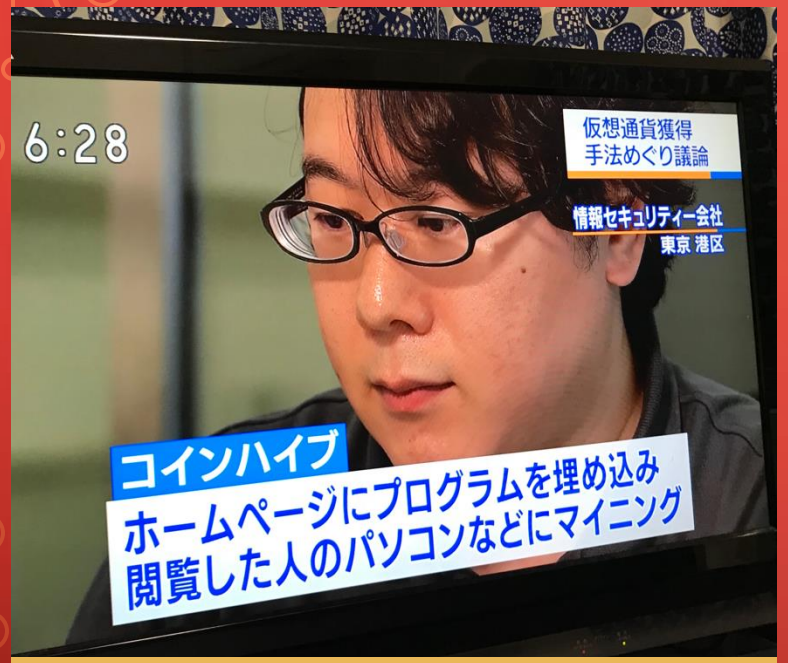
MWS CUP 2018
課題2: 静的解析

2018/12/20

中津留 勇
石丸 傑
石淵 一三

課題作成

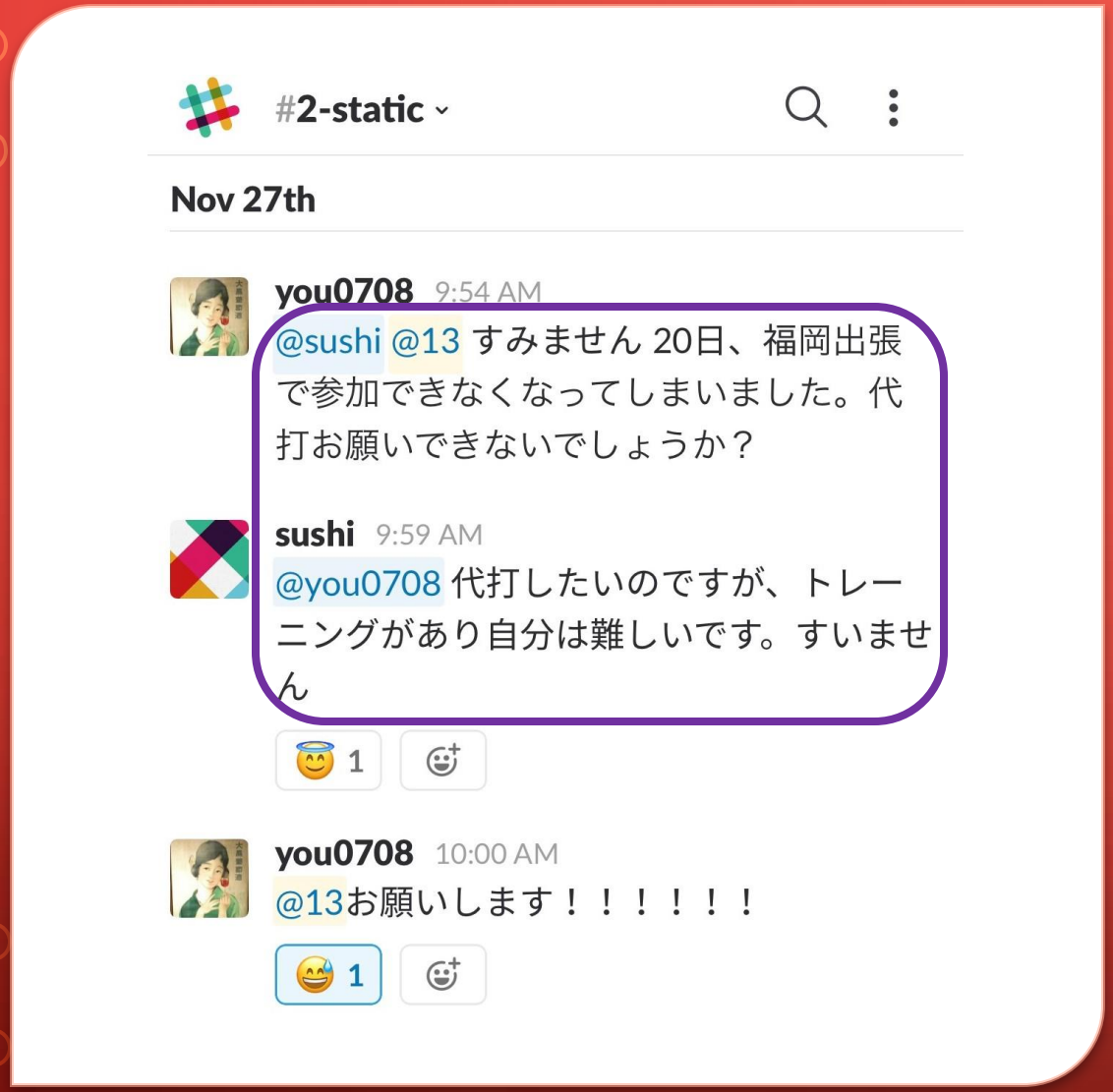


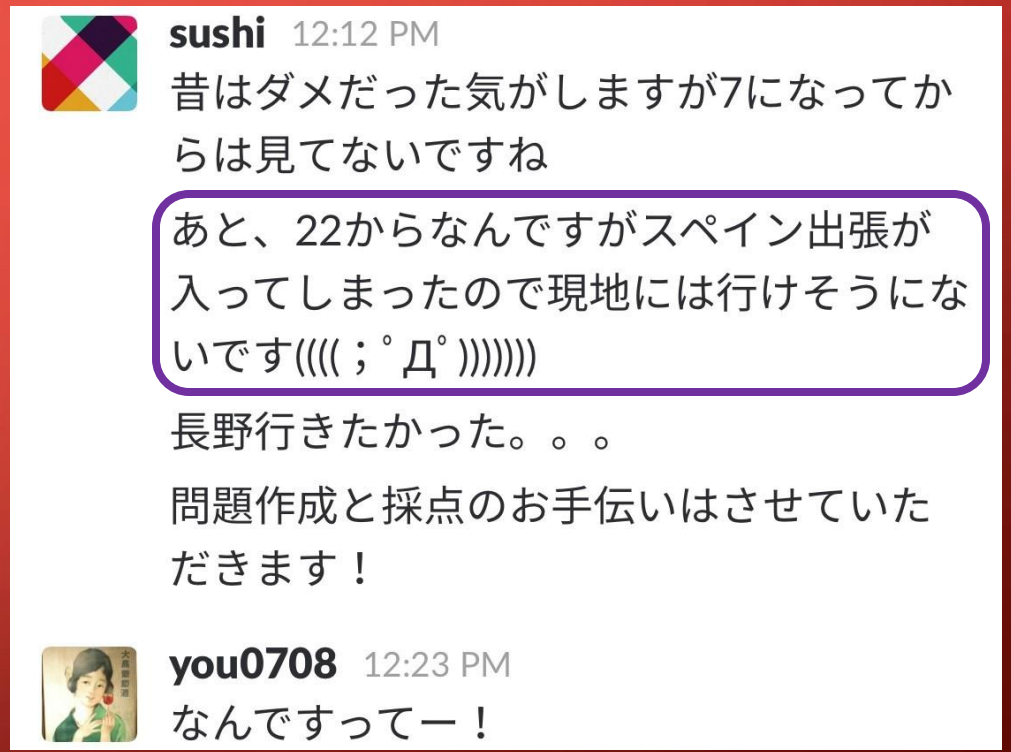
SecureWorks Japan 株式会社
中津留 勇

株式会社カスペルスキー
石丸 傑

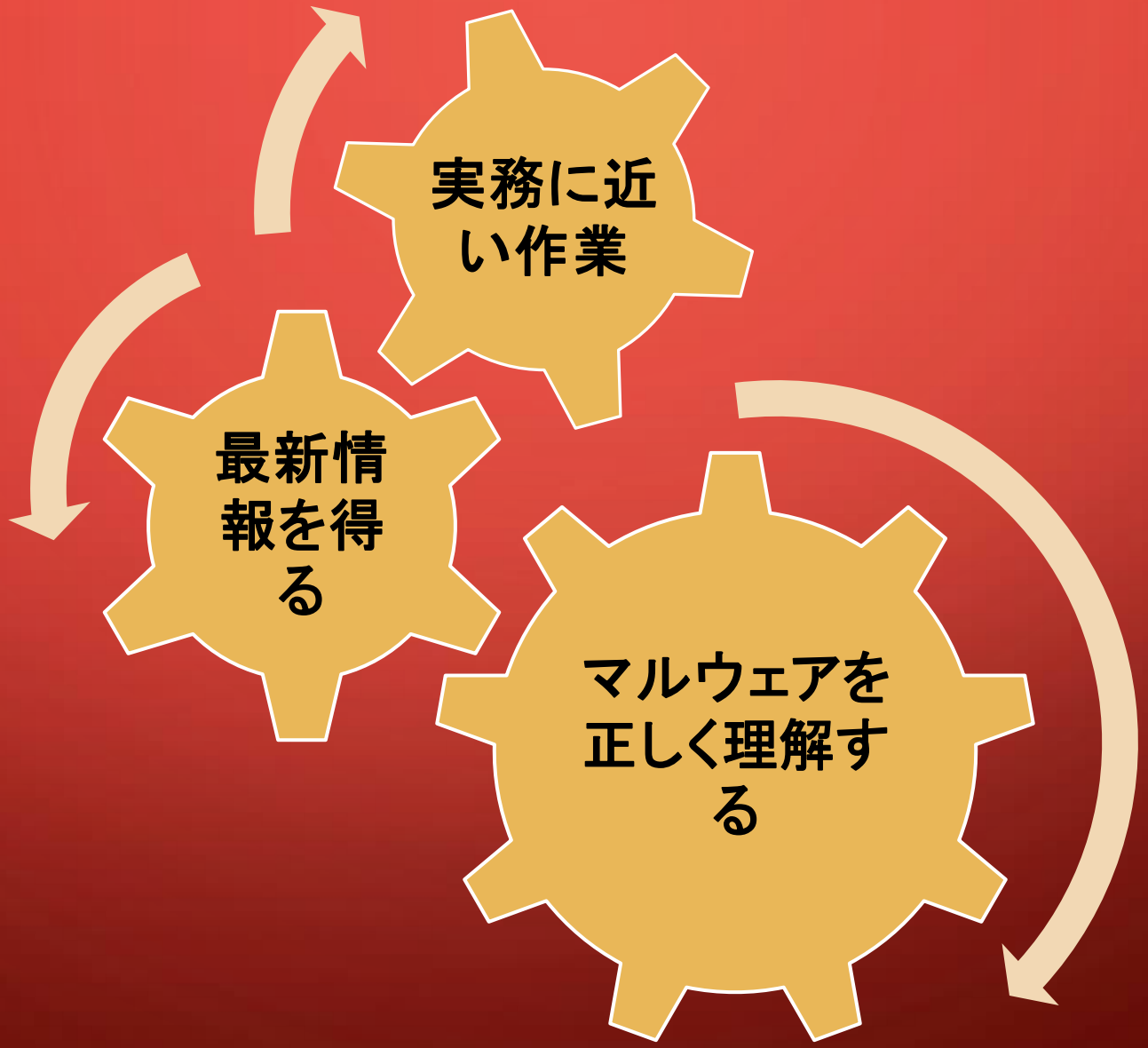
株式会社日立製作所
石淵 一三

歴史は繰り返される…


#2-static
Nov 27th
you0708 9:54 AM
@sushi @13 すみません 20日、福岡出張で参加できなくなってしまいました。代打お願いできないでしょうか？
sushi 9:59 AM
@you0708 代打したいのですが、トレーニングがあり自分は難しいです。すいません
1
you0708 10:00 AM
@13お願いします！！！！！！
1


sushi 12:12 PM
昔はダメだった気がしますが7になってからは見てないですね
あと、22からなんですがスペイン出張が入ってしまったので現地には行けそうにないです((((；゜Д゜))))))
長野行きたかった。。。
問題作成と採点のお手伝いはさせていただきます！
you0708 12:23 PM
なんですってー！

課題2 “変わらぬテーマ”



MWS CUP 2018
課題2: 解説

TREND MICRO トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs
セキュリティ専門家による脅威情報・ニュースをお届けします。

ホーム » 不正プログラム » 台湾の政府機関を狙った標的型攻撃キャンペーン「PLEAD」を確認

台湾の政府機関を狙った標的型攻撃キャンペーン「PLEAD」を確認

投稿日: 2014年5月27日
脅威カテゴリ: 不正プログラム, フィッシング, サイバー攻撃, 脆弱性, TrendLabs Report, Webからの脅威
執筆: Threats Analyst - Kervin Alintanahin

トレンドマイクロは、「2H-2013 Targeted Attack Roundup Report（英語情報）」で、台湾で型攻撃キャンペーンに関連した複数の攻撃を確認したことを報告しました。

弊社は現在、特に台湾の政府機関や行政機関を標的にした攻撃キャンペーンを監視していますお、この標的型攻撃キャンペーンは、関連するバックドア型不正プログラムから実行されるコの文字を取って、弊社では「PLEAD」と名づけています。

2018年04月25日 | ラックピープル

攻撃者グループ "BlackTech"による "PLEAD"を使った日の攻撃を確認

サイバー攻撃

石川 芳浩

当社脅威分析チームでは、台湾を主な標的として活動するBlackTech（ブラックテック）と呼ばれる攻撃者グループが日本の特定組織に対しても攻撃を行っていることを、2017年12月以降確認しています。攻撃で使用されたマルウェアは、「PLEAD（プリード）」と呼ばれるRATであり、BlackTechが標的型攻撃で使用するマルウェアの1つです。そこで今回は、日本の組織を狙った際に用いられた「PLEAD」に焦点を当てその攻撃手口を紹介します。

「PLEAD」を使った標的型攻撃の手口

「PLEAD」を展開する攻撃手口は、確認できた限りでも、図1に示すようなDLLファイルの内包、シェルコードの利用など複数存在し、共通してDLLまたはシェルコードをメモリ上に展開して実行することで、RAT機能を持つ「PLEAD」に感染させます。
以降では、それぞれの攻撃手口について詳しく見ていきます。

JPCERT CC Japan Computer Emergency Response Team Coordination Center JPCERT コーディネーションセンター
JPCERT/CC Eyes

Top > "マルウエア"の一覧 > 攻撃グループBlackTechが使うマルウエアPLEADダウンロータ (2018-05-28)

朝長 秀誠 (Shusei Tomonaga) 2

攻撃グループBlackTechが使うマルウエアPLEADダウンロータ (2018-05-28)

BlackTech

メール

前回の分析センターだより では攻撃グループBlackTech[1]が使用していると考えられるマルウエアTSCookie について紹介し
の攻撃グループはその他にもPLEADと呼ばれるマルウエアを使用することが分かっています。（PLEADは複数のマルウエア種
（TSCookieを含む）とそのマルウエアを使用した攻撃キャンペーン名として使用されています[2]。ここではPLEADをTSCoo
なるマルウエア種別名として使用します。）PLEADにはRATタイプと、ダウンロータタイプ（以降、PLEADダウンロータと記
が存在します。RATタイプは複数のコマンドを持ち、命令を受信することによって動作します。（詳しくは、LAC社が公開し
グ[3]の「攻撃手口3」をご覧ください。）PLEADダウンロータは、TSCookieと同じくモジュールをダウンロードし、メモリ
ます。（上記ブログ内の「攻撃手口2」に該当します。）
今回は、PLEADダウンロータの詳細について紹介します。

課題2: “PLEAD”

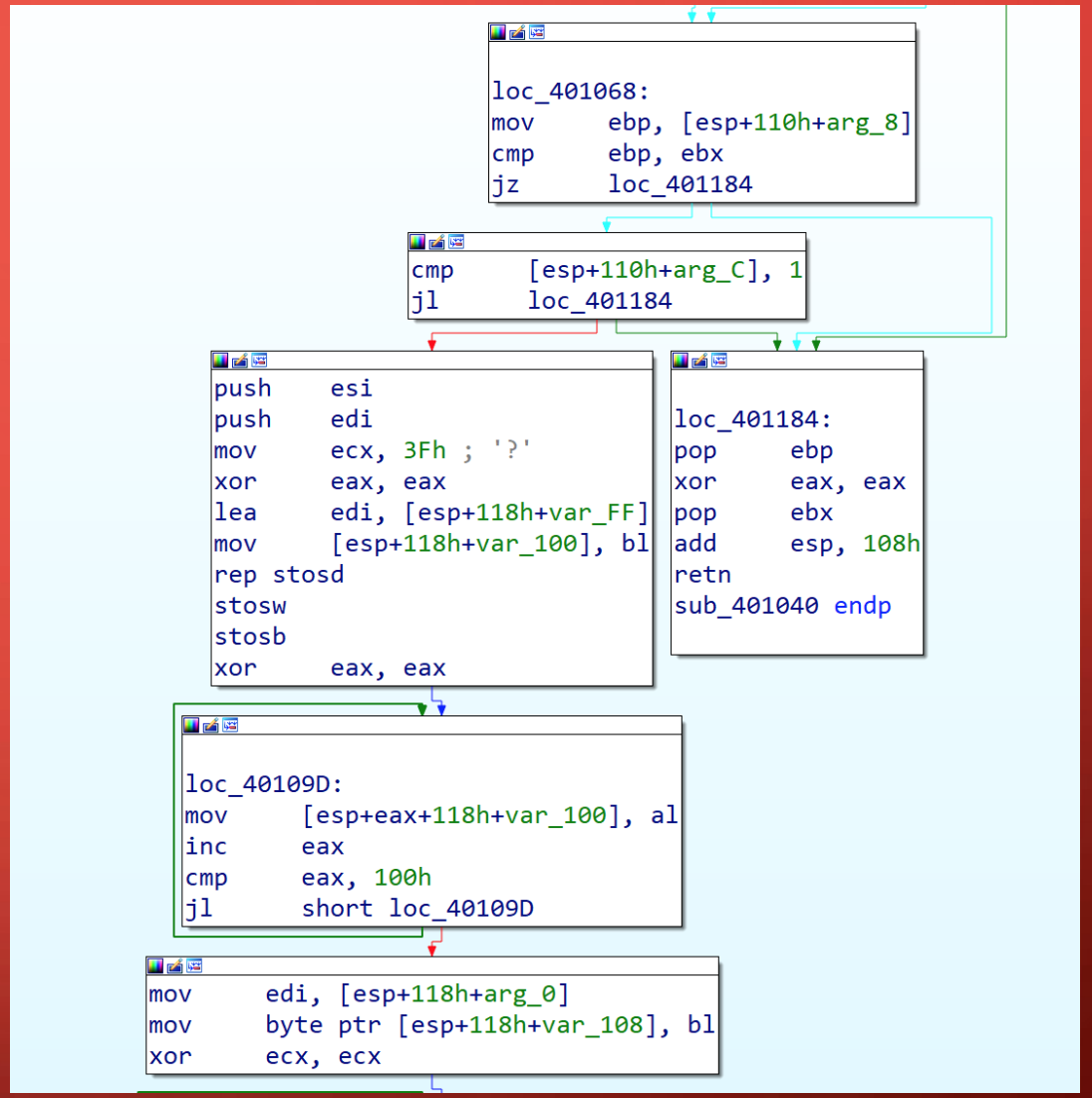
出典:
https://blog.trendmicro.co.jp/archives/9166
https://www.lac.co.jp/lacwatch/people/20180425_001625.html
https://blogs.jpcert.or.jp/ja/2018/05/linopid.html

sample1.i64

1-1.

関数 sub_00401040 が何を行う関数か以下から選択せよ。

- RC4 復号
- AES 復号
- DES 復号
- XXTEA 復号

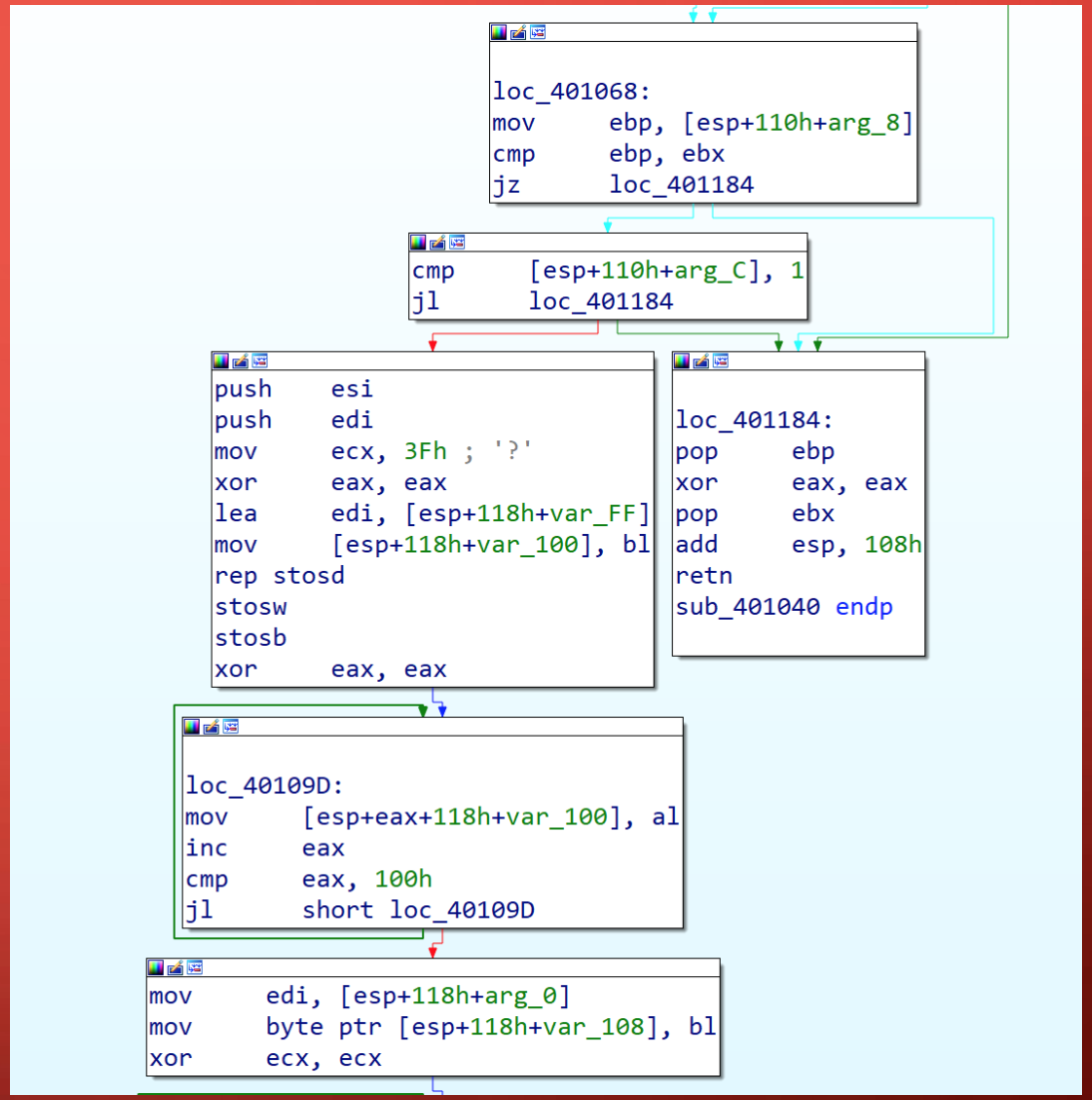


sample1.i64

1-1.

関数 sub_00401040 が何を行う関数か以下から選択せよ。

- **RC4 復号**
- ~~AES 復号~~
- ~~DES 復号~~
- ~~XXTEA 復号~~



参考:
アセンブリで書かれたRC4は見た瞬間分かるか

sample1.i64

1-2.

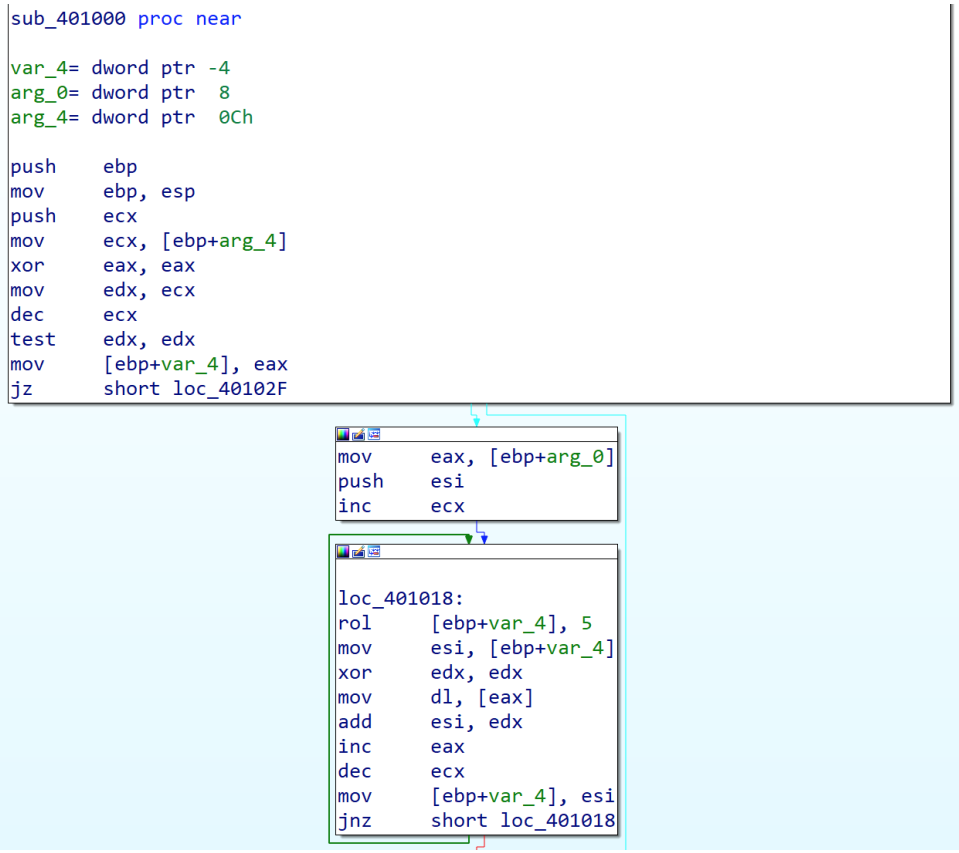
アドレス 0X0040343B の命令に含まれる固定値 0X5EF09604 の意味を答えよ。

```
push    ebx
push    esi
call    sub_401000
xor     ecx, ecx
cmp     eax, 5EF09604h
```

sample1.i64

1-2.

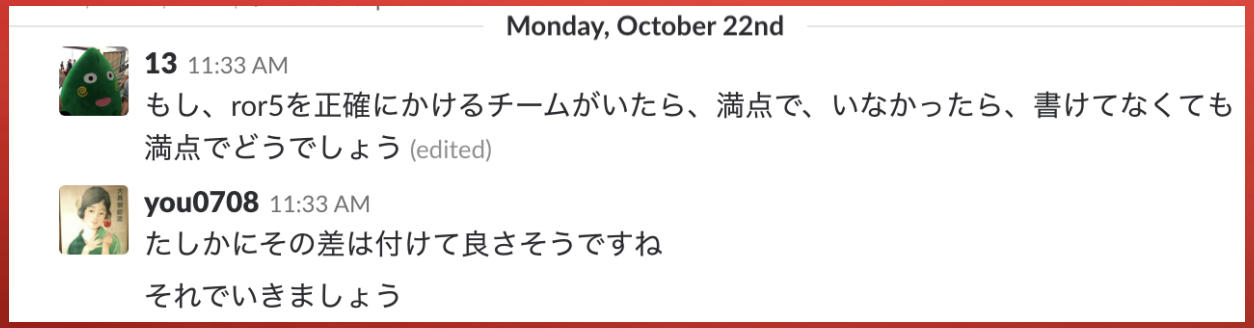
アドレス 0X0040343B の命令に含まれる固定値 0X5EF09604 の意味を答えよ。



sample1.i64

1-2.

アドレス 0X0040343B の命令に含まれる固定値 0X5EF09604 の意味を答えよ。

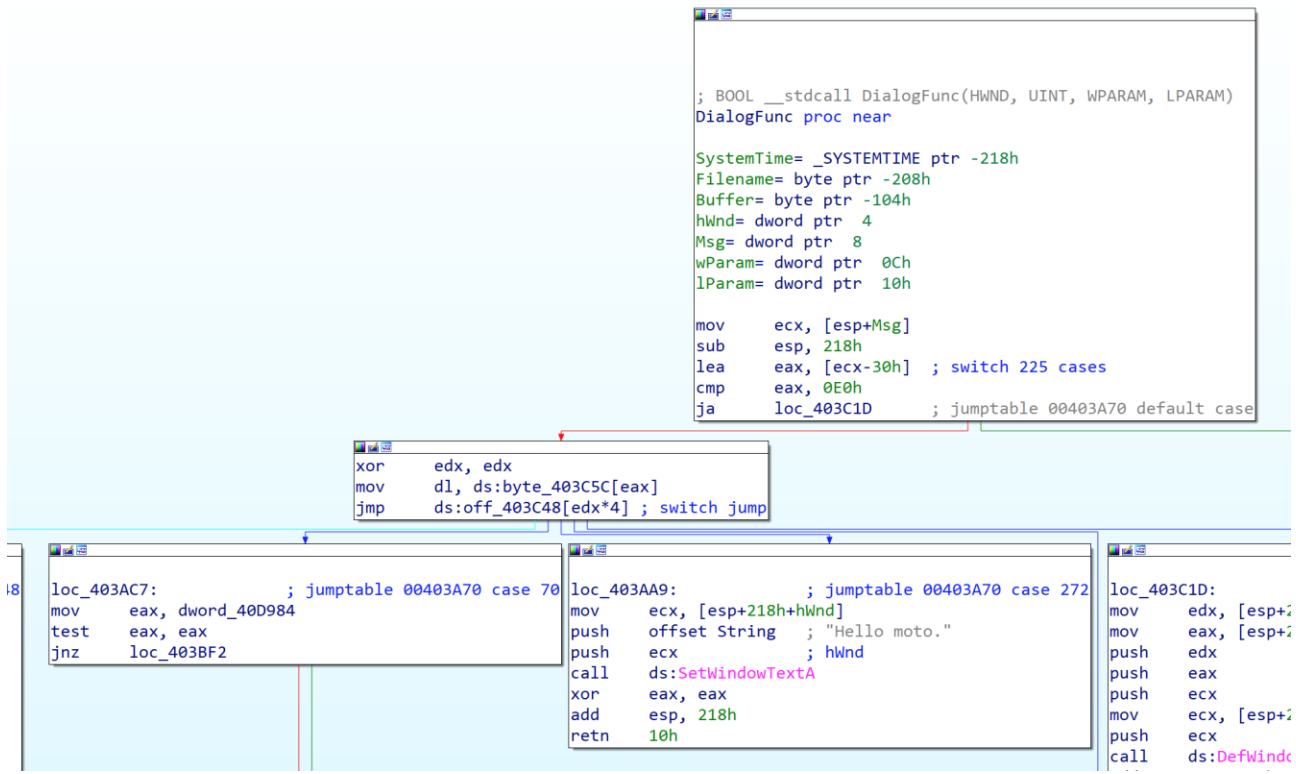


【満点 (3点)の回答】
RC4で復号したデータを以下の手順で集計したチェックサム
集計した結果が0x5EF09604と等しいか確認している

1. 1バイト読む
2. チェックサムを5ビット左ローテートシフトする
3. チェックサムに読み込んだ1バイトを加算する
4. 1~3を全データに対して適用する

sample1.i64

1-3.



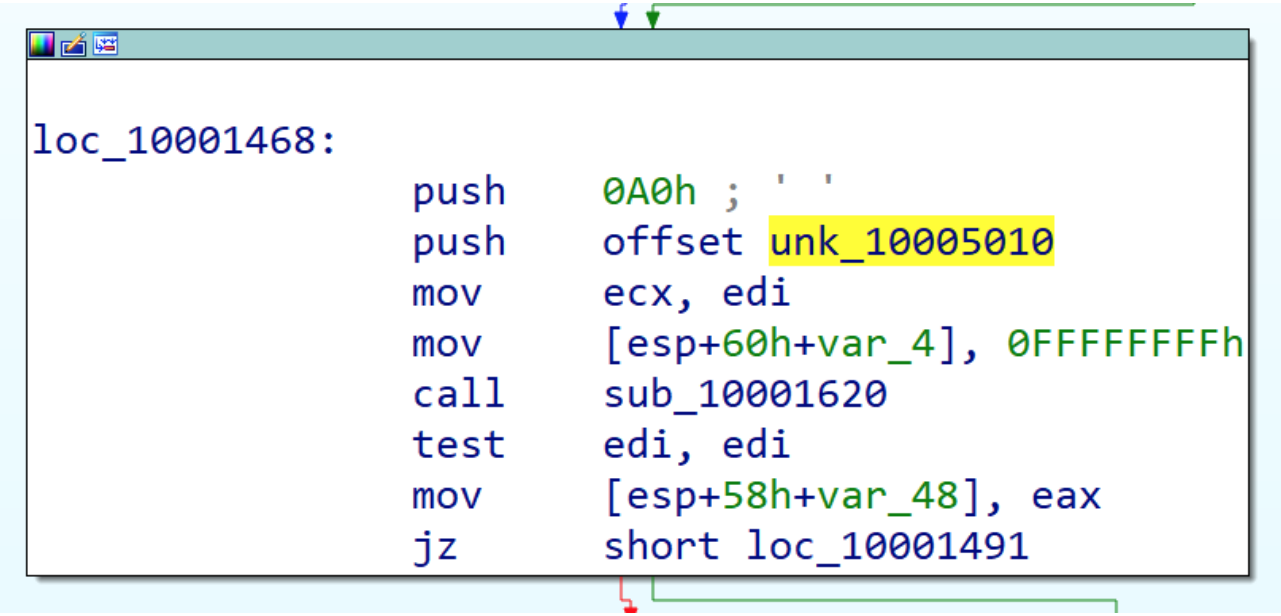
- アドレス 0x00403A50 の DialogFunc 関数は，ダイアログボックスへ送信されたメッセージである第二引数 Msg により挙動が変化する。その挙動の内，悪意のあるコードが実行されるメッセージ名 (WM_CREATE など)を答えよ。

Msg	メッセージ名
48 (0x30)	WM_SETFONT
70 (0x46)	WM_WINDOWPOSCHANGING
130 (0x82)	WM_NCDESTROY
272 (0x110)	WM_INITDIALOG

sample1.i64

1-3.

- アドレス 0x00403A50 の DialogFunc 関数は，ダイアログボックスへ送信されたメッセージである第二引数 Msg により挙動が変化する。その挙動の内，悪意のあるコードが実行されるメッセージ名 (WM_CREATE など)を答えよ。



sample2.i64

2-1.

- アドレス 0x10005010 に格納されているデータは暗号化された設定情報である。このデータを復号して得られる設定情報の文字列を答えよ。なお，暗号化された設定情報はファイル encrypted_config.bin として同梱している。

```
sub_10001620    proc near               ; CODE XF

var_250         = dword ptr -250h
var_24C         = word ptr -24Ch
var_248         = dword ptr -248h
var_244         = byte ptr -244h
String1         = byte ptr -204h
String2         = byte ptr -184h
var_104         = byte ptr -104h
arg_0           = dword ptr  4

                sub     esp, 250h
                mov     eax, [esp+250h+arg_0]
                push    ebx
                push    ebp
                push    esi
                mov     [esp+25Ch+var_248], ecx
                push    edi
                lea     esi, [eax+20h]
                mov     ecx, 20h ; ' '
                lea     edi, [esp+260h+String2]
                add     eax, 7
                rep movsd
                lea     ecx, [esp+260h+var_104]
                push    ecx
                push    17h
                push    eax
                call    sub_10001000
                lea     edx, [esp+26Ch+var_104]
                lea     eax, [esp+26Ch+String2]
                push    edx
                push    80h ; '€'
                push    eax
                call    sub_100010A0
```

RC4 KSA (Key-scheduling algorithm)

RC4

sample2.i64

2-1.

- アドレス 0x10005010 に格納されているデータは暗号化された設定情報である。このデータを復号して得られる設定情報の文字列を答えよ。なお，暗号化された設定情報はファイル encrypted_config.bin として同梱している。

encrypted_config.bin

00	EE53B7AB	D9DAA1B2	C3310CE1	A1C27BD7
10	B2C35FCD	90A3B2C3	7DB3C3A1	D3B0484A
20	A3A1E763	EB181104	830667FA	2616350F
30	BFC9FD10	920E0B22	21F2B8B2	07AE5952
40	8589F78C	E29D5EDD	6630C1C4	EF88656C
50	A1158570	7EC22719	5F7F50D1	0F2A419F
60	845B1B10	13268D21	0AE5E69F	FEE037F1
70	60EED0B2	92924AC0	836A5B7D	33B6BE4C
80	E1A8DD44	F79076AF	9DAFA3EA	30F4CF5E
90	7896543E	EC077C47	49F43FC1	6B7CE753
A0				

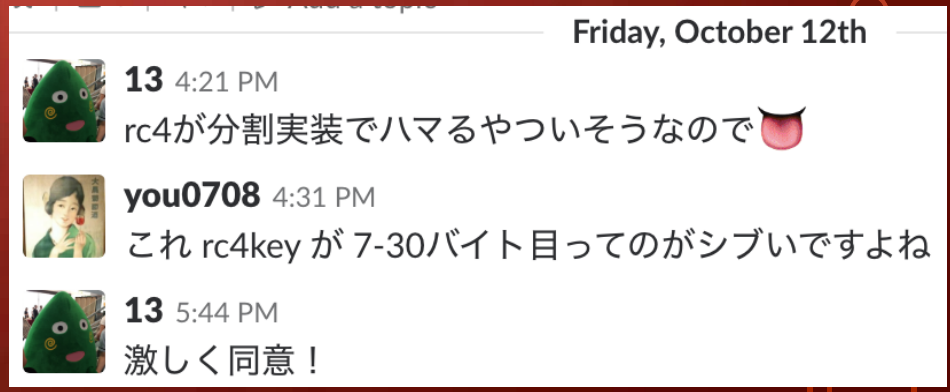
Signed Int | le, dec | (select less data)

23 bytes selected at offset 7 out of 160 bytes

sample2.i64

2-1.

- アドレス 0x10005010 に格納されているデータは暗号化された設定情報である。このデータを復号して得られる設定情報の文字列を答えよ。なお，暗号化された設定情報はファイル encrypted_config.bin として同梱している。



sample2.i64

2-1.

アドレス 0x10005010 に格納されているデータは暗号化された設定情報である。このデータを復号して得られる設定情報の文字列を答えよ。なお，暗号化された設定情報はファイル encrypted_config.bin として同梱している。

"download.ns01.us:8080,443,1863;movies.sixth.biz:8080,443,1863;pats.itsAOL.com:8080,443,1863;"

sample2.i64

2-2.

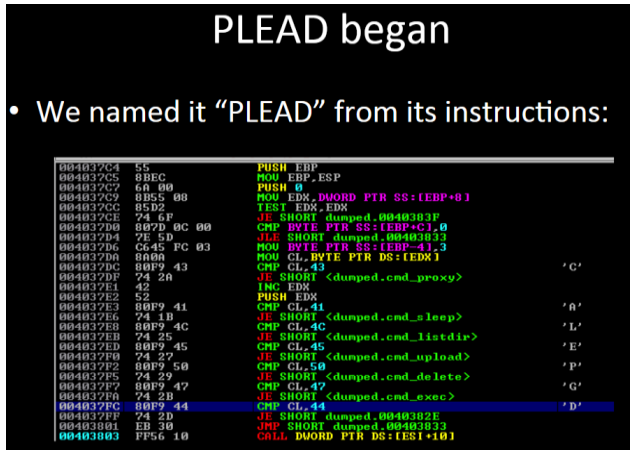
RAT のコマンドとして用意されている関数 sub_10001BB0, sub_10002410, sub_100020F0, sub_10001EB0 それぞれ機能を答えよ。

【満点 (2点 x 4 = 8点)の回答】

- sub_10001BB0: 特定の特殊フォルダ(Recent, Desktop, My Documents, Program Files)の配下に存在するファイル一覧とそれらのファイルサイズや最新の更新日時等，ファイルの詳細情報を取得する
- sub_10002410: C&Cサーバーへ接続し，ファイルをダウンロードする
- sub_100020F0: 指定されたコマンドを実行する
- sub_10001EB0: パスが指定されていなければ，PCに存在するドライブ名一覧とそれらのドライブの種類を取得する．パスが指定されていた場合は指定されたパス配下に存在するファイル一覧とそれらの詳細情報を取得する

```
int result; // eax

if ( !a1 || !a2 )
  return 0;
switch ( 0 )
{
  case 'A':
    result = atol((const char *)(a1 + 1));
    break;
  case 'C':
    result = sub_10001BB0((const char
*)a3);
    break;
  case 'E':
    result = sub_100020F0(a3, (LPCSTR)(a1
+ 1));
    break;
  case 'L':
    result = bc_get_drive_info_(a3,
(LPCSTR)(a1 + 1));
    break;
  case 'P':
    result = sub_10002410(ebp0, edi0,
(LPCSTR)(a1 + 1));
    break;
  default:
    result = 5;
    break;
}
return result;
}
```



トレンドマイクロは、「2H-2013 Targeted Attack Roundup Report（英語情報）」で、台湾での標的型攻撃キャンペーンに関連した複数の攻撃を確認したことを報告しました。

弊社は現在、特に台湾の政府機関や行政機関を標的にした攻撃キャンペーンを監視しています。なお、この標的型攻撃キャンペーンは、関連するバックドア型不正プログラムから実行されるコマンドの文字を取って、弊社では「PLEAD」と名づけています。

全体

3-1.

ここまでの解析結果から，これらの検体が何という名称で呼ばれている検体かを特定せよ。

出典:
https://hitcon.org/2015/CMT/download/day2-f-r0.pdf
https://blog.trendmicro.co.jp/archives/9166

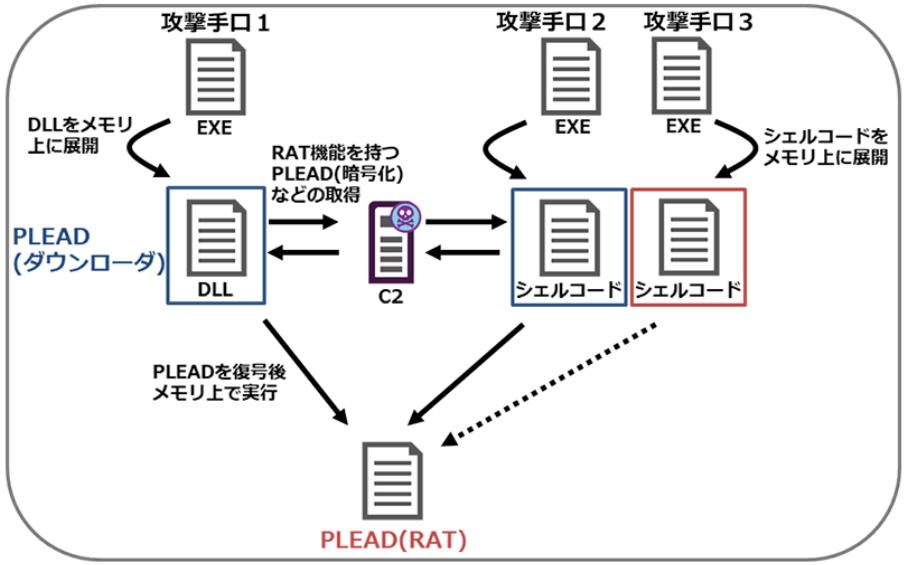
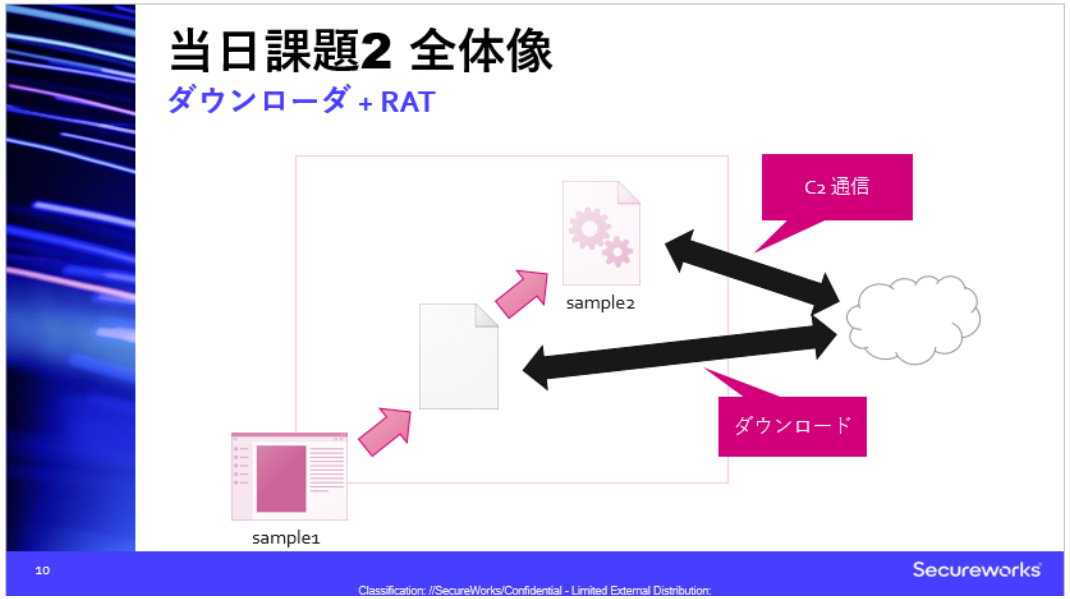


図1 「PLEAD」を展開する攻撃手口



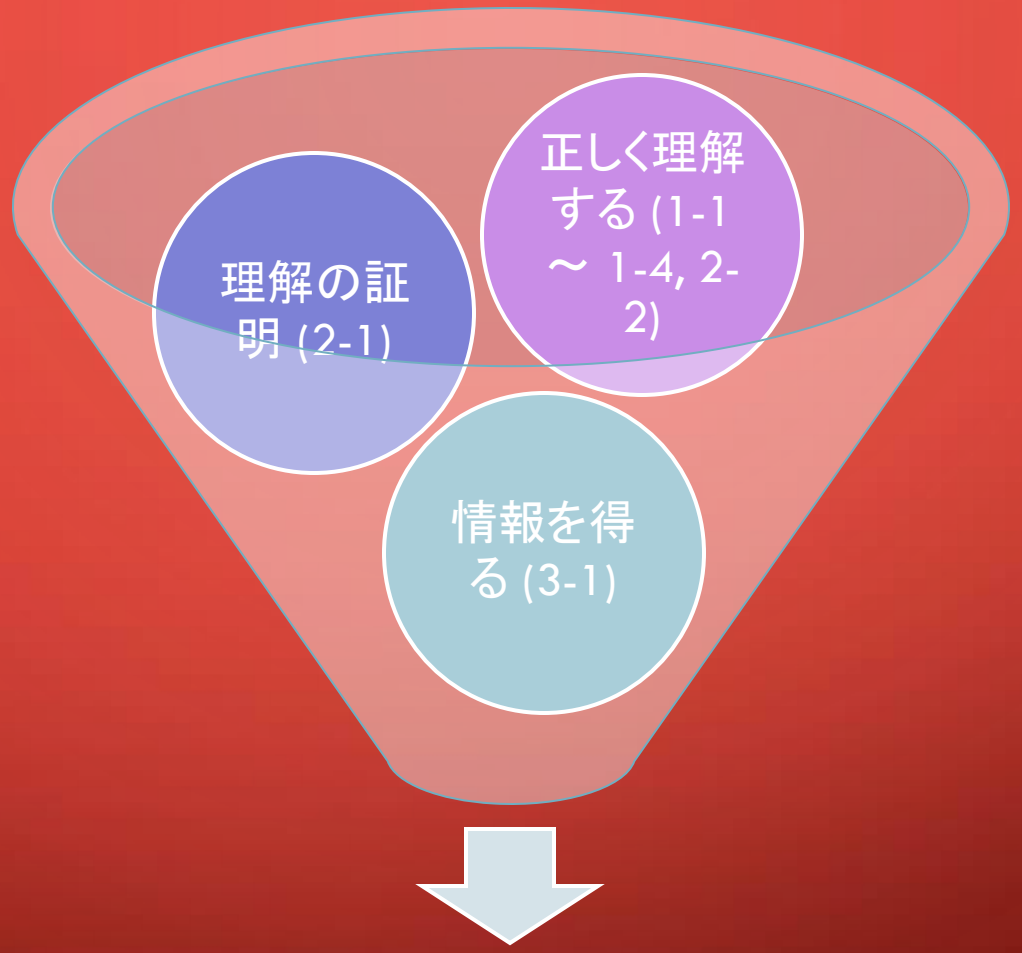
全体

3-1.

ここまでの解析結果から，これらの検体が何という名称で呼ばれている検体かを特定せよ。

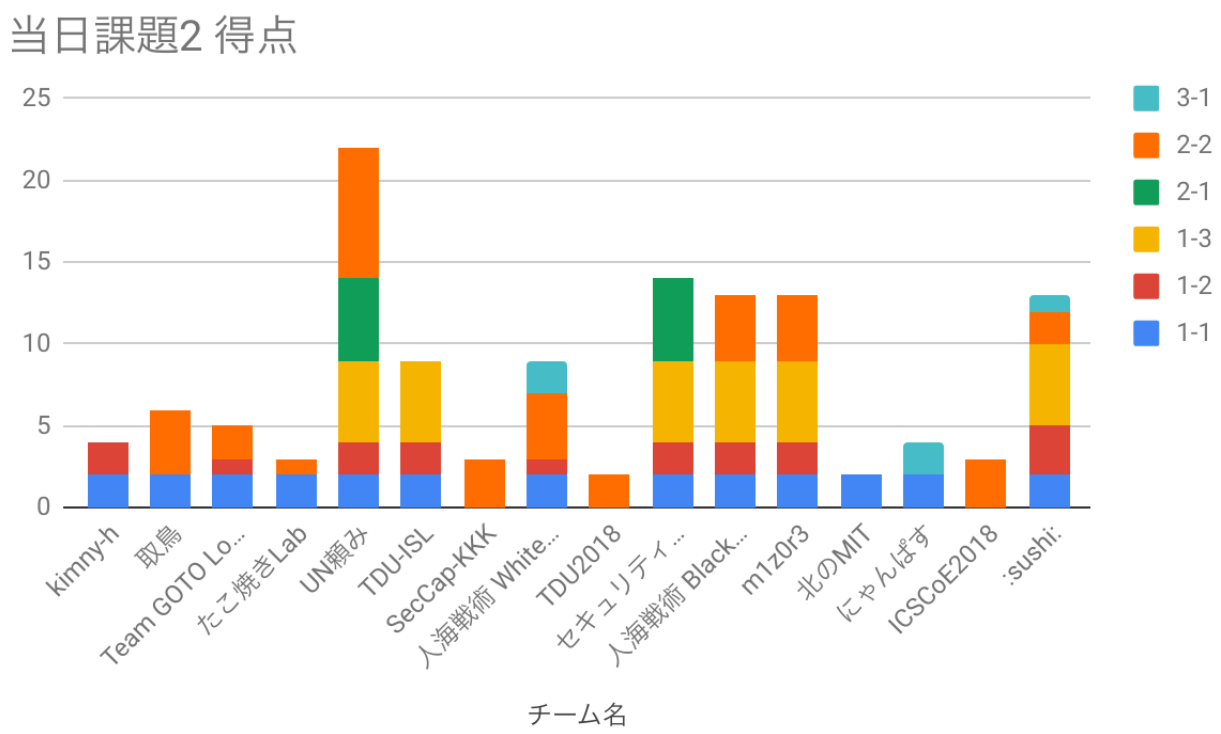
出典:
https://www.lac.co.jp/lacwatch/people/20180425_001625.html

各課題と”変わらぬテーマ”のイメージ



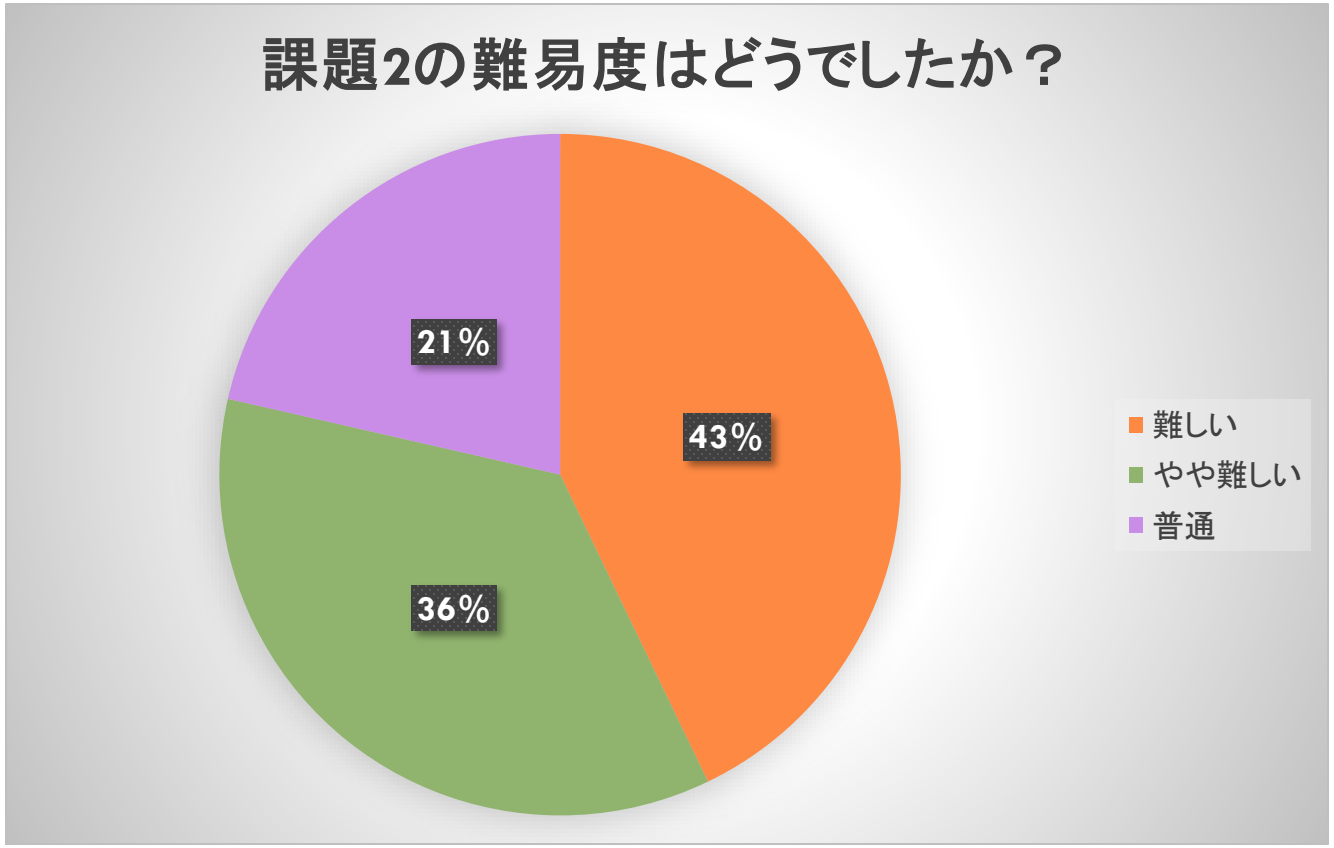
実務体験 (課題2)

課題2 採点結果

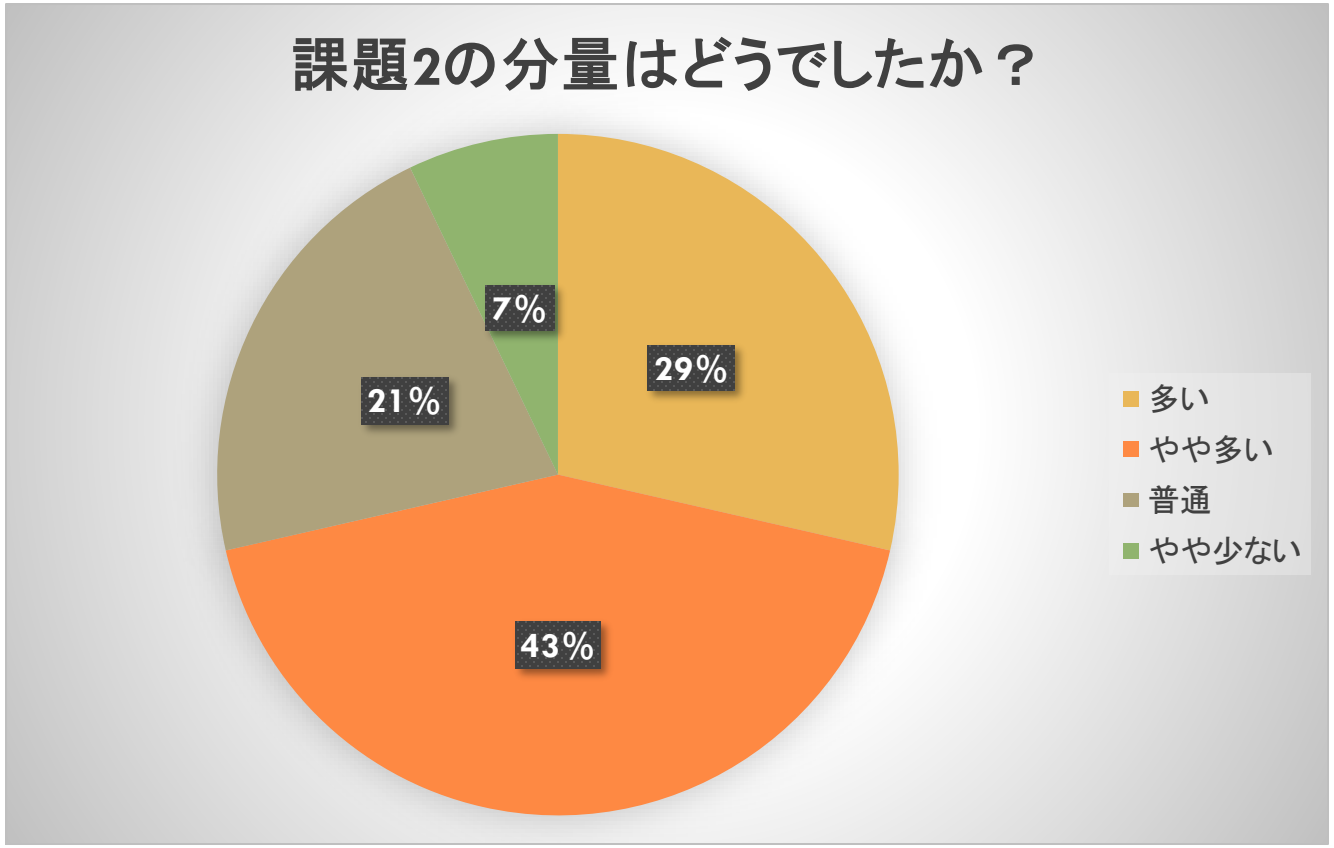

当日課題2 得点
25
20
15
10
5
0
3-1
2-2
2-1
1-3
1-2
1-1
kimny-h
取鳥
Team GOTO Lo...
たこ焼きLab
UN頼み
TDU-ISL
SecCap-KKK
人海戦術 White...
TDU2018
セキュリティ...
人海戦術 Black...
m1z0r3
北のMIT
にゃんぱす
ICSCoE2018
:sushi:
チーム名

MWS CUP 2018
課題2: 今後の課題

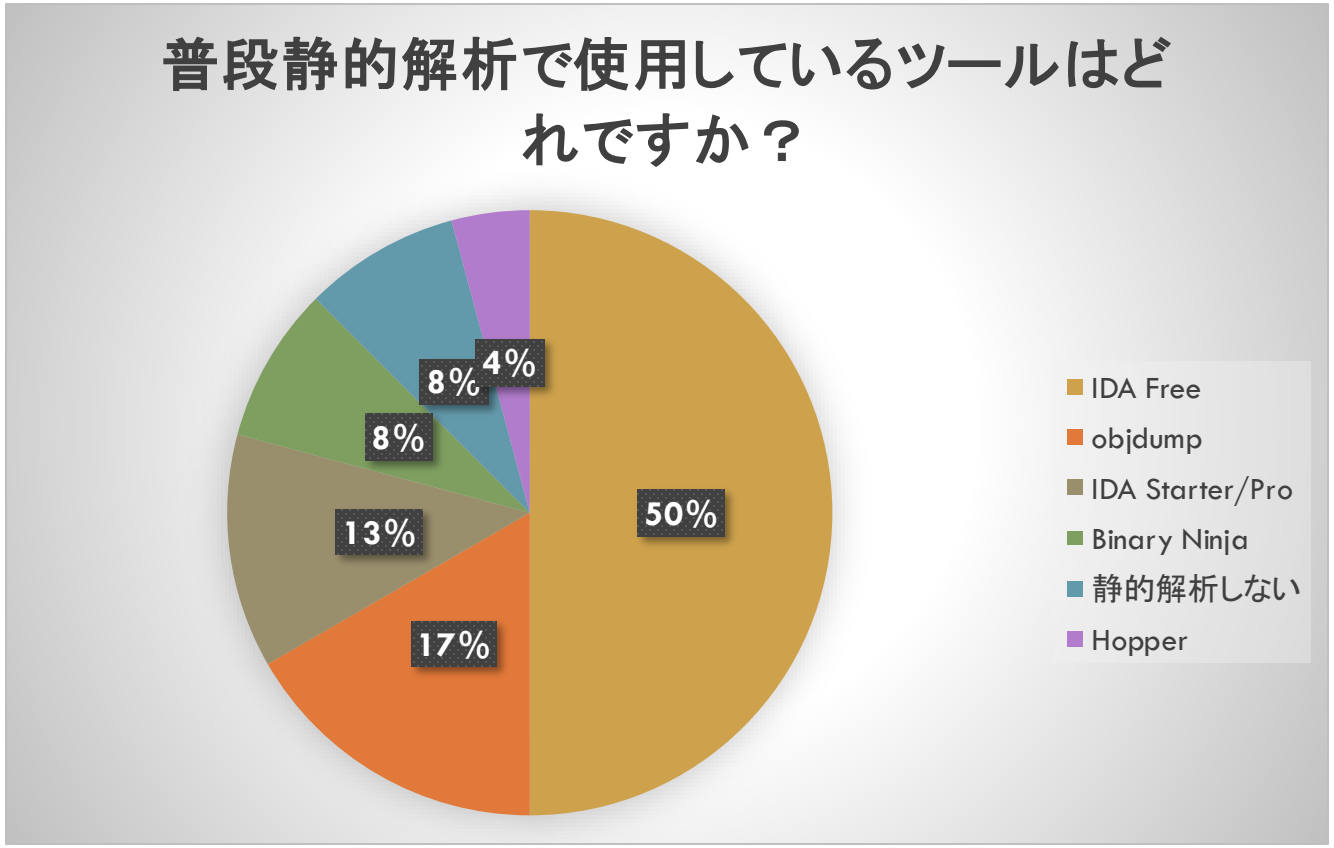
アンケート結果



アンケート結果



アンケート結果


普段静的解析で使用しているツールはどれですか？
50%
17%
13%
8%
8%
4%
IDA Free
objdump
IDA Starter/Pro
Binary Ninja
静的解析しない
Hopper

課題2として取り上げてほしい内容はありますか？

ポジティブ

- ランサムウェア (2件)
- Mirai
- 最新のマルウェア
- Windows以外のマルウェア
- 引き続き静的解析

ネガティブ

- 特になし (5件)
- わかりません (2件)
- “.”

今回の課題2に関して良かった点や悪かった点、意見やコメント等あればお願いします

感想

- 難しかった
- 経験がないと厳しい，レベル未達
- 楽しかった，面白かった
- ステップアップ的な課題が良かった.
- 時間が足りない.
- マルウェアを調べさせるのはいい問題だと思う.

今回の課題2に関して良かった点や悪かった点、意見やコメント等あればお願いします

改善点

- 問題に出てくる固定値の意味がつかめなかった.
- もう少し問題の導線が欲しかった.

→ 次回の問題作成時には，要検討.

問題作成に関する課題

テーマ選定の難しさ

- 自動化などを静的解析で適用することの困難さ
- より実務に近い検体から，規定時間で解答可能なレベルの設問作成

問題の出し方

- 高配点問題の解答が二択となり，点数の偏りを生んでしまった
- 解答内容に求めるレベルを明示できていなかった

作成委員

- 例年，作成委員が海外出張でいない
  → “UN頼み”から1人参加してくれる(らしい)

参加者側に関する課題 / 要望

過去の問題や過去の解答をもとに復習

Write-up 書いてみると勉強になる

予習をしましょう

今年から問題などを公開する方向.
来年は，事前学習よろ～

MWS CUP 2018
課題2: 静的解析

2018/12/20

ynakatsuru[at]secureworks.com

suguru.Ishimaru[at]kaspersky.com

kazumi.ishibuchi.hh[at]hitachi.com