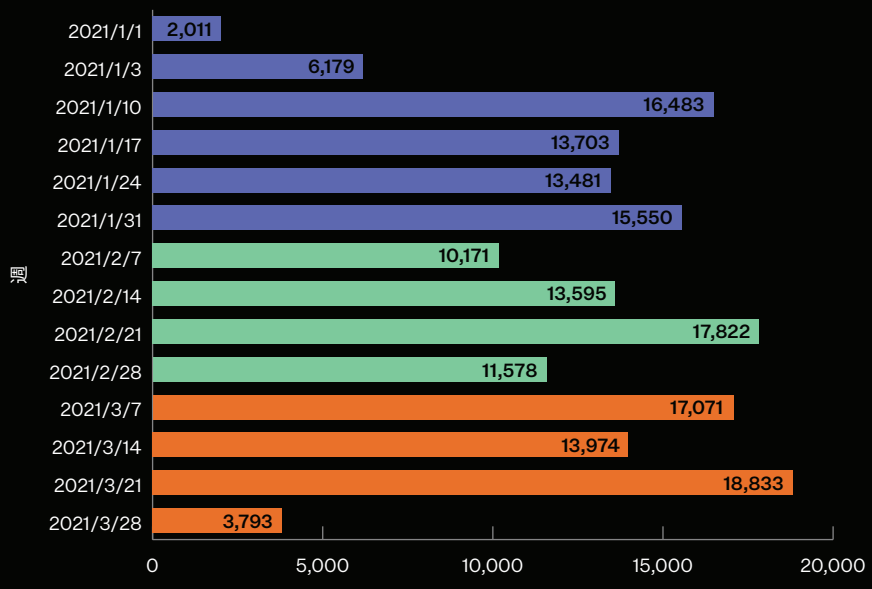
図 1. 2021 年第 1 四半期に検出された固有のランサムウェアは 2020 年第 4 四半期と比べて 50% 減少していますが、これは CryptoDefense の減少がその一因です。2021 年第 1 四半期と第 2 四半期の傾向を見ると、ランサムウェアは大規模な組織や企業にとって最も深刻な脅威となっています。

日 / 週 / 月別のランサムウェアの状況



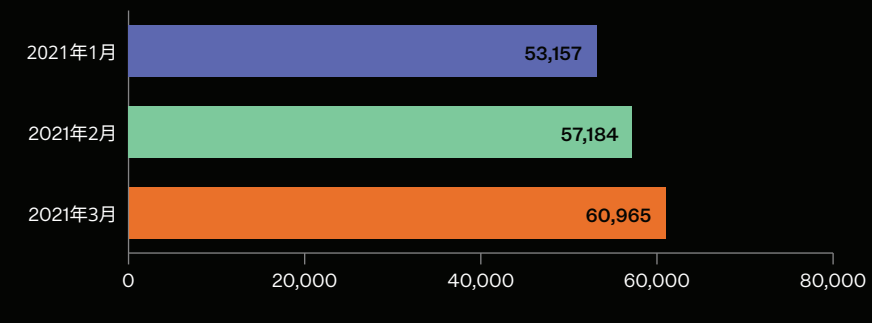
出典: McAfee Labs, 2021.

図 2. 2021 年第 1 四半期に McAfee の顧客で検出されたランサムウェアのスナップショットを見ると、1 日あたりの検出数が最も多かったのは 3 月 25 日で、5,634 件検出されています。3 月の最終週は 1 日あたりの平均検出数が 2,417 件になっています。



出典: McAfee Labs, 2021.

図 3. 2021 年第 1 四半期に最も多くのランサムウェアが検出されたのは 3 月 21 日～ 3 月 27 日の週で、18,833 件が記録されています。



出典: McAfee Labs, 2021.

図 4. 第 1 四半期にランサムウェアが最も検出されたのは 3 月です。

最も多いランサムウェア ファミリーとテクニック

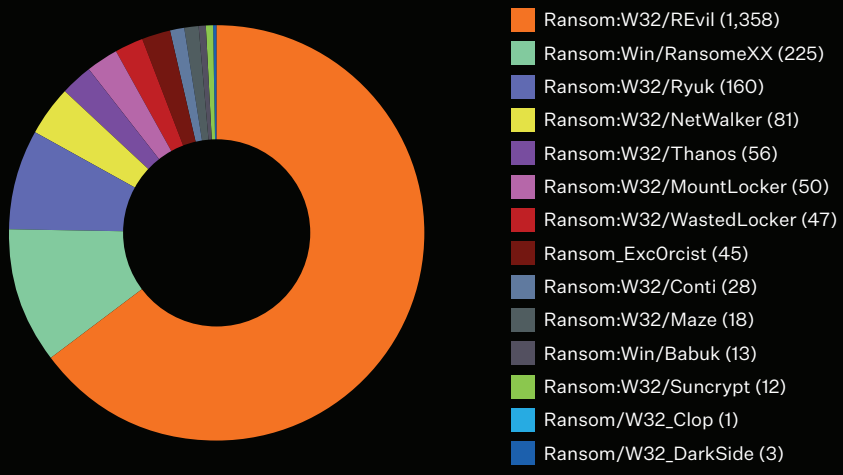


図 5. 2021 年第 1 四半期に検出されたランサムウェア関連のマルウェア ファミリーを見ると、第 2 四半期の 5 月に DarkSide が Colonial Pipeline のシステムをハッキングするまでは、Revil、RansomeXX、Ryuk が大半を占めていました。

固有のランサムウェア ファミリー

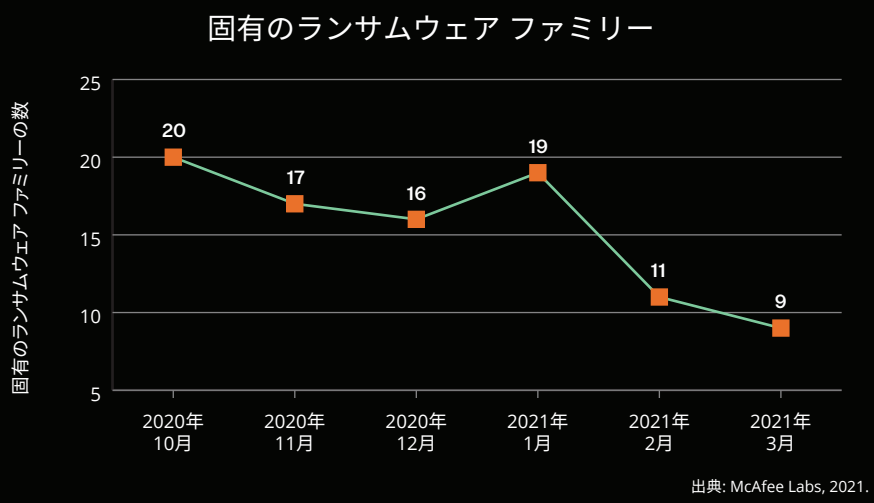


図 6. 固有のランサムウェア ファミリーの数は、2021 年 1 月の 19 件から 2021 年 3 月の 9 件に減少しています。第 1 四半期の後の傾向を見ると、キャンペーンは少なくなっていますが、より多くの身代金が見込める大規模な組織や企業を狙う攻撃が増えています。

ランサムウェアのカバレッジと保護

実際のランサムウェアのバイナリに対しては、エンドポイント保護の更新とアップグレードを行い、改ざん防止やロールバックなどのオプションを有効にすることを強くお勧めします。ランサムウェアを阻止するための ENS 10.7 の最適な構成については、こちらのブログをご覧ください。

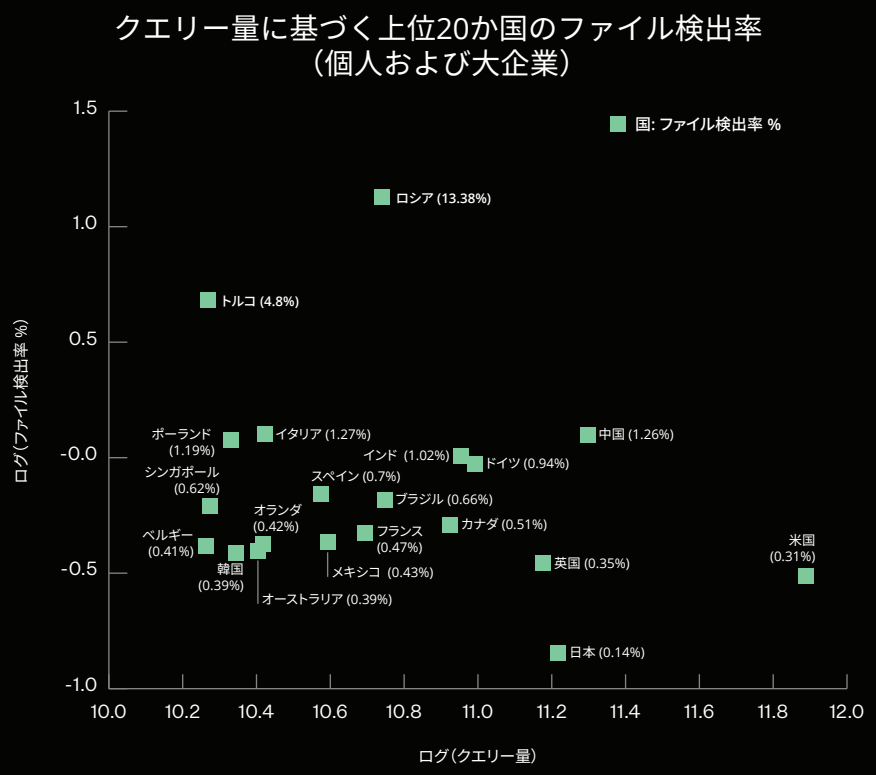
McAfee が参加している Ransomware Task Force では、ランサムウェア攻撃がどのように発生しているのか、どのような対策を講じるべきかについて情報を提供してきました。私たちがこれまで調査、研究、発表してきたことを行動に移す時が来ました。

McAfee Global Threat Intelligence

様々な脅威研究を行っている McAfee Labs は、世界各地に配備している数百万台のセンサーを利用し、McAfee Global Threat Intelligence（GTI）経由で脅威情報をリアルタイムで提供しています。このクラウド ベースの脅威情報サービスで脅威とコンテキストを評価することで、既知の脅威だけでなく、新たに発生する脅威にも的確な対応が可能になります。McAfee GTI は弊社のセキュリティ製品に直接統合されています。これにより、運用コストを削減し、検出から封じ込めまでの時間を短縮できます。

2021 年第 1 四半期の主な統計情報は次のとおりです。

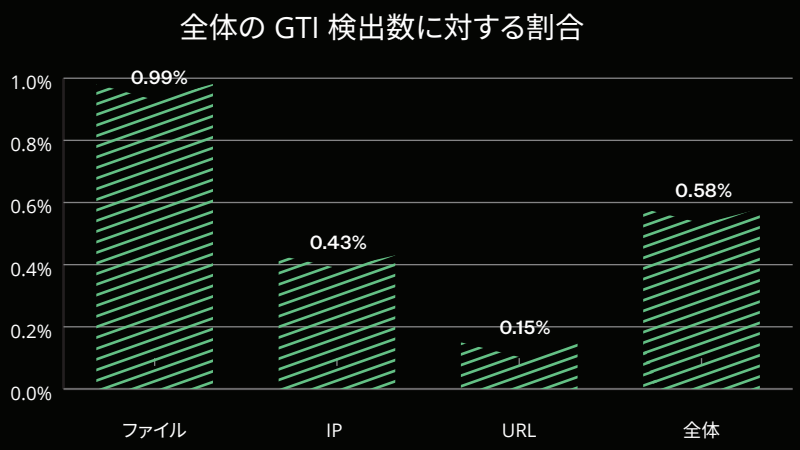
国別のファイルの状況



出典: McAfee Labs, 2021.

図 7. 2021 年第 1 四半期、クエリ量が最も多かったのは米国で 7,750 億クエリでしたが、検出率は低く、0.31% でした。ロシアの GTI クエリは 550 億件で、その 13.38% でマルウェアが検出されました。そのため、上位 20 か国の中でロシアのマルウェア検出率が最も高くなっています。前の四半期から最も変化が大きかったのはトルコで、検出率は 9.76% から 4.8% に減少し、クエリ量は 190 億になっています。日本は上位 20 か国の中で最も検出率が低く、0.14% でした。クエリ数は 1,650 億です。中国の検出率は 1.26% ですが、クエリ量は 1,990 億で 2 番目に多い結果となりました。

クエリと検出



出典: McAfee Labs, 2021.

図 8. 2021 年第 1 四半期、1 日に検出されたファイルの平均数は 2 億 5,200 万（検出率 0.9%）で、2020 年第 4 四半期の 2 億 4,300 万（1.03%）から増加しています。また、1 日に検出された URL の平均数は 2,600 万件（検出率 0.15%）で、第 4 四半期の 3,500 万件（0.21%）から減少しています。1 日に検出された IP の平均数は 7,900 万個（検出率 0.43%）で、第 4 四半期の 6,300 万回（0.34%）から増加しています。

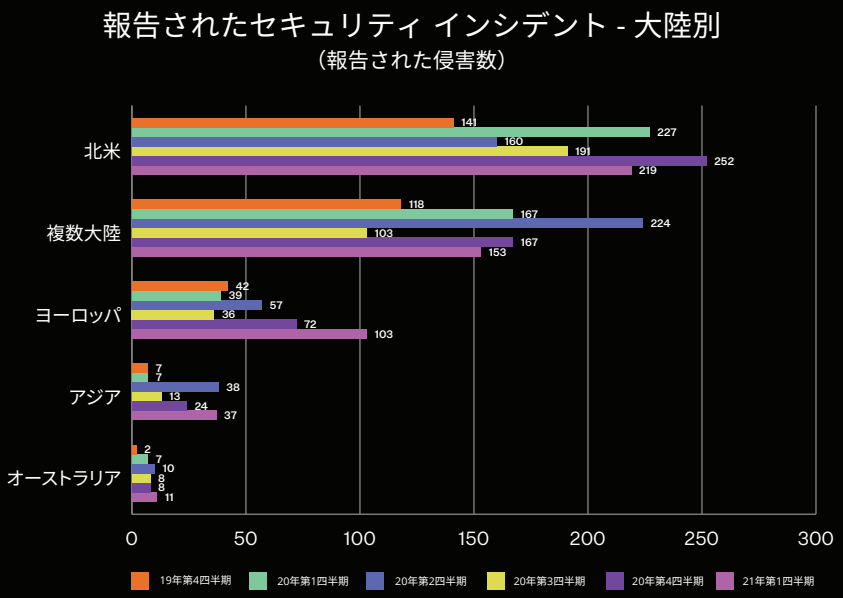
セクターに対する脅威とベクター

2021 年第 1 四半期、McAfee Labs は 1 分あたり平均で 688 件のマルウェア脅威を発見しました。1 分あたりに換算すると 40 件（3%）増加しています。

2020 年第 4 四半期から第 1 四半期にかけて増減の多かったセクターは次のとおりです。

- テクノロジー 54%
- 教育 46%
- 金融 / 保険 41%
- 卸売り / 小売 -76%
- 公的部門 -39%

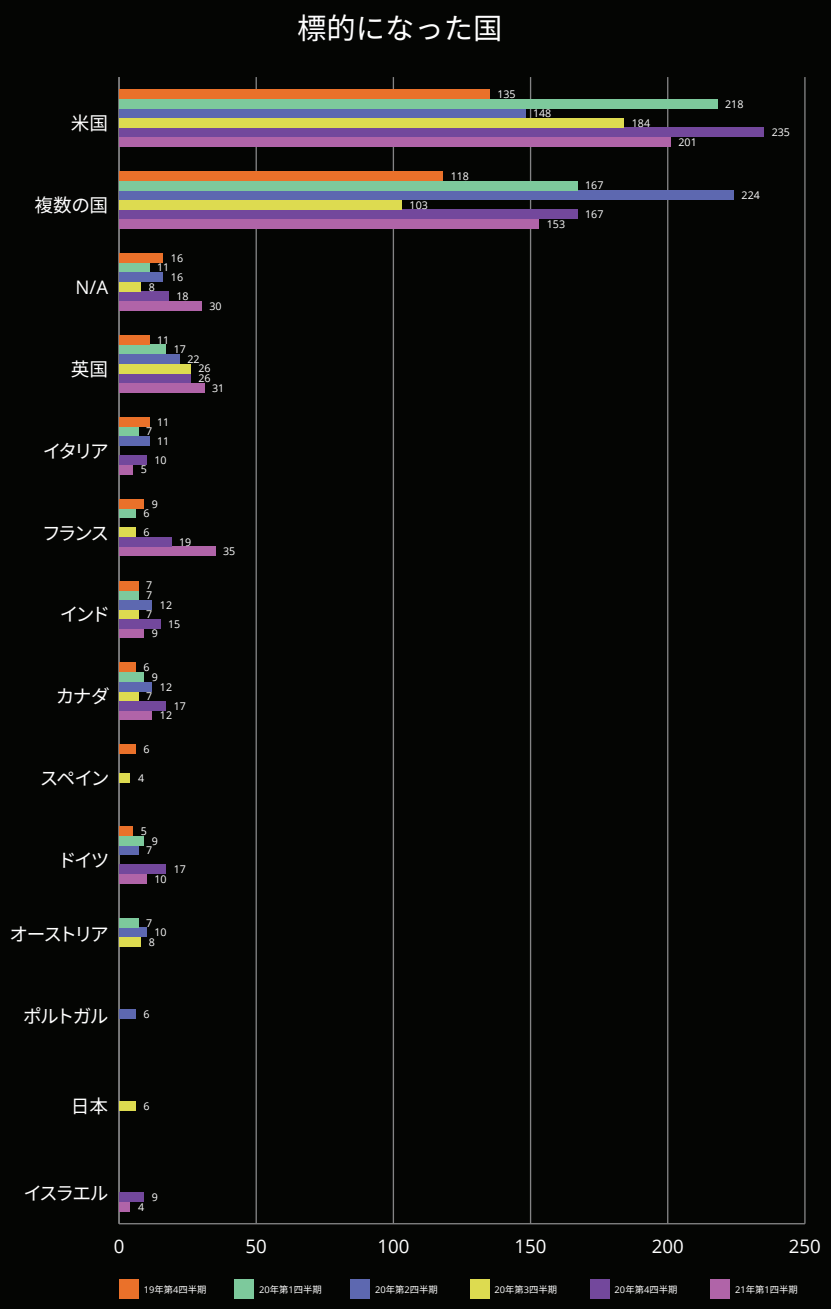
報告されたセキュリティ インシデント（大陸別）



出典: McAfee Labs, 2021.

図 9. 報告されたインシデント数を見ると、2020 年第 4 四半期から 2021 年第 1 四半期にかけてヨーロッパでは 54% 増加しています。インシデント件数はアジアで 54%、ヨーロッパで 43% 増加していますが、北米では 13% 減少しています。

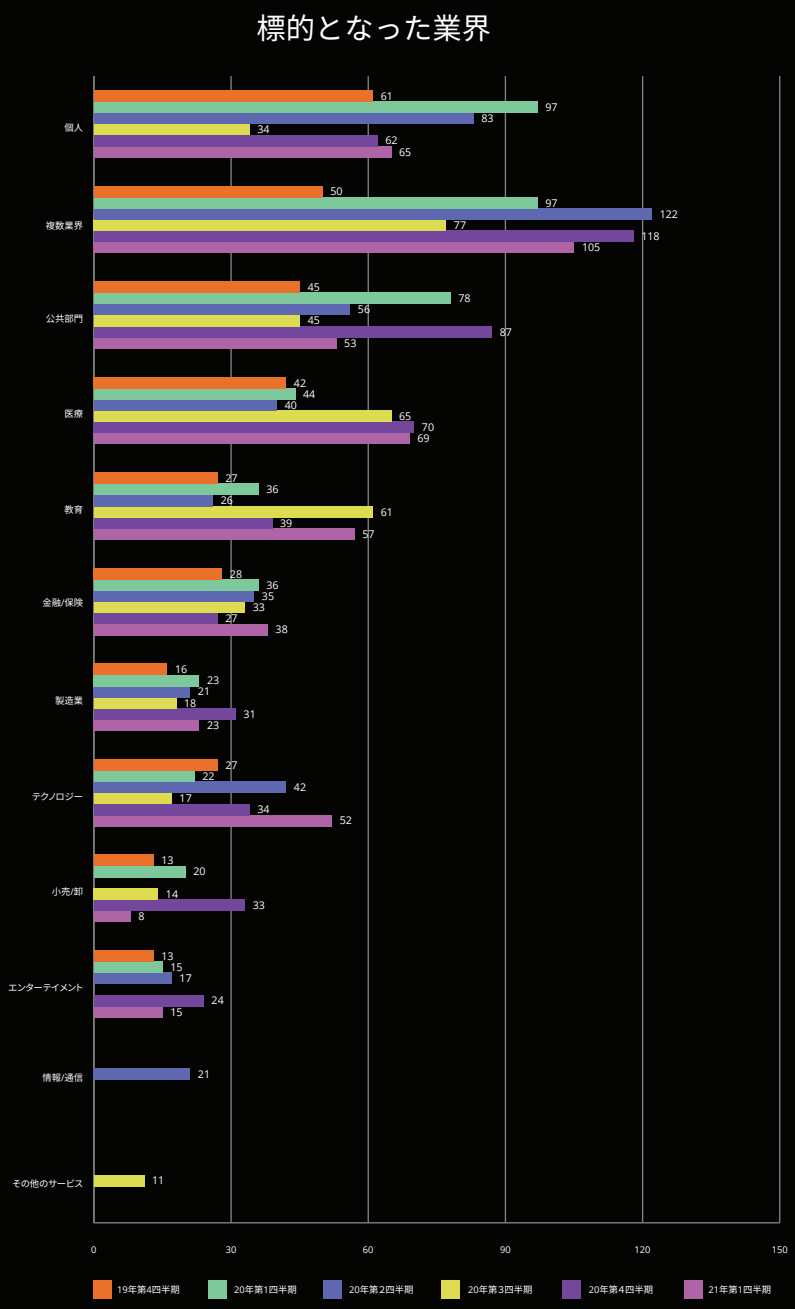
報告されたセキュリティ インシデント（国別）



出典: McAfee Labs, 2021.

図 10. 2020 年第 4 四半期から 2021 年第 1 四半期にかけて変化が大きかったのはフランス（84%）と英国（19%）です。米国のインシデント数は 14% 減少しています。米国のインシデントは、上位 10 か国で報告されたインシデント数の 40% を占めています。

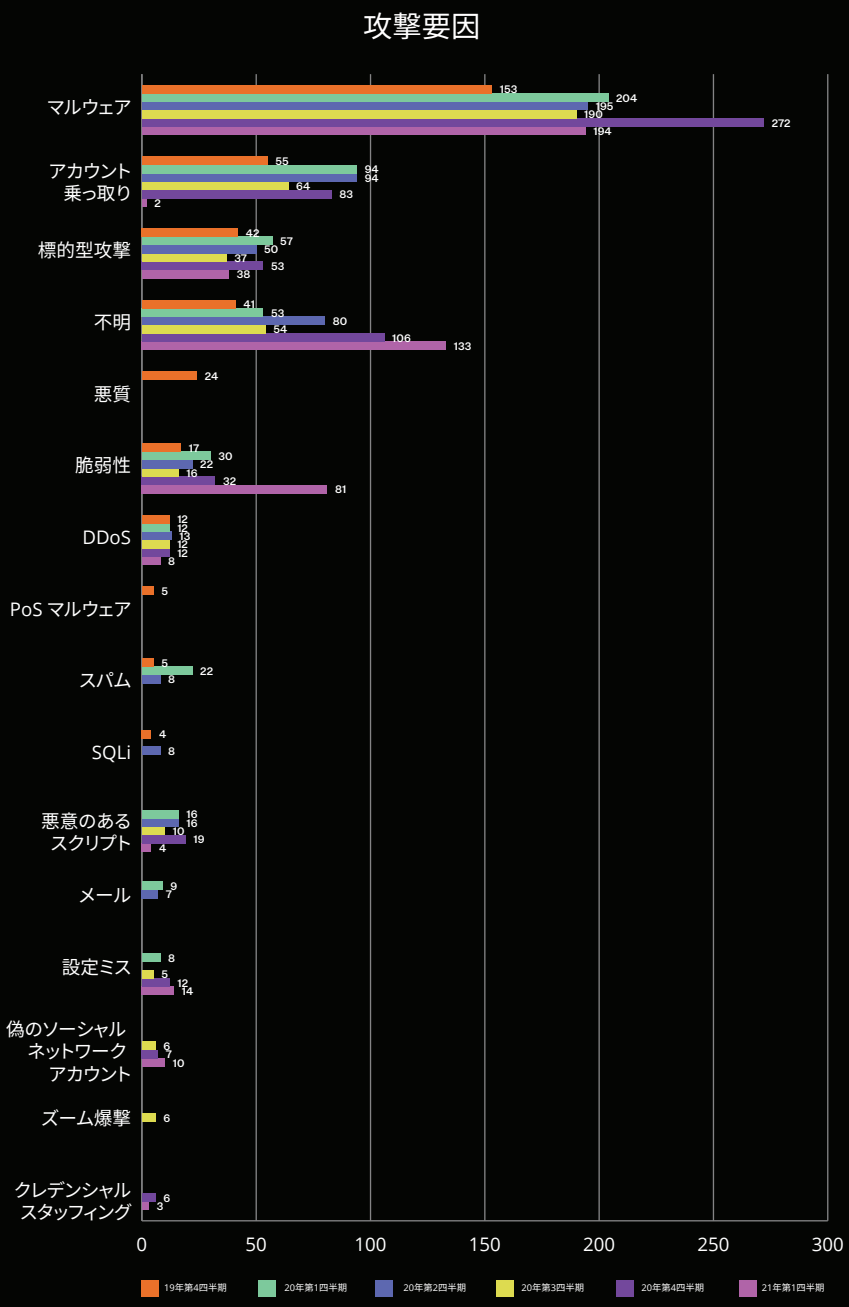
報告されたセキュリティ インシデント（業界別）



出典: McAfee Labs, 2021.

図 11. テクノロジー業界で報告されたインシデント数は、2020 年第 4 四半期から 2021 年第 1 四半期にかけて 54% 増加しています。この他に増減の多かった業界は教育（46%）と金融 / 保険（41%）です。

報告されたセキュリティ インシデント（ベクター別）



出典: McAfee Labs, 2021.

図 12. 2020 年第 4 四半期から 2021 年第 1 四半期にかけて偽のソーシャル ネットワーク アカウントによる攻撃は 43% 増加しています。標的型攻撃は 28% です。大きく減少しているのは脆弱性（-153%）、アカウントの乗っ取り（-98%）、悪意のあるスクリプト（-79%）です。

マルウェア脅威統計情報

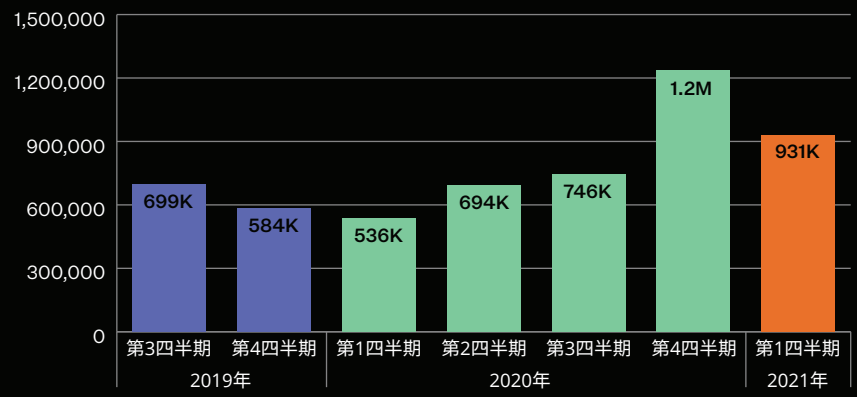
2021 年第 1 四半期は、複数の脅威カテゴリで顕著な増加が見られました。

- コインマイナー マルウェアは 117% 増加していますが、これは主に 64 ビットのコインマイナー アプリケーションの普及に起因しています。
- IoT は 55% 増加していますが、これは Mirai の影響です。
- 同様に、Mirai の影響で Linux も増加しています（38%）。

2021 年第 1 四半期、次の脅威カテゴリは大幅に減少しています。

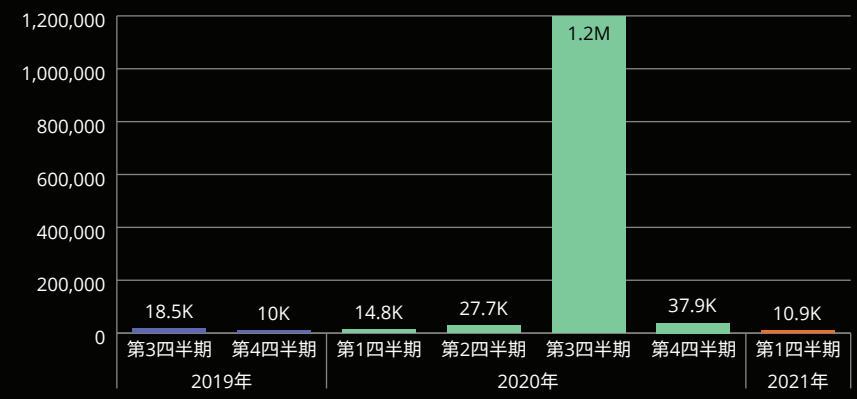
- 新しい PowerShell は Donoff の減少により 89% 減少しました。
- 新しい Office マルウェアは 87% 減少していますが、これも Donoff が減少したことに起因します。
- MacOS のマルウェアは、EvilQuest の減少により 70% 減少しています。
- ランサムウエアは、Cryptodefense の減少に伴い、50% 減少しました。

署名付きの新しい不正なバイナリ



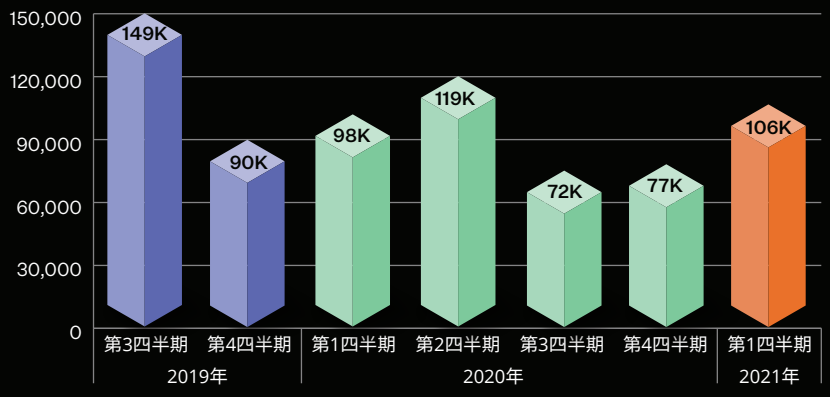
出典: McAfee Labs, 2021.

新しい Mac OS マルウェア



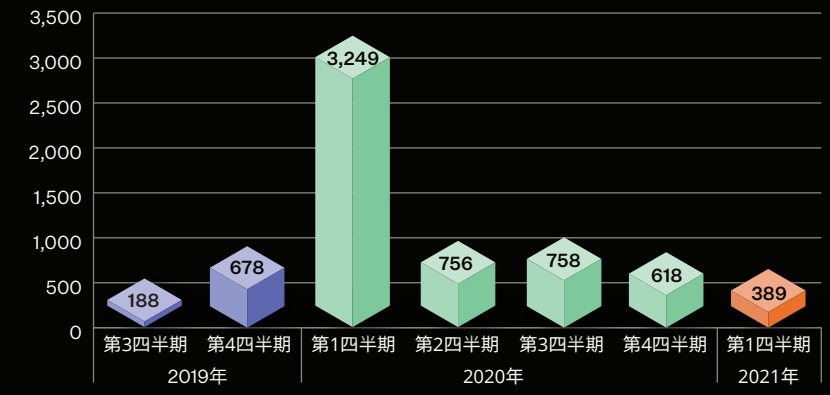
出典: McAfee Labs, 2021.

新しい Linux マルウェア



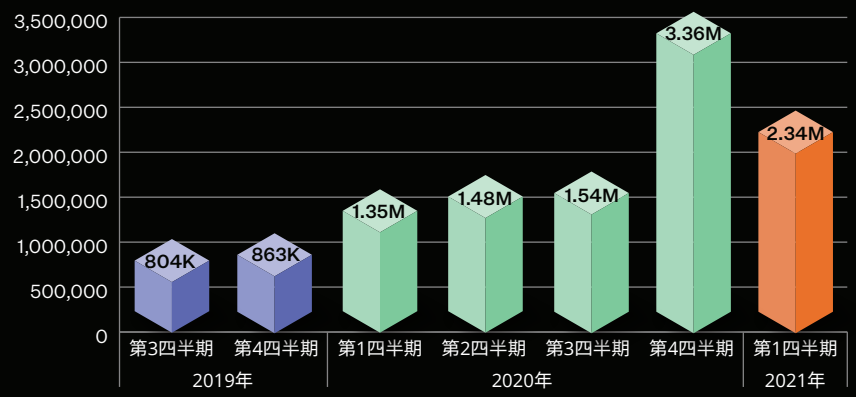
出典: McAfee Labs, 2021.

新しい iOS マルウェア

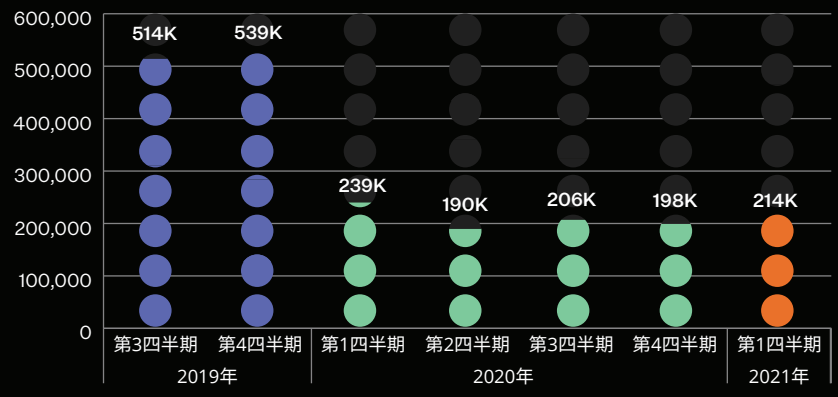


出典: McAfee Labs, 2021.

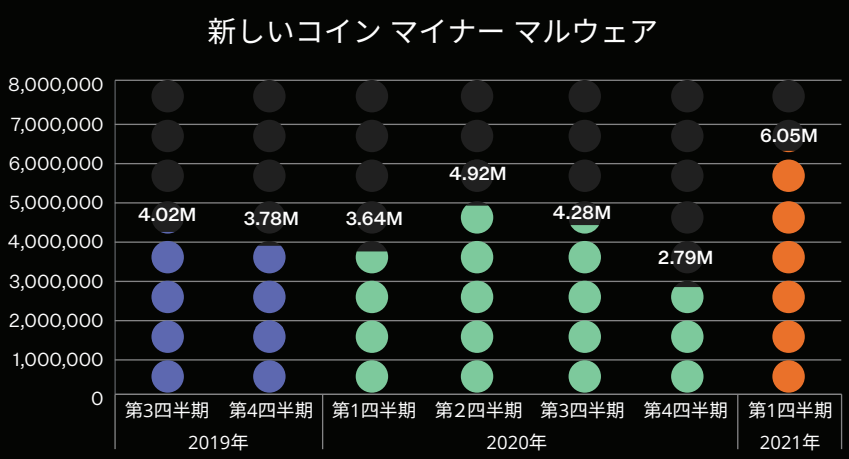
新しいモバイル マルウェア



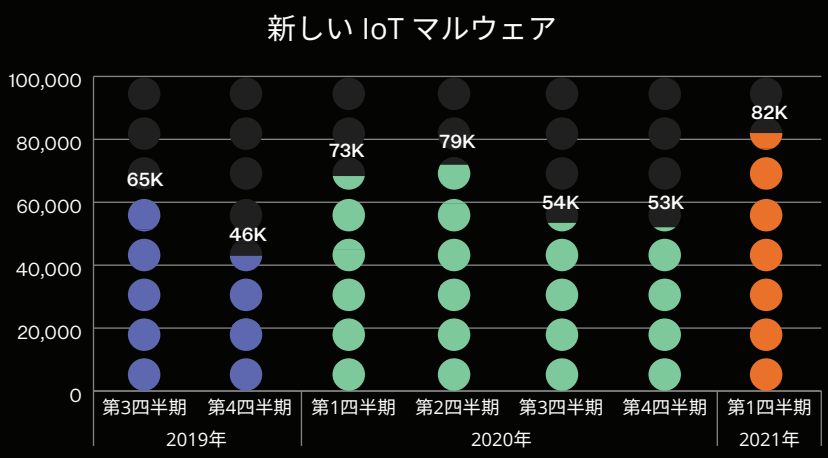
出典: McAfee Labs, 2021.



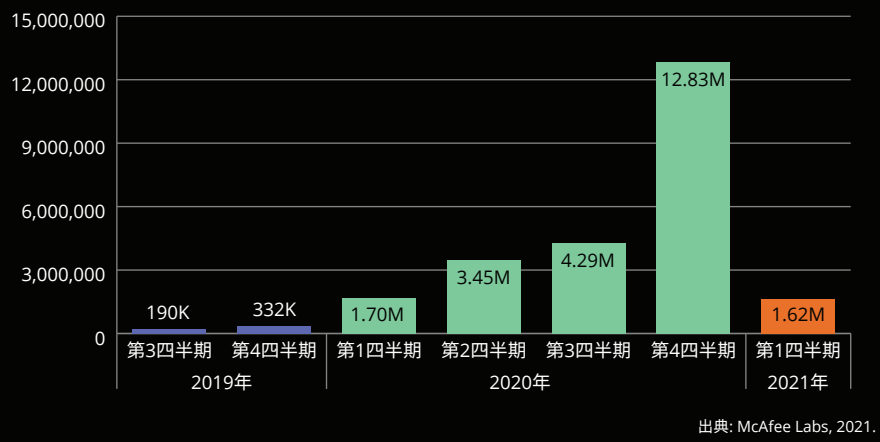
出典: McAfee Labs, 2021.



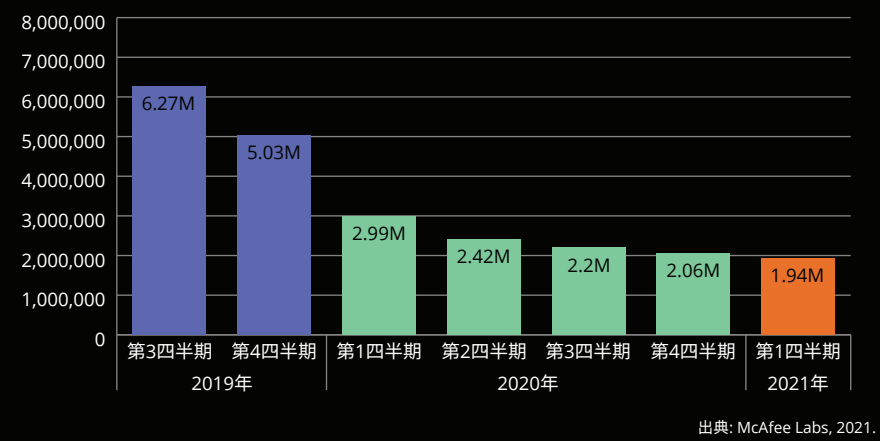
出典: McAfee Labs, 2021.



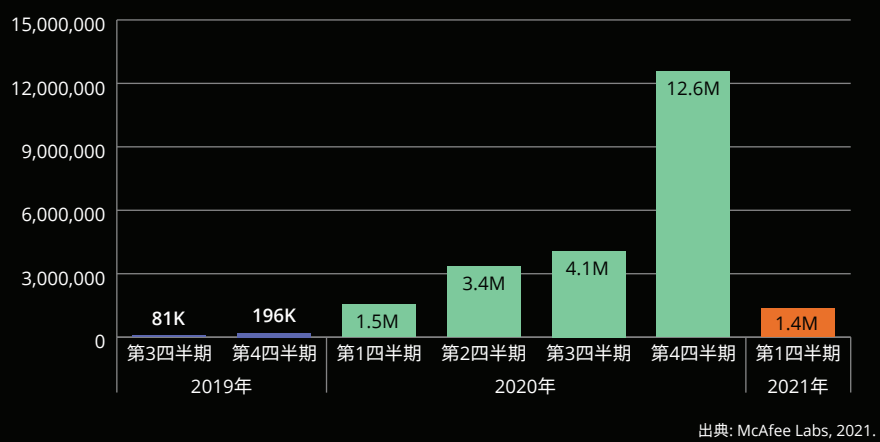
出典: McAfee Labs, 2021.



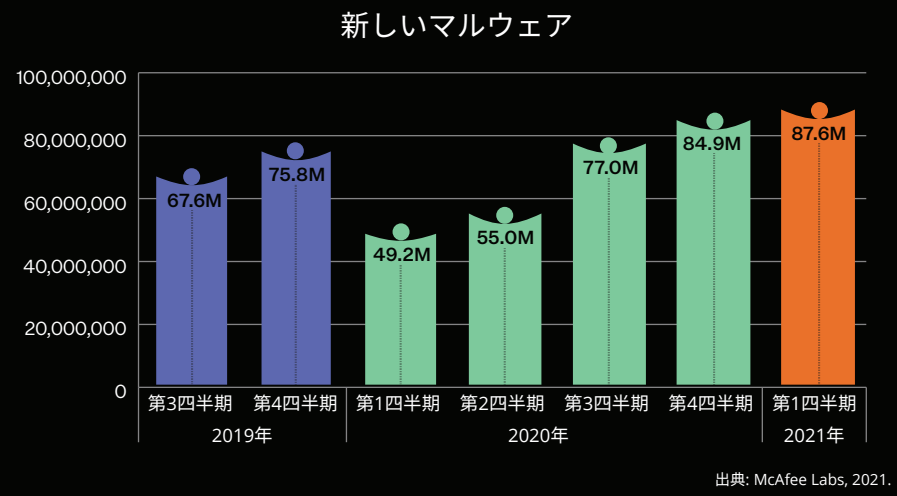
出典: McAfee Labs, 2021.



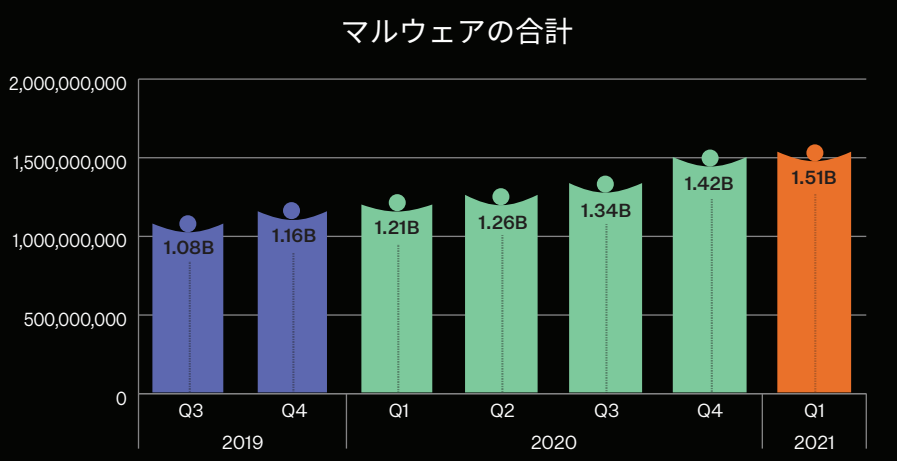
出典: McAfee Labs, 2021.



出典: McAfee Labs, 2021.



出典: McAfee Labs, 2021.



出典: McAfee Labs, 2021.

トップ MITRE ATT&CK テクニック APT/ 犯罪者

戦術	テクニック（各戦術のトップ 5）	コメント
Initial Access	Spearphishing Link	スピアフィッシング リンク（リンクと添付ファイル）はトップ 5 にち返り咲き、その後に公開アプリケーションのエクスプロイトが続きます。 公開アプリケーションのエクスプロイトは、初期アクセスのトップ 3 に残っていますが、これは、Microsoft Exchange の重大な脆弱性が公開され、世界中で数千の組織が影響を受けたためです。
	Spearphishing Attachment	
	Exploit public facing application	
	Phishing	
Execution	Windows Command Shell	Windows コマンド シェルや PowerShell などのコマンドラインとスクリプト インタープリターの使用は、攻撃者がペイロードを実行するために最もよく利用する手法です。簡単に実行できるため、コマンドライン スクリプトは Cobalts Strike などのペネトレーションテストフレームワークに組み込まれていることが少なくありません。
	Malicious File	
	Powershell	
	User execution	不正なバイナリを実行するために、ユーザーによる操作が必要になることがあります。多くの場合、これは初期アクセスの手法である（スピア）フィッシングに関連しています。
	Visual Basic	
Persistence	Windows Service	
	Registry Run Keys / Startup Folder	
	Scheduled Task	
	Web Shell	
	DLL Side-Loading	
Privilege Escalation	Windows Service	
	Process Injection	この四半期でも、プロセス インジェクションは特権昇格で最もよく使用される手口の一つになっています。
	Registry Run Keys / Startup Folder	
	Scheduled Task	
	Process Hollowing	
Defense Evasion	Deobfuscate/Decode Files or Information	
	Obfuscated Files or information	
	Software Packing	
	Process Injection	
	File Deletion	
	Modify Registry	

戦術	テクニック（各戦術のトップ 5）	コメント
Credential Access	Keylogging	
	Credentials from Web Browsers	Lazange や Grabff などのオープンソースのペネトレーションテスト ツールや大半の RAT ツールでは、Web ブラウザーから認証情報を抽出する機能が用意されています。2021 年第 1 四半期では、様々なランサムウェアで Lazange や Grabff の使用が確認されました。
	Brute Force	
	OS Credential Dumping	
	Credentials from Password Stores	
Discovery	System Information Discovery	
	File and Directory Discovery	
	Process Discovery	
	System Network Configuration Discovery	
	System Owner/User Discovery	
Lateral Movement	Remote File Copy	
	Remote Desktop Protocol	
	SMB/Windows Admin Shares	
	Exploitation of Remote Services	
	SSH	
Collection	Data from Local System	
	Screen Capture	
	Keylogging	
	Archive Collected Data	
	Clipboard data	
Command and Control	Web protocols	
	Ingress Tool transfer	
	Standard Encoding	
	Symmetric Cryptography	
	Application Layer Protocol	

戦術	テクニック（各戦術のトップ 5）	コメント
Exfiltration	Exfiltration Over Command and Control Channel	
	Exfiltration Over Alternative Protocol	
	Automated Exfiltration	
	Exfiltration over unencrypted/obfuscation Non-C2 Protocol	
	Exfiltration to Cloud Storage	MEGAsync、Rclone などのツールは、攻撃先のネットワークからクラウド ストレージに機密データを引き出すためによく利用されています。これらのツールは、REvil、Conti、DarkSide などの複数のランサムウェア グループで利用されています。
Impact	Data Encrypted for impact	
	Resource Hijacking	
	Service Stop	
	System Shutdown/ Reboot	
	Direct Network Flood	

表 1. 2021 年第 1 四半期のトップ MITRE ATT&CK テクニック APT/ 犯罪者に関する注 : スピアフィッシングが再びテクニックのトップ 5 に入り、その後に公開アプリケーションのエクスプロイトが続いています。公開アプリケーションのエクスプロイトは、Microsoft Exchange の重大な脆弱性により世界中の何千もの組織が影響を受けたため、初期アクセスのトップ 3 に残っています。Windows コマンド シェルや PowerShell などのコマンドラインとスクリプト インタープリターの使用は、攻撃者がペイロードを実行するために最もよく利用する手法です。簡単に実行できるため、コマンドライン スクリプトは Cobalts Strike などのペネトレーションテスト フレームワークに組み込まれていることが少なくありません。不正なバイナリを実行するために、ユーザーによる操作が必要になることがあります。多くの場合、これは初期アクセスの手法である（スピア）フィッシングで使用されています。この四半期でも、プロセス インジェクションは特権昇格で最もよく使用される手口の一つになっています。Lazange や Grabff などのオープンソースのペネトレーションテスト ツールや大半の RAT ツールでは、Web ブラウザーから認証情報を抽出する機能が用意されています。2021 年第 1 四半期では、様々なランサムウェアで Lazange や Grabf の使用が確認されました。MEGAsync、Rclone などのツールは、攻撃先のネットワークからクラウド ストレージに機密データを引き出すためによく利用されています。これらのツールは、REvil、Conti、DarkSide などの複数のランサムウェア グループで利用されています。データの暗号化による影響は、2021 年第 1 四半期最大のサイバー脅威であるランサムウェアにのみ関係しているようです。

リソース

最新の脅威や研究については、以下の McAfee のリソースをご覧ください。

McAfee COVID-19 ダッシュボード — 国、経路および脅威の種類を含む COVID-19 関連の悪意あるファイル検出状況の最新情報をご覧いただけます。

MVISION Insights プレビュー ダッシュボード — 新しい脅威に対応するプロアクティブなソリューションのプレビューをご覧いただけます。

McAfee 脅威センター — McAfee の脅威研究チームが現代の影響力の強い脅威についてご説明します。

McAfee Labs と研究者の Twitter

McAfee Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Eoin Carroll

Thomas Roccia

Douglas McKee

McAfee について

McAfee は、デバイスからクラウドまでを保護するサイバーセキュリティ企業です。McAfee では、より安全なデジタル世界を構築するため、個々の力を結集し、企業と個人を保護するソリューションを提供しています。McAfee は他社製品と連携するソリューションを提供することで、お客様企業を脅威から保護し、脅威の検出や修正を連動して行えるような、真に統合されたサイバー環境を構築するサポートをしています。McAfee の個人向けのソリューションは、すべての種類のデバイスに対応しています。自宅でも外出先でも、安心してデジタル ライフを楽しむことができます。McAfee では、他のセキュリティ企業との連携を強化し、力を合わせてサイバー犯罪者と戦っています。

www.mcafee.com/jp

McAfee Labs と Advanced Threat Research について

McAfee Labs は McAfee Advanced Threat Research が主導する世界最先端の脅威研究機関で、脅威情報やサイバーセキュリティの最新情報を提供しています。世界各地に配備した数百万台のセンサーからデータを収集し、ファイル、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs と McAfee Advanced Threat Research は、リアルタイムで脅威情報、重要な分析結果、専門的な情報を提供し、保護対策の向上とリスクの軽減に貢献しています。

https://www.mcafee.com/enterprise/ja-jp/threat-center.html

脅威情報を受け取るには購読登録をお願いします。

〒 150-0043
東京都渋谷区道玄坂 1-12-1
渋谷マークシティウエスト 20F
www.mcafee.com/jp