# A-2「標的型攻撃を受けているらしいとの連絡があった時の調査と対応の演習」

### 実習環境について

- 攻撃側 PC (attacker-pc) と感染側 PC (sjk-pc) の2台の PC を使用します。
- 攻撃側 PC (attacker-pc) から感染側 PC (sjk-pc) 操作してみましょう。



### <u>実習の進め方</u>

【実習1】初期潜入

- ・感染側 PC を RAT に感染させましょう。
- ・攻撃側 PC から感染側 PC をリモート操作しましょう。

#### 【実習2】基盤構築

・攻撃側 PC からのリモート操作で、感染側 PC に内部調査ツール (nmap) をインストールしましょう。

### 【実習3】内部侵入・調査

・攻撃側 PC からのリモート操作で nmap を実行し、感染側 PC の内部ネットワークの調査を実施しましょう。

### 【実習4】撤収

--・攻撃側 PC からのリモート操作で、感染側 PC で動いている RAT を停止しましょう。



## 【実習1】初期潜入

#### 攻撃側 PC 操作

### 1. RAT コントローラーの起動

攻撃側 PC のデスクトップにある "Bozok 1.4"を開き、中にある "Client.exe"をダブルクリックして起動 します。"Bozok 1.4 – 0 Online"のウィンドが開くが、何も表示されないことを確認します。

| Bozok 1.4 | <ul> <li>登理 ● ライ</li> <li>登理 ● ライ</li> <li>☆ お気に入り</li> <li>ダウンロー</li> <li>デスクトッ</li> <li>図 最近表示し</li> </ul> | Bozok 1.4<br>ブラリに追加 マ ま<br>名前<br>・ド ブ O Client<br>ブ Dign<br>た場所<br>を Setting | 持▼ 書き込む | 0<br>20<br>20 | 新日時<br>15/07/20 15:10<br>15/07/20 15:10<br>16/08/05 7:01 | <b>住口</b><br>理類<br>アプリケーション<br>アプリケーショ…<br>構成設定 | サイズ<br>2,830 KB<br>267 KB<br>1 KB | ×<br>~<br>@ |
|-----------|--|--|---------|---------------|--|---|-----------------------------------|-------------|
|           |  | P Username   | Creven  | Ver Pugh      | Cam Active Vil   | ndor  |                                   |             |

#### 感染側 PC 操作

2. 感染側 PC のデスクトップにあるコマンドプロンプトのショートカットを使ってコマンドプロンプトを開き ます。コマンドプロンプトの画面が表示されたら、"ipconfig"コマンドを使って感染側 PC のネットワー ク設定を確認しましょう。



### ■ 演習1 感染側 PC のネットワーク設定を記録しましょう。(ipconfig コマンドを使用)

| IPアドレス      |  |
|-------------|--|
| サブネットマスク    |  |
| デフォルトゲートウェイ |  |

3. RAT に感染

感染側 PC のデスクトップにある"不正アクセスログ.zip"を解凍します。解凍されたフォルダにある"logs" フォルダを開いて、**"不正アクセス調査ログ.xlsx"**をダブルクリックします。空の Excel が開くことを確認 します。



(補足)

右の様に "Microsoft Office ライセンス認証ウィザード" が表示された場合は、"閉じる(C)" を押してして終了して ください。

| Microsoft Office ライセンス認証ウィザード  | <b>.</b>                |
|--|-------------------------|
| Microsoft Office Professional Plus 2016<br>ライセンス認証ウィザード  | 🚺 Office                |
| この Microsoft Office は、ライセンス認識されていません。<br>3 日以内にライセンス認証を実行する必要があります。目動ライセンス認証を実行できるように、企<br>いることを確認してください。詳細については、システム管理者に問い合わせてください。 | 業のネットワークに接続されて          |
| - <u>この</u> Office 製品のライセンス認証方法の詳細   |                         |
|  |                         |
| (  | プロダクト キーの変更( <u>K</u> ) |
|  |                         |
| エラー コード: 0x4004F00C  | プライバシーに関する声明            |
| ハレプ(出)   | 閉じる( <u>C</u> )         |

#### 攻撃側 PC 操作

- 4. RAT コントローラーの感染側 PC の補足
  - RAT コントローラーに感染側 PC の情報が表示されます。演習 1 で記録した IP アドレスが表示されている ことを確認しましょう。



感染側 PC を補足することができたら、攻撃側 PC から様々な操作を RAT コントローラー経由で実行できます。RAT コントローラーの設定をした後、4 つの攻撃操作を行いましょう。

5. RAT コントローラーの設定

感染側 PC を選択し、右クリックで表示されるメニューから "Upload Extension" を選択します。再度右ク リックでメニューを表示すると、内容が増えていることがわかります。

| er       192,158,0,2       sik       SJK-PC         Image: Signed | IP   | Username    | Computername |
|--|--|-------------|--------------|
| Open Download Folder   | 192.168.0.2<br>File Explorer<br>Registry Editor<br>Processmanager<br>Windows<br>Services<br>Remote Shell<br>Upload Extensio<br>Server<br>Open Download | n<br>Folder | SJK-PC       |

#### ≪攻撃操作1≫ 感染側 PC のデスクトップ画面をモニターする

1. Screenviewer の起動 感染側 PC を選択し、右クリックメニューから "Screenviewer" を選択し起動します。[Start] を押すこと で、感染側 PC のモニターが開始されます。モニターを終了する場合は [Stop] を押します。

|            | IP  | Username  | Computername      | OS            | Charth ( | Cattion | -                                     |  |   |                         |
|------------|---|-----------|-------------------|---------------|----------|---------|---------------------------------------|--|---|-------------------------|
| TestServer | Eile Explorer         Registry Edita         Processmana         Windows         Services         Remote Shell         Screenviewer         Kevlagger | or Screen | swer<br>viewer を選 | windows<br>計択 | Start    | Settin  | nviewer - sjk@SJ                      | <-PC   |   |                         |
|            | Password Red  | covery    |                   |               |          | II Stop | Settings 19.1                         | 7 KB   | •]4; ] (gatesi<br>4-  | Familie HGB<br>F - CL P |
|            |   | ad Folder |                   |               |          |         | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | Control     Contro     Control     Control     Control     Control     Control     C | вой         ча           законства         (4) 25-24           законства         (4) 25-24           законства         (5) 25-15-25 | DCL<br>IVIB<br>IVI      |

■ 演習2 感染側 PC の画面をモニターできましたか?

| 画面モニター可否 | Ъ | • | 否 |
|----------|---|---|---|
|          | 1 |   |   |

### ≪攻撃操作2≫ 感染側 PC のネットワーク情報、及びシステム情報を窃取する

1. Remote Shell の起動

感染側 PC を選択し、右クリックメニューから "Remote Shell"を選択し起動します。[Activate] にチェッ クを入れることで、感染側 PC のコマンドプロンプトを起動した状態と同じになります。コマンド入力欄に コマンドを入力し、[Send] を押すことで画面に結果が返ってきます。

| • Bozok 1.4        | - 1 onlir | ne  |                      |                                    |               | • Re    | mote Shell - sj | k@SJK-PC  |  | _              |   |  |
|--------------------|-----------|---|----------------------|------------------------------------|---------------|---------|-----------------|---|--|----------------|---|--|
| ID                 | IP        | )   | Username             | Computername                       | OS            | Shell d | eactivated      |   |  |                | ~ |  |
| ID<br>• TestServer |           | Eile Explorer<br>Registry Editor<br>Processmanager<br>Windows<br>Services<br>Remote Shell<br>Sgreenviewer<br>Keylogger<br>Password Recove | Username<br>Remote S | Computername<br>SHEPC<br>Shell を選护 | os<br>Mindows | Shel d  | eactivated      | Remote Shell Shel started Microsoft Windows [ Copyright (c) 2009 M C: VUsersVisjki/Desktr | - sjk@SJK-PC<br>Version 6.1.7601]<br>Krosoft Corporation. All rij<br>py¥註她写典¥註她写典> | yhts reserved. |   |  |
|                    |           | <u>O</u> pen Download F   | Folder               |                                    |               | 5       |                 |   | ΥΥL  | 下八刀棟           |   |  |

Activate ipconfig /a

平成 28 年度 大学情報セキュリティ研究講習会 A-2 「標的型攻撃を受けているらしいとの連絡があった時の調査と対応の演習」実習資料

### ■ 演習3 感染側 PC のネットワーク情報を調べましょう。(ipconfig コマンドを使用)

| IPアドレス      |  |
|-------------|--|
| サブネットマスク    |  |
| デフォルトゲートウェイ |  |

### ■ 演習4 感染側 PC のシステム情報を調べましょう。(systeminfo コマンドを使用)

| ホスト名       |  |
|------------|--|
| OS 名       |  |
| 登録されている所有者 |  |
| システムモデル    |  |

### ≪攻撃操作3≫ 感染側 PC に対してファイルのダウンロード(窃取)を実行してみる

1. File Explorer の起動

感染側 PC を選択し、右クリックメニューから "File Explorer"を選択し起動します。対象ドライブから "C:¥[FIXED]"を選択することで、感染側 PC の C ドライブの情報が表示されます。

| • Bozok 1.4 - | 1 online   |          |              |         | <ul> <li>Filemanager - sjk@SJK-PC</li> </ul>                      |   |
|---------------|--|----------|--------------|---------|---|---|
| ID            | IP   | Username | Computername | OS      | Files Transfer  |   |
| TestServer    | 🛃 🛛 <u>F</u> ile Explorer  |          | SJK-PC       | Windows |   | Size  |
|               | Registry Edit         Processma         Windows         Services         Remote Shell         Screenviewer         Keylogger         Password Rec         Server         Open Download | overy    | を選択          |         | D:# (CD-ROM) 操作対象ト 伊ィック・アン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン | Size<br>ジライブの選択<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory<br>Directory |
|               |  |          |              |         | Files listed!   |   |

#### 2. 感染側 PC 内のファイル窃取

感染側 PC の C ドライブ情報が表示されたら、後はフォルダをクリックしていけばそれぞれの中を確認する ことができます。ここでは [Users]-[sjk]-[Desktop] フォルダ内にある" 学生情報.xlsx"ファイルを攻撃 側 PC にダウンロードします。

対象のファイルを選択し、右クリックメニューから [Download File] を選択するだけで、攻撃側 PC のデス クトップにある [Bozok 1.4]-[Users]-[SJK-PC] 内にファイルがダウンロードされます。

| <ul> <li>Filemanager - sjk@SJK-PC</li> </ul> |                         |              |  |                   |                        |                  |                 |              | × |
|--|-------------------------|--------------|--|-------------------|------------------------|------------------|-----------------|--------------|---|
| 🧮 Files 🍶 Transfer                           |                         |              | C:¥Users¥sjk-  | -attack¥Desktop¥B | lozok 1.4¥Users¥SJK-PC | - <del>-</del> - | SJK-PCの検索       |              | P |
| C:¥Users¥sjk¥Desktop¥                        |                         | 整理 ▼         | ライブラリに追加   | □ ▼ 共有 ▼          | 書き込む 新しいファ             | †ルダー             | l               | = <b>-</b> ( | 0 |
| Name   | Size                    | 🗙 お気         | に入り  | 名前                | ^                      | 更新日時             | 種類              | サイズ          |   |
| - <u>-</u>                                   | Directory               | <b>1</b> 5   | ウンロード  | Screen            | _                      | 2016/08/19 9:57  | ファイル フォル        |              |   |
| del  | Directory               | 📃 7          | スクトップ  | 🖉 学生情報            |                        | 2016/08/19 10:09 | Microsoft Excel | 30 KB        |   |
| sjk-pic                                      | Directory               | 9 <u>.</u> f | 近表示した場所  |                   |                        |                  |                 |              |   |
|  | Directory               |              |  |                   |                        |                  |                 |              |   |
| Command Prompt, Ink                          | 1.25 KB                 | 3-           | ブラリ  |                   |                        |                  |                 |              |   |
| ATT アクセスログ zin                               | 20.94 KB                | B F          | キュメント  |                   |                        |                  |                 |              |   |
| 「学生植報.xix                                    | ad File<br>File<br>Ider |              | クチャ<br>デオ<br>ュージック<br>ビューター<br>ーカルディスク<br>トワーク<br>2 個の項目 | ファイ               | 'ルのダウン                 | - ロー ドカ          | <b>》完了</b>      |              |   |
| Files listed!                                |                         |              |  |                   |                        |                  |                 |              |   |

### ■ 演習5 ファイル窃取は成功しましたか?

| ファイル窃取 | 成功 | • | 失敗 |
|--------|----|---|----|
|--------|----|---|----|

### ■ 演習6 窃取したファイルにはどんな情報がありましたか?

| 窃取した情報 |  |
|--------|--|
|        |  |
|        |  |
|        |  |

A-2 「標的型攻撃を受けているらしいとの連絡があった時の調査と対応の演習」実習資料

### ≪攻撃操作4≫ 感染側 PC のキー入力情報を窃取する

1. Keylogger の起動

感染側 PC を選択し、右クリックメニューから"Keylogger"を選択し起動します。[Get Keylog] を押すこ とで、RAT 起動後に感染側 PC で入力されたキー情報が表示されます。



#### ■ 演習7 キー入力情報の窃取は成功しましたか?

| キー入力情報窃取 | 成功 | • | 失敗 |
|----------|----|---|----|
|----------|----|---|----|

### 【実習2】基盤構築

攻撃側 PC 操作

 感染側 PC のコマンド確認 感染側 PC を選択し、右クリックメニューから "Remote Shell"を選択し起動します。[Activate] にチェッ クを入れた後コマンド入力欄に "nmap" と入力し、[Send] を押します。

#### ■ 演習8 感染側 PC に nmap コマンドはありましたか?

| nmap の有無 | 有 | • | 無 |
|----------|---|---|---|
|----------|---|---|---|

2. 感染側 PC への nmap インストールファイルの混入

感染側 PC に nmap インストールファイルを混入させます。攻撃側 PC のデスクトップ ([Users]-[sjk]-[Desktop]) にある "nmap-7.12-setup.exe "を感染側 PC の C ドライブ直下 に送り込みま す。"File Explorer"で感染側 PC の C ドライブ直下に移動します。画面中ファイル名が表示されていない 場所で右クリックメニューから [Upload File] を選択し、感染側 PC に送り込みたいファイル ("nmap-7.12-setup.exe ") を選択します。

平成28年度 大学情報セキュリティ研究講習会

A-2 「標的型攻撃を受けているらしいとの連絡があった時の調査と対応の演習」実習資料

| Filemanager - sik@SJ   | K-PC             |                   |
|------------------------|------------------|-------------------|
| Files Transfer         |                  |                   |
|                        | 4                | ]                 |
| C:# [FIXED]            | •                |                   |
| Name                   |                  | Size              |
| sRecycle.Bin           |                  | Directory         |
| Documents and Settings |                  | Directory         |
| Intel                  |                  | Directory         |
| MSOCache               |                  | Directory         |
| PerfLogs               |                  | Directory         |
| Program Files          |                  | Directory         |
| Progra                 |                  |                   |
| Recov Unload           | d File を選択       |                   |
| Syster                 |                  |                   |
| Users                  |                  |                   |
| Windows                |                  | Directory         |
| hiberfil.sys           |                  | -1235222528 bytes |
| pagefile.sys           |                  | -215306240 bytes  |
|                        |                  |                   |
|                        | C Refresh        |                   |
|                        | A Developed City |                   |
|                        |                  |                   |
|                        | 🔮 Upload File    |                   |
| Files listed!          | New Folder       |                   |
|                        | Execute          |                   |

 感染側 PC への nmap インストール 感染側 PC を選択し、右クリックメニューから "Remote Shell"を選択し起動します。[Activate] にチェッ クを入れた後、初めに感染側 PC の C ドライブ直下に移動するために、コマンド入力欄に " cd c:¥ "と 入力し、[Send] を押します。

次に"nmap-7.12-setup.exe"が感染側 PC の C ドライブ直下に混入されたことを確認するために、コマン ド入力欄に"**dir**"と入力し、[Send]を押します。"nmap-7.12-setup.exe"があることを確認します。

最後にコマンド入力欄に"**nmap-7.12-setup.exe** /**S**"と入力し、[Send] を押します。

4. 感染側 PC のコマンド確認

"Remote Shell"のコマンド入力欄に "nmap" と入力し、[Send] を押します。

#### ■ 演習9 感染側 PC に nmap コマンドはありましたか?

| nmap の有無 | 有 |  | 無 |
|----------|---|--|---|
|----------|---|--|---|

配布資料訂正

## 【実習3】内部侵入・調査

#### 攻撃側 PC 操作

1. 感染側 PC の内部ネットワーク調査実行

"Remote Shell" のコマンド入力欄に "nmap -F -O -PO 192.168.1.0/24 > nmap.txt "と入 力し、[Send] を押します。(※この調査には時間が掛かります。)

2. 調査結果 (nmap.txt) のダウンロード

感染側 PC を選択し、右クリックメニューから"File Explorer"を選択し起動します。対象ドライブから "C:¥[FIXED]"を選択して感染側 PC の C ドライブの情報が表示し、目的のファイル(nmap.txt)を攻撃 側 PC にダウンロードします。

| sjk@SJK-PC            |                   |   |                 |
|-----------------------|-------------------|---|-----------------|
| Transfer              |                   | Image: Simple state         Image: Simple state         Image: Simple state         Simple state | の検索             |
| [FIXED] VC:¥          |                   | 整理 ▼ ライブラリに追加 ▼ 共有 ▼ 書き込む 新しいフォルダー  | 8≡ - □ (        |
|                       | Size              | ☆ お気に入り<br>名前 更新日時 種類<br>2016/08/19 9:57 ファイ.   | サイズ             |
| Recycle.Bin           | Directory         | ■ デスクトップ 📋 nmap 2016/08/20 10:03 テキス  | トドキュ 4 KB       |
| ocuments and Settings | Directory         | 3 最近表示した場所 4 学生信報 2016/08/19 10:09 Microse 2016/08/19 10:09 Microse   | oft Excel 30 KB |
| Intel                 | Directory         |   |                 |
| MSOCache              | Directory         | 🥫 ライブラリ   |                 |
| PerfLogs              | Directory         | K+==X×  |                 |
| Program Files         | Directory         | E 2051  |                 |
| Program Files (x86)   | Direct ,          | ビデオ   |                 |
|                       | Directory         | ↓ ミュージック ファイルのダウンロードが学  | 急了 🛛            |
| Download Eile 去语也     | Directory         |   |                 |
| Download File を迭代     | Directory         | ■ コンピューター   |                 |
|                       | Directory         | 🚢 ローカル ディスク   |                 |
| Windows               | Directory         | 🕳 リムーバブル ディン  |                 |
| hiberfil.sys          | -1235222528 bytes |   |                 |
| nmap-7.12-setup.exe   | 25.2 MB           | 📭 ネットワーク  |                 |
| nmap.txt              | 9 KB              |   |                 |
| pagefile.sys          | 15306240 bytes    |   |                 |
| <u>Download</u>       | File              | 3 個の項目  |                 |
| 🚖 Upload File         | 2                 | · •   |                 |
| New Folde             | r                 |   |                 |
| isted!                | •                 |   |                 |
| Rename                |                   |   |                 |

### ■ 演習10 nmapの調査結果からファイル共有サーバーを探し出し、サービスポートを書き出しましょう?

| ファイル共有サーバーIP アドレス |  |
|-------------------|--|
| サービスポート           |  |