kaspersky

「Digital Footprint Intelligence」のご紹介
～法人向け脅威モニタリングサービス～

2024年03月05日
株式会社カスペルスキー
セールスエンジニアリング本部

V1.2

■攻撃対象領域とは？

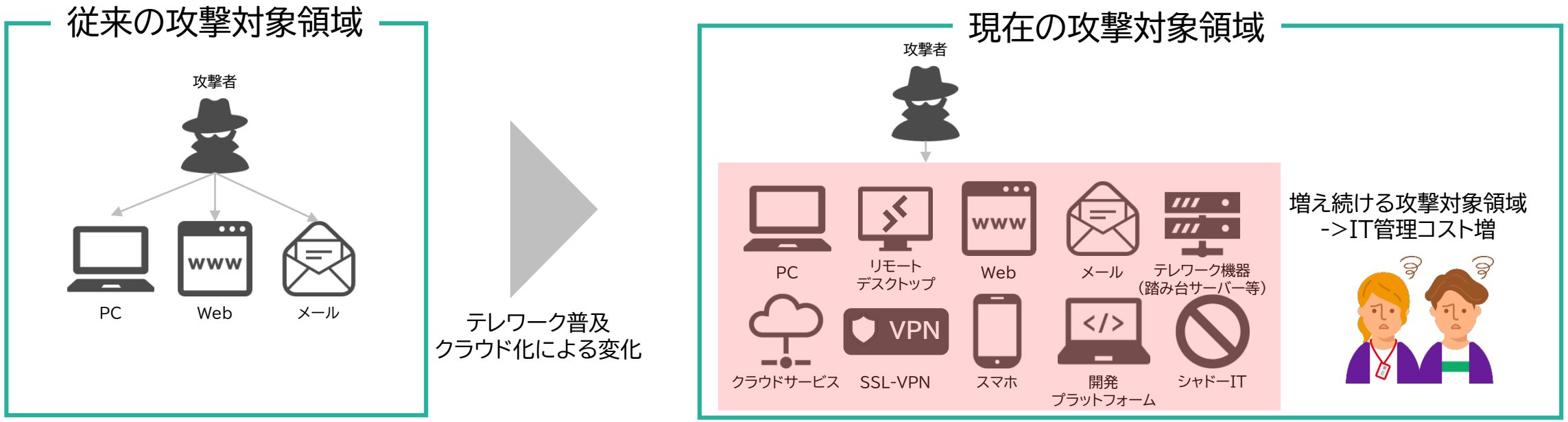
Kaspersky
Digital Footprint
Intelligence

・**攻撃対象領域**： サイバー攻撃を受ける可能性があるデバイス・ソフトウェアのこと

・テレワークの普及・クラウド化によってIT環境が拡大したことで攻撃対象領域が広がり、**管理はより複雑**に

->結果として、IT資産やシステムの管理漏れ・設定ミスが発生。サイバー攻撃による侵入の起点となりうる「弱点」が意図しない状態で公開されたままに・・・

＝サイバー攻撃の被害を減らすためには、攻撃対象領域を把握し、**「弱点」の無い状態**に正しく管理することが重要



kaspersky

■Digital Footprint Intelligence: サービス概要

Kaspersky
Digital Footprint
Intelligence

・攻撃対象領域(外部から確認可能なIT資産)を調査し、脆弱性や設定ミスなどのセキュリティリスクを報告

<分析項目一例>

-ネットワーク境界に存在する脆弱性・設定ミス

-会社名やブランド名を悪用するフィッシングサイトの検知

・ダークweb・Telegramで発見した攻撃計画・情報漏えいといった潜在的なリスクに関する情報を提供

<分析項目一例>

-ハッカーに対するバグハント(脆弱性検出)依頼、攻撃計画

-情報漏えい(侵害された従業員のアカウント・クレジットカード情報・内部情報など)

・Kasperskyが別サービスとして提供する脅威インテリジェンスを活用し、調査・分析を強化

<脅威インテリジェンスサービス一例>

-APT Intelligence Reporting: Kasperskyのエキスパートが調査したAPT攻撃に関するTTPsなどの詳細情報

-Anti-Phishing Feeds: お客様のブランド、オンラインサービスまたはお客様情報を狙うフィッシング攻撃に関する情報

kaspersky

■Digital Footprint Intelligence とは

Kaspersky
Digital Footprint
Intelligence

・カスペルスキーのエキスパートがお客様リソースを調査・分析し、悪用される可能性のある脆弱性などの「弱点」や、
個人情報の漏えい・お客様に対する攻撃計画の証拠などを脅威アラートで報告するサービス

・アドオンライセンスを購入することで検知した脅威の統計情報や推奨事項などまとめたレポートを提供

ネットワーク境界の調査

- 外部から悪用可能なサービス
- サービスのフィンガープリント
- 存在する脆弱性
- エクスプロイト分析
- リスク分析とリスクレベル

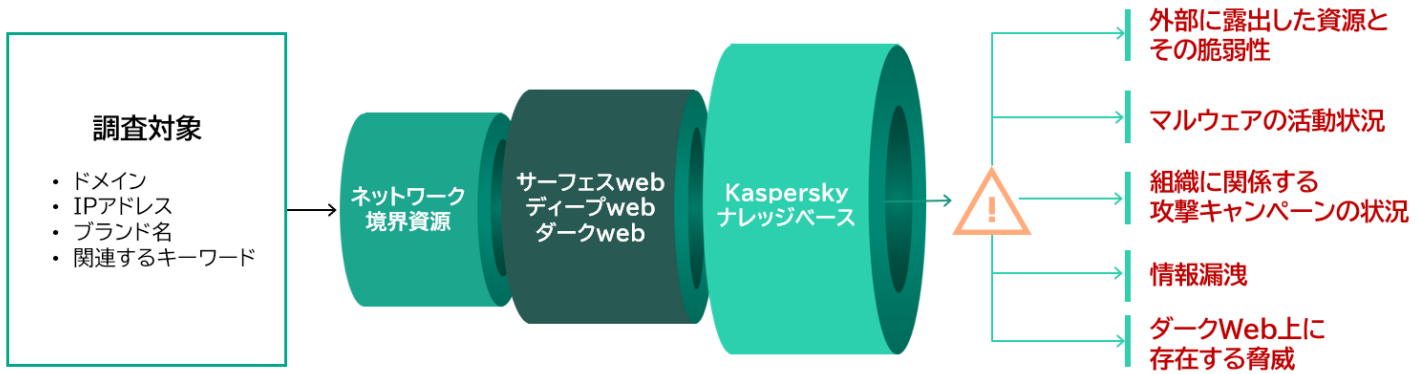
サイバー空間調査

✓サーフェスweb
✓ディープweb
✓ダークweb

- サイバー犯罪者の活動
- 漏洩したデータと認証情報
- 悪意あるインサイダー
- 関係者のソーシャルメディア活動
- メタデータからの漏洩

Kaspersky エキスパートによる分析

- マルウェアコレクション
- ボットネットとフィッシングの追跡
- APTリサーチデータ
- シンクホールとマルウェアホスト
- 脅威インテリジェンスデータベース



kaspersky

■操作方法

Kaspersky
Digital Footprint
Intelligence

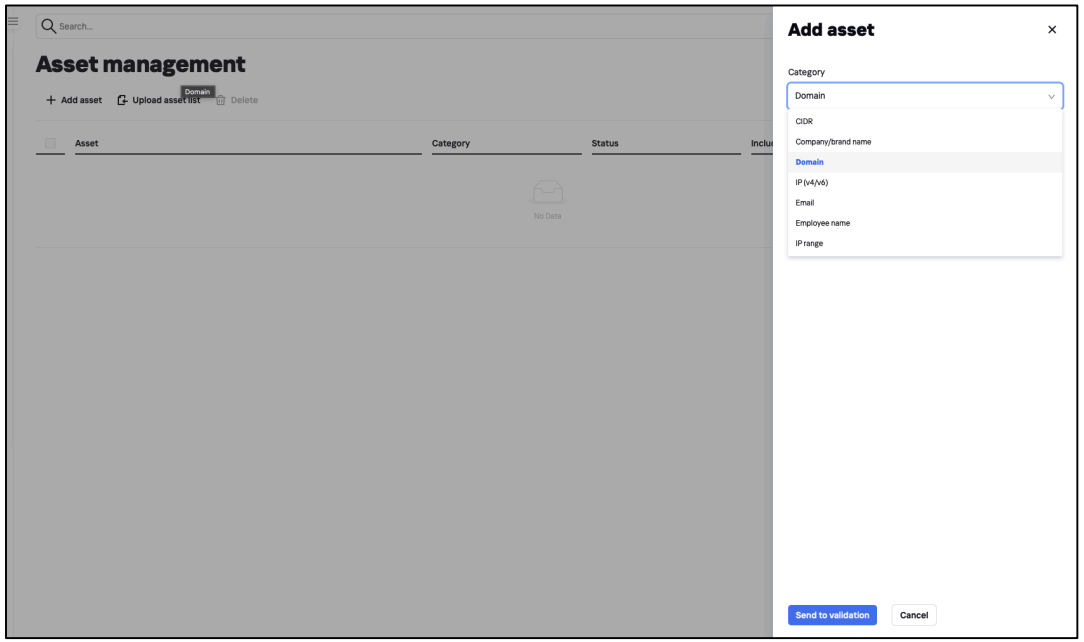
監視対象アセットの登録方法

・脅威インテリジェンスサービスを提供するポータルサイト「Kaspersky Threat Intelligence Portal」から
監視対象のアセットを登録、監視対象数が多い場合、Excelファイル等での登録も可能

<登録可能なアセット>

-IPアドレス / IPアドレス範囲 / CIDR
-会社名 / ブランド名 (※)
-ドメイン名またはサブドメイン名
-従業員氏名(※)
-メールアドレスまたはマスク
-任意のキーワード (※)
-IIN(カード発行金融機関識別番号) / BIN(銀行識別番号)
-正規のソーシャルアカウントへのリンク
-正規のモバイルアプリへのリンク
-製品およびデバイス名

<監視対象登録画面>



※ローカル言語を使用可能

kaspersky

■操作方法

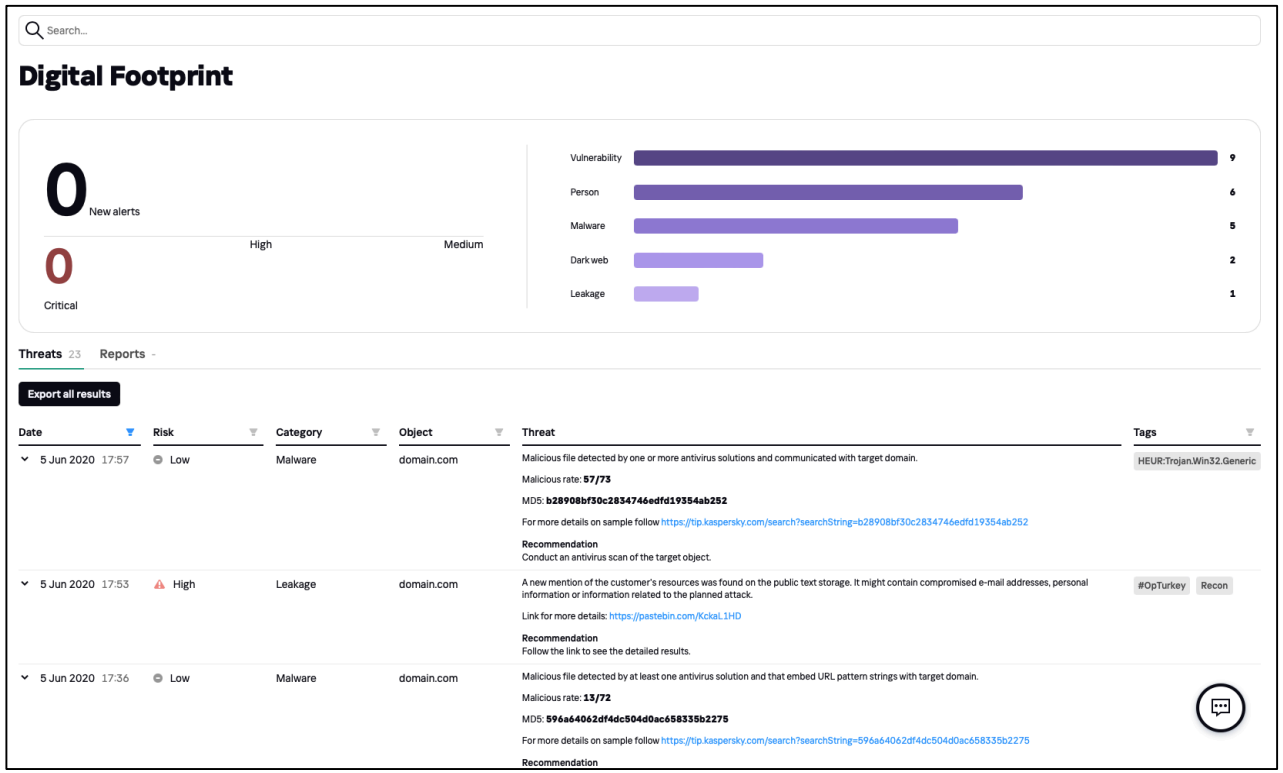
Kaspersky
Digital Footprint
Intelligence

脅威アラート通知方法

・脆弱性などの弱点や企業情報の漏洩が検知された場合、脅威アラートで情報を提供

・脅威アラートはポータル上に通知、ポータルの設定で検知時に管理者にメール通知することも可能

＜脅威アラート通知画面＞



kaspersky

■脅威アラート

Kaspersky
Digital Footprint
Intelligence

・組織の保護レベルを低下させる可能性がある以下の情報が検知された場合、ポータル上に脅威アラートを通知

＜脅威アラートによって通知される項目＞　　2024年03月現在

項目	説明
脆弱性	攻撃対象領域で発見された脆弱性に関する情報
マルウェアのサンプルと URL	お客様をターゲットにしたマルウェアに関する情報
メールアドレス	悪用が確認されたメールアドレス
ダークウェブのエントリ	ダークウェブ上で発見されたお客様に関連する投稿
Pastebin エントリ	Pastebin上で発見されたお客様に関する情報
侵害されたアカウント	侵害されたアカウントの漏えい情報
新規サブドメイン	新たに発見されたお客様に関連するサブドメイン
設定の不備	攻撃対象領域で発見された設定の不備
APT 被害者	APT 脅威に関連付けられたお客様の IP アドレス
パッシブ DNS レコード	お客様のドメインから解決された悪意のある IP アドレス
決済カード	お客様に関連するクレジットカードの漏えい情報
フィッシング/タイポスクワッティング	お客様のブランド / Webリソースに合わせて調整されたフィッシングおよびタイポスクワッティング

kaspersky

■脅威アラート -フィッシング検知-

Kaspersky
Digital Footprint
Intelligence

・フィッシングのリアルタイム通知機能では、会社のブランド、会社名、オンラインサービス、商標を狙ったフィッシングサイトの出現を積極的に追跡し、リアルタイムで警告
・すべての通知には、フィッシング攻撃について精度と信頼性の高い広範な情報が示されているため、フィッシングの発生だけでなく、動的に生成されるフィッシングのドメインやURLに対しても迅速な対応が可能

＜フィッシング通知に含まれるコンテキスト＞　　2023年09月現在

項目
フィッシングURL、スクリーンショット、HTMLコード、解決したIPアドレス
攻撃が最初（最後）に検知された日時のタイムスタンプ
フィッシングURLが標的にしたブランド名、影響を与えるユーザーの地理的情報、検知数（知名度）
窃取されたデータのタイプ（クレジットカード情報、銀行の認証情報、メールやSNSのアカウント、個人情報など）
フィッシングキット（存在する場合）
WHOISデータ

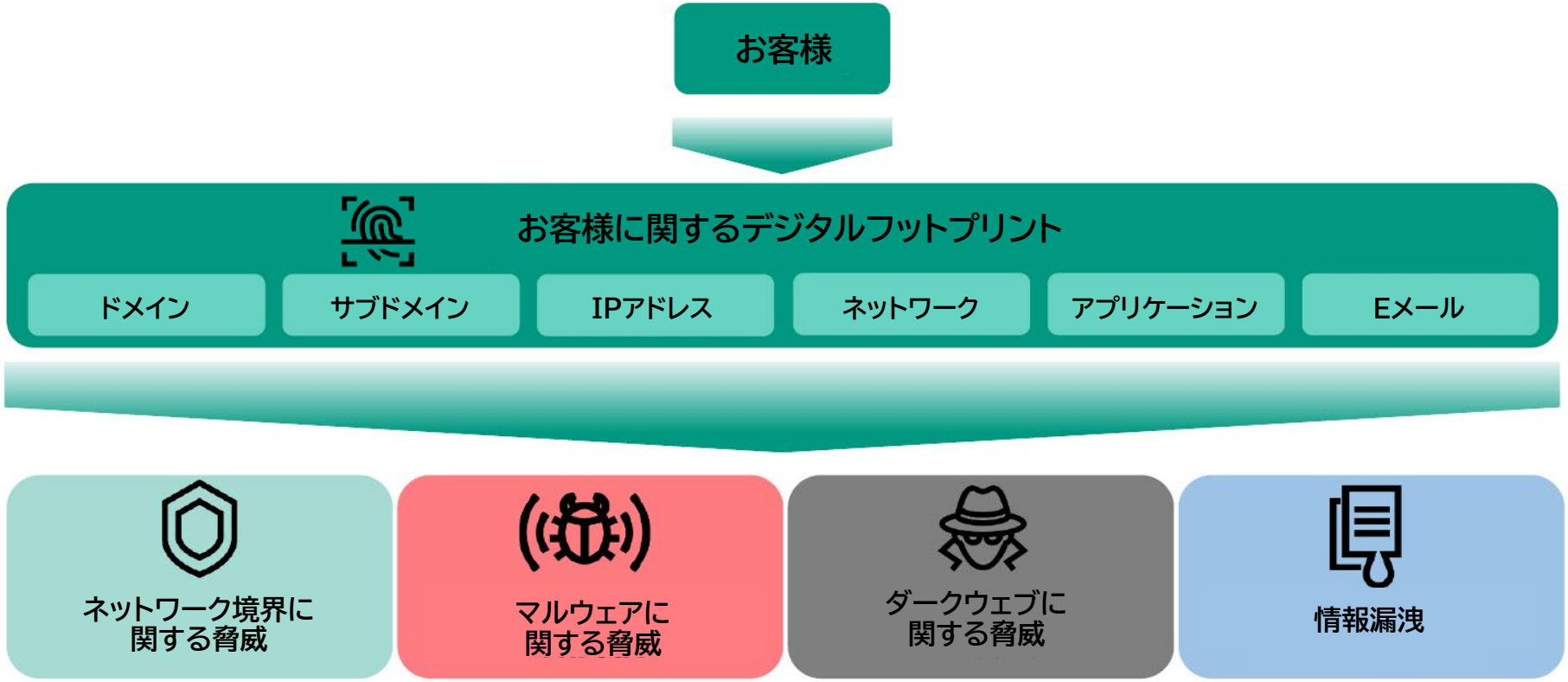
kaspersky

■Digital Footprint Intelligence：サービス提供の仕組み

Kaspersky
Digital Footprint
Intelligence

・お客様からご提供いただいた情報を基にカスペルスキーのエキスパートがネットワーク境界/マルウェア/ダークウェブに関する脅威および情報漏洩について調査・分析

・調査・分析は誤検知を防ぐために、自動検知システムによる検知に加えてエキスパートによる追加調査を実施



kaspersky

■ネットワーク境界に関する脅威

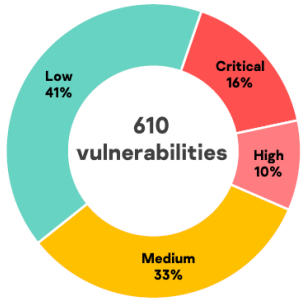
Kaspersky
Digital Footprint
Intelligence

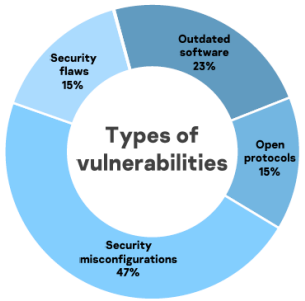
ネットワーク境界の脆弱性/エクスプロイト情報を確認、リスクを判定

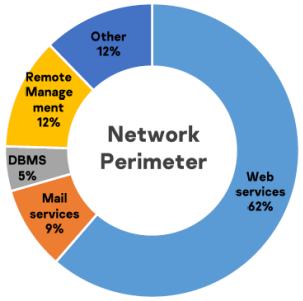
・OSINT（Shodan、scans.ioなど）を利用した受動的な偵察を実施し、お客様のネットワーク境界に関する情報を収集
この偵察作業によって、お客様のネットワークリソース上で利用可能なサービスを特定し、脆弱性やtelnet等の安全ではないプロトコルの使用や不要なポート開放といった設定ミスに起因するリスクの有無を確認

・CVSSのスコアに基づくリスク評価に加え、エクスプロイト成功時の可用性に対する影響やネットワーク攻撃に関する統計情報などを利用して包括的にリスクを評価

⇒お客様ネットワーク境界に存在する脆弱性や侵害されたリソースなどを特定し、セキュリティリスク低減に繋がる情報を提供







#	Top 5 Most Critical Security Issues	Risk
1	Telnet service without authentication	Critical
2	Remote Code Execution in SMB service (MS17-010)	Critical
3	Compromised website (deface)	Critical
4	Outdate version of WebMin. Public exploit for Remote Code Execution is available.	Critical
5	ElasticSearch without authentication	Critical

kaspersky

■ネットワーク境界に関する脅威

Kaspersky
Digital Footprint
Intelligence

<調査・分析による検知例>

①調査で確認されたパブリックIPアドレス・ドメイン情報

②EDNSへの対応確認

③脆弱性に関する分析

-旧バージョンの利用が確認されたソフトウェア情報

-セキュリティ上望ましくないプロトコルの使用有無・設定ミス

④セキュリティ上の欠陥

-アクセス権限設定がされていないリモート管理インターフェイス

-無効になっていないデフォルトページ・ディレクトリリスティング

⑤SSL/TLSに関する調査

-非推奨バージョンや信頼されていない証明書の利用有無

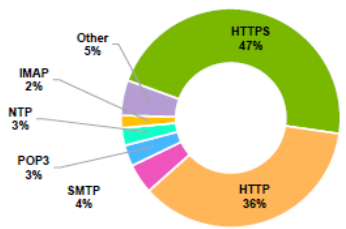


Figure 4. Statistics on externally available services

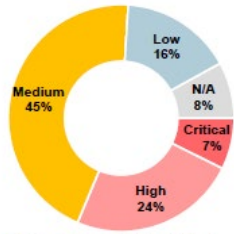


Figure 5. Vulnerabilities statistics by risk level

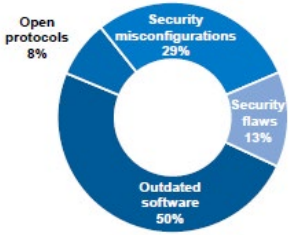


Figure 6. Statistics on found vulnerabilities by categories

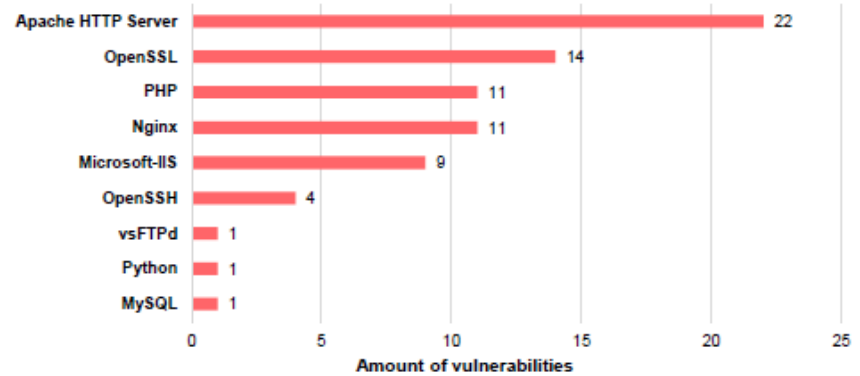
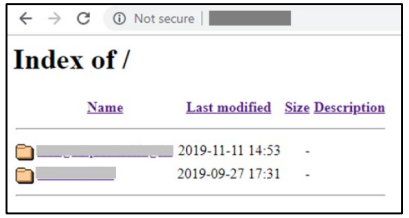


Figure 7. Distribution of vulnerabilities in outdated software



kaspersky

■マルウェアに関する脅威

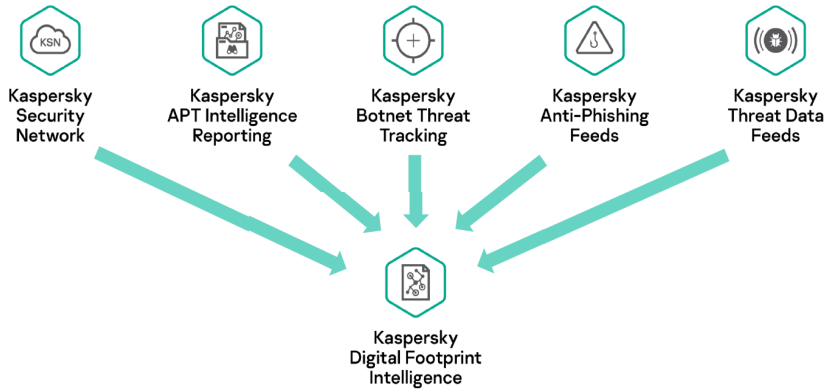
Kaspersky
Digital Footprint
Intelligence

お客様に対する攻撃の識別、脅威の特定

・Kasperskyが調査、分析してきた脅威データを使用し、お客様の組織を標的とするフィッシング攻撃やマルウェアサンプル、ボットネットの動向、継続的なAPT活動の監視、不正アクセスの痕跡（IoC）の収集など攻撃情報を総合的に確認し、お客様の活動拠点で流行するマルウェアの統計やAPTキャンペーン、従業員を狙うフィッシング攻撃の情報を報告

<攻撃の識別に使用されるKasperskyの脅威インテリジェンスサービス>

- **・Kaspersky Security Network**　：Kaspersky製品を利用しているお客様から同意の上で収集した脅威インテリジェンス情報のソース
- **・APT Intelligence Reporting**　：APT攻撃者が使用する手段、戦術、ツール（TTPs）を明らかにする弊社アナリストの調査情報
- **・Botnet Threat Tracking**　：お客様を対象とした攻撃に関する情報、キーワードをボットネット内で監視
- **・Anti-Phishing Feeds**　：お客様のブランド、オンラインサービスまたはお客様情報を狙うフィッシング攻撃に関する情報
- **・Threat Data Feeds**　：集積された不正アクセスの痕跡（IOC）に実用的なコンテキスト情報を付加した脅威インテリジェンスを提供



kaspersky

■マルウェアに関する脅威

Kaspersky
Digital Footprint
Intelligence

<調査・分析による検知例>

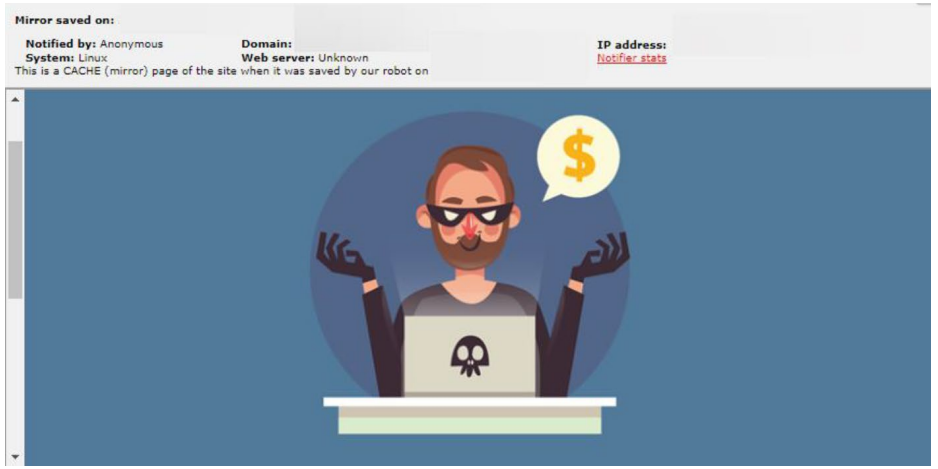
①お客様企業の活動地域で流行するマルウェアや
APTキャンペーンの情報(※)

②お客様を標的とした脅威調査
-シンクホールを活用した調査
-マルウェアのサンプル分析
-フィッシング攻撃の統計(※)
-ターゲットにされたwebページ情報

③攻撃者によって改ざんされたリソースに関する情報

④関連するボットネットの動向

※レポートのみ、脅威アラートでは通知されません



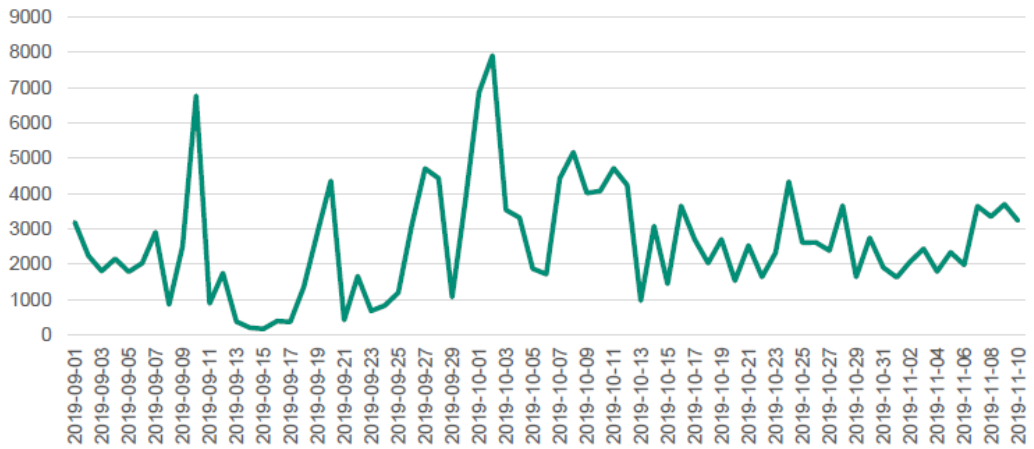


Figure 16. Phishing activity (September 01, 2019 - November 11, 2019)

kaspersky

■ダークウェブに関する脅威

Kaspersky
Digital Footprint
Intelligence

ディープウェブ/リアルダークウェブ上の不審な動向を監視

・誰でもアクセス可能な一般公開されたWebページ（＝サーフェスウェブ）やお客様ご自身で調査することが難しい検索エンジンで検索出来ないWebページ（=ディープウェブ）、犯罪目的や違法な商品やサービスを購入できる闇市場となっている違法コンテンツのWebページ(=リアルダークウェブ)上で実際にやりとりされているお客様を狙う攻撃者の情報の不正な取引(攻撃経路になりうる情報の売買)やお客様に対する攻撃計画に関するやり取りを監視・特定し、潜在的なセキュリティリスクの把握に繋がる情報を提供

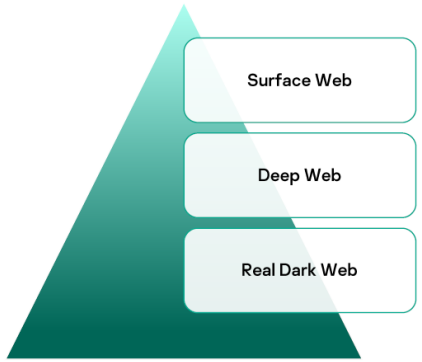
＜監視対象の不正な取引の一例＞

■ディープウェブ

・ハッカーに対するバグハント(脆弱性検出)依頼　/　・お客様に関連するゼロデイ脆弱性、データ漏洩

■リアルダークウェブ

・お客様に対する攻撃計画　/　・侵害された従業員のアカウント/クレジットカード情報/内部情報の売買



kaspersky

■ダークウェブに関する脅威

Kaspersky
Digital Footprint
Intelligence

レポートで提供される情報の一例

①詐欺、攻撃計画

-お客様をターゲットにした攻撃計画や情報の提供依頼

-ダークweb上のフォーラム・コミュニティでやり取りされる機密情報（従業員の個人情報など）の違法な売買

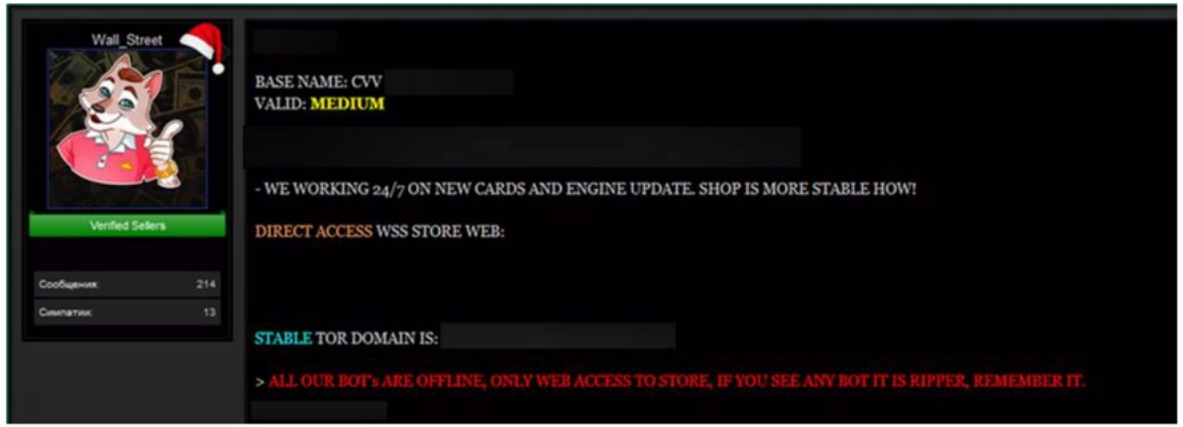
-お客様の活動拠点を専門に上記情報を不正に取引するコミュニティの情報

Looking for Accounts!

Thread URL : https://

Forum name	Thread name
Bank Carding	Looking for Accounts!

Post date	Post
20211206	Member Messages 4 Reaction 0 Yesterday at 10:18 AM #5 said: Im am looking for someone who can provide Accounts for me to Load long term. Account must have full card access/mobile drop access/have positive balence. Click to expand... What about bank account and the credit card I've that Post automatically merged: Yesterday at 10:19 AM said: can you provide fullz/profiles?? we can work bro. I have hella experience opening accounts Click to expand... I've bank account and credit card I need loader Post automatically merged:



kaspersky

■情報漏洩

Kaspersky
Digital Footprint
Intelligence

意図せず公開されている機密データを特定

・SNSに意図せず公開されてしまっている機密データや、Githubなどのホスティングサービス上に誰もがアクセスできる状態で公開されてしまっているトークン、暗号化キー、公開資料に残ったユーザ名やメールアドレス等の個人情報、ソフトウェア情報といった攻撃者がソーシャルエンジニアリングや武器化（攻撃のためのエクスプロイトキットやマルウェア等を作成）に利用可能なメタデータの有無の確認・特定し、アカウントへの不正アクセス被害の原因となるデータ漏洩を特性し、セキュリティリスク低減に繋がる情報を提供

kaspersky

■情報漏洩

Kaspersky
Digital Footprint
Intelligence

<提供される情報の一例>

①攻撃者が利用する可能性のある従業員に関する情報

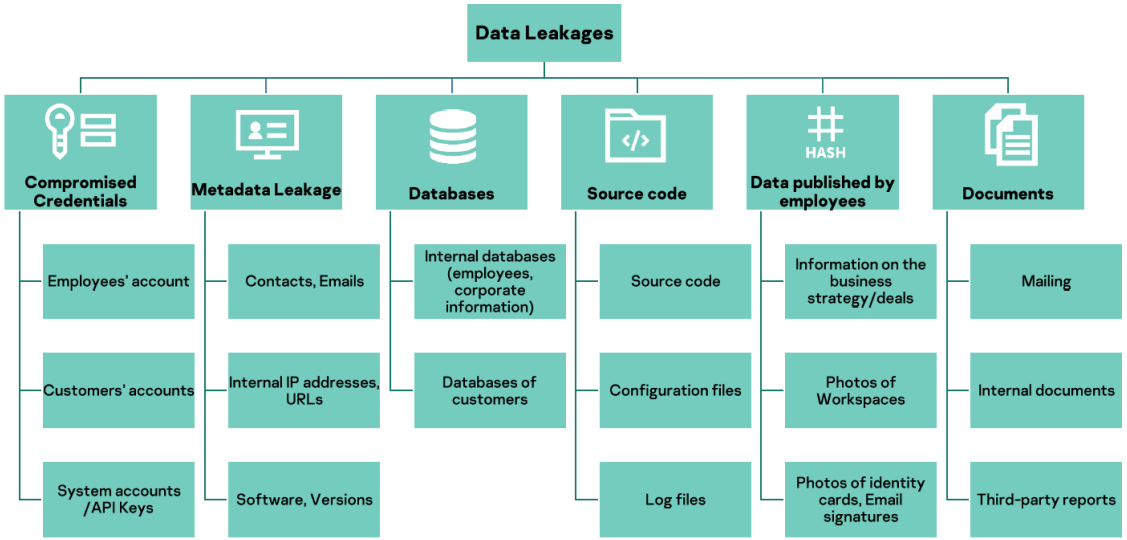
-検索エンジン、SNS、情報収集ツールを使用して発見された
メールアドレス、氏名、役職・部署といった個人情報

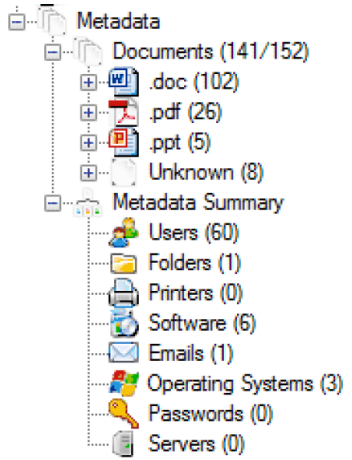
-会社のメールアドレスをSNSのリソースとして利用している
アカウント

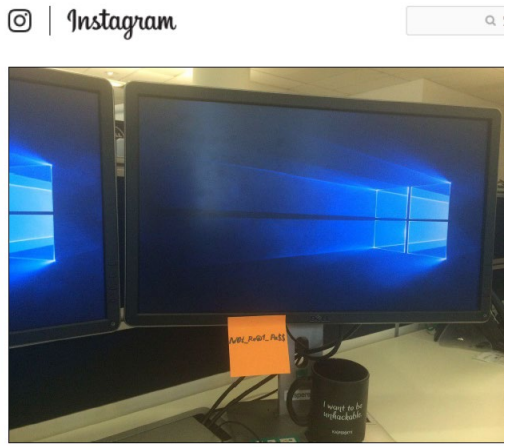
②既に侵害された可能性があるアカウント

-公開ソースや攻撃者のフォーラムで発見された侵害された
資格情報を分析、発見されたお客様に関連するアカウント

③SNSやホスティングサービスで公開されている重要なデータ







kaspersky

■レポート：推奨事項

Kaspersky
Digital Footprint
Intelligence

統計情報・状況改善のための推奨事項・地域で流行するマルウェア情報などをレポートで提供

・アドオンライセンス購入することで追加でレポートを提供

<条件>

・1ライセンス購入で1レポートを提供（1年間で4レポートまで）

・アドオンライセンスのみの**購入不可**

・レポート作成の対象期間はライセンス購入時に協議

<レポートで提供する情報>

・対象期間中に検知した情報および項目ごとの統計情報

・状況改善のための推奨事項

・お客様が直接関係しない脅威情報

例：お客様活動地域で流行するマルウェア・APTキャンペーン

kaspersky

4 Recommendations

4.1 Vulnerability management

To reduce the identified risks the Service Provider recommends the following:

- 推奨事項

4.2 Endpoint protection system

- 推奨事項

4.3 Protection against planned attacks

- 推奨事項

4.4 Compromised resources and user accounts

- 推奨事項

kaspersky

Dark Web Search / Surface Web Search

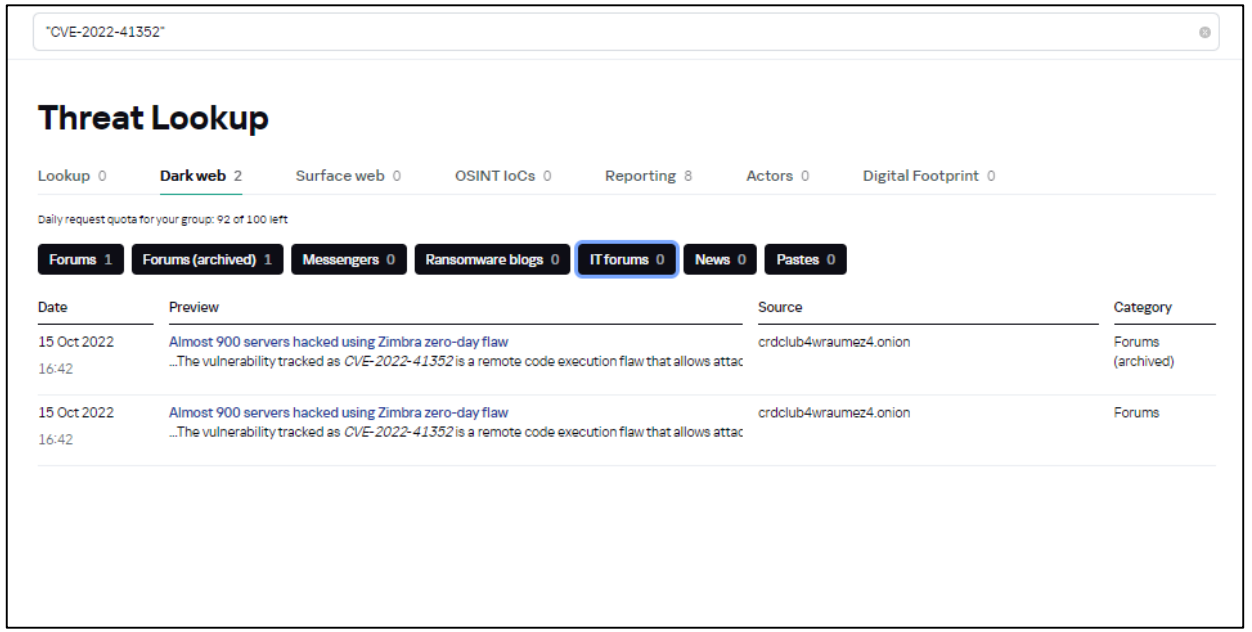
Kaspersky
Digital Footprint
Intelligence

Dark Web Search:

カスペルスキーのエキスパートが発見したダークwebやディープweb上でやり取りされるサイバー攻撃の計画や攻撃経路になり得る脆弱性に関するディスカッション、漏洩した認証情報やクレジットカード情報、個人情報などを提供するサービス

Surface Web Search:

カスペルスキーのエキスパートが選定した信頼できるセキュリティ関連の公開情報を提供するサービス



kaspersky

Dark Web Search / Surface Web Search：活用方法例

Kaspersky
Digital Footprint
Intelligence

① Dark Web Searchで特定企業名やブランド名、脆弱性をキーワードに検索

例：Kaspersky、CVE-2022-xxxx

-検索した企業に関する情報漏洩やバグハント依頼の確認

-該当の脆弱性が存在する企業の情報や悪用するツールの売買などの不正なやり取りの確認

② Surface Web Searchで脆弱性、マルウェア、サイバー攻撃に関連するキーワードを検索

例：(Log4j)、CVE-2022-xxxx、CryWiper

-世界で流行が確認されたマルウェアや脆弱性(CVE)を検索することで、カスペルスキーのエキスパートが選定したキーワードに関する記事を表示

kaspersky

kaspersky