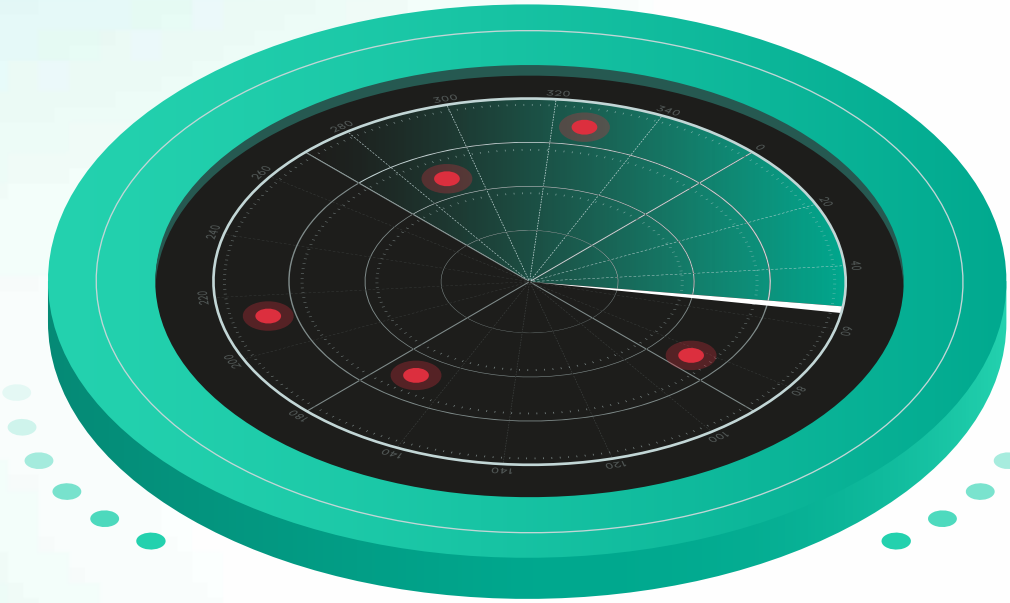
Incident response analyst report

日本語版

2020年8月



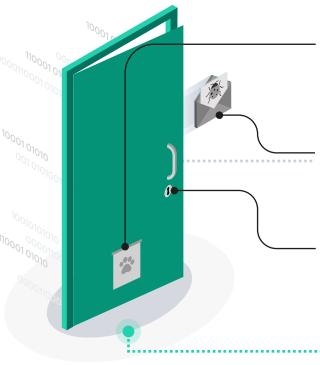
kaspersky

エグゼクティブサマリー

当インシデント対応分析レポートの統計は、2019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

最初の攻撃経路

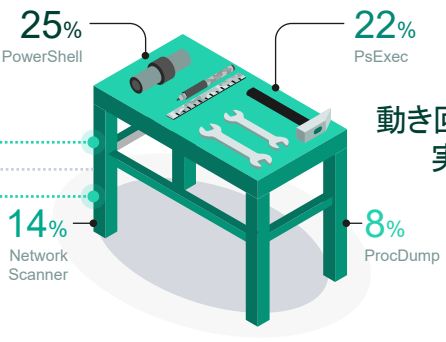


- 37% 脆弱性の悪用
- 30% 悪意のあるメール
- 13% 総当たり攻撃

- 公開されているサービスへ速やかにパッチを当てる
- メール保護を強化し、従業員の意識を高める
- パブリックアクセスから管理インターフェースを削除

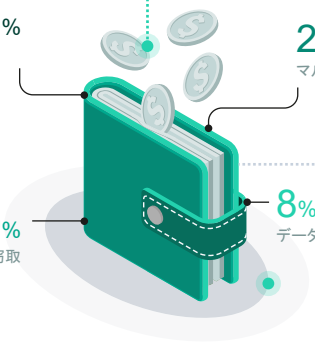
- 攻撃の検知には、豊富なテレメトリとPowerShellの詳細なトレースによる脅威ハンティングが必須である
- PsExecは不審なイベントではないが、管理の必要なインシデントである

動き回って攻撃を実行する



- 25% PowerShell
- 22% PsExec
- 14% Network Scanner
- 8% ProcDump

影響



- 34% ランサムウェア
- 21% マルウェアの感染
- 8% データ漏洩
- 9% 金銭の窃取

- ランサムウェア対策を徹底する
- 頻繁にデータを隔離されたインフラストラクチャーへバックアップする

業界

29%	16%	15%	10%
製造	金融	政府	通信

業界や地域を狙う攻撃者と攻撃内容を知り、セキュリティ投資に優先順位をつける

地域

32%	24%	21%	15%
中東	欧州	CIS	中南米

セキュリティ対策の視点

攻撃の期間

31%	24%	22%	13%
数日	数か月	数週間	数時間

短時間で検知されたインシデントの大半はランサムウェアによるもので、目に見える形でインフラストラクチャーまたはプロセスが阻害されています

検知の理由

32%	27%	13%	11%
不審なファイル	ファイルの暗号化	疑わしいエンドポイントの動作	その他のセキュリティツールのアラート

インシデントの識別において、セキュリティ対策とセキュリティツール群が大きな役割を果たしています

修復にかかる期間

43%	27%	15%	13%
数週間	数日	数か月	数時間

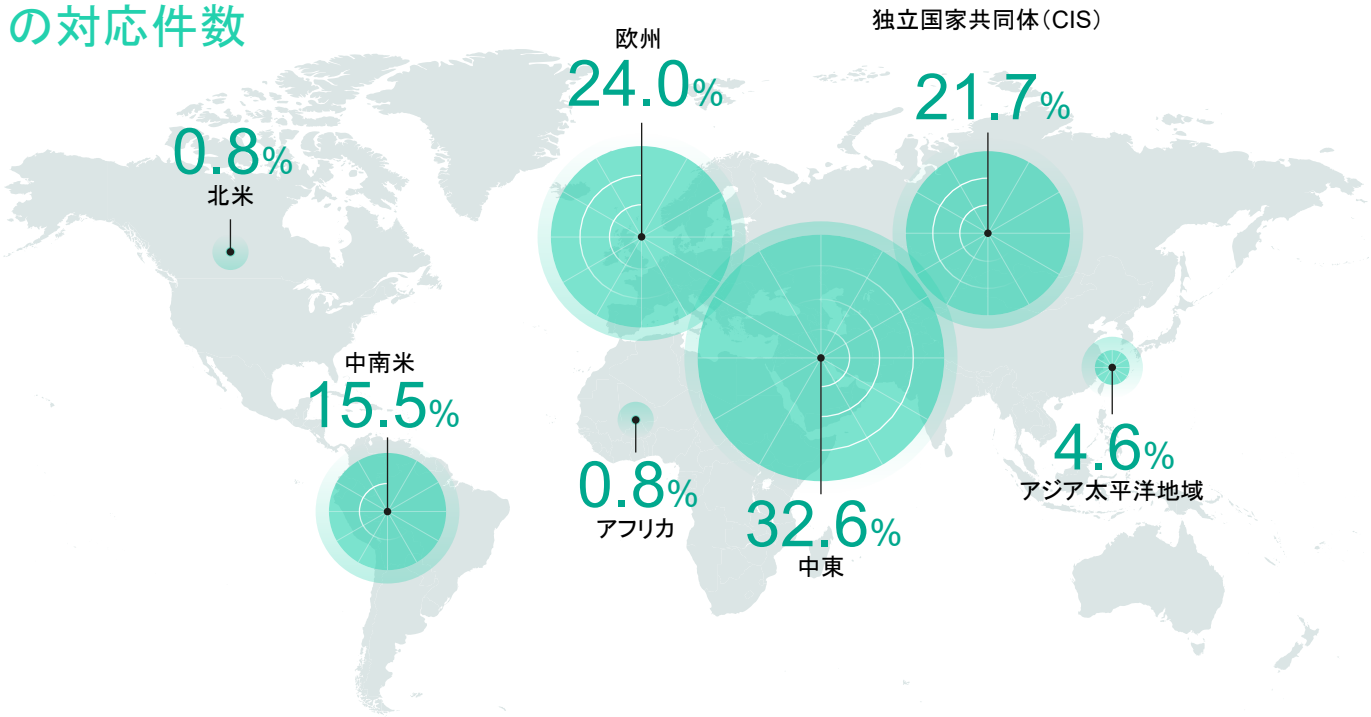
改善の余地はいつでもあります。インシデントレスポンス支援の年間リテナーサービスを利用するか、事前にインシデントレスポンスのサービス提供事業者を探しておくことを推奨します

はじめに

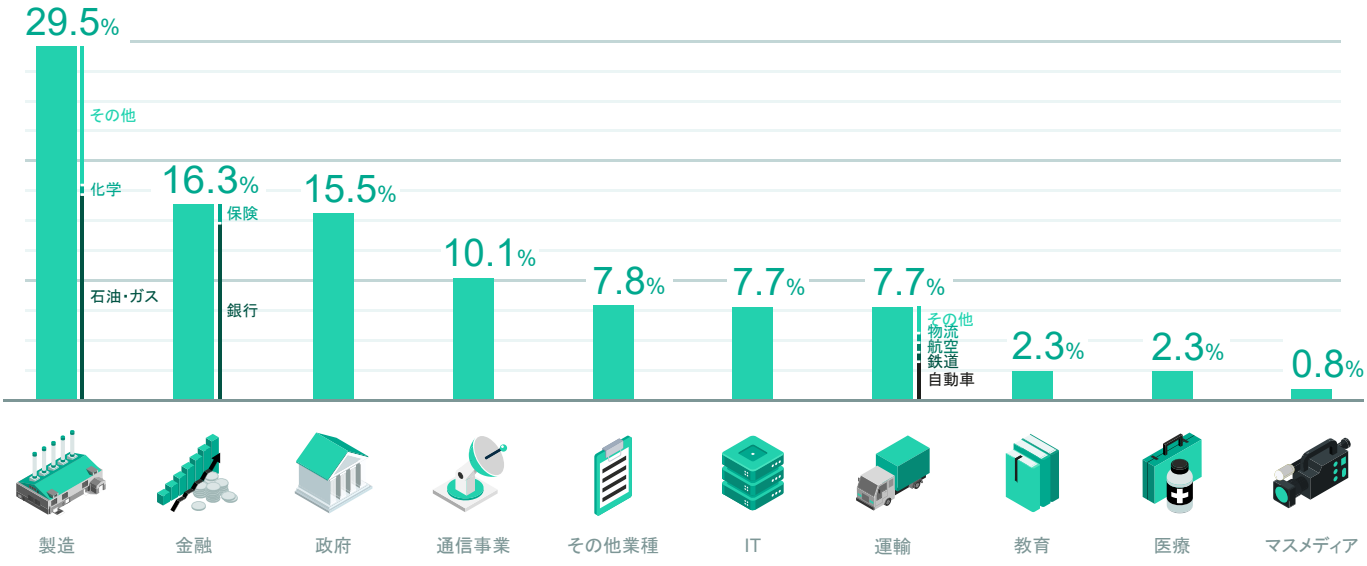
当インシデントレスポンスの分析レポートは、2019年に当社が実施したインシデントの調査サービスについての所見をまとめたものです。当社は、インシデントレスポンス、デジタルフォレンジック、マルウェア解析など、さまざまなサービスを提供しています。このレポートのデータは、本格的なインシデントレスポンスへの支援を求める組織や、組織内のインシデントレスポンスチームに無償で提供している当社の専門的な活動など、日々の実践から得たものです。

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

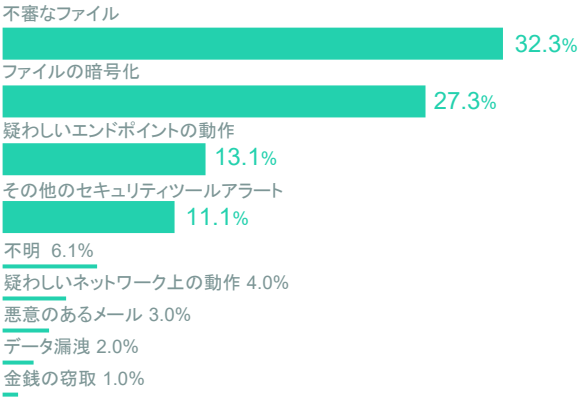


インシデントレスポンス実施の理由

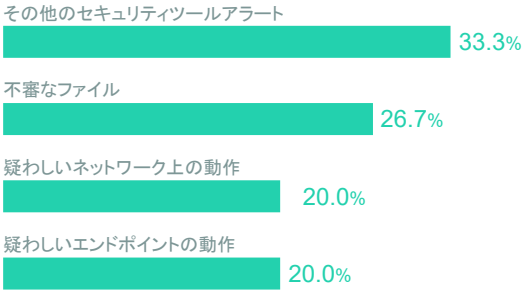
当社が依頼を受けたインシデントレスポンスのうち、30%はアセットの暗号化、金銭的損害、データ漏洩、不審なメールなどインフラストラクチャーに対する顕著な影響によるものでした。50%超が、エンドポイント（EPP、EDR）、ネットワーク（NTA）、その他（FW、IDS/IPSなど）のセキュリティツール群のアラートによるものでした。

基本的なセキュリティツール群が攻撃の一部を検知し、アラートを出していたとしても、顕著な影響が出るまで組織がインシデントに気づかないことはよくあります。このような兆候を見逃す最大の理由はセキュリティ運用スタッフの不足です。ケースの75%で、セキュリティ対策により特定された不審なファイルや、エンドポイントの怪しい動作がインシデントの発見につながりましたが、ネットワーク上の怪しい動作の60%は誤検知でした。

正しい検知



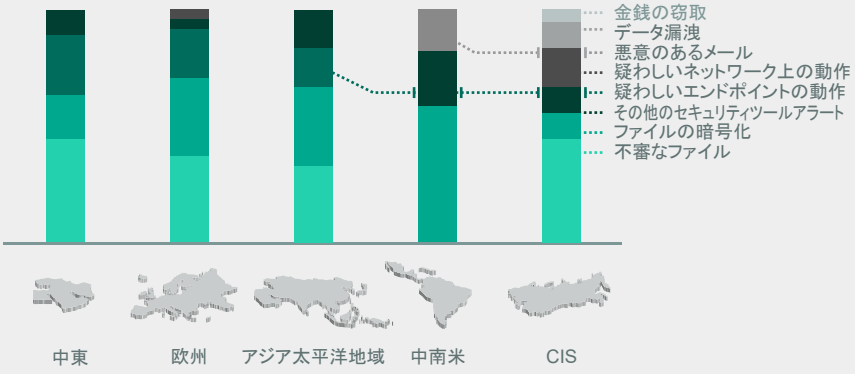
誤検知



インシデントレスポンス支援の依頼の中で、最も多い理由の1つはランサムウェアによる攻撃です。これは、十分なセキュリティ対策を取っていても検知は困難です。ランサムウェアの種類とセキュリティ対策について詳しくは、「Cities under ransomware siege（ランサムウェアに包囲された都市）」をご覧ください。

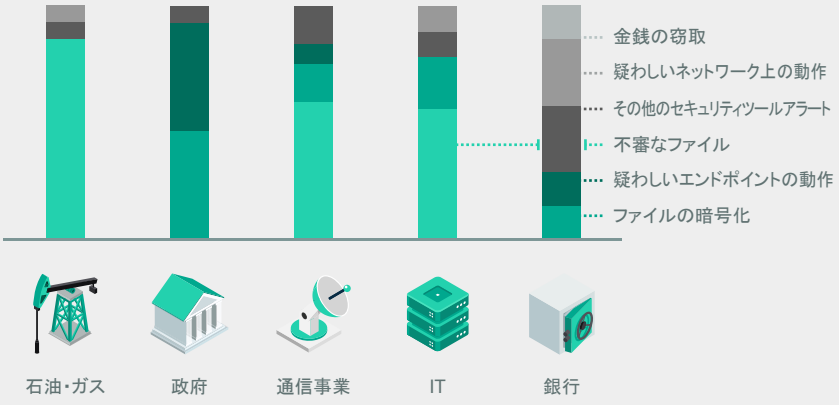
地域別の理由

- 最大の割合が「不審なファイル」であることから、現時点でも、多くの組織でファイルに由来する検知が多発しています
- 調査した金銭的な動機によるサイバー犯罪、およびデータ漏洩が関連するケースのすべてが、CIS諸国で発生していました



業界別の理由

- 意外なことに、金銭の窃取の100%が、金融機関（銀行）の内部で起きていました
- ランサムウェアは主に政府機関、通信事業、IT業界で影響を与えています

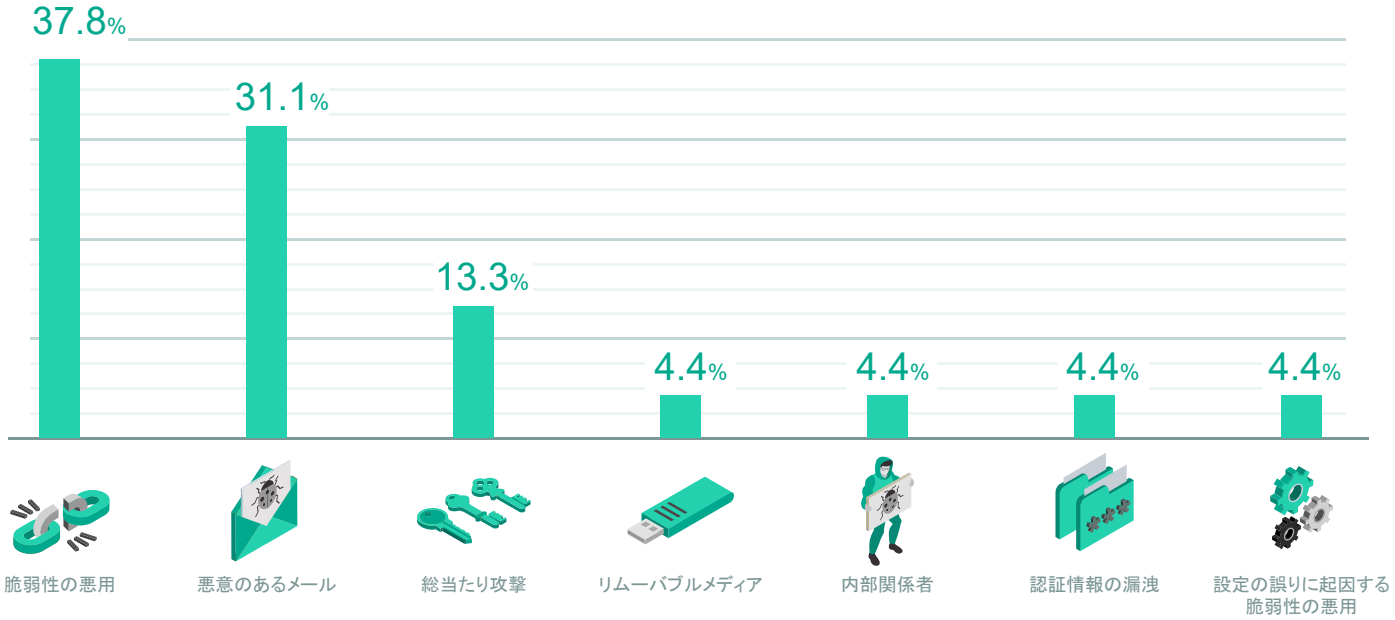


サイバー攻撃の経路

攻撃者はどのように侵入するか

主な初期の侵入経路は、脆弱性（ゼロデイおよびワンデイ）の悪用、悪意のあるメール、総当たり攻撃です。ほとんどの場合、ワンデイ脆弱性のパッチ管理、パスワードポリシーの適用、管理インターフェイスをインターネット上にさらさないことにより対応できます。

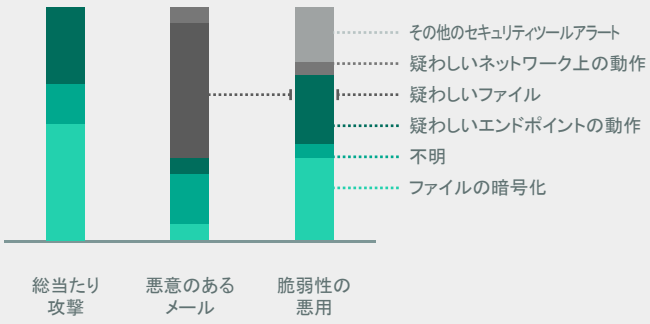
メールを介したゼロデイ脆弱性およびソーシャルエンジニアリング手法の攻撃への対応は難しく、内部のセキュリティ対策を相当レベルまで引き上げる必要があります。



主な初期の侵入経路とインシデント検知の関連性

場合によって、当社はサイバー攻撃の標的となった組織で一次対応を行うチームのために、無償でサポートすることがありますが、その際、お客様のチームによるそれまでの調査内容が明確でないケースがあるため、グラフに「不明」という項目があります

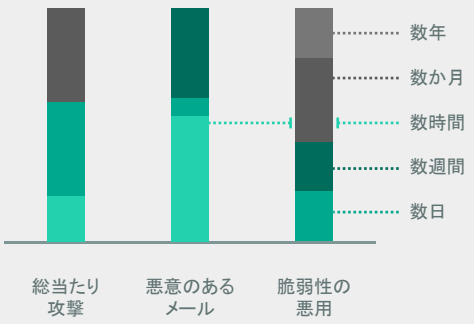
悪意のあるメールは、セキュリティ調査のためのツール群によって通常は検知されますが、検知されないケースがゼロデイあるいはワンデイ脆弱性によるものであることを示している訳ではありません



組織への侵入方法と、攻撃が気づかれずに続く期間との関係

組織のネットワーク境界に潜む脆弱性を悪用したケースが、最も長期にわたり発見されませんでした

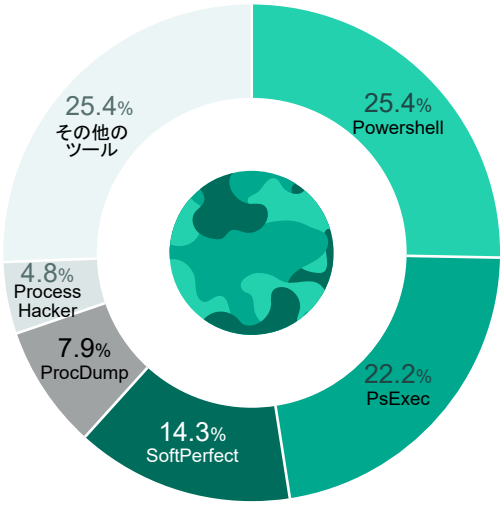
最も短時間で発見されたのは、メールを使ったソーシャルエンジニアリング手法による攻撃でした



ツールとエクスプロイト

すべてのインシデントのうち、30%は正規ツールを使用

サイバー攻撃者は、悪意のあるユーティリティとして検知されないように、通常業務に使われることが多い正規のツールを使用します。
日常の業務に紛れ込んだ不審なイベントは、悪意のある攻撃、およびこれらの正規ツールの使用とインシデントとの関係を詳細に分析して初めて特定することができます。最も頻繁に使われるツールは、PowerShell、PsExec、SoftPerfect Network Scanner、ProcDumpです。



正規ツールの大半は、メモリからの認証情報の収集、セキュリティソリューションをアンロードすることによるセキュリティメカニズムの回避、ネットワーク上に存在するサービスの発見に使用されます

正規ツールが使われた割合とその戦術*は次のとおりです

実行 Execution	セキュリティ対策の回避 Defense Evasion	認証情報へのアクセス Credential Access	探索 Discovery	水平展開 Lateral Movement	収集 Collection	コマンド&コントロール Command and Control	影響 Impact
38.6%	9.6%	10.8%	16.9%	19.3%	1.2%	1.2%	2.4%
Powershell PsExec PsTools Rexec	PC Hunter Powertool Process Hacker Sdelete	Mouse Lock Recovery NirSoft Password Powertool ProcDump PsTools	Advanced Port Scanner KPortScan Nmap PsTools SoftPerfect	PsExec PsTools Rexec	Mouse Lock	TightVNC	DiskCryptor

エクスプロイト

インシデントのケースで特定されたエクスプロイトの大半は、2019年に多くの攻撃者が積極的に悪用していたWindows SMBサービスにおける既知のリモートコード実行の脆弱性（MS17-010）とともに出現しました。

MS17-010

Microsoft WindowsのSMBサービス

リモートコード実行の脆弱性。WannaCry、NotPetya、WannaMineなどいくつかの大規模な攻撃で使用された

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-2019-19781

Citrix Application Delivery ControllerとCitrix Gateway

この脆弱性により、Citrixインフラストラクチャーに接続されたすべてのホストで、リモートコードを認証なしに実行可能になる

CVE-2019-0708

Microsoft WindowsのRDPサービス

リモートコード実行の脆弱性（コード名：BlueKeep）。このRDPサービスは、広く普及し、残念ながら頻繁に公開されている

CVE-2018-7600

Drupal

リモートコード実行の脆弱性。Drupalgeddon2とも呼ばれる。侵害されたWebサーバーにおけるバックドアのインストール、Webマイナーなどのマルウェアで広く利用される

CVE-2019-11510

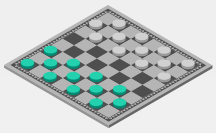
Pulse Secure SSL VPN

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、標的の組織に即座にアクセスできる

* MITRE ATT&CK

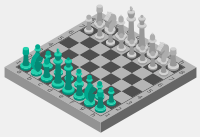
攻撃の期間

当社のエキスパートが、攻撃活動の開始から終了までの期間について調査しました。攻撃期間を基準に、すべてのインシデントを3つのカテゴリーに分類しました。



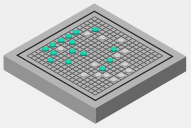
短期の攻撃

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

一般的な脅威

短期の攻撃	平均的な攻撃	長期にわたる攻撃
ランサムウェアに感染	金銭の窃取	サイバースパイ活動と機密情報の窃取

一般的な攻撃経路

短期の攻撃	平均的な攻撃	長期にわたる攻撃
▪ メール内のリンク経由で悪意のあるファイルをダウンロード ▪ 感染したサイトから悪意のあるファイルをダウンロード ▪ ネットワーク境界上の脆弱性を悪用 ▪ 認証情報を推測した総当たり攻撃	▪ メール内のリンク経由で悪意のあるファイルをダウンロード ▪ ネットワーク境界上の脆弱性を悪用	▪ ネットワーク境界上の脆弱性を悪用

攻撃期間（中央値）

短期の攻撃	平均的な攻撃	長期にわたる攻撃
1日	10日間	122日間

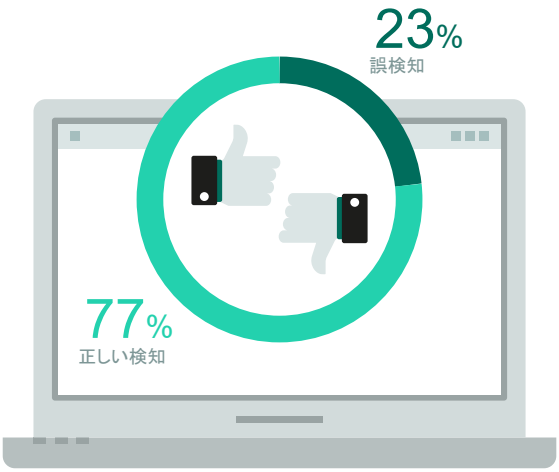
インシデントレスポンス期間

短期の攻撃	平均的な攻撃	長期にわたる攻撃
数時間から数日	数週間	数か月
このカテゴリーには、最長で1週間継続する攻撃が分類されます。主にはランサムウェア攻撃が関係するインシデントです。このような攻撃は展開が速いため、効果的な対抗策は予防しかありません。一部のケースでは、最初の侵入から活動開始までに、最長1週間の遅延が見られました	このカテゴリーには、1週間から数週間かけて展開された攻撃が含まれます。ほとんどの場合、直接金銭を窃取することを目的としています。 通常、攻撃者は1週間以内に目的を達成しています	1か月を超えて継続するインシデントはこのカテゴリーに入ります。ほとんどの場合、機密情報の窃取を目的にしています。このような攻撃には、活動が活発に行われる期間と、そうでない期間が交互になる特徴があります。活動が活発な期間を合計すると、平均して「数週間」カテゴリーの攻撃期間とほぼ同じになります

実施の指標

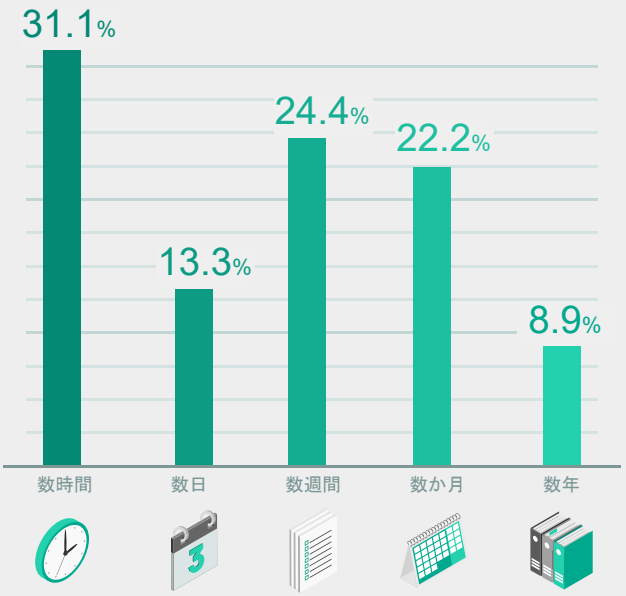
誤検知率

インシデントレスポンスにおける誤検知は、コスト高になります。これは、セキュリティイベントのトリアージにより、インシデントレスポンスのエキスパートが調査に関与し、インシデントが起きていなかったことが判明した場合です。通常、組織に脅威ハンティングの専門家がいないか、セキュリティイベントの背景を把握していない外部のSOCにより管理されていることを意味します。



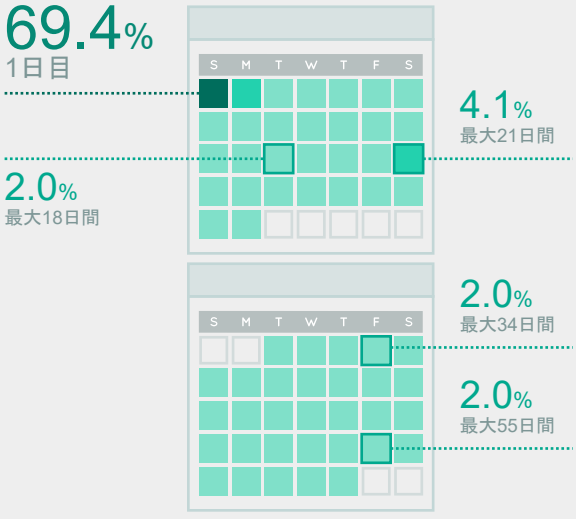
攻撃期間

攻撃開始後、組織がインシデントを検知するまでにかかった時間を示しています。通常、早くて数時間、または数日のうちに攻撃を検知できれば良いでしょう。目立たない攻撃の場合は、数週間かかることがありますが、数か月、数年かかることは間違いなく良くありません。



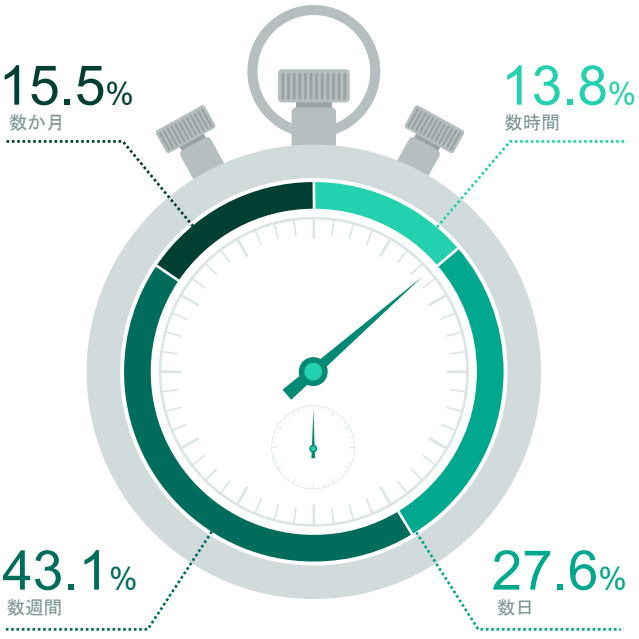
対応開始までの時間

当社が被害組織から連絡を受け、対応を開始するまでにはどのくらいの時間を要したでしょうか。70%が初日に対応を開始していますが、さまざまな要因が開始までに影響を与えることがあります。



対応に要する時間

インシデントレスポンス活動に必要な期間を示しています。



MITRE ATT&CK tactics and techniques

ATT&CK フレームワークへのマッピングは、対応した全インシデントレスポンスの約50%で実施しました。

>0% >5% >10% >25% >50%

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Valid Accounts	Windows Remote Management	Accessibility Features	Accessibility Features	Obfuscated Files or Information	Credential Dumping
Replication Through Removable Media	Service Execution	DLL Search Order Hijacking	DLL Search Order Hijacking	Masquerading	Network Sniffing
External Remote Services	Windows Management Instrumentation	New Service	New Service	DLL Search Order Hijacking	Input Capture
Drive-by Compromise	Scheduled Task	Scheduled Task	Scheduled Task	Software Packing	Credentials in Files
Exploit Public-Facing Application	Command-Line Interface	Registry Run Keys / Startup Folder	Process Injection	Process Injection	Account Manipulation
Spearphishing Link	Graphical User Interface	Valid Accounts	Valid Accounts	Scripting	Brute Force
Spearphishing Attachment	Scripting	Windows Management Instrumentation Event Subscription	Web Shell	Indicator Removal on Host	LLMNR/NBT-NS Poisoning and Relay
	Third-party Software	Account Manipulation	Access Token Manipulation	Valid Accounts	Password Filter DLL
	Rundll32	Web Shell	Hooking	Rundll32	Hooking
	PowerShell	External Remote Services		Disabling Security Tools	Kerberoasting
	Execution through API	Create Account		Connection Proxy	
	Trusted Developer Utilities	Office Application Startup		Web Service	
	Execution through Module Load	Hidden Files and Directories		File Deletion	
	Mshta	Hooking		Modify Registry	
	Component Object Model and Distributed COM			Code Signing	
	User Execution			Trusted Developer Utilities	
	Signed Binary Proxy Execution			Access Token Manipulation	
				Deobfuscate / Decode Files or Information	
				Hidden Files and Directories	
				Mshta	
				Process Doppelgänging	
				DCShadow	
				Signed Binary Proxy Execution	
				Group Policy Modification	

>0% >5% >10% >25% >50%

Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Impact
Application Window Discovery	Windows Remote Management	Data from Network Shared Drive	Data Compressed	Data Obfuscation	Data Encrypted for Impact
Query Registry	Third-party Software	Input Capture	Automated Exfiltration	Fallback Channels	Inhibit System Recovery
System Network Configuration Discovery	Pass the Hash	Screen Capture	Data Encrypted	Custom Cryptographic Protocol	Stored Data Manipulation
Remote System Discovery	Remote Desktop Protocol	Email Collection	Exfiltration Over Command and Control Channel	Standard Cryptographic Protocol	Runtime Data Manipulation
Network Sniffing	Windows Admin Shares	Clipboard Data	Exfiltration Over Alternative Protocol	Commonly Used Port	Resource Hijacking
Network Service Scanning	Replication Through Removable Media	Data from Information Repositories	Exfiltration Over Physical Medium	Standard Application Layer Protocol	
System Network Connections Discovery	Pass the Ticket			Multilayer Encryption	
Process Discovery	Remote File Copy			Connection Proxy	
Permission Groups Discovery	Component Object Model and Distributed COM			Custom Command and Control Protocol	
System Information Discovery	Exploitation of Remote Services			Standard Non-Application Layer Protocol	
File and Directory Discovery	Exploitation of Remote Services			Web Service	
Account Discovery				Remote File Copy	
Peripheral Device Discovery				Data Encoding	
Network Share Discovery				Domain Fronting	
				Remote Access Tools	
				Domain Generation Algorithms	

PR-1054-202012
©2020 Kaspersky

無断複写・転載を禁じます。カスペルスキー、KasperskyはKaspersky Labの登録商標です。