

実習

- ランサムウェアの感染実習
 - □ ランサムウェアに感染し,被害範囲を確認する
 - 暗号化されたファイルの拡張子は?暗号化される前の拡張子は?
 - 暗号化されたファイルの保存場所(ディレクトリ)は?

■ 事後対応

□ 暗号化されたファイルを復元する

■ 事前対策

 ランサムウェア対策ツールをインストールし、再度ランサムウェアを起動 する

公益社団法人 私立大学情報教育協会

■実習概要	Page 4
sjk-pc たストOS (ファイル共有PC) 実習1 被害範囲を確認をする	sjk-victim CORACS (被害PC) Sytachat Constant Const
∧ 1 祢伎枕をり町しに上で美省を打つ	

PC教室LAN

実習をはじめる前に

実習環境の確認

公益社団法人 私立大学情報教育協会

<text><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item><list-item>

ホストOSログイン後画面 公益社団法人 私立大学情報教育協会

本セッションで使用するファイルの確認(ホストOS)

- A3(VirtualBoxを使用したゲストOS)…①
- パブリック-ショートカット(ゲストOSとファイル共有を行うためのパブリックディレクトリ)…②
 - □ [会議資料]ディレクトリ…②-a
 - □ [機器調達]ディレクトリ…②-b

■ A-3(被害範囲確認用ファイルを保存したディレクトリ)…③



公益社団法人 私立大学情報教育協会



ゲストOSログイン後画面 公益社団法人 私立大学情報教育協会

本セッションで使用するファイルの確認(ゲストOS)

- TeslaCrypt(ランサムウェアを保存している ディレクトリ)…①
 被害範囲確認用ファイル

 A-3.pdf …②-a
 A-3.rtf …②-b
 A-3.txt …②-c

 RansomFree(ランサムウェア対策ツールを 保存してるディレクトリ)…③
 復号ツール
 - □ Ransomware File Decryptor Tool …④-a
 - □ ESET TeslaCrypt Decryptor … ④-b

共有ディレクトリの確認

- ホストOSとゲストOSの共有ディレクトリの中身が同じである ことを確認する
 - ホストOS側:パブリック-ショートカット
 - 「ゲストOS側:[ネットワーク]>[SJK-PC]>[Users]>[パブリック]

2理・ ライブラリに追加・	月有 • 書き込む	新しいフォルダー		II • 🗇	0				
★ お気に入り 参 ダウンロード ■ デスクトップ 副 最近表示した場所	5.55	。 (語 A3 のクローン (家)	第新日時 2017/08/20 14:06 2017/08/20 14:06 行中] - Oracle VM Virt	戦加 ファイル フォル ファイル フォル Jァイル フォル	₩-			- 0	×
■ ライブラリ ■ ドキュメント ■ ビクチャ ■ ビデオ	1)•	イス・ヘルフ ク・S3K-PC・U N・ 新しいフォ	wes 、パブリック ルダー	· · [4]	パプリックの検索		р Р
 シミュージック 2 個の項目 状況: 基 p プロシブ 	(M	Teslacity 92	6気に入り ダウンロード デスクトップ 最近表示した場	名初	*	更新日時 2017/08/20 14:06 2017/08/20 14:06	継頃 ファイル フォル ファイル フォル	94X	
		A 3.pd	5イブラリ ドキュメント 2 個の項目 オ オフ	フラインの状態: オン ラインで利用 利用	ライン 不可				
		😗 🙆	(2)			● A 般 S # 0		€ 14:13 2017/08/ Right Cor	20 n/trol



公益社団法人 私立大学情報教育協会



Page 10

実習1

ランサムウェアに感染し, 被害範囲を確認する

公益社団法人 私立大学情報教育協会

Page 12

1-1 感染前のファイルの状態の調査

- ホストOS及びゲストOSの感染前の各種ファイルの状態を調 査する
 - □ ファイルの拡張子の確認
 - □ ファイルの更新日時の確認
 - □ ファイルが閲覧可能か確認(.txt, .rtf, .docのみ)
- ホストOS側の調査
 - □ 調査対象ディレクトリ
 - 共有ディレクトリ(パブリック-ショートカット)
 - [A-3]ディレクトリ
- ゲストOS側の調査
 - □ 調査対象ディレクトリ
 - 共有ディレクトリ([ネットワーク]>[SJK-PC]>[Users]>[パブリック])
 - [デスクトップ]ディレクトリ

1-2 ランサムウェアの起動

ゲストOS上でTeslaCrypt.exeを起動する

□ [デスクトップ]>[TeslaCrypt]>[TeslaCrypt.exe]をクリック



□ [ユーザアカウント制御]ウインドウが表示されたら[いいえ]を選択

公益社団法人 私立大学情報教育協会



1-4 被害範囲の確認

- ホストOS及びゲストOSの感染後の各種ファイルの状態を調査し、被害範囲を調査する
 - □ ファイルの拡張子の確認
 - □ ファイルの更新日時の確認
 - □ ファイルが閲覧可能か確認
 - [ファイルが開けません]ウインドウが表示された場合は, [インスト ールされたプログラムの一覧からプログラムを選択する(S)]を選 択し, [ワードパッド]を選択する

Windows このファイルを開けません:	
ファイル·学科共通機器調達仕様書.docx.ttt	Microsoft Corporation
このファイルを開くには、そのためのプログラムが必要です。インターネットで自動的にプログラムを検	Windows Media Player Microsoft Corporation
糸9のパくよどはコノビューターと1ノストールで1ルとノロクノムの一見れの千動に進かしていたでい。	Kersott Corporation Alersott Corporation
動作を選択してください。	Recreation
◎ Web サービスを使用して正しいプログラムを探す(W)	
◎ インストールされたプログラムの一覧からプログラムを選択する(S)	このファイルの種類の見明の入力(型)
OK キャンセル	この種類のファイルを開たと考え、確認したプログラムないっち(ぞXA) 参照(E).
	使用するプログラムが一覧やエンピューターにない場合は、速切なプログラムをWebで探すことができます。
	OK 年92世み

公益社団法人 私立大学情報教育協会



1-4 被害範囲の確認

- ゲストOS側の調査
 - □ 以下のディレクトリの中身が暗号化されているか確認
 - 共有ディレクトリ
 - [デスクトップ]ディレクトリ
 - [スタートアップ]ディレクトリ
 - [TeslaCrypt]ディレクトリ





実習2

暗号化されたファイルを復元する

公益社団法人 私立大学情報教育協会



2-2 復号されたファイルを確認する

 Ransomware File Decryptor Toolによって複合されたファイ ル数とファイルを確認する

	0					
ごみ箱	RansomwareFile Ho	owto_Restor		🥏 💀 🛛 ランサムウェア復号ツール		×
TeslaCrypt	Decryptor 1.0.1667 MUI ESETTeslaCryp	A-3.pdf	復 号 さ	ランサムウェア ランサムウェアロック	' 復号ツール き化されたファイルを復号します	
A-3.pdf.ttt	how_recover	A-3	れたファ	復号完了 実行時間: 00:02:10		
A-3.ntfittt	how_recover	A-3	」 ル	暗号化されたファイル数:25 復号されたファイル数:256	i6 夏号されたファイルを確認する	
				終了		
A-SIOXLILL	HOWIO_RESIDE			トレンドマイクロサポートサイト	<u> 2ィードバック</u>	0
RansomFree	Howto_Restor				この Windows のコピー(a	Windows 7 ビルド 7601 証規品ではありません
3		0		● A 般 S	🥩 🖲 COPS 🛱 🔺 💦 🛱 👬 🕻	(*) 15:10 2017/08/20



2-4 不要なファイルの削除

■ 暗号化されたファイルや脅迫文ファイルを削除する



公益社団法人 私立大学情報教育協会



2-6 まとめ

- 事後対応
 - □ 復元ツールを試す
 - TeslaCryptのようにマスターキーが公開されているものは復元できることもある
 - しかし、復元できない場合もある

■ 事前対策

- □ バックアップを取る
 - 定期的にバックアップを取る
 - バックアップ用デバイスはバックアップ時のみPCと接続させる
 USBメモリ,外付けHDD,ネットワークドライブ,クラウド上のストレージ等
 - バックアップ用デバイスは複数用意する
 - 定期的にバックアップから復元できることを確認する
- □ ランサムウェア対策ツールを利用する

公益社団法人 私立大学情報教育協会

Page 26

実習3

ランサムウェア対策ツールをインスト ールし, 再度ランサムウェアを起動 する

3-1 ランサムウェア対策ツールをインストールする

- ゲストOSにCybereasonRansomFreeをインストールする
 - デスクトップ画面にある[RansomFree]ディレクトリをクリック
 - [CybereasonRansomFree]を起動する
 - [Next]をクリックする
 - [I accept the terms in the License Agreement]をチェックし、[Next]をクリックする
 - [Install]をクリックする
 - [ユーザアカウント制御]ウインドウが表示されたら, [はい]をクリックする
 - インストールが完了したら[Finish]をクリックする



公益社団法人 私立大学情報教育協会



3-2 ランサムウェアを起動する

- TeslaCryptを起動し、CybereasonRansomFreeによって TeslaCryptが実行されないことを確認する
 - □ [RansomFree]ディレクトリ内の[TeslaCrypt.exe]ファイルをクリック
 - CybereasonRansomFreeが起動したら、[View affected files]をクリックし、暗号化された可能性のあるファイルを確認
 - □ [Yes]を選択を選択し, 暗号化を行うプロセスを停止及び除去





3-3 暗号化されていないことを確認する

- Ransomware File Decryptor Toolを使用し、暗号化されたファイ ルがないことを確認する
 - □ [Ransomware File Decryptor Tool]をクリック
 - [同意する]を選択する
 - [1. ランサムウェア名を選択してください]で, [TeslaCrypt(V3,V4)]を選択する
 - [2. 複合対象のファイルまたはフォルダを選択してください]で, [デスクトップ]を選択する
 - □ 復号が完了したら, 暗号化されたファイル数とファイルを確認する

ØIREND :	ランサムウェア復号ツール	-	. ×
ſ	ランサムウェア復号 ランサムウェアによって暗号(しされた)	ツール ファイルを復号します	
	復号完了 実行時間: 00:02:23 暗号化されたファイル数: 0		
トレンドマイクロサ	復号されたファイル数:0 終了 <u>ポートサイト</u>	<u>74-15/502</u>	0

公益社団法人 私立大学情報教育協会

 Page 30
 3-4 まとめ
 事前対策
 ランサムウェア対策ツールをあらかじめインストールしておくことで、ラ ンサムウェア被害に気づく機会を増やすとともに、暗号化を防止する
 ただし、暗号化された後に検出する場合もあるため、確実に暗号化を 防止できるわけではない
 2-6で紹介したバックアップによる事前対策や他のセキュリティソフト と組み合わせることが重要