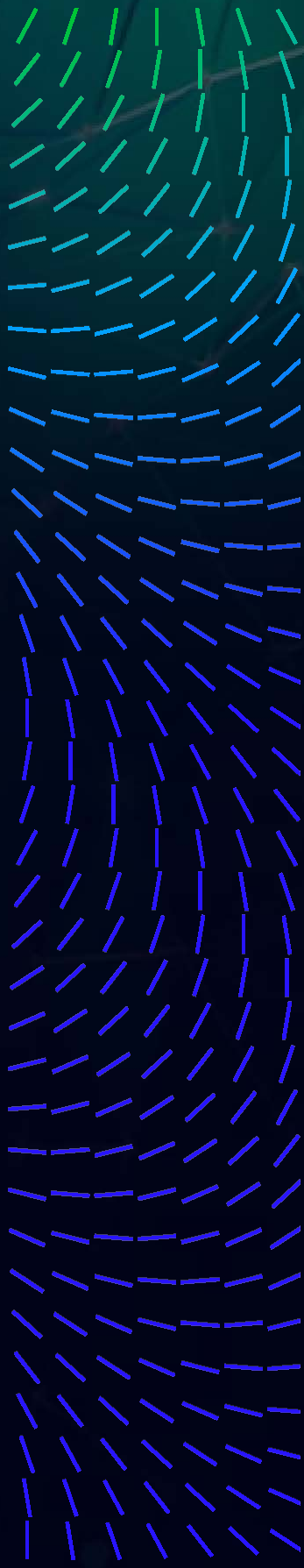
THE THREAT REPORT

Fall 2022
脅威レポート

Presented by

Trellix ADVANCED RESEARCH CENTER

TABLE OF CONTENTS



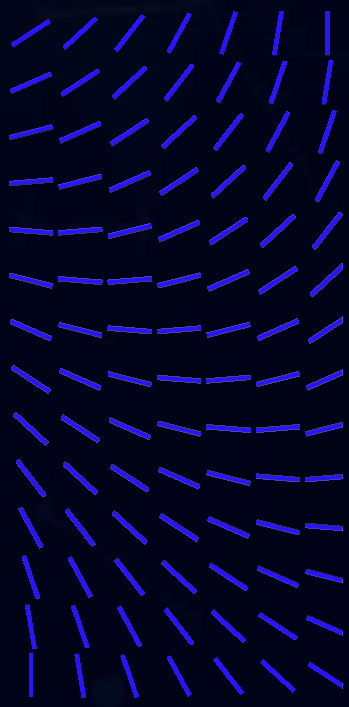
2022年第3四半期の脅威の概要

2022年第3四半期、TrellixはXDR（Extended Detection and Response）とサイバーセキュリティの未来を支えるための強力なリソースを新たに提供しました。お客様による最新のサイバーセキュリティ脅威の検知・対応・修復を支援するため、数百人の精鋭セキュリティアナリストと研究者を擁するTrellix Advanced Research Centerを設立しました。

また、2022年第 3 四半期には、攻撃者についても大きく報じられました。Trellix Advanced Research Centerチームは、世界規模の調査・研究を行うことで、それらの攻撃者に対抗しました。私たちのチームは、「REvil」がサイバー犯罪組織を構築するために採用した手順から、最終的に彼らの破滅につながった失敗など、REvilの解体に関する詳しいレポートを発表しました。コードが教えてくれたことやオールスターズの形成を明らかにしたほか、REvil終焉までの金銭の流れを追跡しました。また、米国のナンシー・ペロシ下院議長が台湾を訪問した際、Trellix Advanced Research Centerチームは台湾政府を標的としたサイバー脅威活動の急増を検知し、ニュースになった地政学的緊張に関する調査を行いました。

Trellix Advanced Research Centerが初めて提供する今回の脅威レポートでは、以下の2022年第3四半期の注目すべきデータと調査結果を含む、当チームの迅速な調査とリアルタイムインテリジェンスのリソースを紹介しています。

- 運輸・海運セクターを狙う脅威の増加
- ドイツを標的とする脅威の増加
- 古いCVEの急速な蔓延（2022年に最も悪用された、2016年、2017年、2018年のCVE）



Trellix 脅威インテリジェンス責任者からのご挨拶

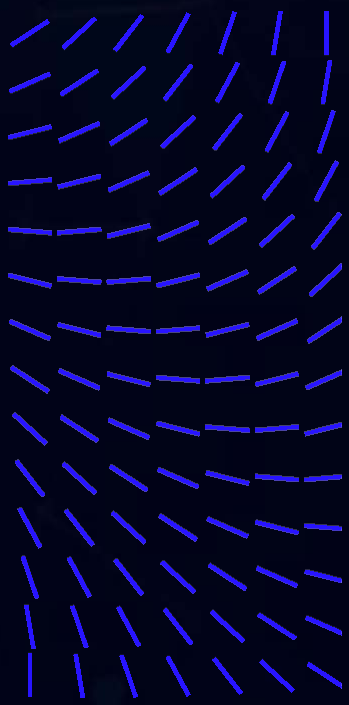
Trellix Advanced Research Centerが初めて提供する、脅威レポートへようこそ。

今年9月のTrellix Advanced Research Centerの開設は、今年初めにTrellixが誕生して以来、私たちの軌跡の中で重要なマイルストーンとなりました。Trellix Advanced Research Centerでは、政府、金融、小売、製造、重要インフラ、ヘルスケア、産業制御、その他多くのセクターを含む、ほぼすべての業界を狙う脅威の研究を通じて、今日の複雑な情勢下で活動している幅広い種類の脅威を特定し、その正体を明らかにする活動を行っています。Advanced Research Centerは、実用的なリアルタイムの脅威インテリジェンスと世界クラスの有効性を生み出し、お客様が最新のサイバーセキュリティの脅威から保護された状態を維持できるようにすること、そして、弊社の最先端の XDR プラットフォームをより強化することを目的とした研究者で構成されています。

前四半期のサイバー攻撃は、技術的に高度化し、経済的・地政学的な影響を及ぼす可能性が高まっています。ロシアから途絶えることのない攻撃、台湾を標的とした中国の攻撃、ミサイル訓練と時期を同じくしてサイバー攻撃を開始した北朝鮮の攻撃など、国家的な支援に起因するものだけでなく、政治的な動機によるハッカー行為の増加も確認されました。また、政治的な動機によるハクティビスト活動も活発化しています。このような状況に加えて、ランサムウェアが標的とする医療・教育システムへの継続的な攻撃や、世界におけるサイバーセキュリティ人材の不足が340万人に達していることから、脅威インテリジェンスの必要性が衰えていないことがわかります。

Trellix Advanced Research Centerを立ち上げて以来、 15年前から存在し、35万件のオープンソースプロジェクトに影響を与えている脆弱性、台湾を標的とした脅威、REvilのメンバーに対する取締当局の措置を支援する私たちのチームの取り組み、BazarCallのキャンペーンで使用されたソーシャルエンジニアリング戦術の進化についてや、米国の選挙関係者を標的としたフィッシング攻撃に関する研究結果を発表してきました。

本レポートを提供することで、 Trellix Advanced Research Centerは、組織がサイバー脅威を理解し、検知し、対応できるよう支援する業界の最前線に立つものとして、その勢いにさらに拍車をかけていきます。本レポートでは、これまでお届けしてきたデータに加え、メール調査の専門家による新たな調査結果や、弊社が24時間365日 稼働させている多数の



サイバー脅威トラッカーの1つであるCobalt Strikeのインフラトラッカーに関する新たな知見をご紹介します。このレポートは、四半期ごとに発行し、新しい洞察、指標、インテリジェンスを継続的に追加していく予定です。私たちの取り組みはまだ始まったばかりです。

本レポートでご覧になりたいテーマがありましたら、お気軽に私のEメール（@John_Fokker）または当チームのTwitter（@TrellixARC）までご連絡ください。 お待ちしています。

ジョン・フォッカー（John Fokker）
脅威インテリジェンス責任者

調査手法

Trellixは、Trellixのバックエンドシステムが提供する遠隔観測で報告された情報を用いて、これらの脅威レポートを作成しています。Trellixはこの情報をランサムウェアや国家主導の活動などの一般的脅威に関するオープンソースのインテリジェンス、そして私たち独自の調査結果と組み合わせて活用しています。

遠隔観測とは、感染ではなく検出のことを指します。ファイル、URL、IPアドレスなどの痕跡がプロダクトのいずれかにより検知され報告された場合に、検出として記録されます。

お客様のプライバシーは重要です。これは、遠隔観測やお客様の業種および国へのマッピングでも重要になります。国ごとに顧客基盤が異なるため、数字では増えているように見えることもありますが、解説はデータを掘り下げてみなければなりません。例えば私たちのデータでは、通信業界で高いスコアが記録されることがありますが、必ずしも同業界が標的になりやすいことを示しているわけではありません。通信業界には、企業が購入できるIPアドレス空間を所有するISPプロバイダも含まれています。これはどういうことかというと、ISPのIPアドレス空間からの送信は通信業界での検出と見なされますが、別の業種で稼働しているISPクライアントからのものである可能性があるのです。

サイバーセキュリティの状況が変化し、組織がより高度化する中で、組織はテストシナリオにおいて本物の痕跡を使用し、セキュリティ運用チームが対応に備えていることに注意することが重要です。つまり、一部のデータが高いスコアを示していたとしても、その中にはセキュリティ対策のための演習で使われた脅威の痕跡が含まれている可能性があるということです。

世界のランサムウェア

2022年第3四半期の世界のランサムウェアに関するハイライト

- Contiが公式に活動を停止。Contiのソースコードとチャット内容が流出しました。
- LockBitは依然として最も多いランサムウェアファミリーです。第3四半期末にLockBitの「ビルダー」がリリースされ、すでにさまざまなグループがこのビルダーを使って独自のRaaSを確立していると言われています。ランサムウェアのPhobosの活動が続いており、遠隔観測の10%を占めています。Phobosは完全なランサムウェアキットを販売し、大規模な組織を避けるという戦術を採用しているため、検知の網をすり抜けて潜伏することができます。

以下に示す世界のランサムウェアに関する統計の円グラフは、脅威インテリジェンスグループが収集・分析した悪意あるキャンペーンと関連する弊社の遠隔観測（お客様のログ）に基づいています。

ランサムウェアが最も検出された顧客セクター

弊社のグローバル遠隔観測から、複数のランサムウェアのキャンペーンに関連する、IoCと呼ばれる侵害の痕跡（侵害の指標）を確認しました。特定されたキャンペーンの影響を最も受けていた業界は以下の通りです。

- 通信
- 運輸＆海運
- メディア＆コミュニケーション
- ビジネスサービス
- 政府

最も影響を受けた国

弊社のグローバル遠隔観測から、複数のランサムウェアキャンペーンに関連するIoCが確認されました。特定された攻撃の影響を最も受けていた国は以下の通りです。

+32%

2022年第2四半期から第3四半期にかけて特定されたIoCのキャンペーン数が最も高い伸びを示した国はドイツで、その増加率は32%となり、米国の増加率は9%でした。イスラエルでは、同期間に特定されたIoCのキャンペーン数が52%減少しました。

2022年第3四半期に世界で検知されたランサムウェアファミリー

1.	LockBit	22%
2.	HelloXD（ソースコードが流出した「Babuk」の亜種）	11%
3.	Zeppelin	11%
4.	Phobos	10%
5.	BlackCat	10%

2022年第3四半期において世界のランサムウェアのキャンペーンで最も利用された悪意のあるツール

弊社のグローバル遠隔観測では、複数のランサムウェアのキャンペーンに関連するIoCが確認されました。特定された攻撃で最も使用されていた悪意のあるツールは次の通りです。

1.	Cobalt Strike	33%
2.	Mimikatz	22%
3.	RCLONE	10%
4.	BloodHound	7%
5.	WinPEAS	6%

2022年第3四半期の最も報告されたランサムウェア MITRE ATT&CK 手法

弊社のグローバル遠隔観測から、複数のランサムウェアのキャンペーンに関連するIoCを確認しました特定された攻撃で最も利用されていたMITRE ATT&CK手法は以下の通りです。

1. 事業に影響を及ぼすデータ暗号化
2. システム情報の検出
3. ファイルとディレクトリの検出
4. システム回復の阻害
5. サービスの停止

27%

2022年第3四半期にIoC（indicators of compromise）の影響を受けた国のうち、ドイツが最上位にランクインし、特定されたランサムウェアキャンペーンによって影響を受けた上位10カ国のうち27%を占めました。

米国のランサムウェア

2022年第3四半期 米国のランサムウェアセクター

以下の統計データは、Trellix Advanced Research Centerが2022年第3四半期中に収集・分析した悪意のあるキャンペーンと関連する弊社の遠隔観測に基づいています。米国のお客様に関する弊社の遠隔観測から、複数のランサムウェアに関連するIoCを確認しました。特定されたキャンペーンの影響を最も受けたセクターは以下の通りです。

38%

2022年第3四半期に米国の上位10業種におけるマルウェアの総検出数では、ビジネスサービスでの検出が38%を占め、運輸・海運（23%）、通信（9%）、政府（9%）、メディア＆コミュニケーション（9%）を大きく上回る結果をなっています。

+100%

2022年第2四半期から第3四半期にかけて、運輸セクターにおけるランサムウェア検出数は100%増加しました。通信業界においても56%増加しました。その一方、金融業界における検出数は59%減少しています。

2022年第3四半期 米国ランサムウェアファミリー

最も蔓延していたマルウェアファミリーはLockBitです。2022年第3四半期の米国におけるランサムウェアファミリーのクエリトップ10のうち、19%で使用されています。次いで、Phobos（16%）、AvosLocker（13%）、Zeppelin（10%）、Cuba（9%）がこれに続いています。

2022年第3四半期、米国で最も検出されたランサムウェア ツール

米国のお客様に関する弊社の遠隔観測から、複数のランサムウェアに関連するIoCを確認しました。特定された攻撃で最も利用されていた悪意のあるツールは以下の通りです。

1. Cobalt Strike	34%
2. Mimikatz	22%
3. RCLONE	10%
4. Bloodhound	6%
5. Grabff	6%

2022年第3四半期に最も検出されたMITRE ATT&CK手法

米国のお客様に関する弊社の遠隔観測から、複数のランサムウェアのキャンペーンに関連するIoCを確認しました。特定された攻撃で最も利用されていたMITRE ATT&CK 手法は以下の通りです。

1. 事業に影響を及ぼすデータ暗号化
2. システム情報の検出
3. ファイルとディレクトリの検出
4. レジストリの変更
5. プロセスの検出

国家主導に関する統計データ

以下の統計データは、Trellix Advanced Research Centerの脅威インテリジェンスグループが収集・分析したキャンペーンと関連する弊社の遠隔観測に基づいています。

最も活発なAPTグループ

弊社のグローバル遠隔観測から、複数のAPT（持続的標的型攻撃または高度標的型攻撃）グループによるキャンペーンに関連するIoCを確認しました。これらのAPTグループはキャンペーン時にさまざまなツールを使用することが知られています。そのようなツールは、多数の攻撃者に使用される汎用的な悪意のあるツールから、特定のAPTグループのみが利用するカスタムマルウェアまで、多岐にわたります。特定されたキャンペーンにおいて最も活発に活動しているAPTグループは以下の通りです。

- Mustang Panda
- APT 29
- APT36
- MuddyWater
- Turla

2022年第3四半期の米国のランサムウェアで利用されている悪意のあるツールに関するハイライト

弊社のIoC追跡結果によると、2022年第3四半期に最も活発に活動していたAPTグループはMustang Pandaでした。

2022年第3四半期における国家主導の攻撃者の標的国

弊社のグローバル遠隔観測から、複数のAPTグループによるキャンペーンに関連するIoCを確認しました。特定された攻撃の影響を最も受けた国、セクター、およびツールは以下の通りです。

29%

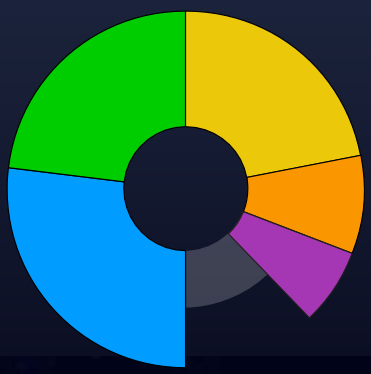
2022年第3四半期に最もAPTグループの標的とされた国はドイツです。全体の29%を占め、上位にランクインした標的国の中で最も多く検出されました。

2022年第3四半期の主な標的国

1.	ドイツ	29%
2.	米国	16%
3.	トルコ	12%
4.	イスラエル	10%
5.	インド	7%

2022年第3四半期における国家主導の攻撃者の標的となったセクター

弊社のグローバル遠隔観測から、複数のAPTグループによる攻撃に関連するIoCを確認しました。特定された攻撃の影響を最も受けていたセクターは以下の通りです。



- 運輸・海運
- 通信
- メディア＆コミュニケーション
- テクノロジー
- ビジネスサービス

国家主導の攻撃者が利用している悪意のあるツール

弊社のグローバル遠隔観測から、複数のAPTグループによる攻撃に関連するIoCを確認しました。特定された攻撃で最も利用されていた悪意のあるツールは以下の通りです。

1.	Mimikatz	24%
2.	PlugX	20%
3.	Cobalt Strike	18%
4.	Crimson RAT	7%
5.	Metasploit	6%

2022年第3四半期のメールセキュリティの傾向

これらの統計データは、世界中のお客様にインストールされている複数のメールセキュリティアプライアンスから生成された遠隔観測に基づいています。以下のセクションでは、検出ログを集計・分析した結果をご紹介します。

2022年第3四半期に最も影響を与えた悪意のあるメールのベクトル（侵入経路）

URL

91%

2022年第3四半期に検出された悪意のあるメールから悪意のあるペイロードをパック（圧縮）する手段として最も利用されたのはURLで、上位トップ10全体の実に91%を占めています。

2022年第3四半期に最も検出されたメール攻撃カテゴリ

1. フィッシング	68%
2. マルウェア	22%
3. 詐欺	9%
4. エクスプロイト	<1%
5. APT	<1%

2022年第3四半期に最も悪用されたメールのCVE

Microsoft Officeの数式エディターに影響する脆弱性

75%

2022年第3四半期において、CVE-2017-11882、CVE-2018-0798、CVE-2018-0802に含まれる「数式エディタの脆弱性」がお客様の受信した悪意のあるメールで最も悪用されたエクスプロイトです。これらの脆弱性を狙うエクスプロイトは、Formbook、Netwire、Generic Downloadersといった非常に蔓延しているマルウェアファミリーに組み込まれています。

2022年第3四半期に最も悪意のあるメールの影響を受けたセクター

金融サービス

20%

2022年第3四半期に最も悪意のあるメールの影響を受けたセクターは金融サービスでした。それに続き、州政府・自治体（13%）、製造業（12%）、連邦政府（11%）、サービス・コンサルティング（10%）が大きな影響を受けています。

トロイの木馬

83%

2022年第3四半期に検出された悪意のあるメールのうち、トロイの木馬が攻撃カテゴリ上位トップ5の83%を占めています。

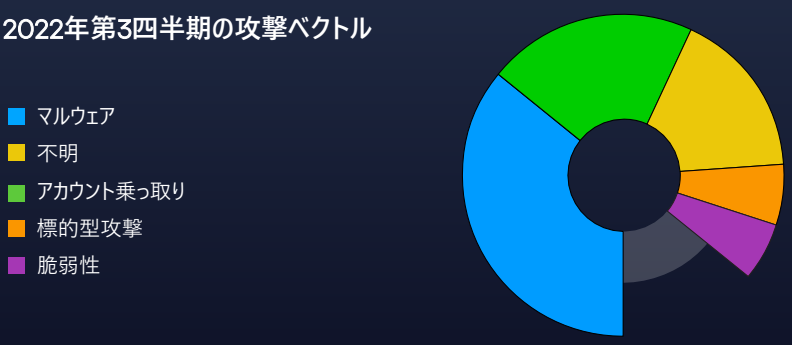
2022年第3四半期に最も確認されたメールのマルウェアファミリー

1. Exsto	17%
2. Agenttesla	16%
3. Formbook	15%
4. Leonem	7%
5. Guloader	7%

2022年第3四半期の国家、セクター、ベクトルに対する脅威

2022年第3四半期に、オープンソースで公開されているインシデントのうち、顕著なデータへの侵害は、以下の通りです。

2022年第3四半期の攻撃ベクトル



35%

2022年第3四半期に最も多くのインシデントが検出された国は米国でした（35%）。

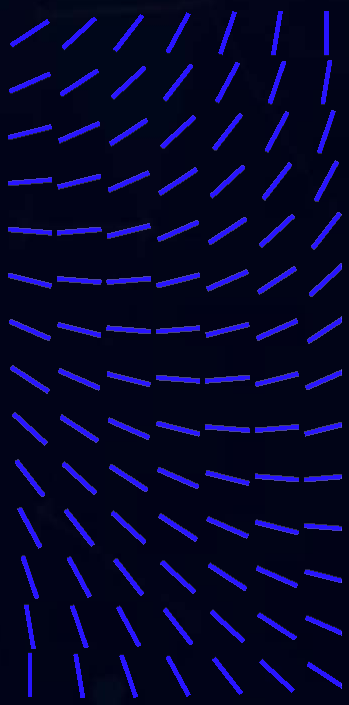
2022年第3四半期の攻撃セクター

1.	複数の業界	20%
2.	個人	11%
3.	公共	11%
4.	ヘルスケア	9%
5.	テクノロジー	6%

環境寄生のバイナリ（LOLBIN）とサードパーティーツール

2022年第3四半期のOSバイナリ

APTグループやランサムウェアグループなどの攻撃者は、 2022年第3四半期も継続的にOSバイナリを利用して定常的なタスクを実行していました。Windowsのコマンドシェル（CMD）やPowerShellなどのOSバイナリを使用することで、環境寄生型の攻撃者は、今まで以上に手間をかけずに、初期アクセスから偵察、そして標的情報の流出（持ち出し）まで、キャンペーンの各フェーズをスクリプト化することが可能になります。CMDとPowerShellは、引き続き最も悪用されたバイナリであり、そのあとにschtasksが続いています。過去3四半期および2021年を通して、攻撃者は初期アクセスからマルウェアの展開、侵入ツールの送り込み、そしてMITRE ATT&CKマトリクスに記載されているような影響を与えるまで、あらゆる段階においてOSバイナリを利用しています。例えばローダーとダウンローダーは、CMDを利用してMSHTAを起動し、ペイロードのロードしたり、追加のマルウェアをダウンロードしたり、システムやインフラ情報の流出させたり、スケジュールされたタスクを使用して、Webシェルをインストールして持続的アクセスを維持したり、ランサムウェアのキャンペーンで暗号化プロセスを開始したりすることがあります。



APTグループは、ADのユーザー、グループ、および権限の探索、およびトラストドメインの探索、セキュリティ障害の回避、権限の昇格などのタスクを実行する際に、OSバイナリを使用します。ランサムウェアのキャンペーンでは、OSバイナリやサードパーティツールを利用して、有効な認証情報を盗み出し、追加のペイロードを展開し、データの収集や流出タスクなどを開始することが確認されています。

2022年第3四半期に最も蔓延したOSバイナリ

1. Windowsのコマンドシェル（CMD）	38%
2. Powershell	37%
3. Schtasks	21%
4. WMI/WMIC	18%
5. Rundll32	13%

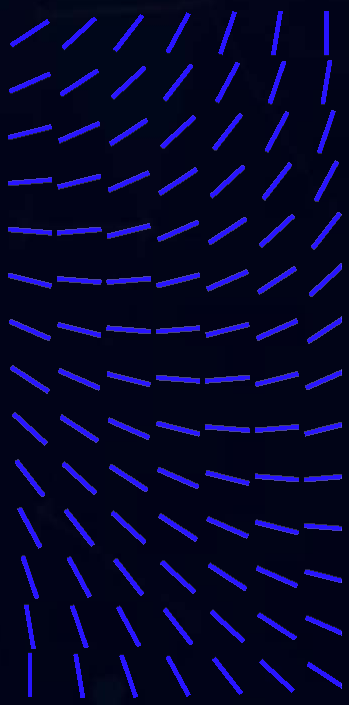
私たちは日々の業務を通じて、これらのOSバイナリが攻撃ライフサイクルの全域で繰り返し利用されていることを確認しており、また、今後もOSバイナリの悪用について報告していく予定です。

サードパーティーツールは、攻撃者が最も抵抗の少ない方法を追求する中で、引き続き関心を集めています。リモートアクセスツールは攻撃者にとって大きなリソースとなっています。最近では、レッドチームのツールがキャンペーンに利用されるケースが増えており、以前からあるツールでCobalt Strikeのような、検知を逃れるためのツールが数多く開発されています。システム管理者やセキュリティ専門家が使用するようなサードパーティーツールとOSバイナリを組み合わせれば、脅威アクターは労せずして武器化することができます。これらのツールは、ネットワークアセットの探索、標的データの収集と圧縮、攻撃者が管理するC2サーバへの持ち出しなどに利用することができます。

最近、サードパーティツールのセクションに「レッドチームツール」という項目が追加され、脅威者が悪用しているレッドチームツールに焦点が当てられるようになりました。これらのツールには、Cobalt Strike、BruteRatel 、Sliver Implantなどのツールが含まれますが、これらに限定されません。過去数年間、Trellix Advanced Research Centerでは、レッドチームツールであるCobalt Strikeの存在と悪用を継続的に追跡してきました。追跡を通じて、アジア、ヨーロッパ、北米で稼働するCobalt Strike C2サーバーの大部分を確認しました。

2022年第3四半期に使用されたサードパーティーツール

1. リモートアクセスツール	29%
2. レッドチームツール	16%
3. ファイル転送	10%
4. ネットワーク検出	9%
5. ADの検出	4%



さらに、私たちの脅威探索活動により、使用されているライセンスの種類を特定し、データを集計して、Cobalt Strikeのライセンス版、クラック版、盗用版の使用を特定し、その使用を脅威者のクラスターに帰属させることができました。このうち、56%強がツールのトライアル版、26%がEvilCorpとMazeグループによって悪用されたライセンス、17%がUNC1878（RYUK）によって悪用されたライセンス、残りの1%が正規のセキュリティ企業、クラック版、REvilグループによって悪用されたライセンスに起因していることが判明しています。

Cobalt Strikeはもともと、セキュリティ専門家が攻撃シナリオをエミュレートし、卓上演習を行うためのレッドチームツールとして開発されました。ハッカーがハッカーであるように、脅威者もこのツールの性能に注目し、悪意を持ってこのツールを再利用しています。Cobalt Strikeは、脅威グループの間で人気を博し、クラックされたバージョンがダークウェブフォーラムに流れ、トレールバージョンが攻撃に使われるようになると、すぐに常用ツールとなりました。検出機能の開発により、このツールを善意と悪意の両方の目的で使用することは難しくなりました。Sliver ImplantやBruteRatelといった他のツールは、Cobalt Strikeの代替品として開発されました。これらはキャンペーンに登場し、攻撃中に気づかれないように検出回数が少ないツールを求める脅威アクターによって徐々に採用されています。

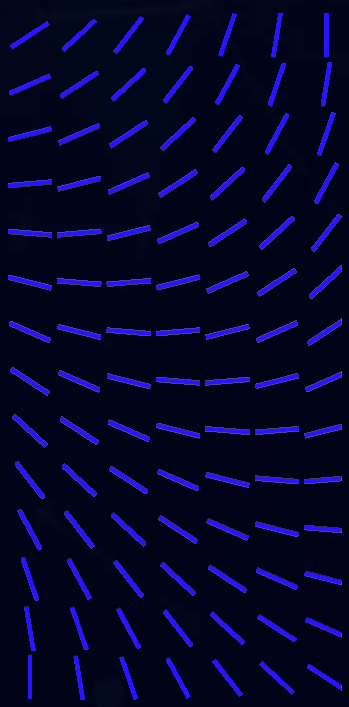
Cobalt Strikeは、最初のアクセスから脱出までのタスクを実行する際に、攻撃者の間でよく選ばれるツールであり続けています。2022年第3四半期、Trellix Advanced Research Centerでは、政治的な動機のある脅威グループから国家が支援するAPTに至るまで、攻撃のライフサイクルを通じてCobalt Strikeを利用するキャンペーンが確認されています。また、レッドチームツールは、スタンドアロン型ランサムウェアファミリーやランサムウェア・アズ・ア・サービスの運営者によって、暗号化段階の前に「認証情報の回復」、インフラの発見、および流出タスクが実行されているキャンペーンでも確認されています。このようなサードパーティのレッドチームツールの使用は、脅威を取り巻く環境において増加し続けているため、攻撃に使用されるサードパーティツールの上位に存在する場合は、レポートに含まれるツールの一部として記載することが重要です。

2022年第3四半期 Insightsでのランサムウェアの追跡

Insightsプラットフォームで処理されるランサムウェアイベントは、彼らが悪用する脅威のアクターとツールを追跡します。ほぼすべてのランサムウェアイベントは、システム上に存在するOSバイナリや、ITおよび情報セキュリティチームが日々のタスクを実行するために使用するサードパーティツールの不正使用を含む、Living off the Landの証拠を示しています。これらのツールは、自動化、タスクのスケジューリング、権限の昇格、パスワードの「回復」、侵入ツールの転送などに悪用される可能性があります。ランサムウェアが最終的なペイロードとなった2022年第3四半期において、Insightsプラットフォームで処理されたイベント数は15%強にとどまりました。キャンペーンの中には、複数のランサムウェアファミリーを含んでいたり、この統計の時点ではランサムウェアがまだ特定されていないものもあります。ここに挙げたランサムウェアのファミリーは、業界団体から報告されたもの、およびTrellix Advanced Research Centerが追跡しているものを表しています。興味深いことに、新しいランサムウェアや生き残ったランサムウェアのうち、ヘッドラインを飾り続けているいくつかのファミリーは、遠隔測定によって、Phobosのように、まだ活動を続けているランサムウェアのファミリーがあることがわかっていますが、一般のレポートではあまり目にすることはありません。

2022年第3四半期 ランサムウェア

LockBit Ransomware
BianLian Ransomware
BitLocker
Black Basta Ransomware
BlackByte Ransomware
Maui Ransomware
ROADSWEEP Ransomware
Agenda Ransomware
BlueSky Ransomware
Crytox Ransomware
Cuba Ransomware
FARGO Ransomware
GwisinLocker Ransomware
H0lyGh0st
HavanaCrypt Ransomware
Industrial Spy Ransomware
Karma
LILITH
MedusaLocker
Noberus Ransomware
Ragnar Locker
Ransomware RedAlert
Redeemer Ransomware
Slam Ransomware SolidBit Ransomware



著者および調査者

Alfred Alvarado
Sushant Arya
John Fokker
Lennard Galang
Tim Hux
Tim Polzer
Srini Seethapathy
Rohan Shah
Sal Vashisht
Leandro Velasco

リソース

以下の Trellix のリソースをご活用いただき、Trellix Advanced Research Centerによる最新の脅威や調査結果の把握にお役立てください。

TWITTER

Trellix ARC

脅威レポートのアーカイブを見る

Trellix Advance Research Center

TRELLIX ADVANCED RESEARCH CENTERについて

Trellix Advanced Research Centerは、サイバーセキュリティ業界で最も包括的な憲章を掲げ、あらゆる脅威の状況における新たな手法、傾向、そして攻撃者に対する最前線を担っています。Trellix Advanced Research Centerは、世界のセキュリティオペレーションチームの主要パートナーとして、セキュリティアナリストにインテリジェンスと最先端のセキュリティ情報を提供すると同時に、業界をリードするTrellixのXDRプラットフォームを強化しています。

TRELLIX について

Trellixは、サイバーセキュリティの未来を再定義するグローバル企業です。TrellixのオープンかつネイティブなXDR（Extended Detection and Response）プラットフォームは、現在最も高度な脅威に直面するお客様が業 務の保護や回復に確信を持って対応するための支えとなります。Trellixのセキュリティ専門家は、広範なパートナーエコシステムとともに、データサイエンスと自動化によりテクノロジーイノベーションを加速させ、4万を超える企業や政府機関のお客様の力となっています。詳しくは、www.trellix.comをご覧ください。

Trellix Advance Research Center

ご登録いただくことで、Trellixが提供する脅威情報をご入手いただくことができます。

詳しくは、 Trellix.comをご覧ください。

072022-05