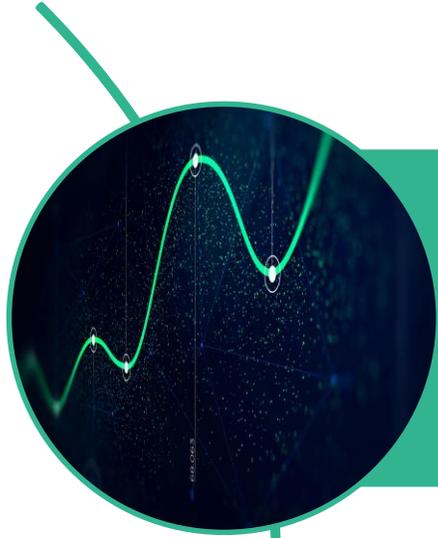


【概要解説】

2021年上半期サイバーセキュリティレポート について

**Presented by
Cyber Security Laboratory,
Canon IT Solutions, Inc.**

本日のアジェンダ

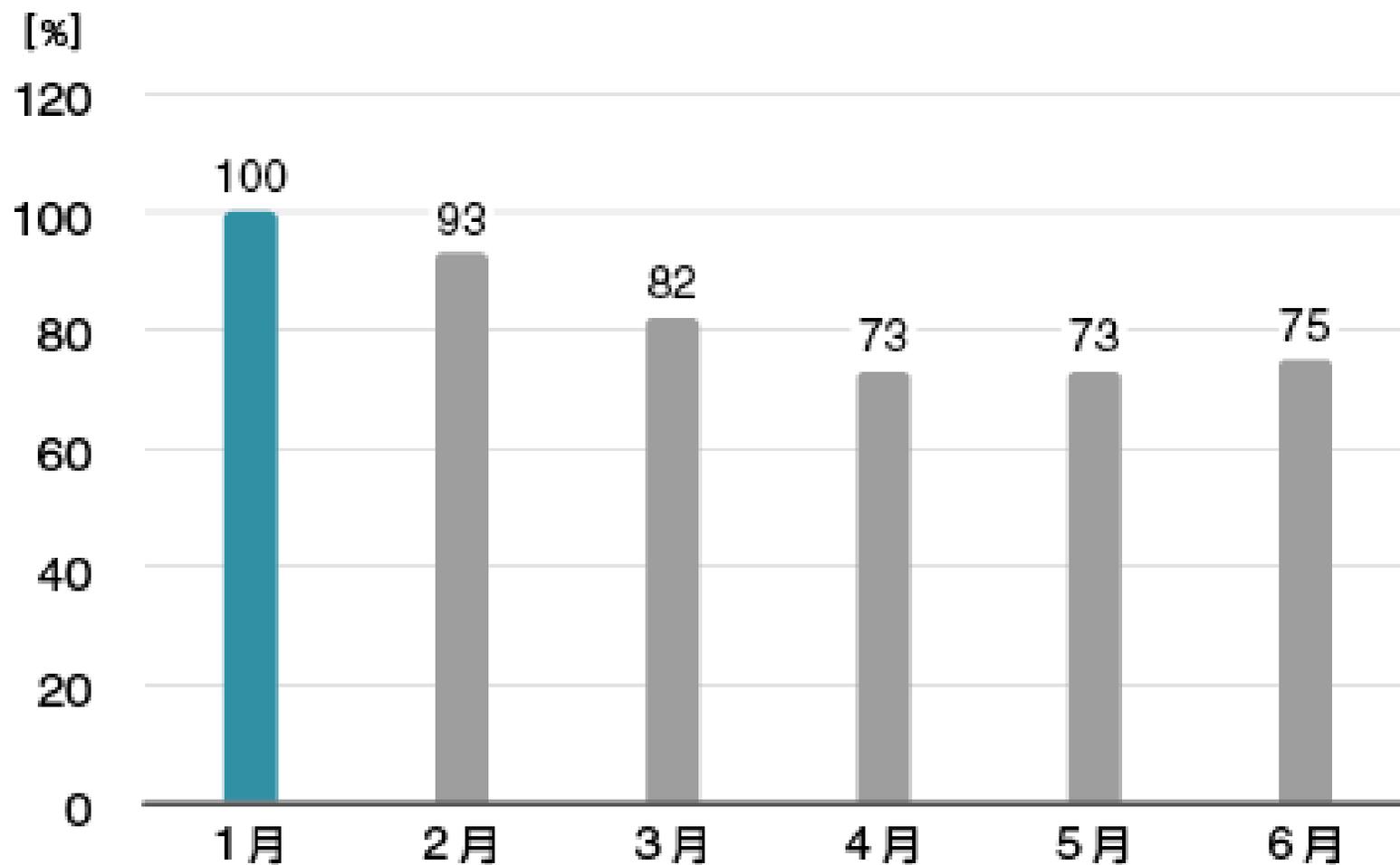


2021年上半期マルウェア検出統計



5つのトピックの概要

2021年上半期検出統計



2021年上半期検出統計

日本におけるマルウェア検出数*1のTOP10

前年1位



1位 JS/Adware.Agent

前年圏外



6位 DOC/Fraud

前年圏外



2位 JS/Adware.Sculinst

前年4位



7位 HTML/ScrInject

前年圏外



3位 HTML/Phishing.Agent

前年3位



8位 JS/Adware.PopAds

前年圏外



4位 JS/Adware.TerraClicks

前年10位



9位 VBA/TrojanDownloader.Agent

前年2位



5位 JS/Adware.Subprop

前年9位



10位 HTML/Refresh



Web上ブラウザ上で実行される脅威



メールの添付ファイルとしての脅威

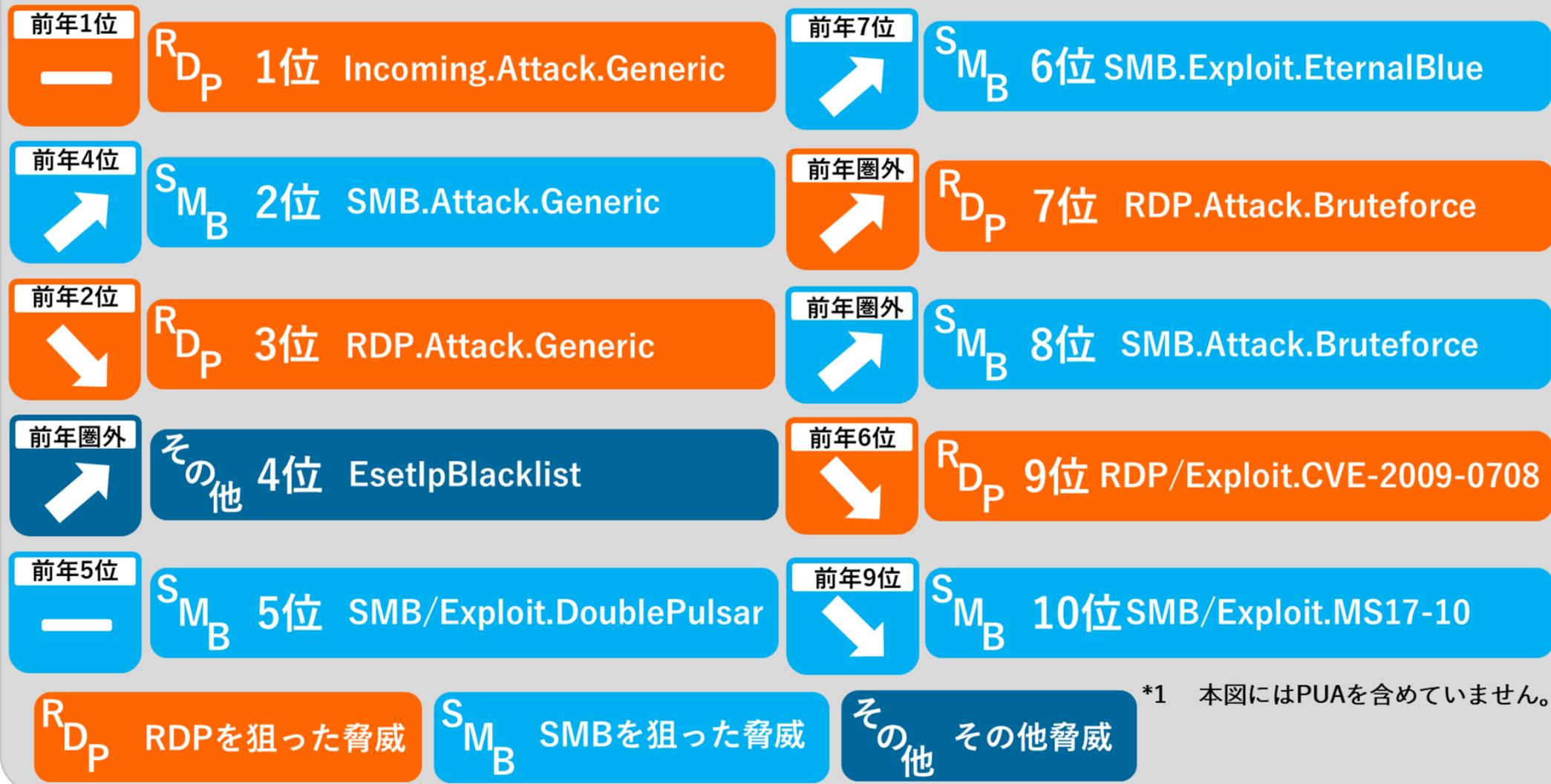


その他

*1 本図にはPUAを含めていません。

2021年上半期検出統計

ネットワーク攻撃保護で検出された脅威*1のTOP10



*1 本図にはPUAを含めていません。

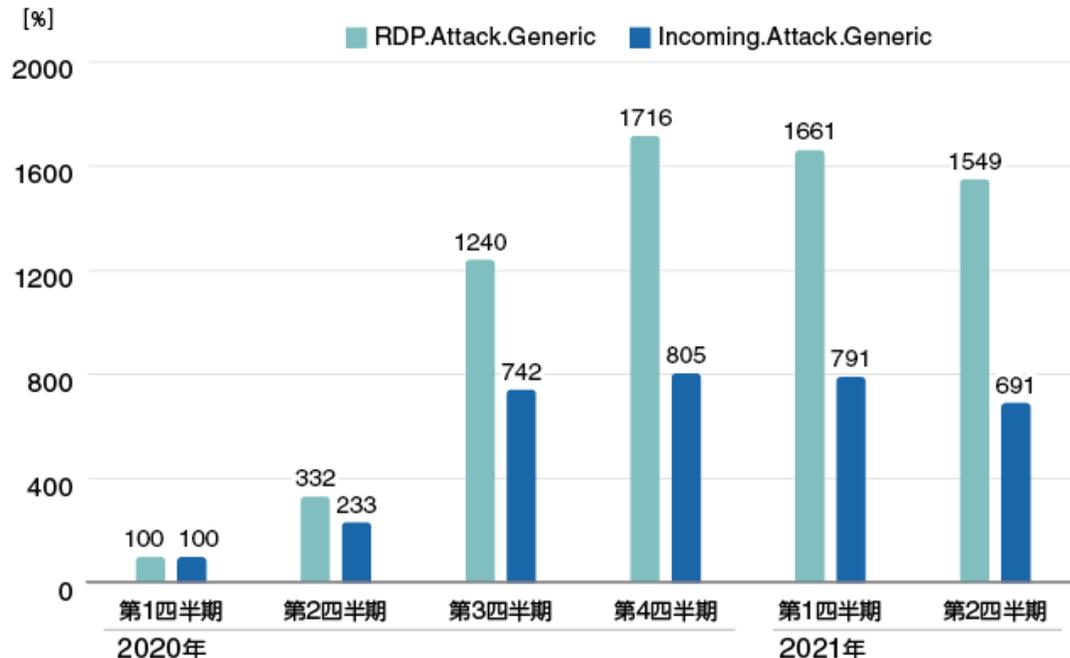
テレワーク環境を狙った攻撃

RDPを使用した攻撃・VPN機器を狙った攻撃が増加

コロナ禍においてRDPをインターネット上に公開している機器が世界的に増加(※)

(※)参考 : Shodan | Trends in Internet Exposure <https://blog.shodan.io/trends-in-internet-exposure/>

VPN機器の脆弱性の悪用によって、国内組織で機密情報の窃取の被害が生じている



(※)ESETの国内検出データより作成

ランサムウェアの感染経路や
窃取された認証情報がダークウェブ上で
売買されるなど、

様々な被害につながる可能性

使用する場合は、VPNとの併用や、
接続にあたり十分な認証を行うなど

セキュリティ対策と組み合わせて使用

Android環境で動作するマルウェアについて

「Flubot」は、ヨーロッパ全体で感染拡大中

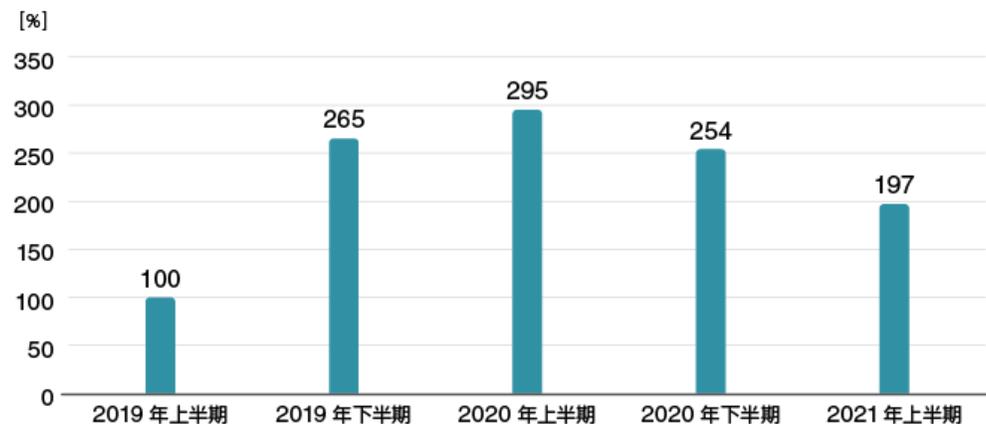


主な機能

- ・ Botとして感染を拡大させる機能
- ・ 情報窃取を行う機能

感染経路

- ・ 物流会社を装ったSMSのURL
- ・ ボイスメールを騙ったSMSのURL



物流会社のアプリを装っているFlubotに与えられた権限の一覧

米国で3億4千万ドルの被害を出しているロマンス詐欺

日本においてもロマンス詐欺の被害が発生

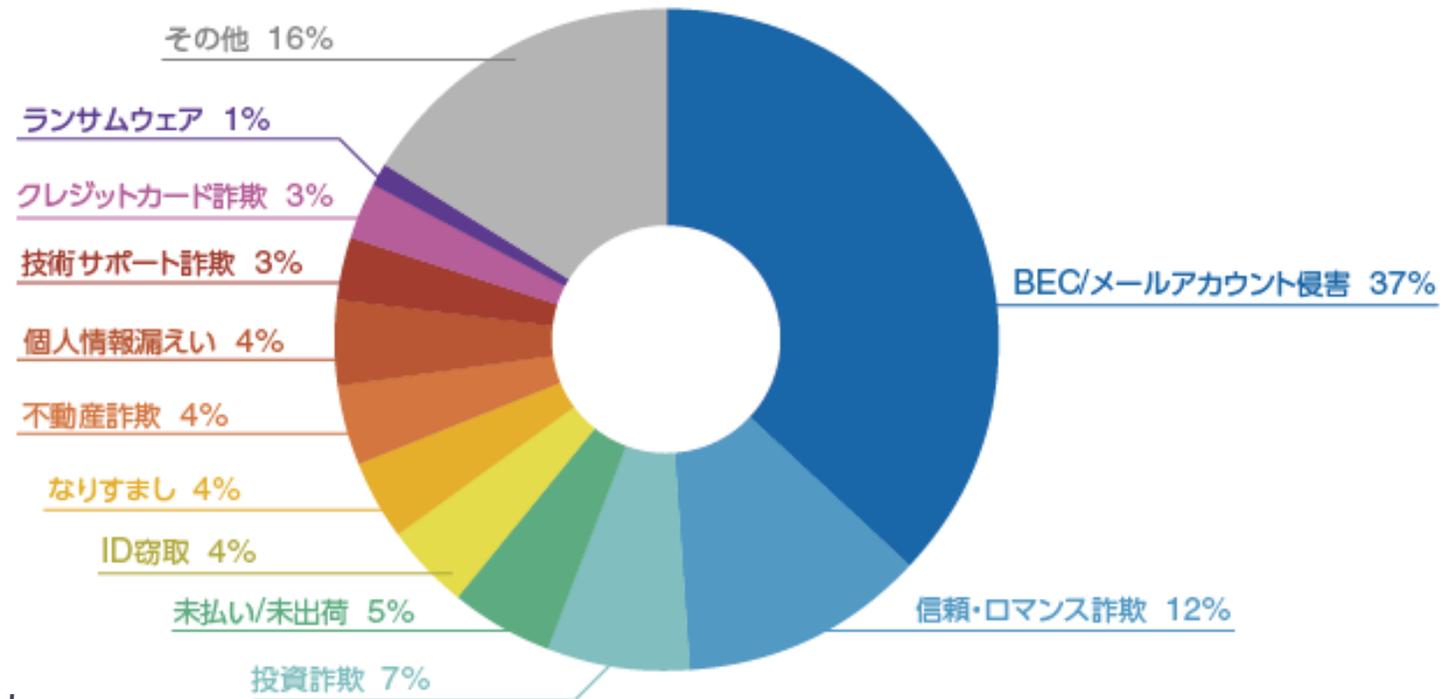
信頼・ロマンス詐欺の被害額は、
BEC/メールアカウント侵害に次ぐ2位で、
1位・2位は 2015年以来変わりません



海外の難民キャンプで医師として働いています。病気や貧困で苦しむ子供たちをなくすのが夢です。
両親も医師で子供の頃からそうするように言われてきました。母が生まれ育った北欧では、高校からボランティア活動につく生徒が多いそうです。

こんな僕で良ければ話し相手になってもらえますか。

詐欺師はマッチングサイト等で知り合った人に対し、SNSを通じて頻繁に連絡を取り、ターゲットと信頼関係を構築します

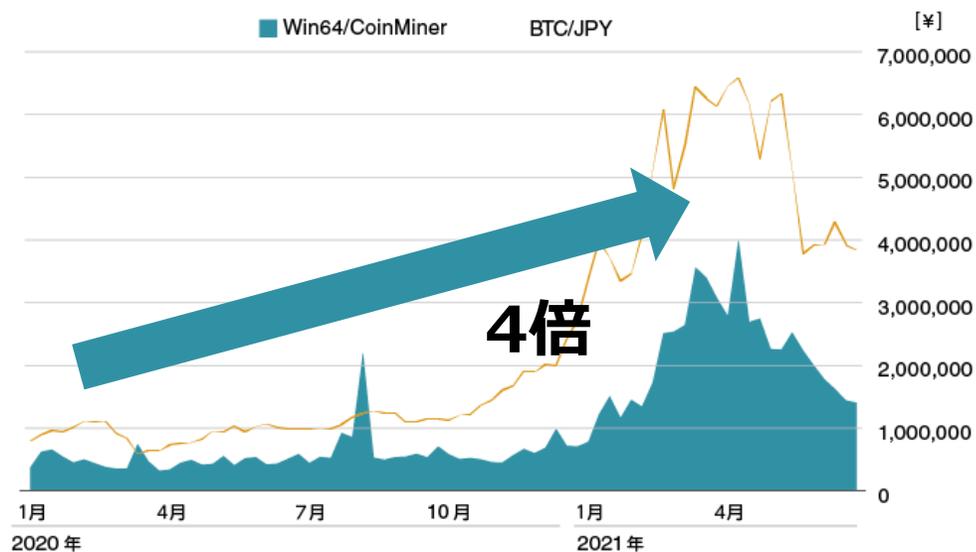


米国でのインターネット犯罪における被害額の割合（2020年）

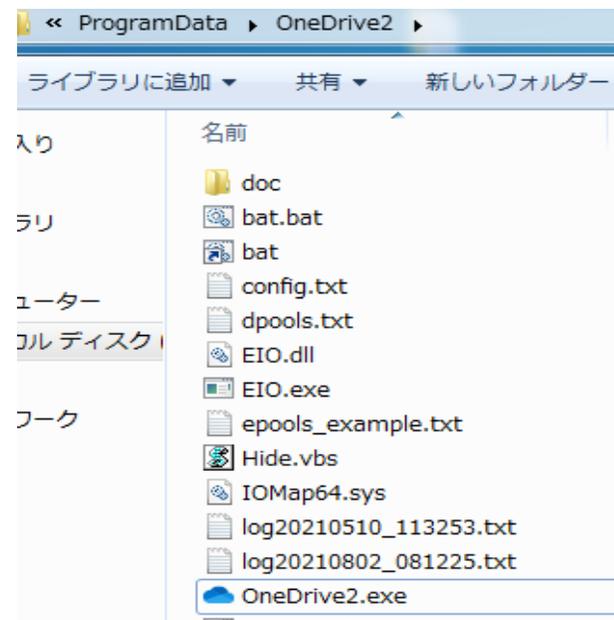
暗号資産（仮想通貨）の高騰とコインマイナーの検出状況

Win64/CoinMinerの検出数が2020年より約4倍に増加

- CoinMinerは、暗号資産のマイニングを行うプログラムの検出名
- PUAとして検出される正規のマイニングソフトが悪用されていることも多い
- PUAの検出を有効化し検査することで発見できる場合もある



暗号資産の高騰に伴い検出数も増加

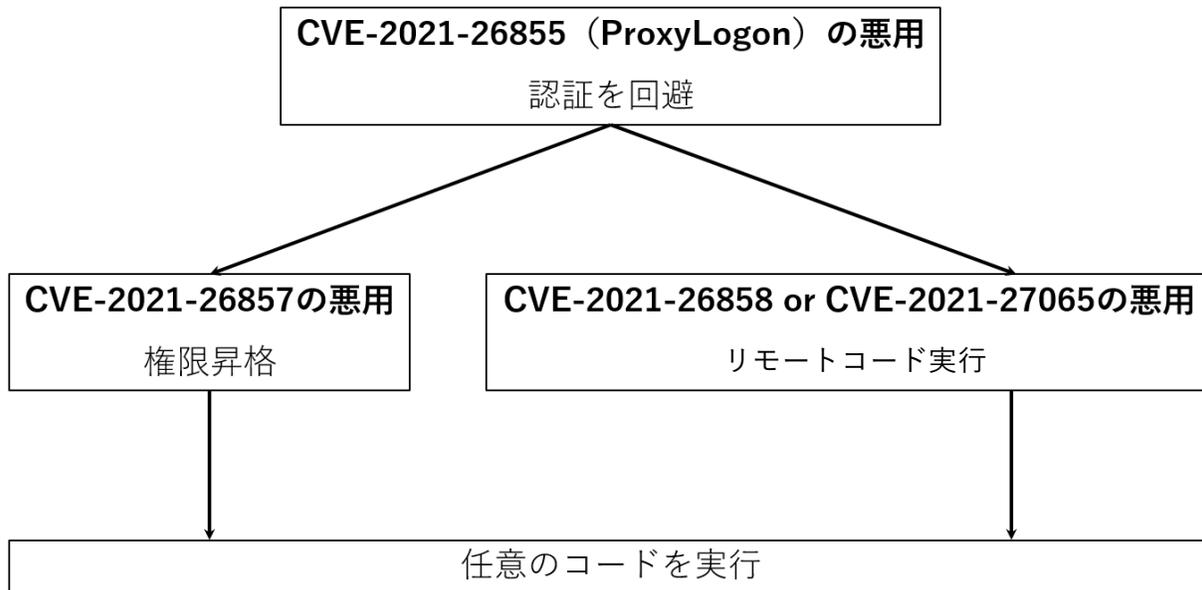


正規のマイニングソフトが悪用されていると思われる事例

ゼロデイ脆弱性悪用後に設置されるWebShell

2021年上半期にExchange Serverのゼロデイ脆弱性を複数悪用する攻撃が発生

ゼロデイ脆弱性悪用後は、
WebShellを介して
任意のコード実行するものが確認



```
C:\inetpub\wwwroot\aspnet_client\> wmic process list full

CommandLine=
OSName=マルウェア解析
Description=System Idle Process
ExecutablePath=
ExecutionState=
Handle=0
HandleCount=0
InstallDate=
KernelModeTime=1762187500
MaximumWorkingSetSize=
MinimumWorkingSetSize=
Name=System Idle Process
OSName=Microsoft Windows 10 Pro[C:\Windows]\Device\Harddisk0\Partition3
OtherOperationCount=0
OtherTransferCount=0
PageFaults=9
PageFileUsage=60
ParentProcessId=0
PeakPageFileUsage=60
PeakVirtualSize=8192
PeakWorkingSetSize=12
Priority=0
PrivatePageCount=61440
ProcessId=0
QuotaNonPagedPoolUsage=1
QuotaPagedPoolUsage=0
QuotaPeakNonPagedPoolUsage=1
QuotaPeakPagedPoolUsage=0
ReadOperationCount=0
ReadTransferCount=0
SessionId=0
Status=
TerminationI
ThreadCount
UserModeTim
VirtualSize=
WindowsVer
WorkingSetS
WriteOperati
WriteTransfe

CommandLi
OSName=マルウェア解析
```

攻撃者側の端末から
WebShellが設置された端末の
プロセス情報を列挙している様子

サイバーセキュリティ情報局について

キヤノンマーケティングジャパンと ESETが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか
サイバーセキュリティラボがまとめた
日本におけるマルウェア動向を
詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局

Search

The screenshot shows the ESET Special Site interface. At the top, there's a navigation bar with 'Canon | ESET SPECIAL SITE' and a search box. Below that, the main header reads 'キヤノンMJがお届けする安全なデジタル活用のためのセキュリティ情報 サイバーセキュリティ情報局' with the ESET logo. A menu bar includes 'トップ', 'トピック別', '立場別', 'キーワード事典', 'ホワイトペーパー', and 'セキュリティ注意喚起'. The main content area features a 'ニュース' (News) section with a date of '2021.9.24' and a featured article titled 'ソフトバンクをかたるフィッシングについての注意喚起'. To the right, there's an 'アクセスランキング' (Access Ranking) section with several article titles, such as 'スマホがウイルスに感染!? 不安に思ったら試したい5つの方法' and 'ダークウェブの基礎知識 何が取引され犯罪に利用されているのか'. At the bottom, there's a list of numbered items, including 'カメラアプリを使う際に気をつけたいセキュリティのポイント' and 'ハッキングの方法、手口を知ることが'.



ご視聴ありがとうございました