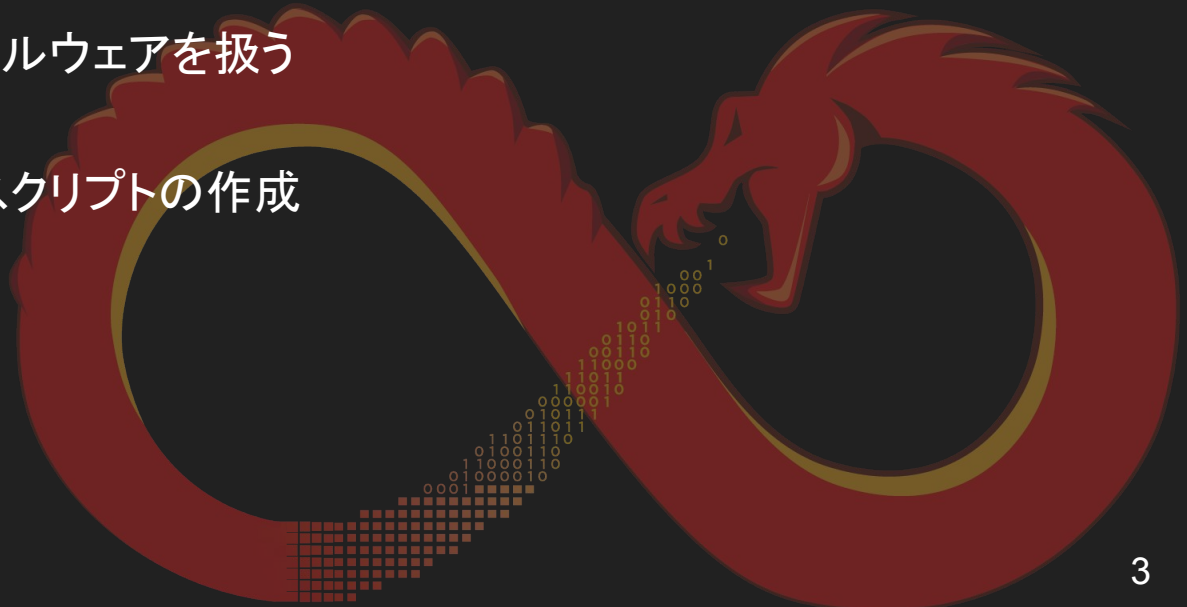
MWS Cup 2022
ポストミーティング

2022の問題担当

- 課題2主担当
  - 株式会社サイバーディフェンス研究所 中島 将太
- 問題作成委員
  - 株式会社 エヌ・エフ・ラボラトリーズ 皆川 諒
  - 株式会社サイバーディフェンス研究所 森 瑞穂
  - 学生、若手募集中！

課題2のテーマ

- マルウェアを正しく理解する
  - 課題を通して解析のポイントを学習する
- 最新情報を得る
  - 最近のin-the-wildなマルウェアを扱う
- 実務に近い作業
  - 静的解析による復号スクリプトの作成



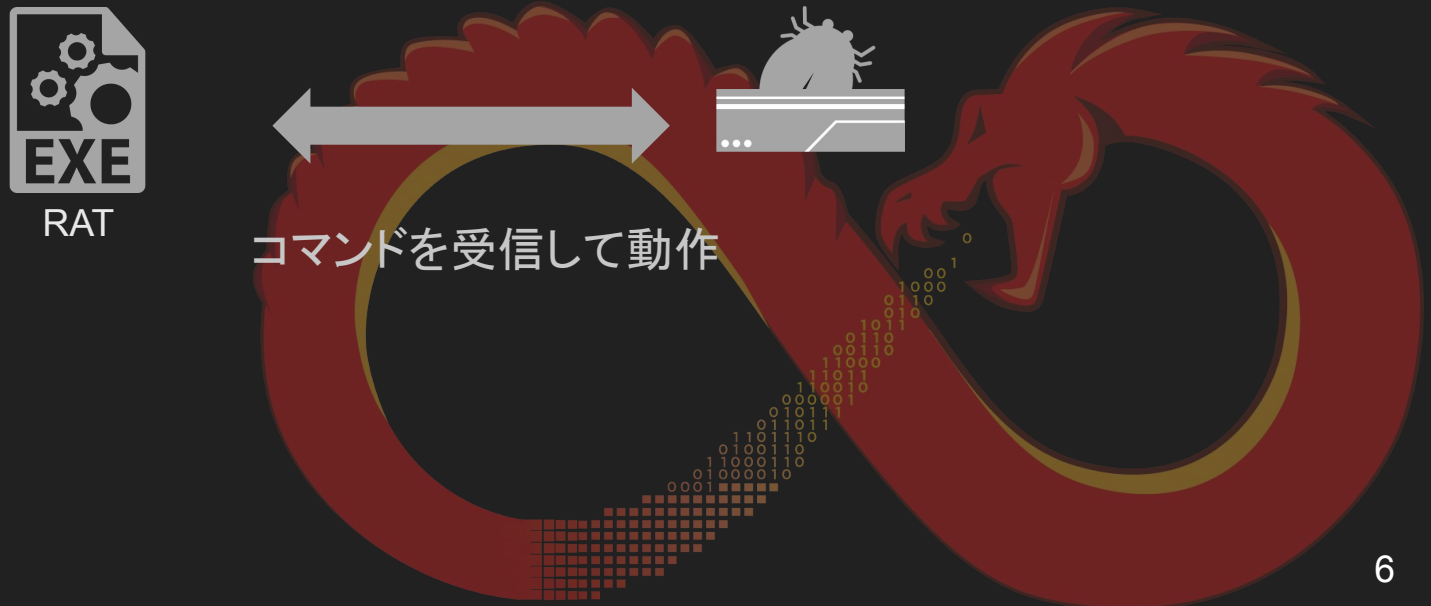
ポイント

- 積極的に変数名や型を変更する
  - 名前を付けて読みやすくしていく
  - デフォルトでは型情報がないことが多い
- デコンパイラを信用しすぎない
  - アセンブリを確認して整合性を確認する
  - 手動で修正する
- 順番に回答する必要はないので解けそうな問題から解く

2022の新しいトピック

初のELFマルウェア!
日本を対象としたAPTでもELFマルウェアが観測されている

マルウェアの動作概要



マルウェアファミリ

- ELF bifrose
  - BlackTechが利用
- 2020年以降Linux環境も狙う

技術分析

RSS

中国のハッカーHUAPIのバックドア型マルウェア「BiFrost」の解析

2020.4.15 | Global Support & Service

Share:

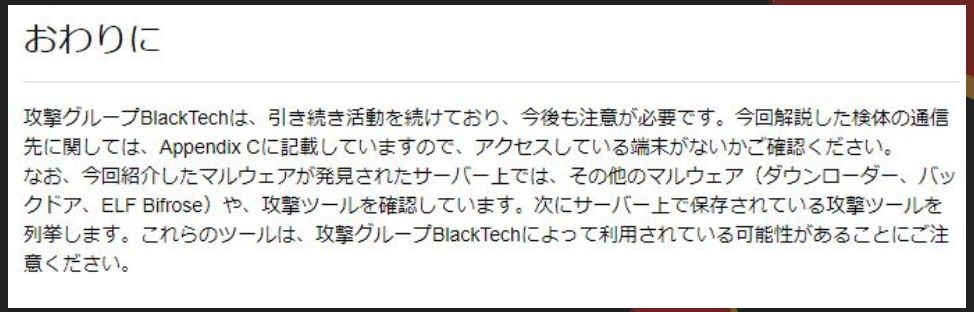
キーワード：HUAPI、PLEAD、GhostCat、CVE-2020-1938、Linux、BiFrost、RC4、RAT

はじめに

最近、TeamT5は台湾のある学術情報ネットワーク図書館のWebサイトでマルウェアが見つかったという情報を得ました。TeamT5の研究員は分析と調査により、同Webサイトのシステムが Tomcat 7.0.73をWebサーバとして使用し、8009番ポートが開放されていることを発見しました。TeamT5の研究員は、WebサイトにGhostcat（CVE-2020-1938）の脆弱性があることを確認しました。詳細は下図のとおりです。

Nmap scan report for [redacted].edu.tw [redacted]

https://teamt5.org/jp/posts/technical-analysis-on-backdoor-bifrost-of-the-Chinese-apt-group-huapi/



おわりに

攻撃グループBlackTechは、引き続き活動を続けており、今後も注意が必要です。今回解説した検体の通信先に関しては、Appendix Cに記載していますので、アクセスしている端末がないかご確認ください。
なお、今回紹介したマルウェアが発見されたサーバー上では、その他のマルウェア（ダウンローダー、バックドア、ELF Bifrose）や、攻撃ツールを確認しています。次にサーバー上で保存されている攻撃ツールを列挙します。これらのツールは、攻撃グループBlackTechによって利用されている可能性があることにご注意ください。

https://blogs.jpcert.or.jp/ja/2021/09/gh0sttimes.html

3.12. ELF_Bifrose

Linux 版の Bifrose マルウェアです。過去の分析記事[14]に記載されている検体と大きく機能は変わっておりませんが、私たちが確認した検体について紹介します。

3.12.1. 特徴

file コマンドや readelf -p .comment コマンドの実行結果は以下の通りです。古い環境でコンパイル・静的リンクされており、攻撃者は環境依存の問題を減らしたいものと考えられます。

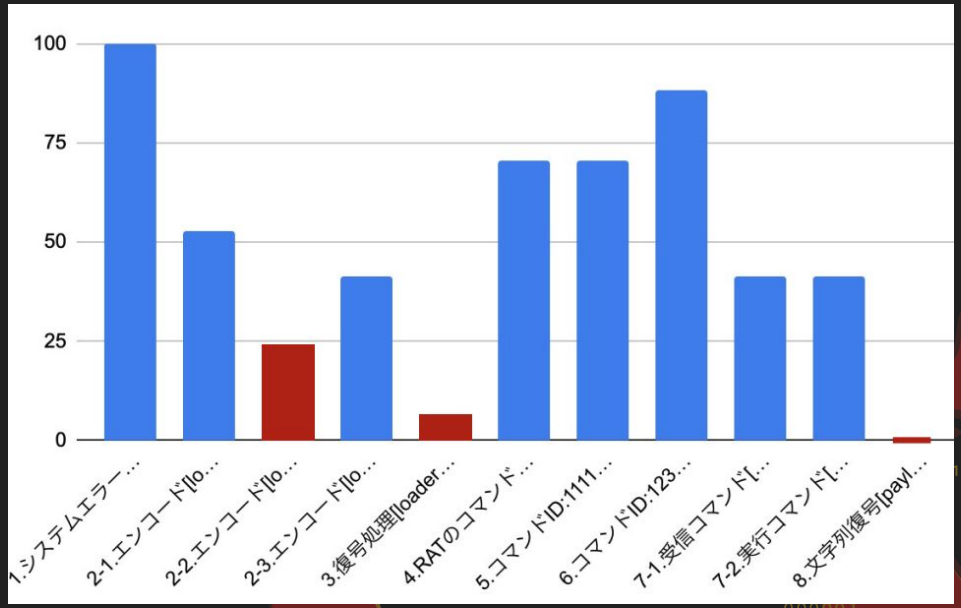
```
$ file a914c729e4816fb49c8b9830694be385460c2cc366bf1ab1410e84295cfa0946
a914c729e4816fb49c8b9830694be385460c2cc366bf1ab1410e84295cfa0946: ELF 32-bit LSB executable, Intel 80386,
 version 1 (SYSV), statically linked, for GNU/Linux 2.6.9, stripped
$ readelf -p .comment a914c729e4816fb49c8b9830694be385460c2cc366bf1ab1410e84295cfa0946

String dump of section '.comment':
  [     1]  GCC: (GNU) 4.1.2 20080704 (Red Hat 4.1.2-44)
  [    2f]  GCC: (GNU) 4.1.2 20080704 (Red Hat 4.1.2-44)
```

図 42 ELF_Bifrose file コマンド実行結果

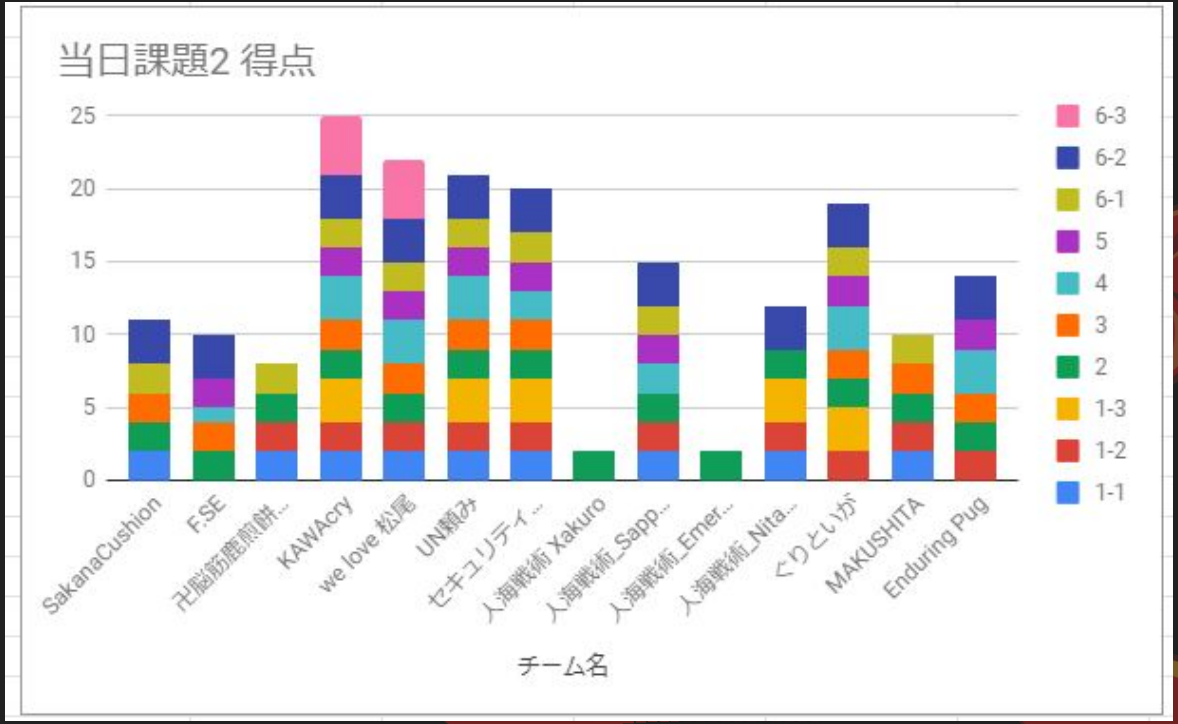
https://jp.security.ntt/resources/BlackTech_2021.pdf

スクリプトの配布



去年は復号問題解けたチーム 0 だったので、
今年は復号に使えるベースのコードを用意しました!!

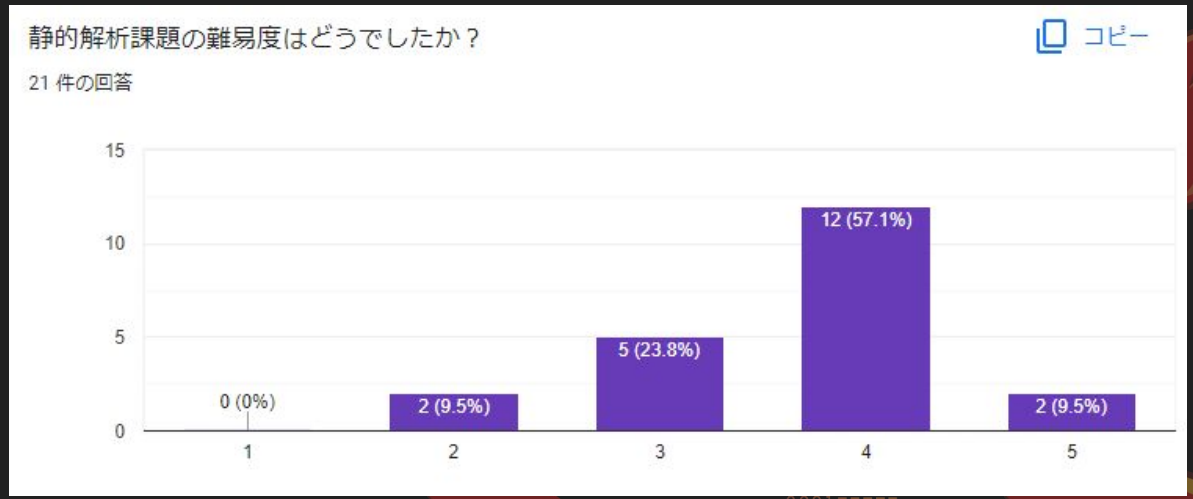
全問正解チーム誕生！


当日課題2 得点
25
20
15
10
5
0
6-3
6-2
6-1
5
4
3
2
1-3
1-2
1-1
SakanaCushion
F:SE
北脳筋鹿煎餅...
KAWAcry
we love 松尾
UN頼み
セキュリティ...
人海戦術 Xakuro
人海戦術_Sapp...
人海戦術_Emer...
人海戦術_Nita...
ぐりといが
MAKUSHITA
Enduring Pug
チーム名

アンケート結果

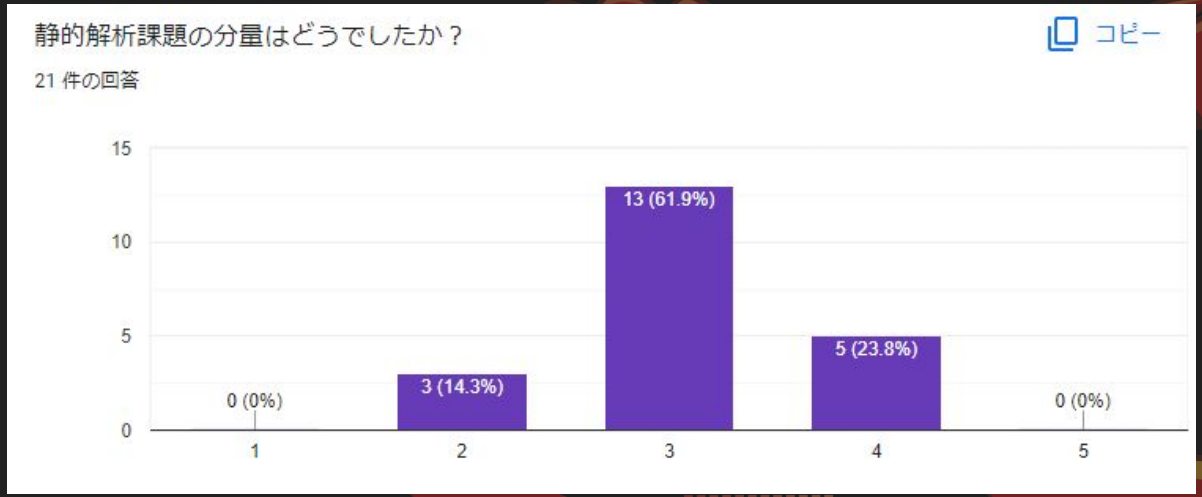
難易度

- 作問時の想定通り



難易度

- 作問時の想定通り
- ちょうどよい分量にできた



静的解析の学習方法

- ghidra実践ガイド
- 過去問題および解説資料
- 学校での勉強会
- 業務でのマルウェア解析（PEファイル）
  - 作問してください

静的解析の学習方法 Q/A

- Ghidraを使った過去問が2年分しかなかったので、もう少し例題がほしいです。
  - IDAでもツールが変わるだけで本質は一緒です！来年度は別のツールになるかも??
- サーバ通信を行うマルウェアの解析はやったことがなかったため、その点は今回の課題で困った
  - 自分で通信するプログラムを書いて、Ghidaで読むと勉強になります！

静的解析として取り上げてほしい内容

- COMやWindowsサービス等のWindowsの機能の悪用みたいな内容とかあると面白いかも。また、Process/DLL Injection等のアンチ解析技術がちょっと入っていても面白いかもです
  - COMは考えたんですが、王道から外れるので除外しました
  - インジェクション技術は触れてもいいかもですね
- 情報窃取内容の特定
  - インフォスティーラーとか？
    - ブラウザとかの情報抜く処理はあまりおもしろくなく悩みどころ
  - RATによる情報窃取は任意コマンド実行経由でおこなわれるので、DFIR課題のログのようなものがないとマルウェア解析ではわからない

意見コメント

- ELFが想定外で、ELFファイルのシステムコール特定の知識がなく苦戦した
  - 毎年同じ問題だと面白みがないので、Windows以外にしてみました
- サンプルスクリプトの配布やヒントが良かった
  - 準備したかいがあった！
- 暗号化の手法を選択する問題については、元の暗号化からあまり追加要素を加えないで欲しかったなと思った
  - 自分たちが暗号を作ってるのではなく、マルウェア開発者が手を加えている！
- 解いている最中に、ビデオや話が発表されると集中力が途切れてしまう
  - 時間の都合で問題説明やヒントを同時に実施してます・・・
- 静的解析、DFIRで組み合わせ、情報共有すると楽に解ける問題があると、チーム内での連携が活発になって面白いかなと思いました
  - 解析しやすいかつコントロール可能なマルウェアがあれば・・・