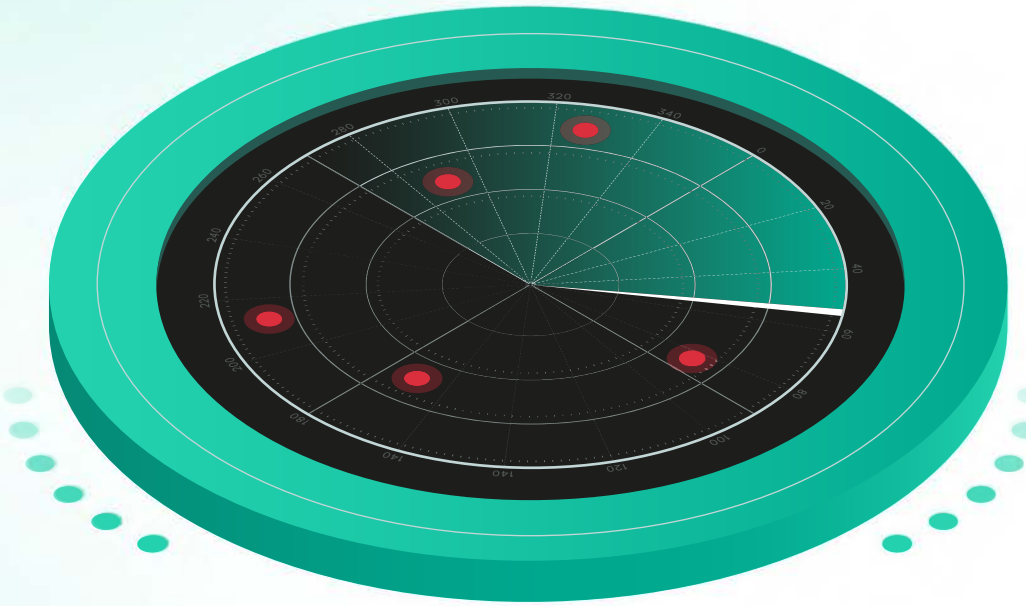
Incident response analyst report

日本語版
2021年9月



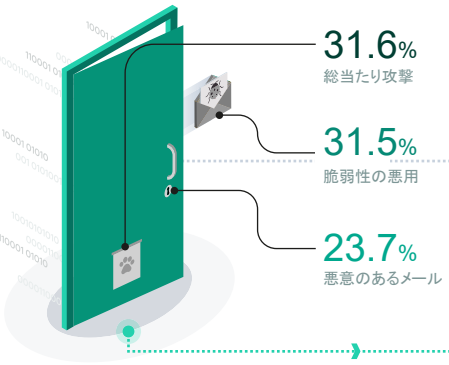
kaspersky

エグゼクティブサマリー

当レポートの統計は、2020年に当社が実施したインシデントレスポンス支援のための
年間リテナーサービスと緊急スポットサービスの内容を集計したものです。

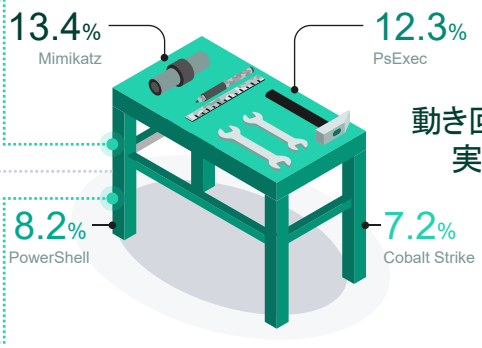
脅威インテリジェンスの視点

初期の侵入経路



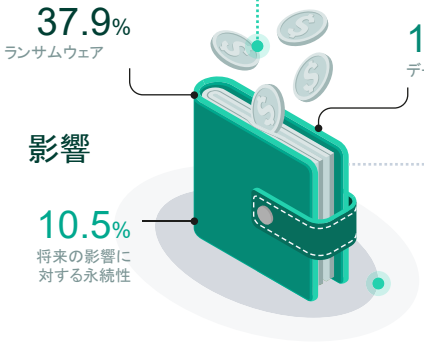
- 堅牢なパスワードポリシーと多要素認証を実装する
- パブリックアクセスから管理ポートを削除する
- 公開アプリケーションのパッチ管理や補償対策には一切妥協しない
- 従業員のセキュリティ意識を高いレベルで維持する

動き回り攻撃を実行する



- 攻撃者間で広く使われているツールを検知するためのルールを実装する
- EDRのようなテレメトリを持つセキュリティツール群を使用する
- 対攻撃演習により、セキュリティオペレーションの反応時間を常にテストする
- 社内ITチームが類似ツールを使用しないようにする

影響



- データのバックアップ（オフラインのバックアップ）
- インシデントレスポンス支援の年間リテナーサービスを利用し、迅速なSLAでインシデントに対応する
- 個人情報を扱うアプリケーションに対して、厳密なセキュリティプログラムを実装する
- トレーニングおよび対攻撃演習を通じて、インシデントレスポンスチームの準備態勢を常に維持する

業界

22% 製造
19% 政府
13% 金融
13% 通信

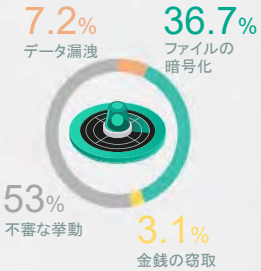
- 業界や地域を狙う攻撃者と攻撃内容を把握し、セキュリティ投資に優先順位をつける

地域

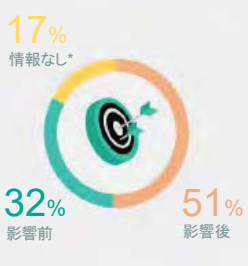
27.8% CIS
26.8% META
24.7% ヨーロッパ
16.5% 南北アメリカ

セキュリティ対策の視点

検知の理由



検知は影響が出る前か後か



攻撃の期間

修復にかかる期間

*別のIRチームの補完的なサプライヤーとして活動した場合は、影響に関する情報はありません

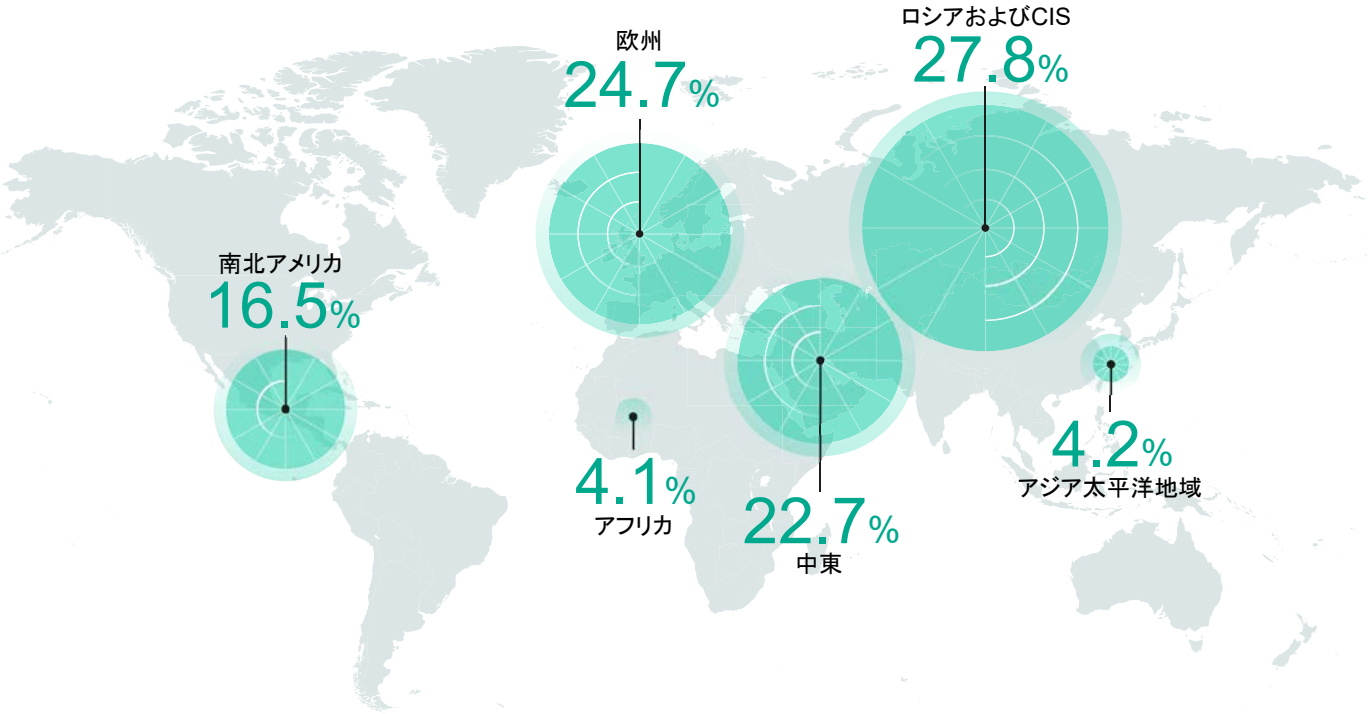
はじめに

当インシデントレスポンスの分析レポートは、2020年に当社が実施したインシデントの調査サービスについての所見をまとめたものです。当社は、インシデントレスポンス、デジタルフォレンジック、マルウェア解析など、さまざまなサービスを提供しています。このレポートのデータは、本格的なインシデントレスポンスの支援や、組織内のインシデントレスポンスチームを補助的にサポートするなど、日々の専門的な活動から得たものです。

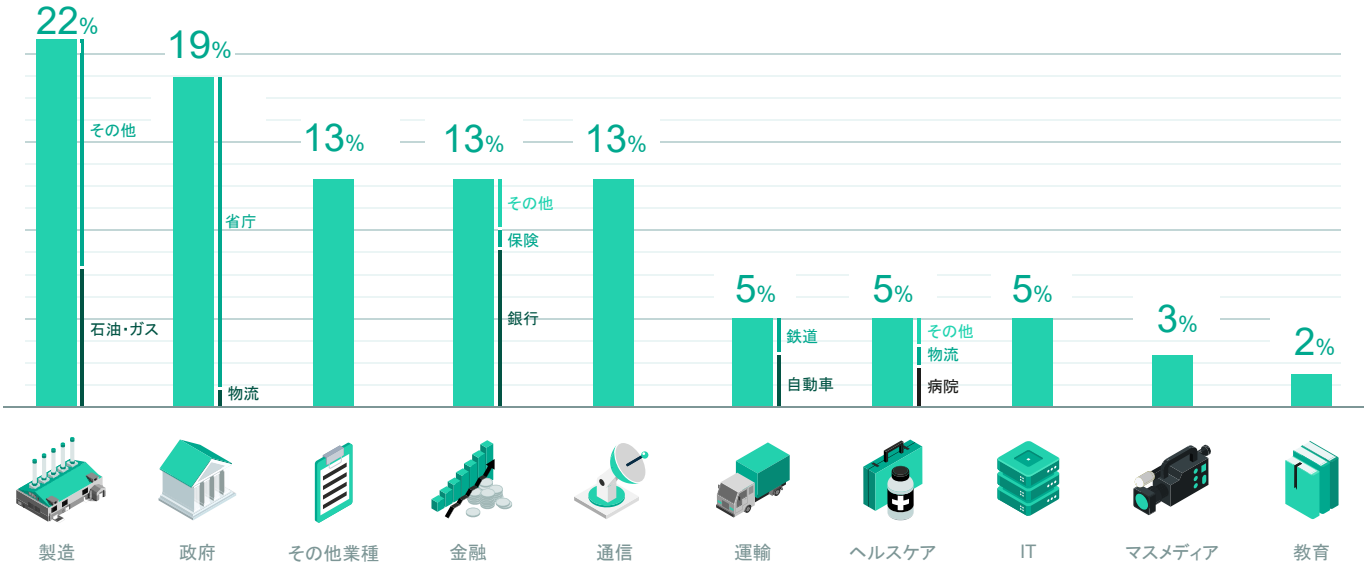
2020年、新型コロナウイルスの世界的感染拡大により、企業は在宅勤務という勤務形態に合わせて、情報セキュリティ対策の再構築を余儀なくされました。サイバー脅威に関していえば、主流のトレンドは変わりませんでしたが、当社のサービス形態は完全に(ケース全体の97%)リモートでの提供に移行しました。

当社でデジタルフォレンジックとインシデントレスポンスを担当しているのは、グローバル緊急対応チーム(GERT)、コンピューターインシデント調査ユニット(CIIU)、グローバル調査分析チーム(GReAT)で、ヨーロッパ、アジア、南北アメリカ、中東、アフリカ在住のエキスパートたちです。

地域別インシデントレスポンスの対応件数



業種および業界

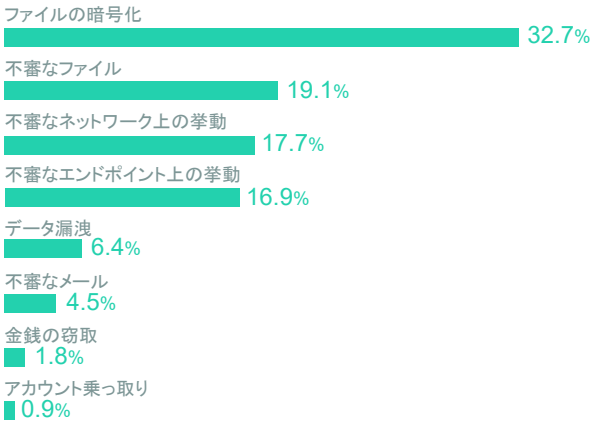


インシデントレスポンス実施の理由

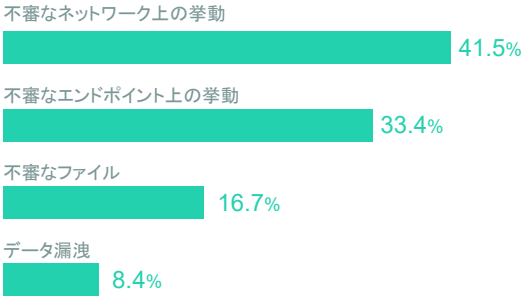
ランサムウェアは、金銭の窃取およびその他の影響を追い越して、金融機関だけではなく、さらに幅広い業界を対象にしたより手軽な収益化の手段となりました。影響が出る前に不審なイベントやツールの警告などがあったインシデントの大半は、ランサムウェアに分類することができます。

当社が依頼を受けたインシデントレスポンスのうち、10%は誤検知でした。誤検知の大半は、ネットワークセンサー（NIDS、ファイアウォール）およびエンドポイント保護製品（EPP）から報告された不審な挙動*です。そのうちの4件に1件は、誤検知でした。データ漏洩として誤検知されたケースは、通常、重複または別の組織からの漏洩です。

正しい検知



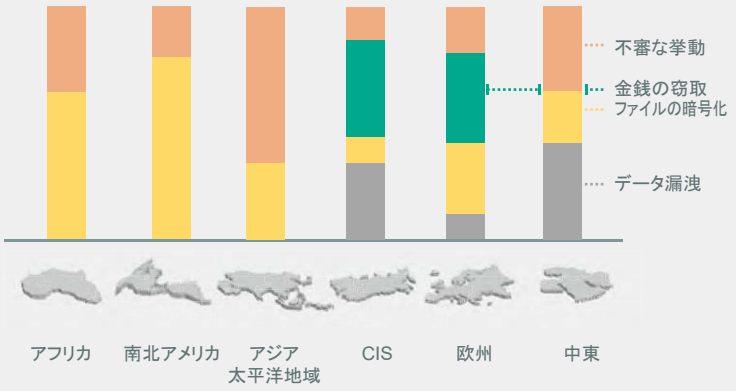
誤検知



ランサムウェアによる攻撃は、長年にわたりサイバーセキュリティの脅威の中で主要な役割を果たしてきました。ランサムウェア攻撃に関する最新の情報は、当社の発行物やNoMoreRansomプロジェクト、および脅威レポートから入手されることを強くお勧めします。

地域別の理由

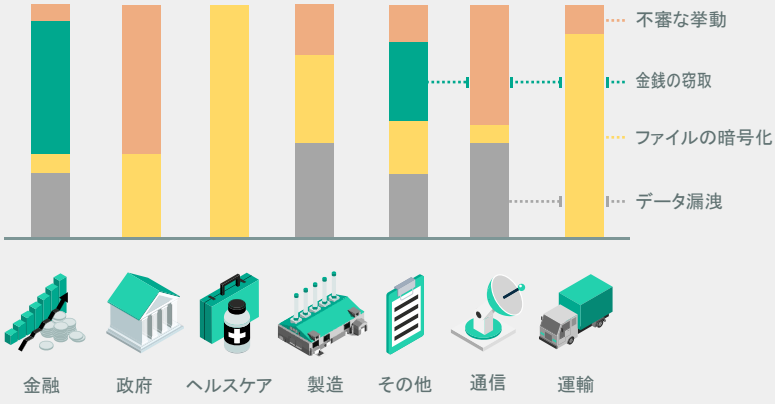
南北アメリカとアフリカでは、ランサムウェアによる攻撃が多くを占めています。その他の地域では、攻撃の種類はさまざまですが、データ漏洩は明らかな脅威となっています。



業界別の理由

従来の金融業界を攻撃対象とした収益化は継続される一方で、ヘルスケア、運輸、製造業界がランサムウェアの大きな影響を受けるようになりました。

政府機関からのデータ漏洩が示されていない理由は、個人情報を多用する政府機関のシステムは通常、通信事業者またはITプロバイダーによりホストされているからだと考えられます。



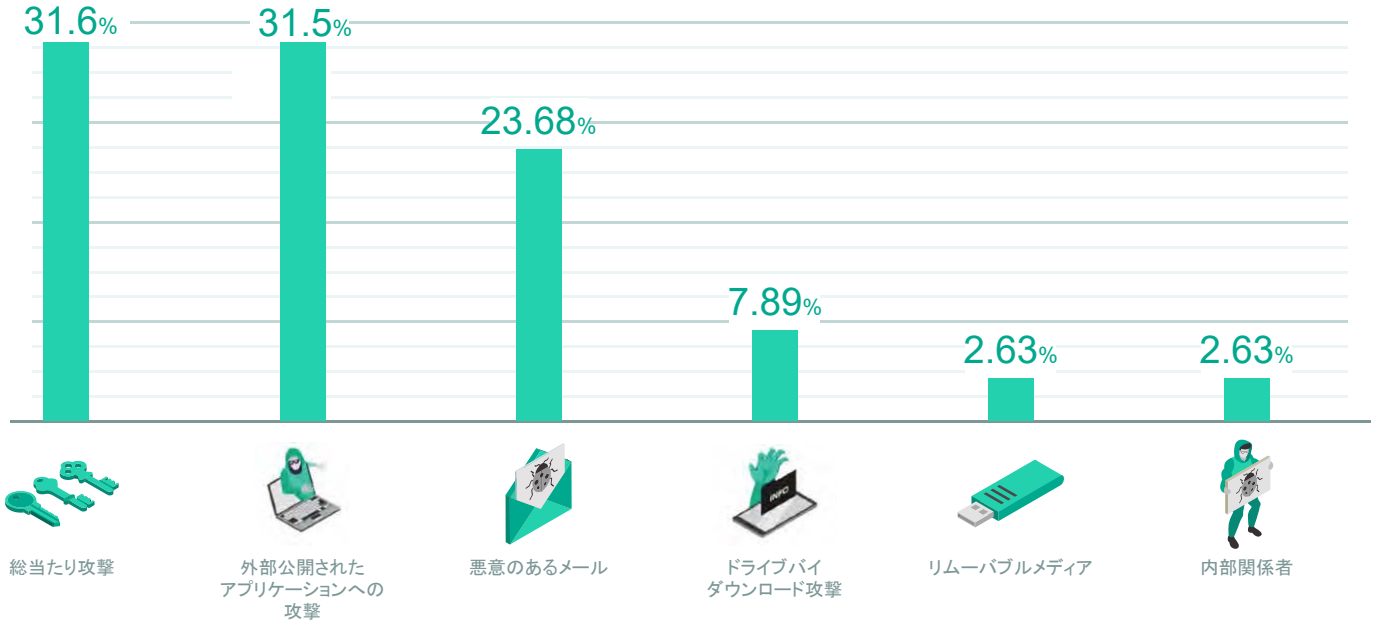
* 不審な挙動とは、セキュリティツール群が生成したアラート、またはユーザーが報告した異常動作を表わすカテゴリーです。

サイバー攻撃の経路

攻撃者はどのように侵入するか

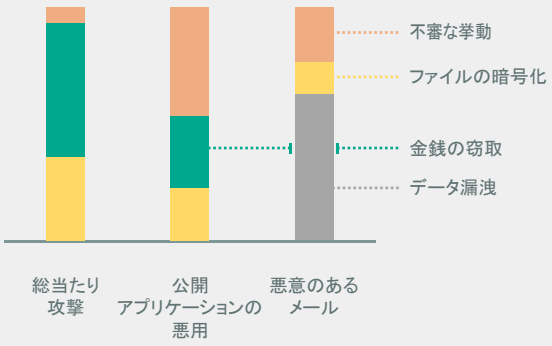
初期の侵入経路*として、パスワードのセキュリティ問題、ソフトウェアの脆弱性、およびソーシャルエンジニアリングが占める割合が年々増えており、今ではその大半となっています。パスワードポリシーの適用と制御、セキュリティパッチの管理、フィッシング対策に伴う従業員の意識向上により、外部からの攻撃活動を大幅に抑えることができます。

攻撃者は悪意のある攻撃を実行する際に、よく知られた脆弱性や既知のセキュリティ上の弱点が存在するパブリックサーバーなど、容易に使用できる攻撃口を見つけようとします。標的になる可能性は、適切なパッチ管理のポリシーを導入すると30%低下し、強固なパスワードポリシーを導入すると60%低下します**。



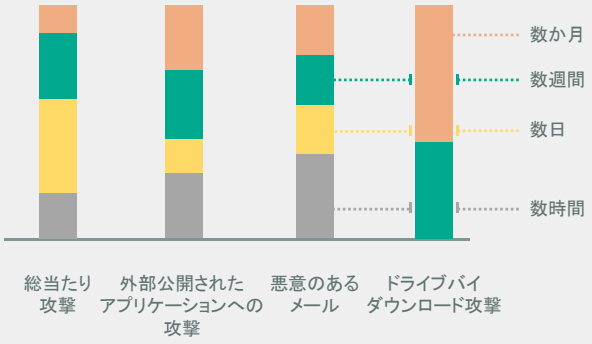
主な初期の侵入経路とインシデント検知の理由

ランサムウェアによる攻撃は、広く知られているほぼ全ての初期アクセス方法を使用します。総当たり攻撃は理論的には検知されやすいはずですが、実際には、影響を受ける前に特定できたケースはごく一部に過ぎません。



主な初期の侵入経路と攻撃発見までの期間

総当たり攻撃、外部アプリケーションの悪用、および悪意のあるメールをきっかけとした全攻撃のうち、半数以上が数時間から数日のうちに検知されました。
初期侵入を特定できなかった多くのケースは、発覚するまでに1年以上経過し、ログの保存ポリシーにより、分析に使用できる攻撃行為の痕跡が残っていませんでした。



* 当社はケースの55%で初期の侵入経路を特定しました。標的ネットワークへの初期侵入方法を特定できなかった原因としては、インシデント発生からかなり時間が経過していた、ログが利用できなかった、被害組織による故意（または意図せず）の証拠隠滅、サプライチェーン攻撃など多岐にわたります。
** 当社が実施したインシデント調査データ。

ツールとエクスプロイト

全インシデントのうち、44%は正規ツールを使用

全インシデントケースのほぼ半分で、既存のOSツール（LOL bin：環境寄生型バイナリなど）、GitHubにあるツール（例：Mimikatz、AdFind、Masscan）、標的型攻撃を模倣することができる商用製品（Cobalt Strike）が使用されていました。

全インシデントケースにおいて、ツールが使用された割合

頻繁に使われる

11-13%

Mimikatz、PsExec、Advanced IP Scannerなど

ある程度使われる

4-8%

Powershell、Cobalt Strike、Process Hacker、ProcDumpなど

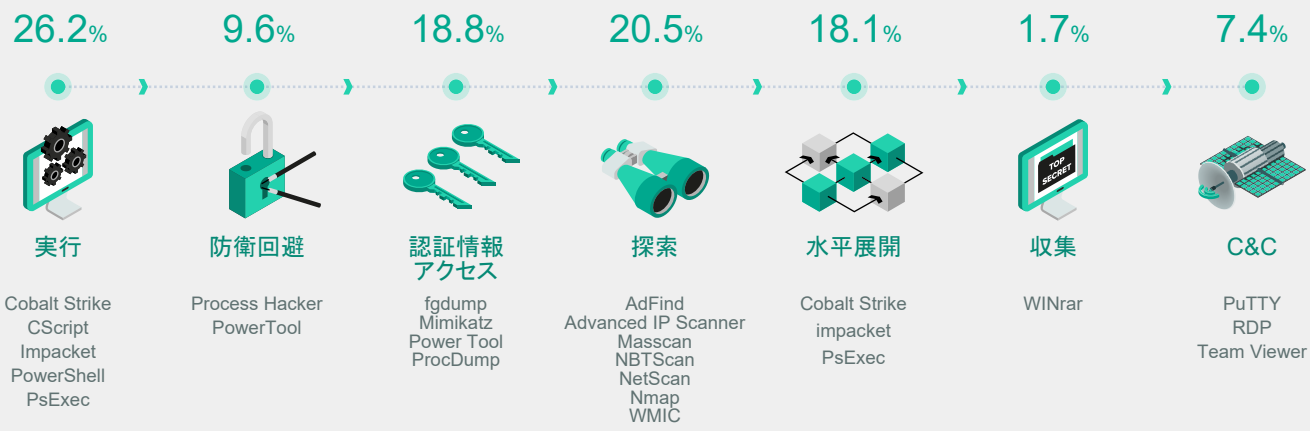
稀に使われる

2-3%

Team Viewer、Impacket、WMIC、Power Tool、Nmap、fgdump、Masscan、CScript、NetScan、WINrar、AdFind、NBTScan、PuTTY、RDPなど

MITREATT&CKの戦術にツール類の利用と頻度を当てはめてみると、初期アクセスから影響までの全てに明確に焦点を当てていることがわかります。

こういったツール類は、攻撃者が対象のネットワーク内を探索している間に、インシデント検知を高める優れた手段となるはずです。



全インシデントのうち、13%で脆弱性を悪用

2020年に発見された脆弱性を悪用したインシデントはわずかです。その他のケースでは、数年前から存在する既知の脆弱性が悪用されていました。タイムリーなセキュリティアップデートによって、インシデント調査対象となった攻撃の10分の1は阻ぐことができたと考えられます。

CVE-2020-0796

Microsoft WindowsのSMBサービス

リモートコード実行の脆弱性。これにより攻撃者はMicrosoft SMBv3で認証なしに任意のコードを実行できる。MS17-010の後継。

CVE-2020-0787

Windows Background Intelligent Transfer Service（BITS）

Windows BITSの権限昇格の脆弱性。ランサムウェアの攻撃に広く使用されている。

CVE-2019-11510

Pulse Secure SSL VPN

VPNサーバーのユーザー認証情報を認証なしに取得。正規のチャネルを通じて標的の組織に容易にアクセスできる。

CVE-2019-0604

Microsoft SharePoint

リモートコード実行の脆弱性。これにより攻撃者はMicrosoft SharePointで認証なしに任意のコードを実行できる。

CVE-2018-8453

Win32k Microsoft Windows コンポーネント

Win32kコンポーネントが、メモリ内オブジェクトの適切な処理に失敗した場合に、Microsoft Windowsに権限昇格の脆弱性が存在する。Fruity Armor APTグループにより使用されている。

CVE-2017-0144

Microsoft Windows SMBサービス

SMBv1の脆弱性により、リモート攻撃者は細工されたパケット経由で任意のコードを実行できるようになる。EternalBlueエクスプロイトで使用されている。

CVE-2017-11317

Telerik.Web.UI

暗号強度が不十分なRadAsyncUploadを使用する脆弱性で、リモートの攻撃者が任意のファイルアップロード、または任意のコードを実行できるようにする。

CVE-2017-8464

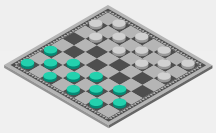
Microsoft Windows Shell

ローカルユーザーまたはリモートの攻撃者が、ショートカットのアイコンを解析するWindows Explorer、または他のアプリケーション上でアイコンの表示が適切に処理されないように細工された .LNKファイルを介して、任意のコードが実行される可能性がある。LemonDuck攻撃で使用されている。

* 各ツールは、インシデントケースの11～13%で特定されている

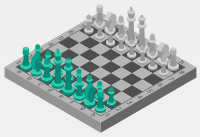
攻撃の期間

インシデントケースは全て、攻撃期間、インシデントレスポンス期間、初期アクセス、攻撃の影響に応じて3つのカテゴリーに分類できます。



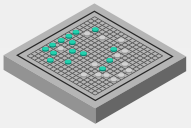
短期の攻撃

数時間から数日



平均的な攻撃

数週間



長期にわたる攻撃

数か月以上

攻撃期間（平均）

短期の攻撃	平均的な攻撃	長期にわたる攻撃
1.5日間	18.1日間	90.4日間

代表的な影響

短期の攻撃	平均的な攻撃	長期にわたる攻撃
ランサムウェア	ランサムウェアと金銭の窃取	データ漏洩とランサムウェア

初期の侵入経路（件数ベースによる評価）

短期の攻撃	平均的な攻撃	長期にわたる攻撃
▪ 総当たり攻撃 ▪ 外部公開されたアプリケーションへの攻撃 ▪ スピア型攻撃のリンク	▪ 外部公開されたアプリケーションへの攻撃 ▪ ドライブバイダウンロード攻撃 ▪ 総当たり攻撃 ▪ リムーバブルメディアを介した複製 ▪ スピア型攻撃のリンク	▪ 外部公開されたアプリケーションへの攻撃 ▪ スピアフィッシングのメール添付ファイル ▪ 総当たり攻撃 ▪ ドライブバイダウンロード攻撃 ▪ 内部関係者

インシデントレスポンス期間（調査時間）

短期の攻撃	平均的な攻撃	長期にわたる攻撃
34.4時間	48.9時間	105.6時間
▪ 最長1週間続く攻撃 ▪ 素早い大規模なランサムウェアの攻撃で、十分なセキュリティ対策を取っていても検知は困難。簡単に手の届くところにある目標、つまり簡単に特定できる公開済みセキュリティの問題を土台にした、表面的にわかりやすい攻撃行動が大半である	▪ 最長1か月続く攻撃 ▪ ランサムウェアが原因で、多くの攻撃が短期の攻撃と区別できない。このグループの多くのケースは、初期アクセスから2回目以降の攻撃段階までの間隔が長い	▪ 1か月を超えて続く攻撃 ▪ 攻撃が活発な期間とそうでない期間が交互に来るが、それぞれの持続時間は一定ではない。活動が活発な期間の持続時間は、平均的な攻撃と非常によく似ている

お問い合わせ先

ビジネスに関するお問い合わせ

intelligence@kaspersky.com

レポートおよびIRに関するお問い合わせ

gert@kasperksy.com

kaspersky