Acronis

#CyberFit

「最新のセキュリティ事情を知って、クラウドケイパビリティを鍛える！」

アクロニス・ジャパン株式会社

Acronis ：サイバープロテクションのリーダー

AI搭載の サイバープロテクション, Cyber Cloud, Cyber Platform

スイス

2008年にスイスの
シャフハウゼンに
コーポレート本部を設立

シンガポール

2003年シンガポールに
国際統括本部を設立

二重保護のため2拠点に本社を設置

拡大＆急成長

取扱高3億ドル超
企業成長率50%達成
クラウドビジネス成長率
100%達成

世界展開

Fortune 1000の選出企業が100%採用
50,000社以上のパートナー企業
500,000件以上のビジネス
5,500,000以上のプロシューマー採用実績

国際的な存在感

1,500名以上の従業員
33か所を超える拠点
150か国以上で販売実績
33言語に対応
11か国にデータセンター

アタックサーフェスの変化と10大脅威

- DXに関連した変化
  - クラウドサービス
  - 仕事環境の変化
- コロナ禍に関連した変化
  - BYOD
  - VPN
  - リモートワーク
  - コミュニケーションツール

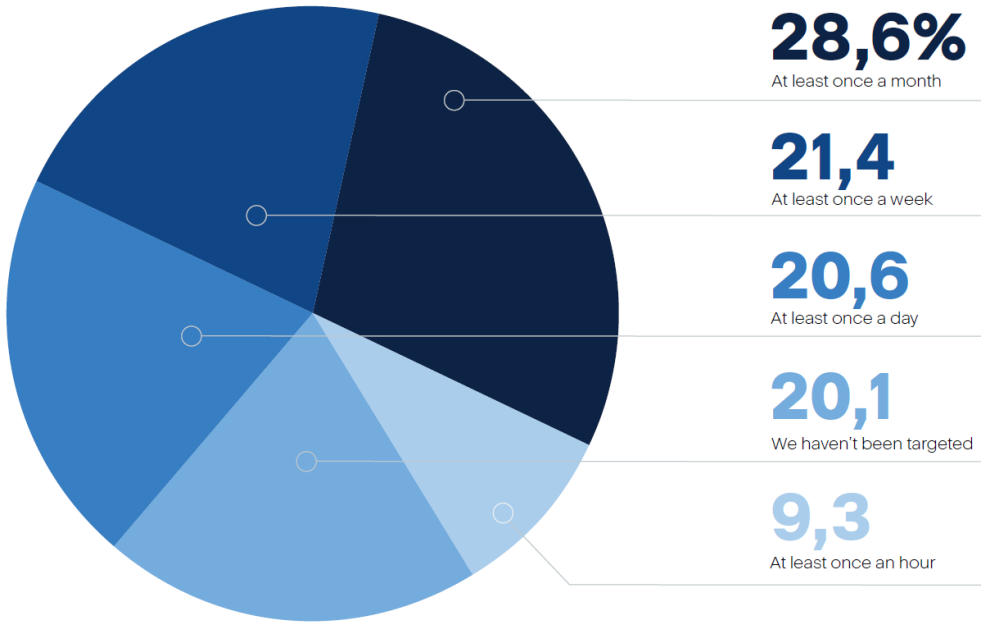
「情報セキュリティ10大脅威 2022」

順位	「組織」向け脅威	昨年順位
1	ランサムウェアによる被害	1
2	標的型攻撃による機密情報の窃取	2
3	サプライチェーンの弱点を悪用した攻撃	4
4	テレワーク等のニューノーマルな働き方を狙った攻撃	3
5	内部不正による情報漏えい	6
6	脆弱性対策情報の公開に伴う悪用増加	１０
7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	NEW
8	ビジネスメール詐欺による金銭被害	5
9	予期せぬ IT 基盤の障害に伴う業務停止	7
10	不注意による情報漏えい等の被害	9

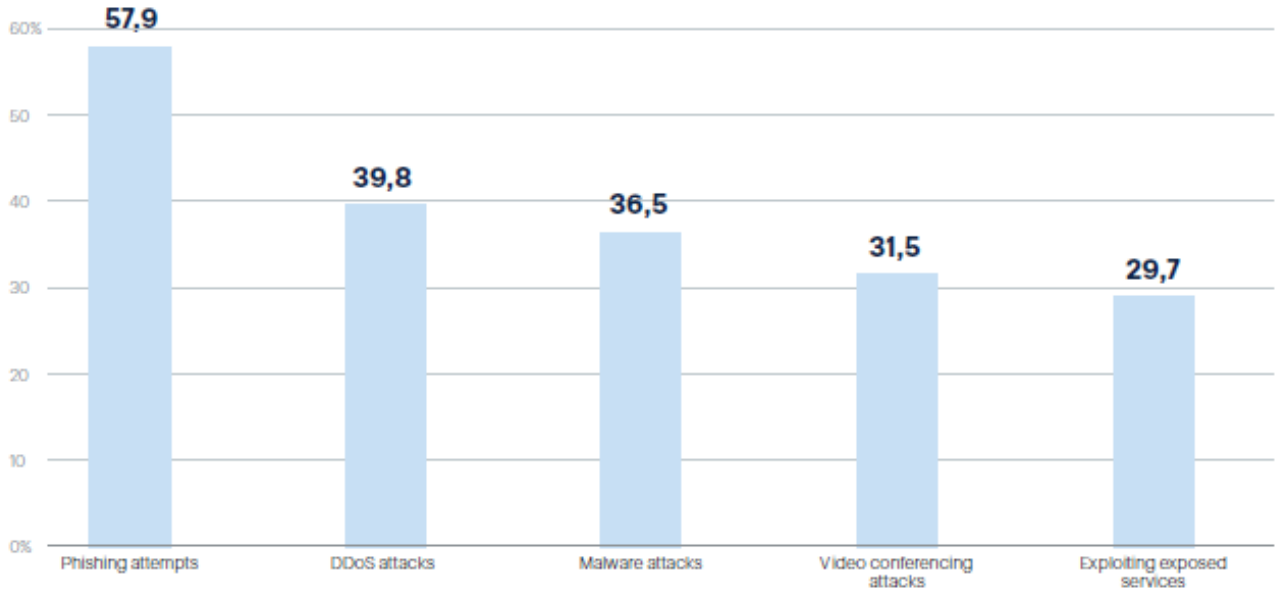
https://www.ipa.go.jp/files/000095773.pdf

サイバー攻撃の頻度が増加

この1年間にどのくらいの頻度でサイバー攻撃の標的になりましたか?



過去1年間で遭遇したサイバー攻撃の種類は何ですか?



Acronis Cyber Readiness Report 2021

エンドポイント防御の観点

•防御

- FW、UTM、EPP、SWG、脆弱性管理、アプリケーションコントロール

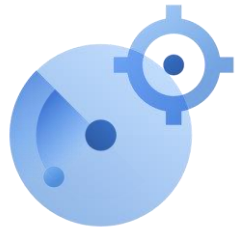
•検知

- EDR、MDR、XDR、SIEM

•拡大防止

- 特権管理、マイクロセグメンテーション

クラウドサービス防御の観点



- 防御
  - 通信制御、権限分離、不要ポートやサービスの閉鎖

- 検知
  - 監視設定、ログ監査

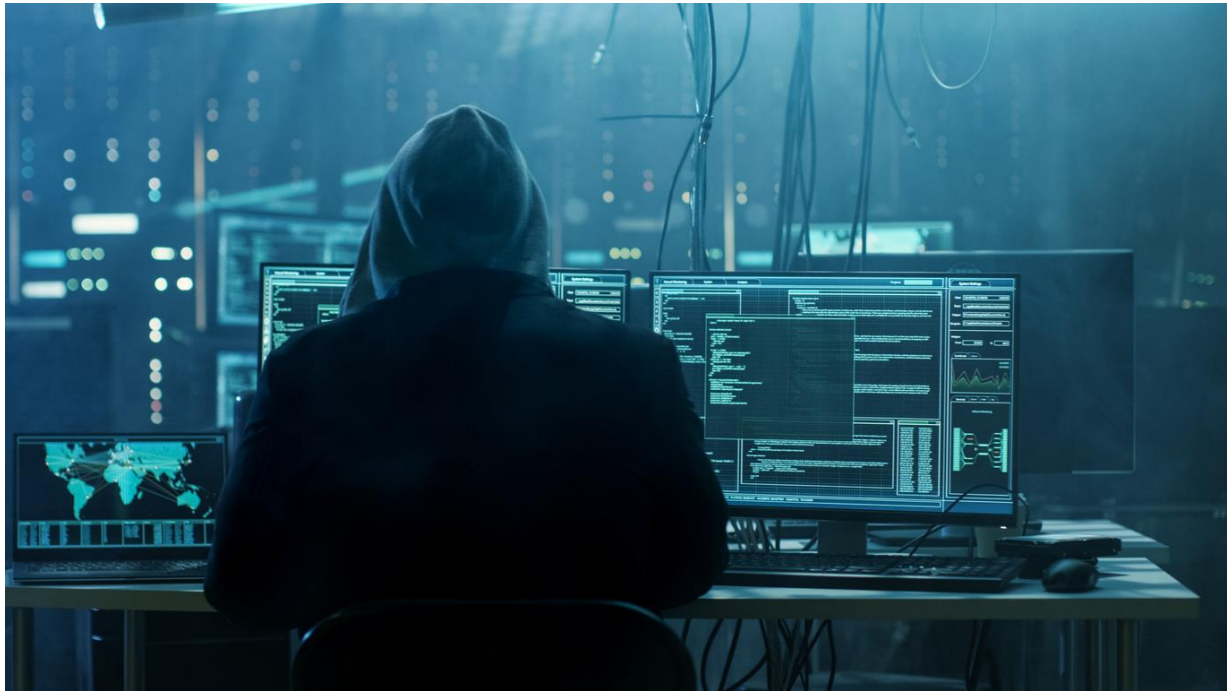
- 拡大防止
  - 権限設定

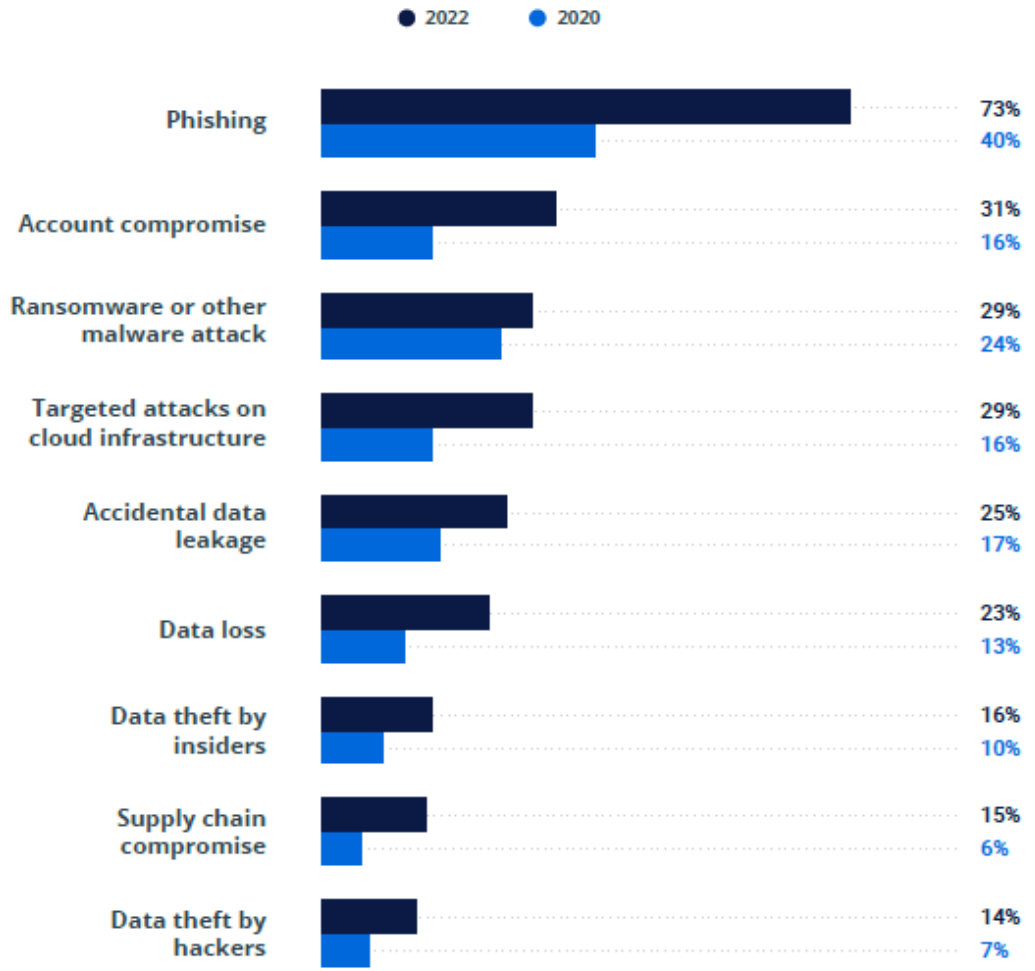
Acronis

#CyberFit

クラウドサービスの セキュリティ事情

クラウドサービスに対してのサイバー攻撃





Netwrix_Cloud_Data_Security_Report_2022

クラウドサービスのセキュリティ対策

- CASB/SWG

接続先の制御、ネットワークコントロール

- CSMP

設定監査

- SDP(Software Defined Perimeter)

権限制御

- CloudDLP

データ漏洩防止

SaaS(M365)インシデント事例

日本経済新聞 Pro

朝刊・夕刊　LIVE

トップ　速報　オピニオン　経済　政治　ビジネス　金融　マーケット　マネーのまなび　テック　国際　スポーツ

文科省がOffice365の偽メールに注意喚起、6大学で被害

BP速報　＋フォローする

2018年7月2日 23:00

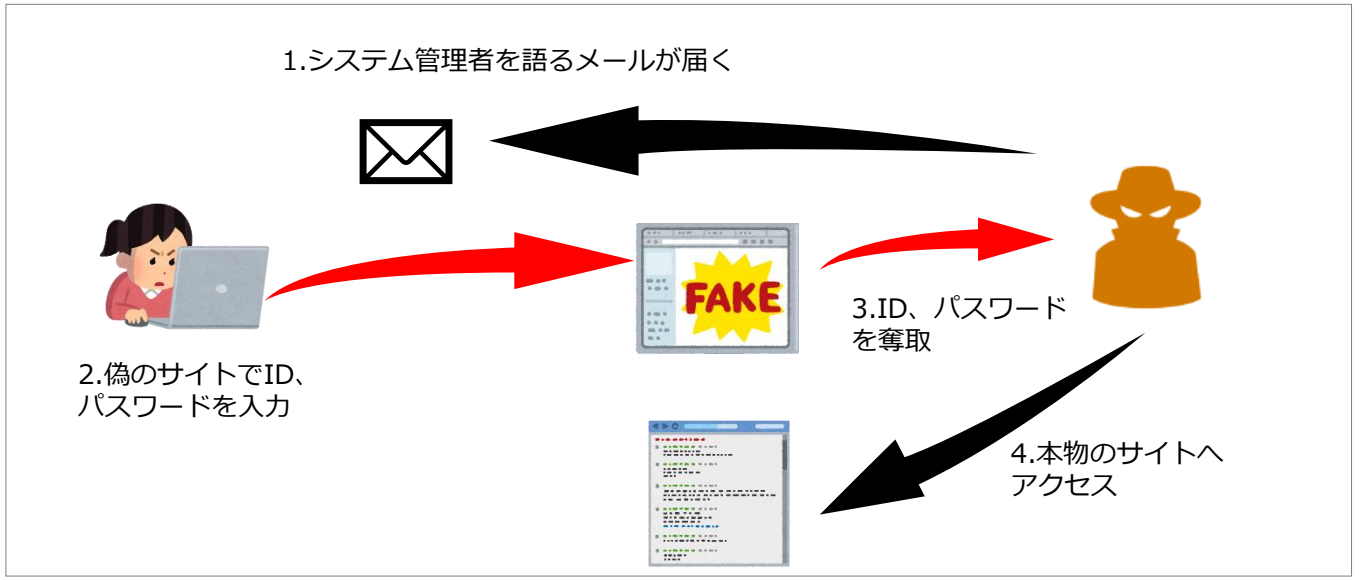
保存　グループシェア

日経XTECH 日経クロステック

文部科学省は2018年6月27日、弘前大学など6つの国公私立大学がフィッシングメールの被害に遭い合計約1万2000人分の個人情報が流出したことを受けて、全国の大学に対策を強化するように注意喚起した。

被害が判明しているのは弘前大学と横浜市立大学、島根大学、富山県立大学、沖縄県立看護大学、立命館大学。6大学がフィッシングメールの被害に遭ったとされるのは2018年4月から6月にかけて。6大学以外の詳細な被害状況については、「各大学が調査している段階」（文科省）という。

https://www.nikkei.com/article/DGXMZO32489620S8A700C1000000/



IaaS(AWS)インシデント事例

過去にもたびたび発生

「Amazon S3」内のデータが設定ミスで公開状態に　漏えいしたデータは？

Amazon Web Services（AWS）のオブジェクトストレージ「Amazon S3」でデータ漏えいが発生した。その中には、Ford MotorやNetflixなどの企業に関するデータが含まれていた。何が起きたのか。

[Michael Heller，TechTarget]

印刷／PDF

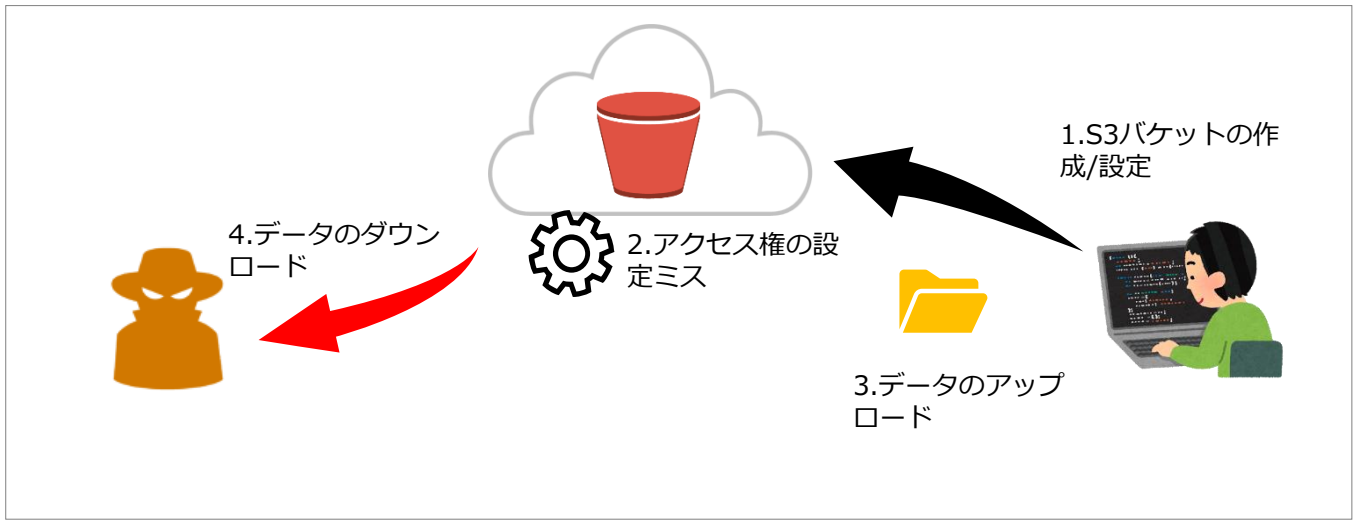
関連キーワード

Amazon Web Services　Amazon S3　クラウドストレージ　データセキュリティ　セキュリティホール

サイバーリスク管理会社UpGuardの調査チームは、Amazon Web Services（AWS）が提供するオブジェクトストレージ「Amazon Simple Storage Service」（Amazon S3）の設定ミスにより、データが公開状態になっていることを発見した。公開されていたデータの中には、Ford MotorやTD Bankなど複数の大企業の情報が含まれていた。

公開状態になっていた3個のAmazon S3バケット（データ保存領域）を利用していたのは、データマネジメントベンダーAttunityだった。合計約1TBのデータのうち750GBは圧縮されたバックアップ用データだ。UpGuardのデータ漏えい調査チームによると、公開状

https://techtarget.itmedia.co.jp/tt/news/1908/15/news07.html



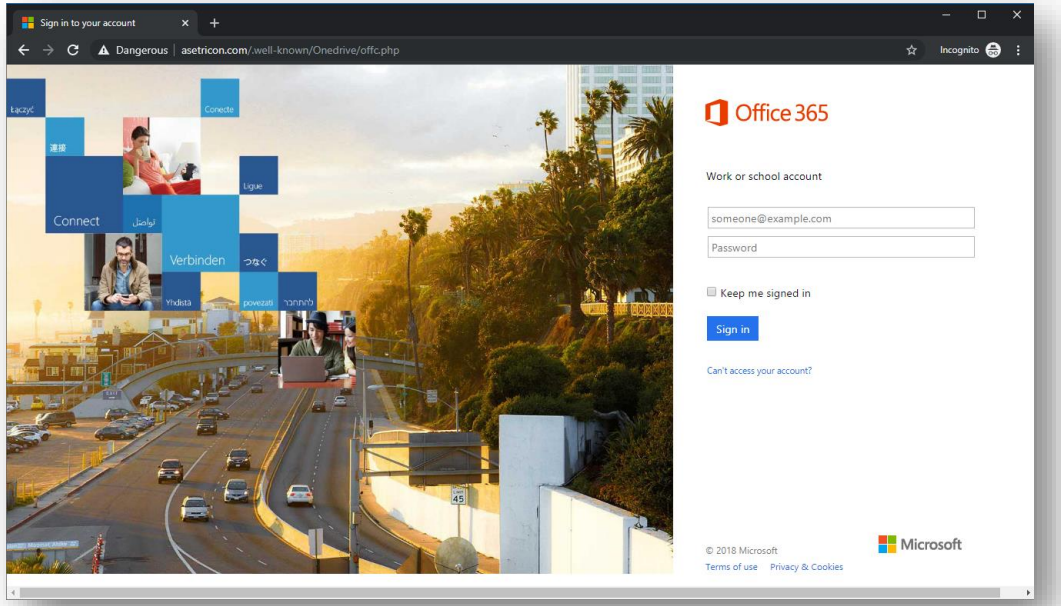
クラウドをターゲットとしたマルウェアのサイバーキルチェーン

初期アクセス	アカウント侵害	ディスカバリー	収集/流出	マネタイズ
				
ID侵害/ハイジャック	権限昇格	アクセス可能なデータを探索	クラウド特有の攻撃によるデータ暗号化、収集	身代金要求

侵入手口の手法1

・アカウント侵害

フィッシング、ブルート フォース攻撃、およびその他の資格情報侵害戦術を通じて、クラウド アカウントに対するユーザーの資格情報を直接侵害します。



・アカウント侵入検知対策

Slow and Low(管理アカウント)やKnockKnock攻撃(検出を避けるために一日数回でIPを変更しながら攻撃)

侵入手口の手法2

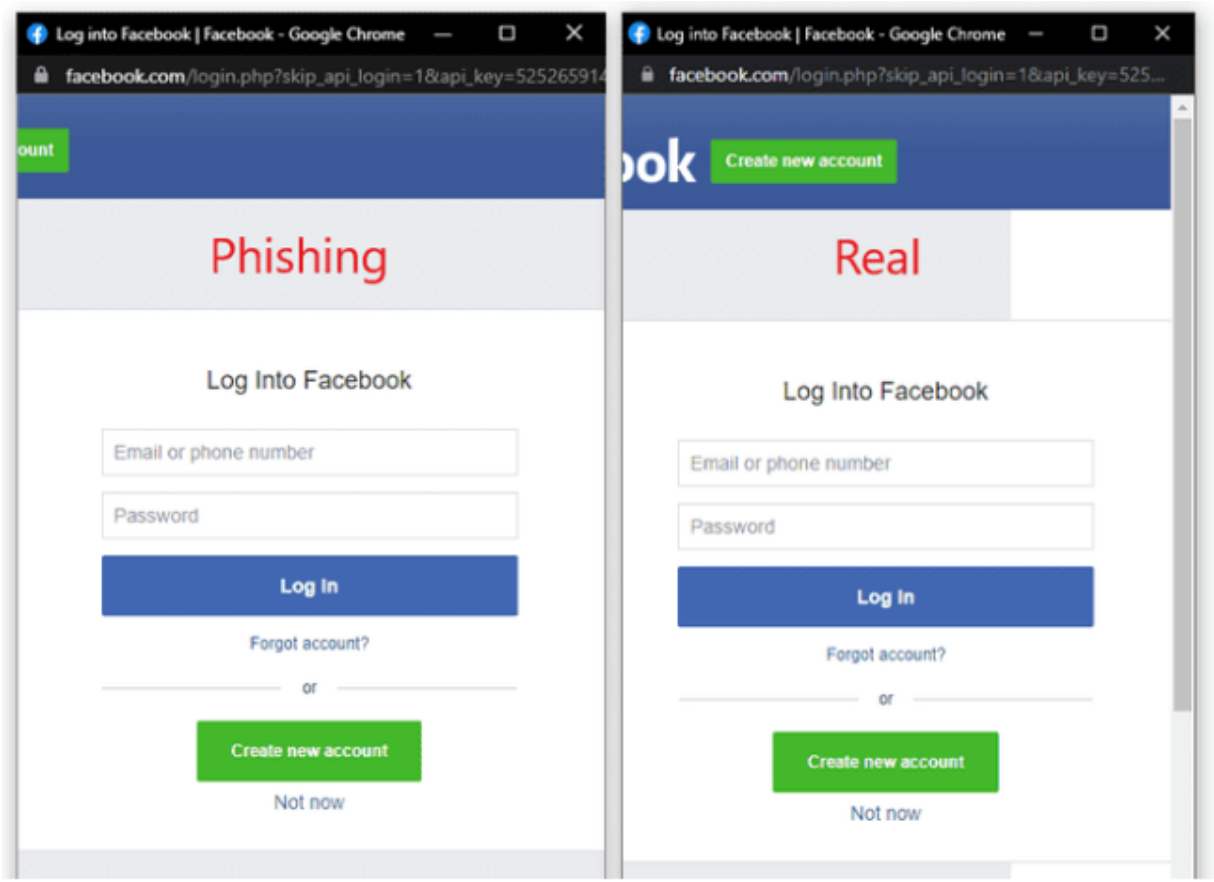
- サード パーティの OAuth アプリケーション

ユーザーをだまして、アプリケーション スコープでサード パーティの OAuth アプリを承認させます。

不正アクセス検知対策としてゴールデンSAMLやOAuth攻撃

- ブラウザ・イン・ザ・ブラウザ

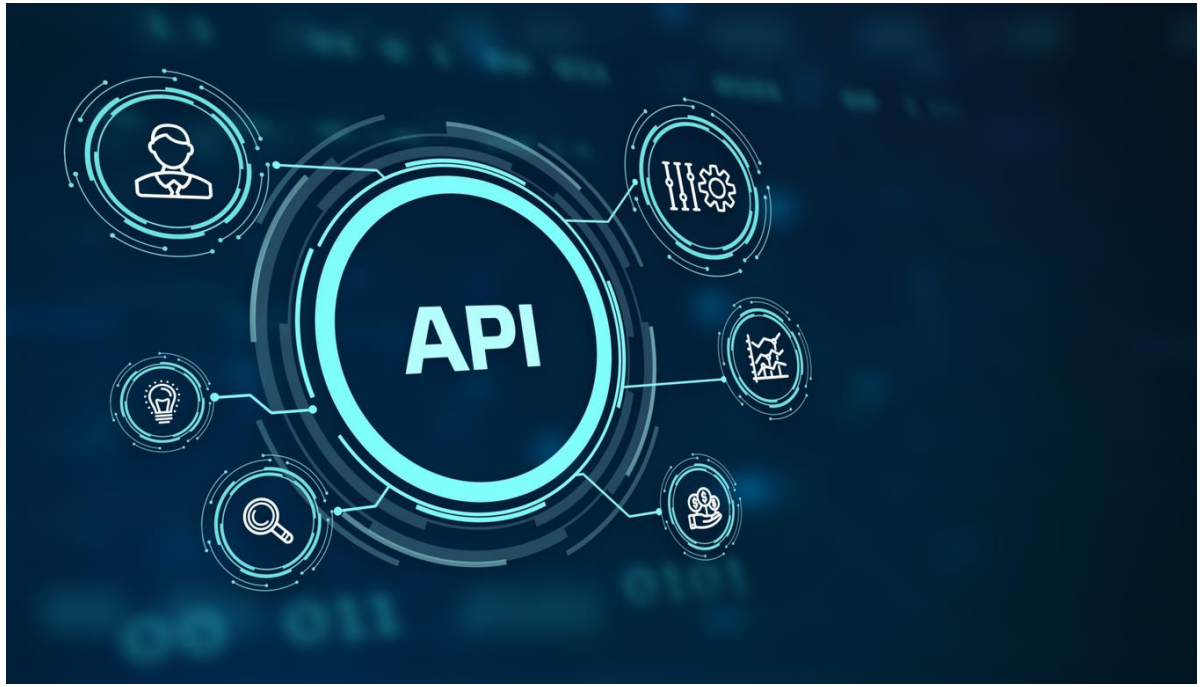
攻撃者は、JavaScriptのコードを書き換え、標的に偽のポップアップ・ウィンドウを表示し、アカウント情報を入力するよう促します。



侵入手口の手法3

・ハイジャックされたセッション

ログインしているユーザーの Web セッションをハイジャックするか、SharePoint Online や OneDrive のライブ API トークンをハイジャックします。



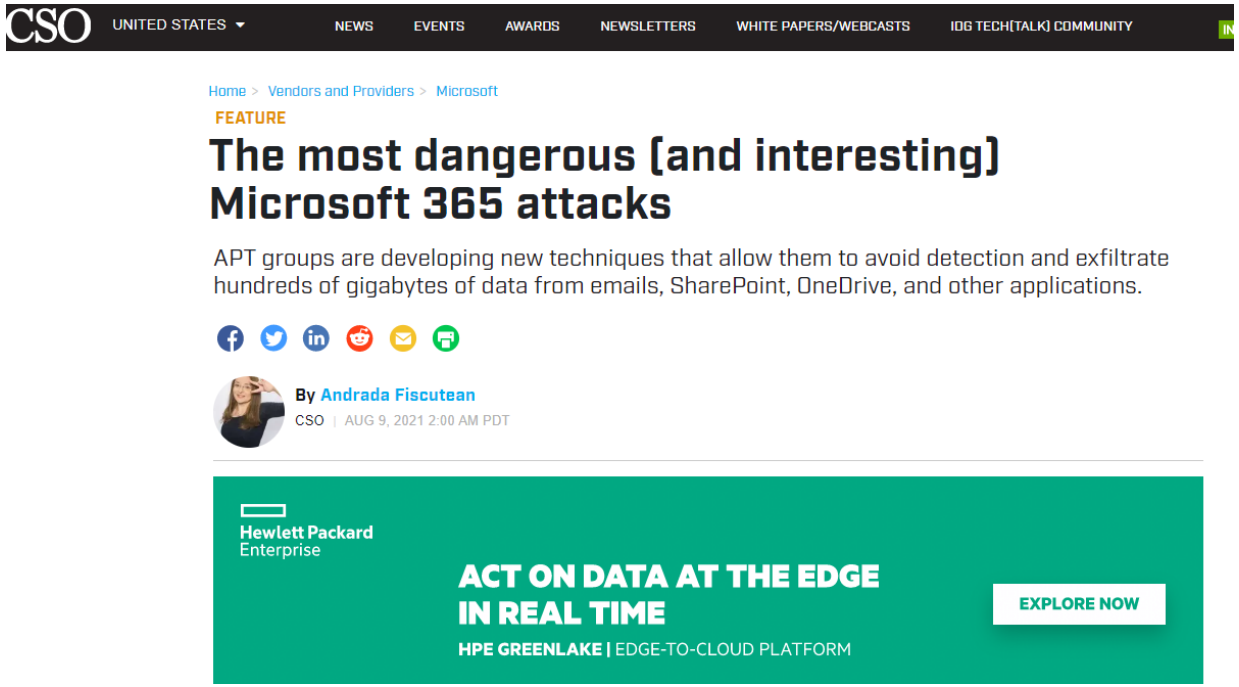
検出の回避

- **新しい検出回避テクニック**

APT グループは以前には見られなかったいくつかの手法を使用して検出を回避する方法を向上させました。「そのうちの 1 つは、ユーザー ライセンスを Microsoft 365 E5 ライセンスから E3 ライセンスにダウングレードすることです」

- **E5 ライセンス無効化による影響**

ID とアプリの管理、情報保護、および脅威からの保護を提供します。これにより、組織は脅威を検出して調査し、オンプレミスとクラウド環境の両方で悪意のあるアクティビティに気付くことができます。これは、E3 ライセンスにはない機能です。「そのため、攻撃者は被害者の組織のお金を節約しているかもしれませんが、実際には、組織が持っている最も効果的な検出メカニズムを非常に簡単に無効にしています。」



https://www.csoonline.com/article/3628330/the-most-dangerous-and-interesting-microsoft-365-attacks.html

データの破壊/収集、収益化

• データ破壊

ファイルのバージョン管理を 1 などの低い数値に減らしたり、バージョン制限を超えてファイルを暗号化します。クラウドで特有なのはファイルを 2 回暗号化し、通常のエンドポイントへのランサムウェアの攻撃とは異なります。場合によっては、二重恐喝戦術の一環としてファイルを収集することがあります。

• 収益化

元ファイルのバージョンはすべて失われ、クラウドには暗号化されたバージョンのみが残り、攻撃者は組織に身代金を要求します。

クラウド特有の攻撃によるデータ暗号化、収集

身代金要求

https://www.proofpoint.com/us/blog/cloud-security/proofpoint-discovers-potentially-dangerous-microsoft-office-365-functionality

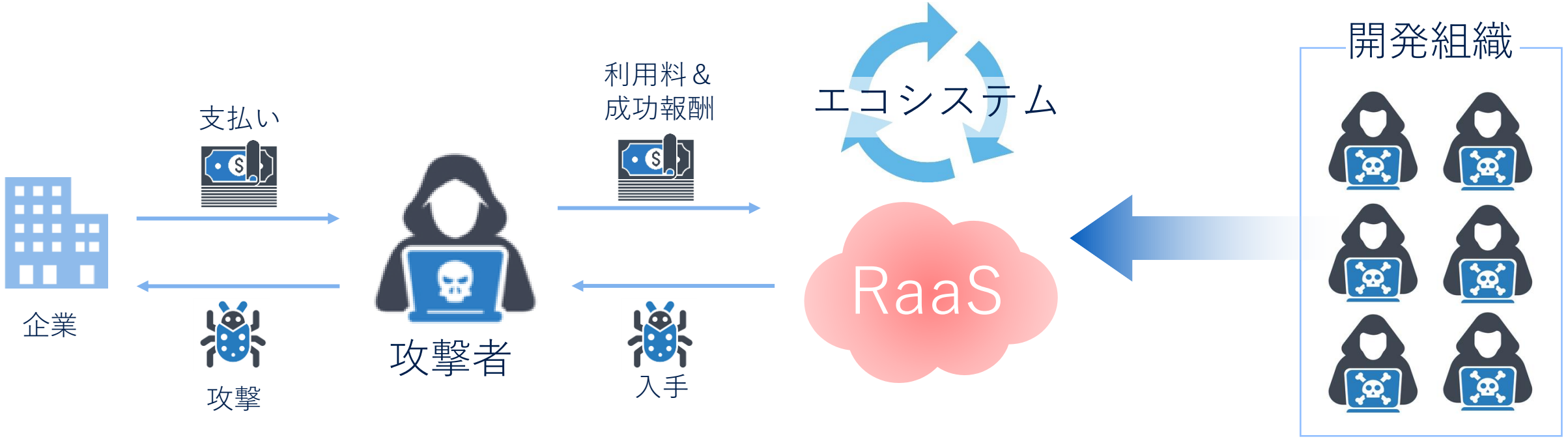
Acronis

#CyberFit

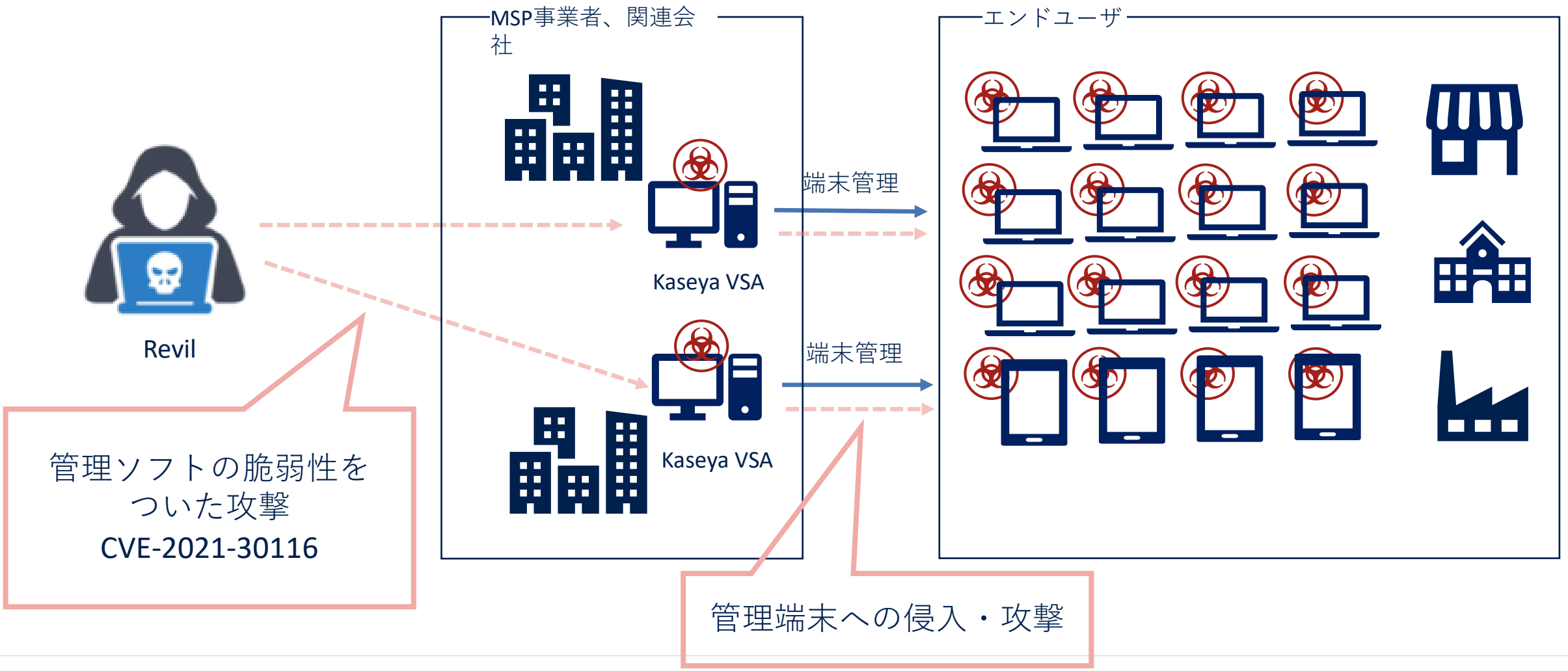
エンドポイントの
セキュリティ事情

今どきのランサムウェア事情

- 確実に儲かる事は日々のニュースで周知されている
- Ransomware as a Serviceを利用することで最新のマルウェアによる攻撃が可能
- ビジネスとしてのサイバー攻撃のエコシステムが形成されている



サプライチェーン攻撃 (KaseyaVSAの例)



トヨタがサイバー攻撃により国内工場停止

Toyota halts production after reported cyberattack on supplier

By Bill Toulas　　February 28, 2022　10:18 AM　0

Giant Japanese automaker Toyota Motors has announced that it stopped car production operations. The outage was forced by a system failure at one of its suppliers of vital parts, Kojima Industries, which reportedly suffered a cyberattack.　引用：https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/

トヨタ自動車は３月1日、取引先企業がサイバー攻撃を受け、国内全ての工場を停止。小島プレス工業がランサムウェアの被害にあったとみられている。

侵入経路はSonicWall社製の脆弱性(CVE-2021-20034)によるものと報道

引用：https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210913034617403/

企業規模に関わらず攻撃

- 日本企業を狙った攻撃
- 企業の足元を見た絶妙な身代金
- 機密情報の抜き取りとインターネットへの晒し
- 致命的なシステムへのダメージ

復旧に2億円

異例の決算発表困難

トヨタ系も

情報搾取と晒し

脅威の状況はより複雑になっています

57%
従来型のウイルス対策で見逃されている攻撃

出典：Acronis Cyberthreats Report 2020、Acronis Cyber Readiness Report 2020、FBI

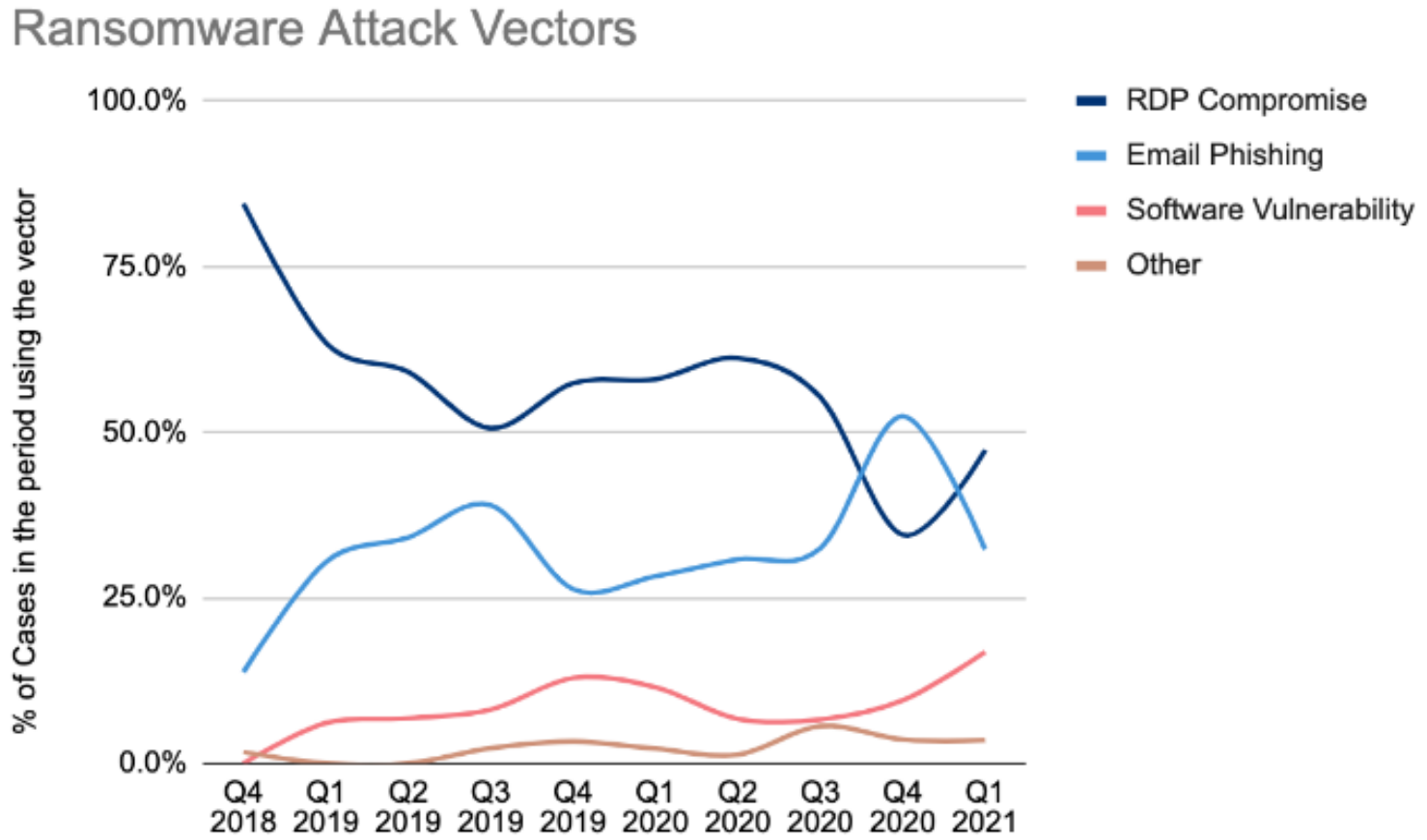
サイバー攻撃の高度化

最新のサイバー攻撃は、解析をすり抜ける技術や解析を妨害する機能が搭載

- ✓動的解析の妨害
- ✓静的解析の妨害
- ✓正規プロセスとしてなりすまし
- ✓回避行動
- ✓難読化
- ✓モジュール化
- ✓Defender無効化

攻撃者はどこからやってくる？

- Eメール経由
- RDPの悪用
- アプリケーションの脆弱性



COVEWARE

https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

NISCが提唱する、セキュリティ対策レベル

- 事業継続のための、感染後の対策が重要（駆除・復旧）
- データ消失等に備えて、データのバックアップの実施及び復旧手順を確認
- ランサムウェアに汚染されないサイバーセキュリティを考慮したバックアップが重要

https://www.nisc.go.jp/pdf/council/cs/jinzai/wg/dai05/05shiryou02.pdf

Acronis
Cyber Foundation

知識に富む未来を築くアクロニスサイバー基金

#CyberFit

知識を創造し、広げ、保護する活動へのご支援をお願いします。

- 新たな学校の建設
- 教育プログラムの提供
- 書籍の出版

www.acronis.org