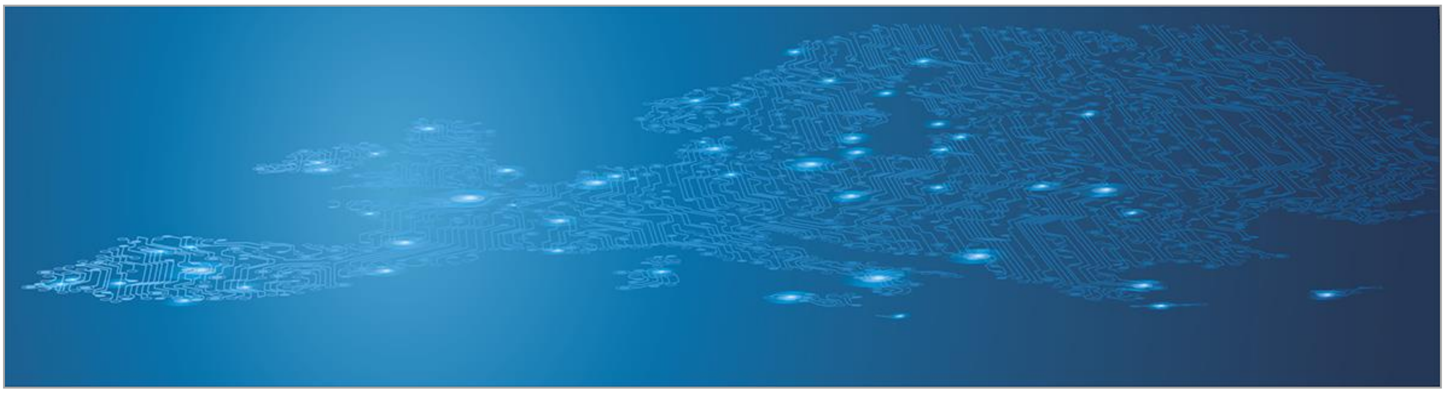
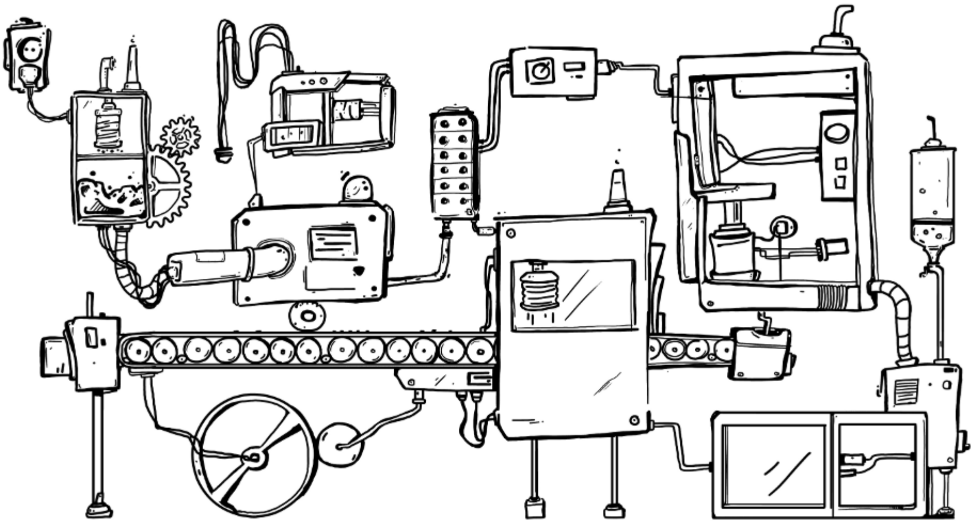




Using indicators to enhance defence capabilities

Actionable information

November 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

This document was created by the CERT capability team at ENISA in consultation with CERT Polska / NASK (Poland)[1]

Contact

For contacting the authors please use cert-relations@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu

Acknowledgements

ENISA wants to thank all institutions and persons who contributed to this document. A special 'Thank You' goes to the following contributors:

Andrew Kompanek (CERT/CC)

Takahiro Kakumaru (NEC)

Przemysław Jaroszewski (CERT Polska / NASK)

Paweł Pawliński (CERT Polska / NASK)

[1] Łukasz Siewierski, Radosław Żuber, Paweł Jacewicz

Contents

Main Objective	The main objective of this exercise is to teach students how to work with threat intelligence platforms like CRITS In the practical part of the exercise, the participants will use the CRITs platform to build a malicious campaign, add the related information and analyse it.	
Targeted Audience	CERT staff involved in the process of incident handling, especially those responsible for detection of new threats related directly to the CERT customers.	
Total duration	6-7 hours	
Time Schedule	**Introduction to the exercise**	0.5 hour
	Task 1:	0.5 hour
	Task 2:	1.5 hours
	Task 3:	1.5 hours
	Task 4:	0.5 hour
Frequency	N/A	

1 Introduction to the exercise

1.1 Goal of the exercise

This exercise was developed as training for Incident Response Team members and other IT security professionals that are responsible for creating and acting on the indicators derived from malicious campaigns and incidents. It should also provide useful information for any network administrator responsible for network security.

The goal of this exercise is to learn how to create indicators and log their usage in the "Collaborative Research into Threats" (CRITs) system, focusing on how to use CRITs to select indicators. While CRITs can help the readers organise their work, including logging of actions and handling objects, ultimately the reader has full responsibility on planning and choosing what the indicators will be. This training is meant to teach how to use CRITs for everyday tasks and provide a foundation for developing more advanced indicator management skills.

The exercise starts with a standard CRITs installation and guides you through every step, so you can get your instance up and running.

1.2 The Scenario

STIRC Inc. is a leading contractor in the defence industry, working on highly classified military projects. In the first week of July 2014, an employee of STIRC Inc. received an e-mail outlining changes in the agenda for the conference which required attendance in the near future. Unfortunately, the new schedule conflicted with other commitments, leading the employee to call the organisers in order to withdraw the participation. The organisers informed the employee that they did not send any message regarding changes in the agenda. This worried him - he became suspicious and reported the case to the STIRC Inc. Security Team.

The security team recognized the fraudulent e-mail as a potential threat to the company network. The team found out that the PDF file sent with the agenda was malicious, and subsequently took the action to disconnect all of the user's devices from the network for further study and analysis by the Security Team.

As part of its response to the incident, the STIRC Inc. Security Team set up a proprietary client-side honeypot, used it to run the code contained in the malicious PDF file, and redirected all traffic between the honeypot and the IP addresses associated with the campaign. This led to the logging of a connection from the malicious code intended to exfiltrate files from the honeypot.

You have received one of user's machines. Your task is to analyse the threat and set up network perimeter defence mechanisms to mitigate against this particular threat, and if possible, defend against similar activity in the future. During the course of this exercise the student will be provided with artefacts obtained from analysis of the incident. You will then use the CRITs[1] software to visualize and better understand the campaign.

[1] http://crits.github.io/

2 Introduction to the analysis environment

2.1 Setup and requirements

In order to make the exercise setup easier, a virtual machine was prepared in the OVA package [2]format . The virtual machine should run on any 64-bit computer running VirtualBox.

Follow the steps outlined below to set up the exercise environment:

Download the ova VirtualBox appliance file[3].

- Run VirtualBox and choose “File | Import Appliance…”.
- Choose the .ova file from the disk.
- Remember to check “Reinitialize the MAC address of all network cards” to resolve any MAC address conflicts that may exist in your internal network.
- Set the Network type to “Host Only” in the VirtualBox Machine settings. If you do not have the “Host Only” VirtualBox adapter, you will have to set it up using the following steps.
  a) Select “File | Preferences” from the VirtualBox main menu.
  b) Go to the “Network” setting, by choosing the entry from the list on the left.
  c) Go to the “Host-only Networks” tab.
  d) If the list is empty, click on the adapter icon with a plus sign on the right of the list.

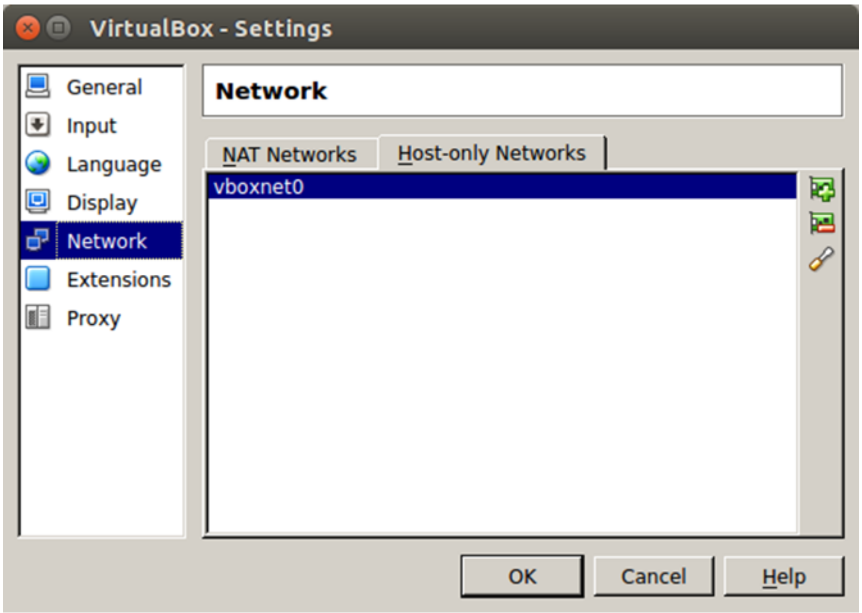


Figure 1 Host Only Networks

- Boot up your machine and log in using following credentials:
  a) username: root
  b) password: root
- Type “ip a” command and see what IP addresses are assigned to the eth0 adapter.
- Add the following entry in your /etc/hosts file on the host machine. This file will be at the following locations:
  a) /etc/hosts in Linux systems.
  b) %SystemRoot%\system32\drivers\etc\hosts in Windows 2000 and newer.

[2] http://en.wikipedia.org/wiki/Open_Virtualization_Format
[3] https://www.enisa.europa.eu/ftp/crits-headless.ova

c) /private/etc/hosts or /etc/hosts on Mac OS X 10.2 or newer.

- You will have to add the following entry (where ip_address is the address that you saw in the previous step).
  <ip_address> crits.lan

The entry above is required for the web server to be able to validate the “Host” header value.

3 Tasks

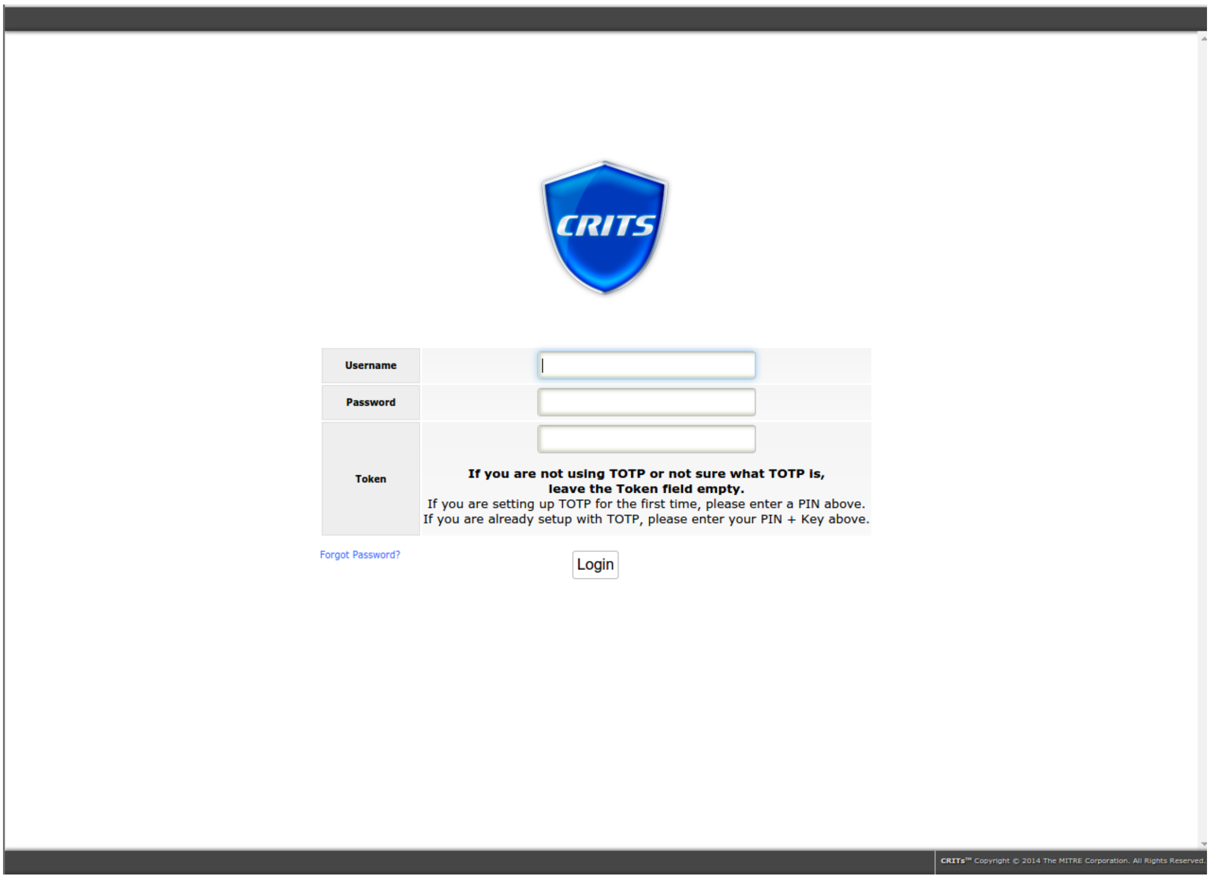
3.1 Task 1: Create the CRITs analyst account

During the first task, you will become familiar with the CRITs interface and create your first analyst account. This account should be created for any employee, who wants to use CRITs.

Login to the CRITs instance (on **https://crits.lan/crits**) using the following credentials:

login: **crits**

password: **O8.{oD'k**



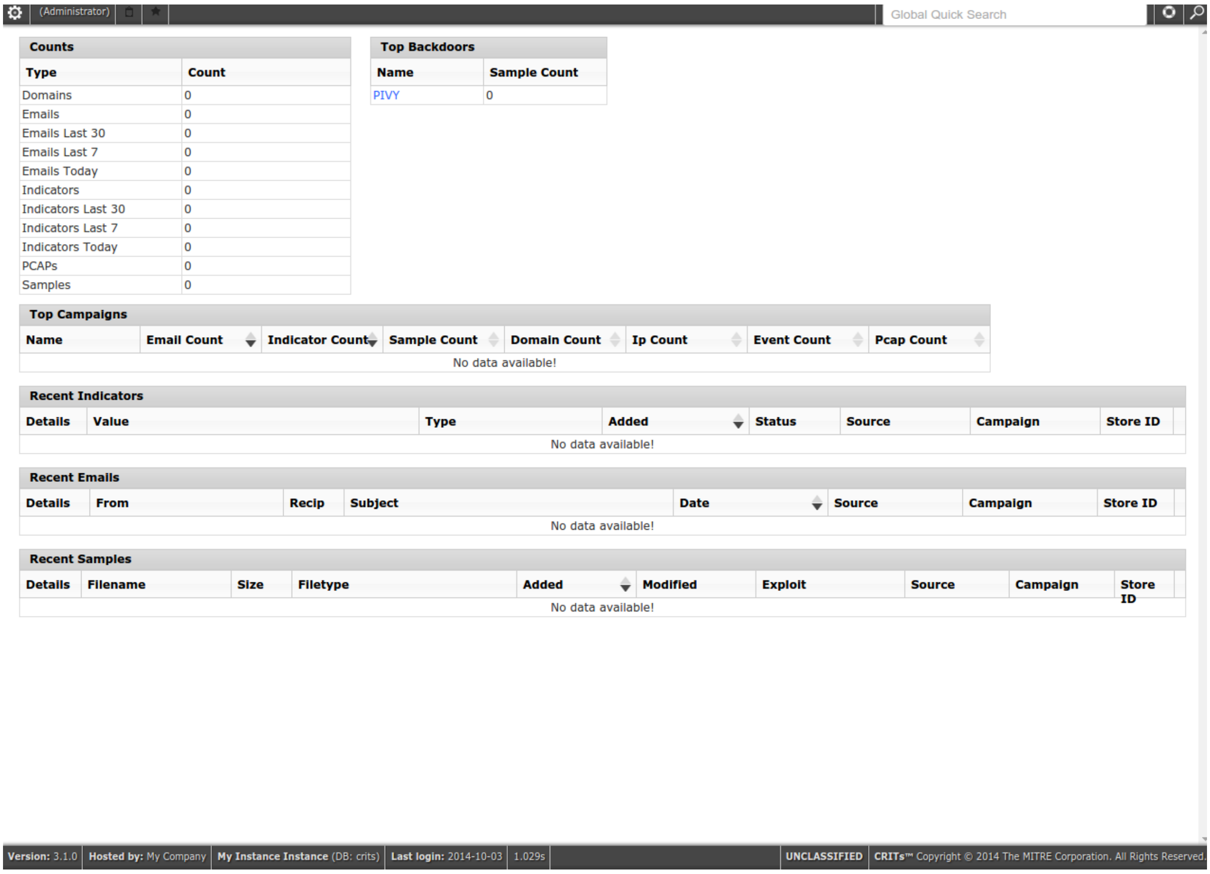
If you are not using TOTP or not sure what TOTP is, leave the Token field empty.
If you are setting up TOTP for the first time, please enter a PIN above.
If you are already setup with TOTP, please enter your PIN + Key above.

CRITs™ Copyright © 2014 The MITRE Corporation. All Rights Reserved.

Figure 2 CRITs Login Page

After you log in, you are redirected to a view called “Dashboard” (as presented below). This is your go-to view for a quick look at the recent changes in the CRITs instance, e.g. someone adding new samples, e-mails or domains.

As you can see it is empty for now, because there are no objects created. Your first task is to create the analyst account. Note: You should not use the Administrator account for any analyst work. Click on the left upper corner on the gear icon (or by clicking the “n” keyboard shortcut). This is the navigation menu and includes all available views. By clicking on the plus signs to the left of some items you can quickly add a new object (this will be covered in the next tasks). By clicking on the ">" signs to the right of some entries you can expand the submenu.



Counts

Type	Count
Domains	0
Emails	0
Emails Last 30	0
Emails Last 7	0
Emails Today	0
Indicators	0
Indicators Last 30	0
Indicators Last 7	0
Indicators Today	0
PCAPs	0
Samples	0

Top Backdoors

Name	Sample Count
PIVY	0

Top Campaigns

Name	Email Count	Indicator Count	Sample Count	Domain Count	Ip Count	Event Count	Pcap Count
No data available!							

Recent Indicators

Details	Value	Type	Added	Status	Source	Campaign	Store ID
No data available!							

Recent Emails

Details	From	Recip	Subject	Date	Source	Campaign	Store ID
No data available!							

Recent Samples

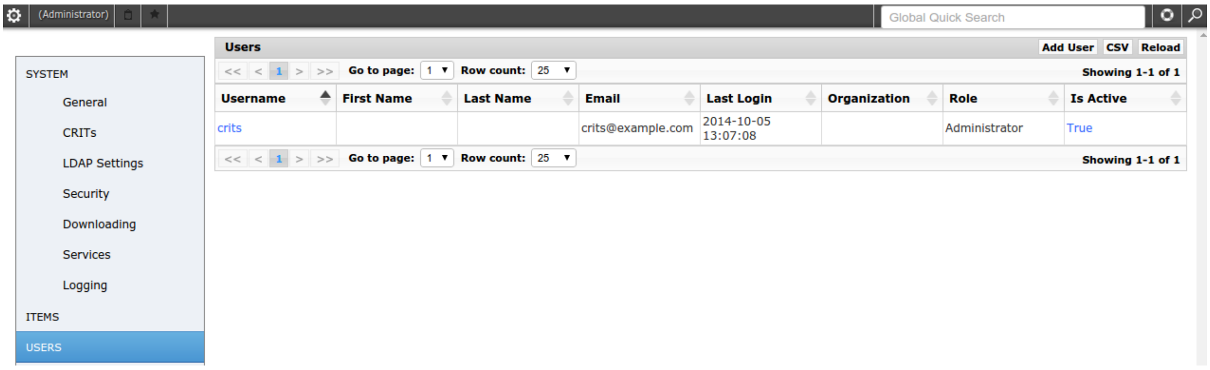
Details	Filename	Size	Filetype	Added	Modified	Exploit	Source	Campaign	Store ID
No data available!									

Version: 3.1.0 | Hosted by: My Company | My Instance Instance (DB: crits) | Last login: 2014-10-03 | 1.029s | UNCLASSIFIED | CRITs™ Copyright © 2014 The MITRE Corporation. All Rights Reserved.

Figure 3 CRITs dashboard view

First, you have to add your organization as one of the so called "Sources". You can do that by clicking on the "CRITs Control Panel" menu and going to the "ITEMS" submenu and select the "Sources" tab. From here you can click on "Add SourceAccess" button and provide the name for your organization. We will be using the "STIRC" name.

Now click on the "CRITs Control Panel" view and go to the "USERS" submenu. You should see the screen similar to the one presented below.



Users

Showing 1-1 of 1

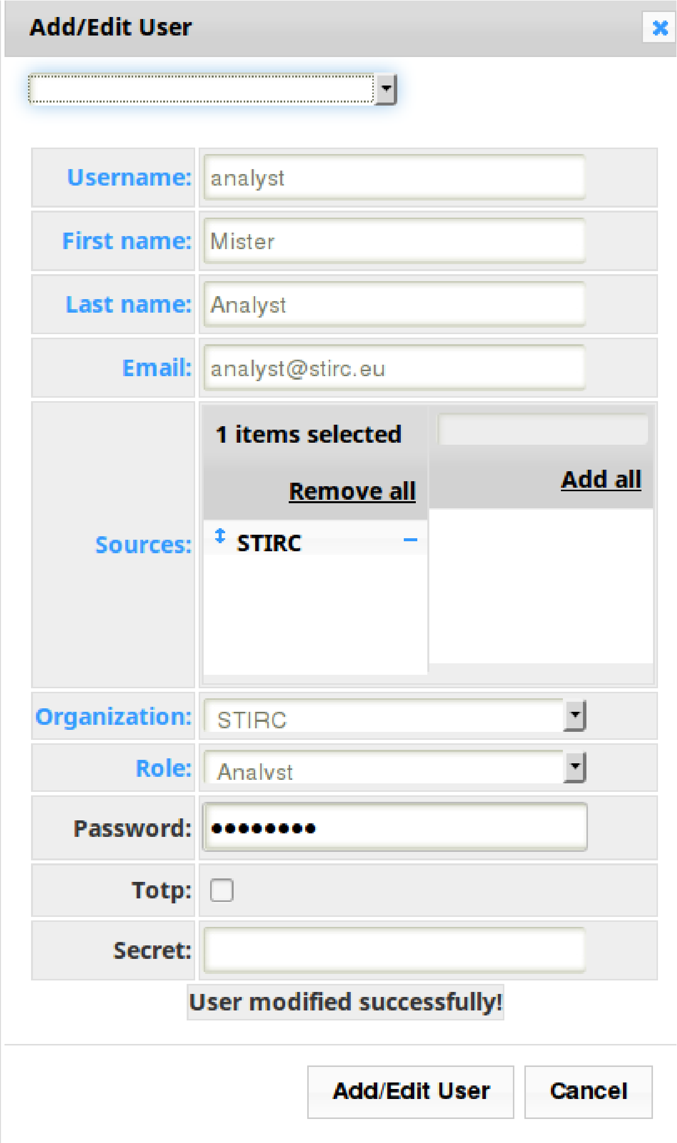
Username	First Name	Last Name	Email	Last Login	Organization	Role	Is Active
crits			crits@example.com	2014-10-05 13:07:08		Administrator	True

Showing 1-1 of 1

Figure 4 CRITs Control Panel users view

Your only account is currently “Administrator”. Click on the “Add User” button and fill in the popup. Click on “Add all” in the “Sources” section to ensure that the new account has access to the “STIRC” source. Next, choose “Analyst” role in the dropdown, as pictured below.

Remember that the password has to be at least 8 characters long, and include at least 1 capital letter, 1 lowercase letter, and 1 digit or special character.



Add/Edit User

Username:	analyst
First name:	Mister
Last name:	Analyst
Email:	analyst@stirc.eu
Sources:	1 items selected Remove all STIRC Add all
Organization:	STIRC
Role:	Analyst
Password:	●●●●●●●●
Totp:	□
Secret:	

User modified successfully!

Figure 5 CRITs Add user dialog

You will be using this account for the remainder of this exercise. Log out - again using the navigation menu - and try to log in as the newly created analyst.

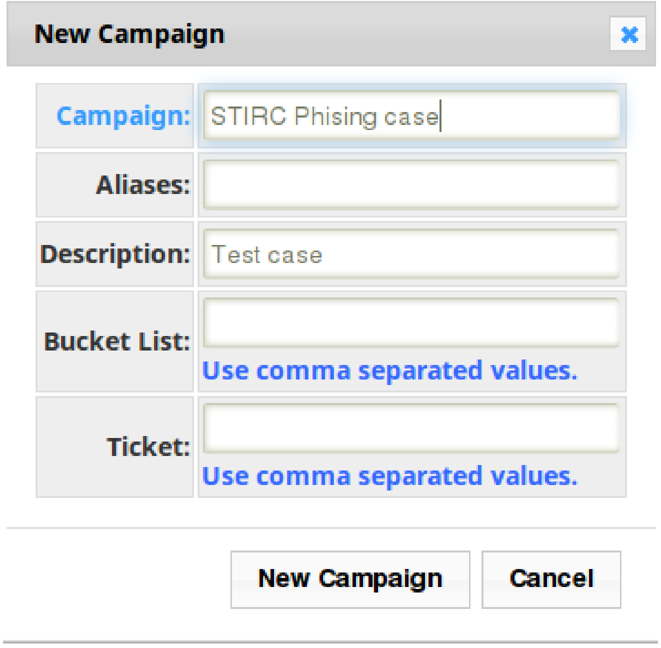
3.2 Task 1: Upload all the information

You should receive three files[4] :

- `dump_sandbox.pcap` - traffic dump from the specially-crafted sandbox on which the Security Team analysed the threat
- `dump_honeypot.pcap` - traffic dump from the data exfiltration event on the honeypot set up by the Security Team after the incident
- `email.eml` - the email message, which the attackers send to the employee. The attachment content has been removed from this message.

These files will help you analyse the course of the campaign and visualise connections between different events. Your first step should be to load all of the data into CRITs.

To create a new campaign you have to be logged in as an administrator, using the credentials presented at the beginning of this exercise. Create a new Campaign using the CRITs Control Panel | Items view. The "Bucket List" is a list of tags associated with this campaign. "Ticket" can be used to list identifiers that reference related tickets in your internal ticketing service. You can leave both fields empty for now, but remember that in a real-life scenario you will generally enter the ticket number corresponding to the action to handle this incident. We will be using the campaign name "STIRC Phishing case", although you are free to choose any name you like. The "New campaign" dialog example is presented below.



New Campaign

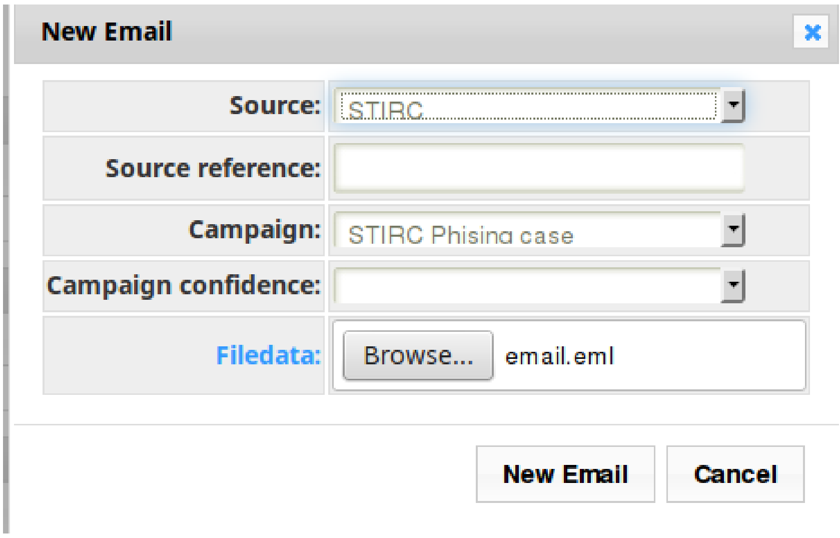
Campaign:	STIRC Phising case
Aliases:	
Description:	Test case
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 6 CRITs New Campaign dialog

A campaign is a logical concept provided by CRITs that corresponds to a set of activities you want to treat as a distinct malicious campaign. This helps you organise the different sets of data you have loaded.

[4] https://www.enisa.europa.eu/ftp/crits-headless-files.zip

First, log in as a newly created CRITs analyst. In order to upload an e-mail message go to the Navigation Menu (by pressing “n”) and click on the “>” sign next to “Emails” menu. Choose “New Email (EML)”. Select your newly created campaign and choose the `email.eml` file. Your upload window should look similar to the one provided below.

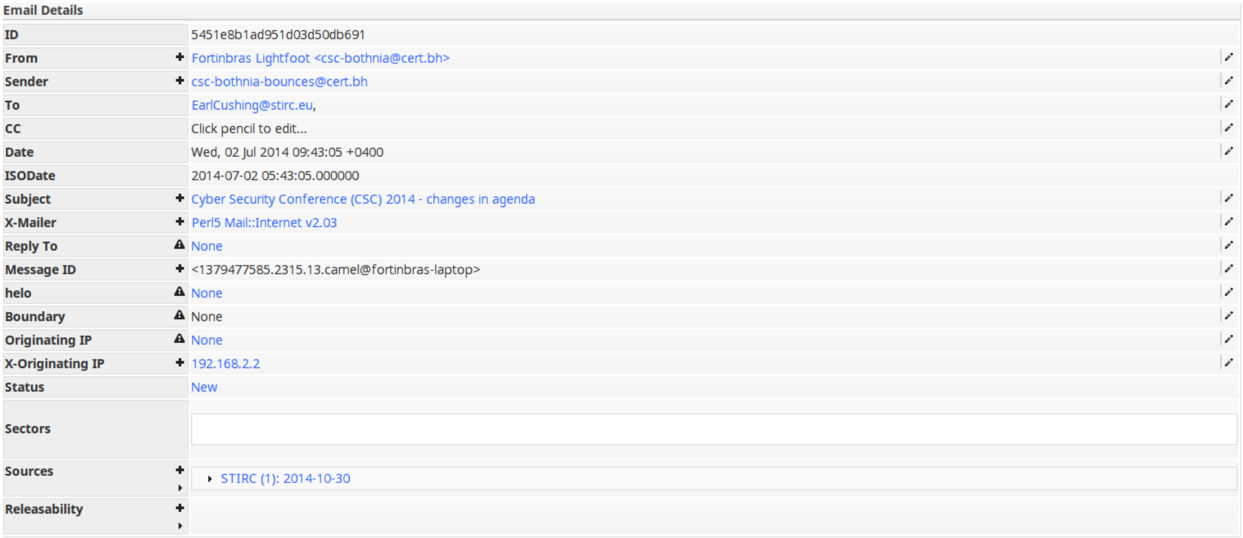


New Email

Source:	STIRC
Source reference:	
Campaign:	STIRC Phising case
Campaign confidence:	
Filedata:	Browse... email.eml

Figure 7 CRITs New e-mail dialog

Now, verify that the e-mail message was uploaded successfully by clicking on the “View email” link. This will provide you with a structured view of the e-mail file you loaded. You should see all of the important headers and some relationships. First look at the “Email details” table pictured below.



Email Details

ID	5451e8b1ad951d03d50db691
From	Fortinbras Lightfoot <csc-bothnia@cert.bh>
Sender	csc-bothnia-bounces@cert.bh
To	EarlCushing@stirc.eu,
CC	Click pencil to edit...
Date	Wed, 02 Jul 2014 09:43:05 +0400
ISODate	2014-07-02 05:43:05.000000
Subject	Cyber Security Conference (CSC) 2014 - changes in agenda
X-Mailer	Perl5 Mail::Internet v2.03
Reply To	None
Message ID	<1379477585.2315.13.camel@fortinbras-laptop>
helo	None
Boundary	None
Originating IP	None
X-Originating IP	192.168.2.2
Status	New
Sectors	
Sources	STIRC (1): 2014-10-30
Releasability	

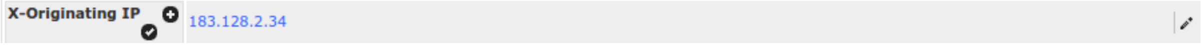
Figure 8 CRITs e-mail details

Some rows are filled with data, while some, due to the lack of data, are left empty. You can edit selected rows by clicking on the pencil icon to the right. As you can see the “X-Originating-IP” is an internal IP address. This should generally be an external IP address: the IP address of the mail server that sent the mail to the local server. The presence of the internal IP is probably due to a misconfiguration of the e-mail server in the STIRC Inc. infrastructure. Edit this IP address to the correct one. In order to find a correct IP address go to the “Raw Email” tab and look at the headers. You should find the following lines:

```
Received: from mail11.stirc.eu ([127.0.0.1]) by localhost
([127.0.0.1]) (maiad, port 10024) with ESMTP id 80214-04 for
<EarlCushing@dayrep.com>; Wed, 02 Jul 2014 09:43:52 -0500 (EDT)

Received: from mail.cert.bh (smarthost.malicouisdoamin.evil.cn
[183.128.2.34]) by mail11.stirc.eu (Postfix) with ESMTP id B814FF61A5
for <EarlCushing@dayrep.com>; Wed, 02 Jul 2014 00:41:55 -0500 (EDT)
```

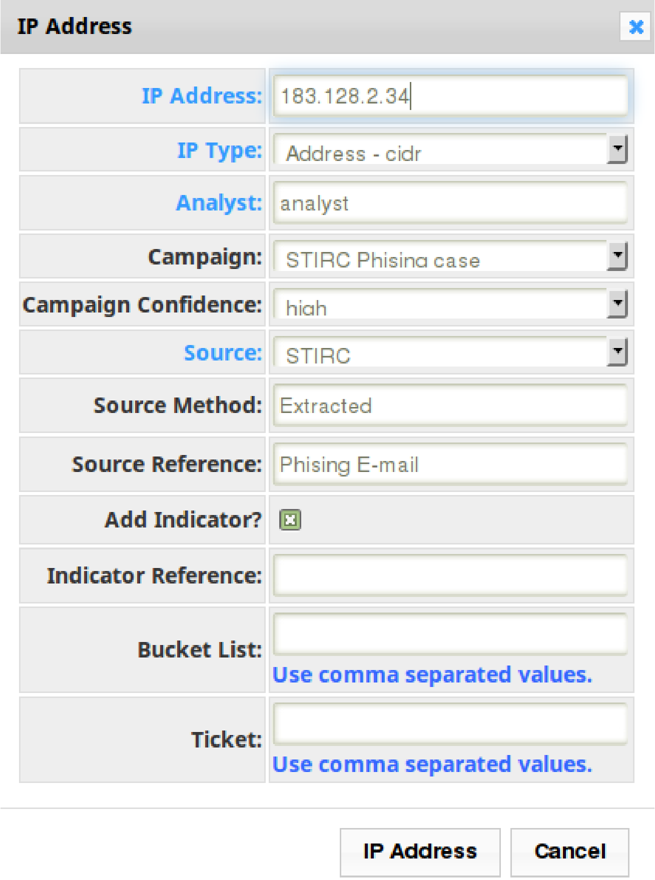
This shows that the originating IP address was in fact 183.128.2.34. Use the pencil icon to correct the CRITs mail server and you should see the information that the edit was successful, as presented below.



X-Originating IP 183.128.2.34

Figure 9 CRITs e-mail X-Originating IP

You can create an IP address by using the "I" (Shift + i) shortcut. Choose an appropriate IP address type ("Address - ipv4-addr") and the correct campaign. Assign a campaign confidence value, which is this case should be "high", because we are sure that this IP is part of the campaign. Finally, check the "Add Indicator" checkbox.



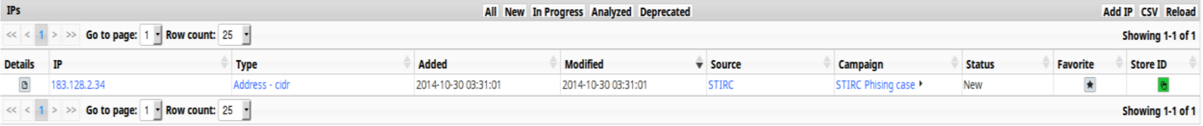
IP Address

IP Address:	183.128.2.34
IP Type:	Address - cidr
Analyst:	analyst
Campaign:	STIRC Phisina case
Campaign Confidence:	hiah
Source:	STIRC
Source Method:	Extracted
Source Reference:	Phising E-mail
Add Indicator?	☒
Indicator Reference:	
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 10 CRITs Add IP address dialog

"Source Method" is a field used to describe the method by which this IP address was obtained. In this case it was extracted from an e-mail message. The field "Source Reference" describes the nature of the data from which the IP address was obtained, a phishing e-mail. The screenshot above shows the filled in dialog box.

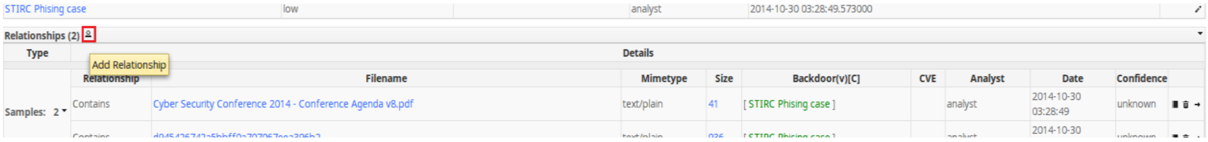
Now you have to create an explicit relationship between the Email and the IP Address. To do so, copy the IP Address again and enter it into the "Global Quick Search" field in the upper right corner of the website. This will show you all the objects which contain (in some way or another) the IP address. Go to the “IPs” tab and click on the “Store ID” icon. “Store ID” should now be highlighted as shown in the screenshot below.



Details	IP	Type	Added	Modified	Source	Campaign	Status	Favorite	Store ID
🗋	183.128.2.34	Address - cidr	2014-10-30 03:31:01	2014-10-30 03:31:01	STIRC	STIRC Phising case	New	★	🟩

Figure 11 CRITs search results

Now you have copied the object to the clipboard. Go back to the Email view and click on the “Add Relationship” icon next to the “Relationships” table, as highlighted in the screenshot below.



Relationship	Filename	Mimetype	Size	Backdoor(v)[C]	CVE	Analyst	Date	Confidence
Contains	Cyber Security Conference 2014 - Conference Agenda v8.pdf	text/plain	41	[STIRC Phising case]		analyst	2014-10-30 03:28:49	unknown
Contains	d945426742a5bbff0a707067eea396b2	text/plain	936	[STIRC Phising case]		analyst	2014-10-30	unknown

Figure 12 CRITs e-mail view

Choose the following options:

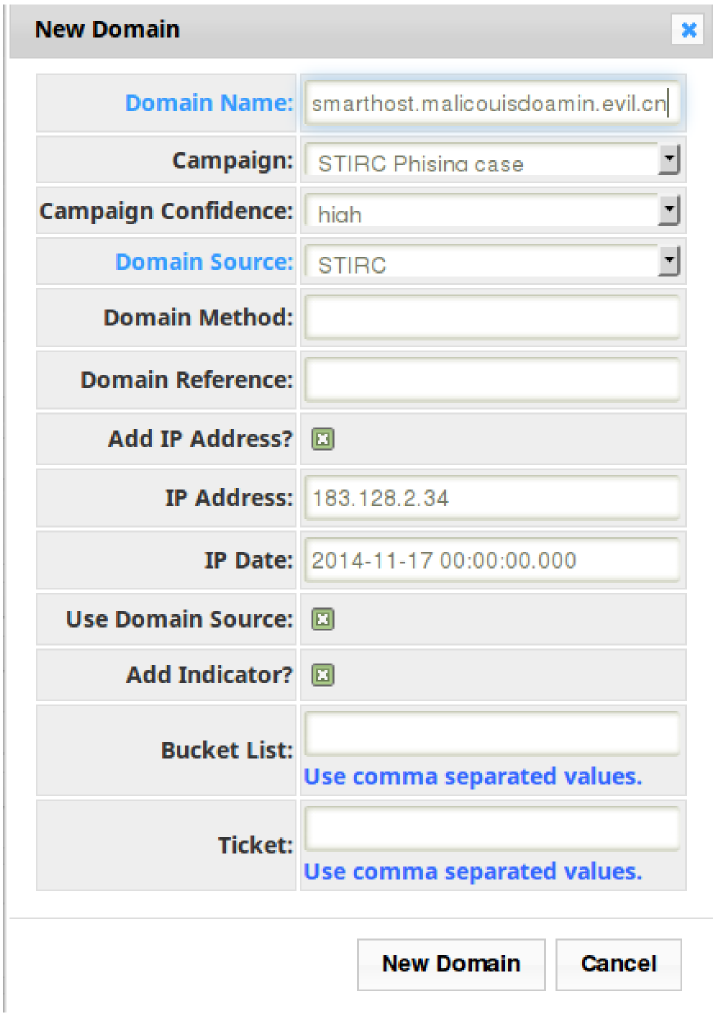
- For “Relationship”, click “More” and choose “Related_to”,
- Set the “Dest Type” to “IP”,
- Set the “Confidence” to “high”,
- Click “Get Clipboard” next to the “Dest ID”. This will fill both the Destination Type and the Destination ID, which is an object identifier of the second part of the relationship.

Now click “Forge Relationship”. You have just created a relationship between the IP address, the Indicator containing an IP address, the campaign and the Email message. This way you create an “Object” associated with a campaign. It is important that you distinguish between an Object, something that was observed during the course of a campaign, and an Indicator, which will form the basis of actions. We will make this distinction clear when we discuss Indicators later in this exercise.

Now create a domain from which the mail has originated according to our analysis of the raw e-mail. Press “d” or click at the “plus” icon next to “Domains” in the Navigation menu and fill in the fields as described below:

- Set “Domain name” to `smarthost.malicouisdoamin.evil.cn`
- Set “Campaign” to “STIRC Phishing Case”.
- Set “Campaign confidence” to “high”.
- Check the “Add IP address” and enter the `183.128.2.34` address.
- Check the “Add Indicator” checkbox.

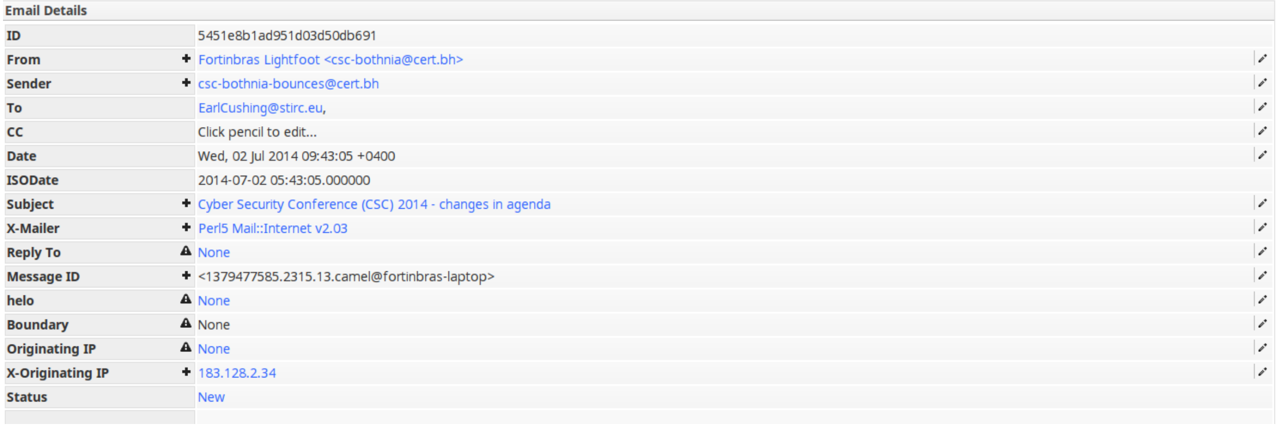
The resulting dialog box is presented below.



Domain Name:	smarthost.malicouisdoamin.evil.cn
Campaign:	STIRC Phisina case
Campaign Confidence:	hiah
Domain Source:	STIRC
Domain Method:	
Domain Reference:	
Add IP Address?	☒
IP Address:	183.128.2.34
IP Date:	2014-11-17 00:00:00.000
Use Domain Source:	☒
Add Indicator?	☒
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 13 CRITs Add new domain dialog

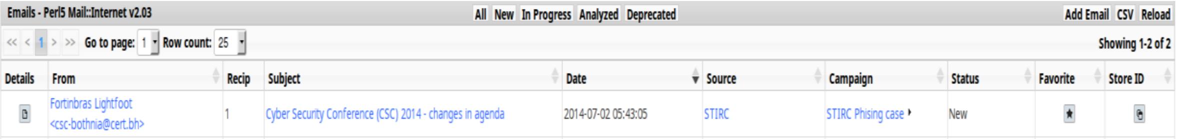
If you click on any of the text marked in blue it will search for Emails with the same headers. In this way you can see and create relationships between different campaigns. Examples of searchable field values are shown below.



Email Details		
ID		5451e8b1ad951d03d50db691
From	+	Fortinbras Lightfoot <csc-bothnia@cert.bh>
Sender	+	csc-bothnia-bounces@cert.bh
To		EarlCushing@stirc.eu,
CC		Click pencil to edit...
Date		Wed, 02 Jul 2014 09:43:05 +0400
ISODate		2014-07-02 05:43:05.000000
Subject	+	Cyber Security Conference (CSC) 2014 - changes in agenda
X-Mailer	+	Perl5 Mail::Internet v2.03
Reply To	⚠	None
Message ID	+	<1379477585.2315.13.camel@fortinbras-laptop>
helo	⚠	None
Boundary	⚠	None
Originating IP	⚠	None
X-Originating IP	+	183.128.2.34
Status		New

Figure 14 CRITs e-mail view

One of the more useful searches can be done by clicking on the `X-Mailer` value (`Perl5 Mail::Internet v2.03`). Because we only have one e-mail in our database, only one search result will be present, as pictured below.



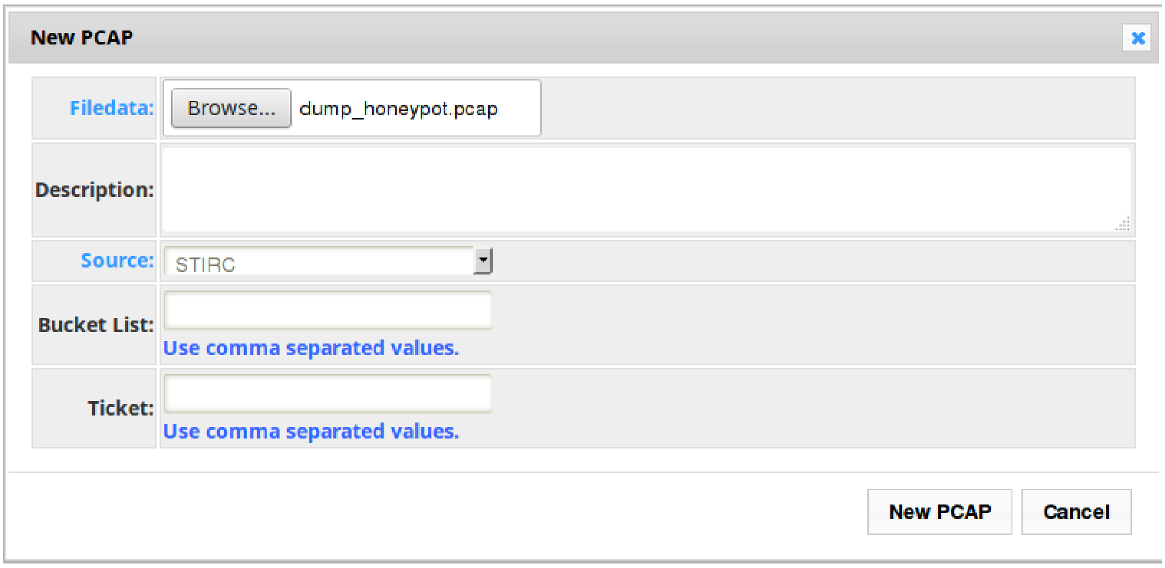
Emails - Perl5 Mail::Internet v2.03

Showing 1-2 of 2

Details	From	Recip	Subject	Date	Source	Campaign	Status	Favorite	Store ID
	Fortinbras Lightfoot <csc-bothnia@cert.bh>	1	Cyber Security Conference (CSC) 2014 - changes in agenda	2014-07-02 05:43:05	STIRC	STIRC Phising case	New	★	

Figure 15 CRITs search results

Next up are the two PCAP files. We will upload them using a "plus" sign next to the PCAPs item in the Navigation menu. You should choose a PCAP file add a description and click on the "New PCAP" button, like pictured below. This will create a new object.

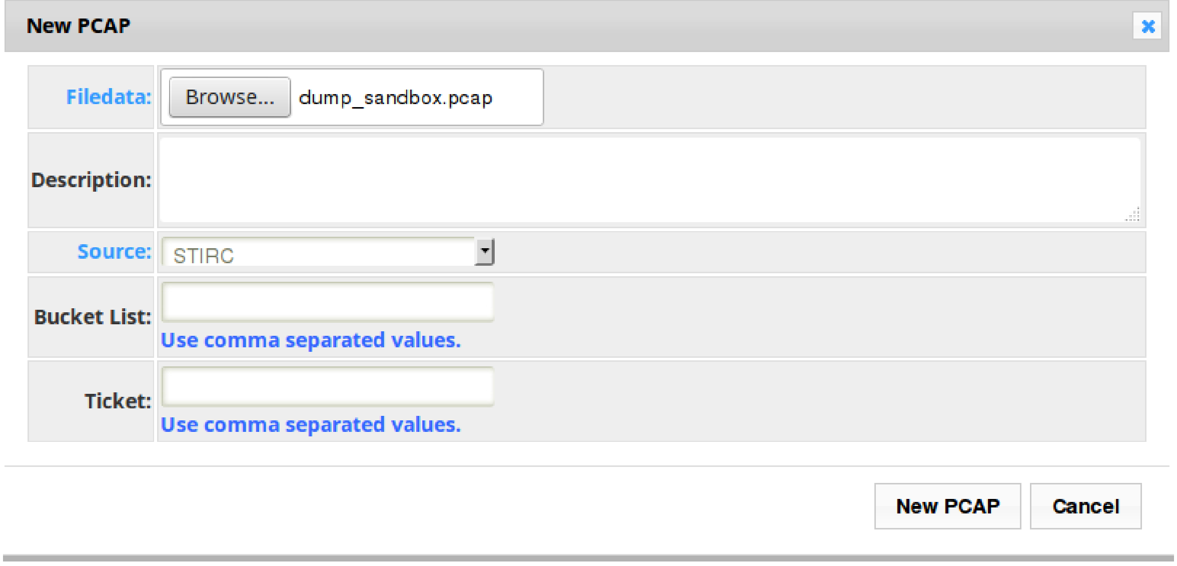


New PCAP

Filedata:	Browse... dump_honeypot.pcap
Description:	
Source:	STIRC
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 16 CRITs add new PCAP dialog

Carry out the same actions for a second PCAP file.



New PCAP

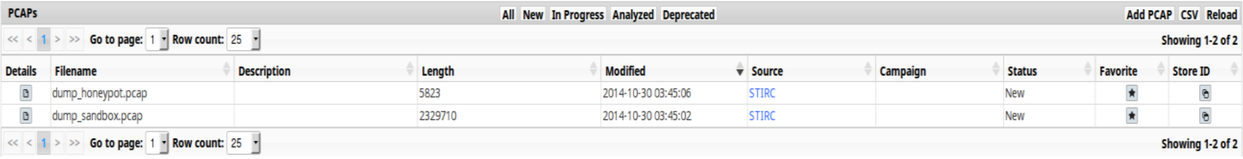
Filedata:	Browse... dump_sandbox.pcap
Description:	
Source:	STIRC
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 17 CRITs add new PCAP dialog

3.3 Task 2: Use CRITs services to extract even more information

CRITs can be extended using 3rd-party extensions called services. They can be used to extract additional information from the files that you have uploaded. That additional information can provide a deeper insight into the campaign. The goal of this task is to show how to use services, how to manage them, and how to create more data based on the output of services.

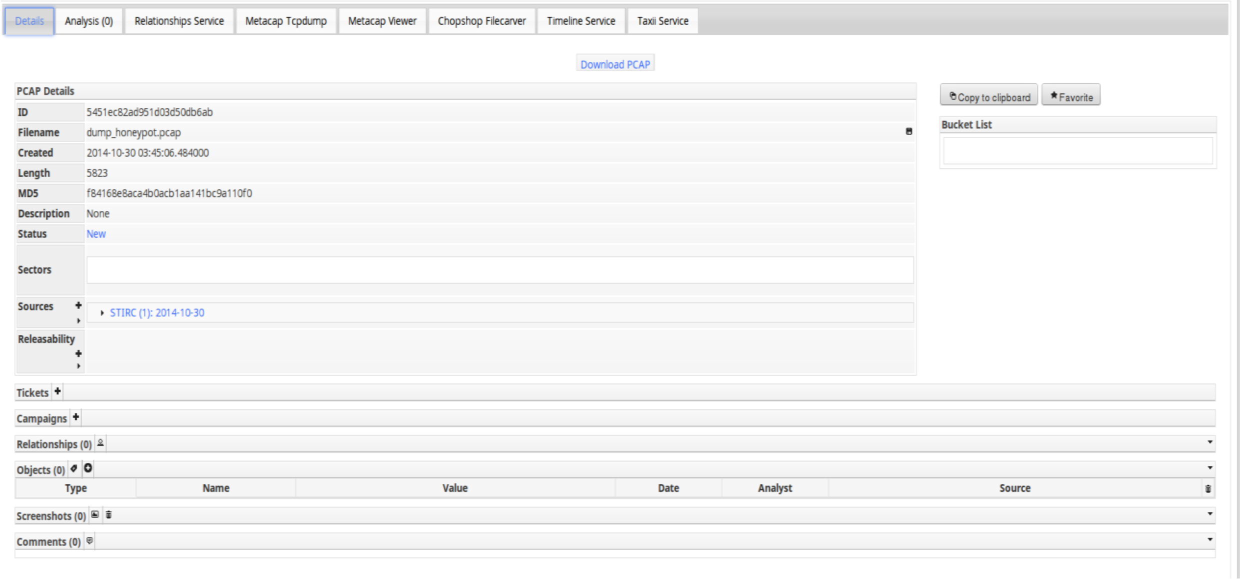
The first service that we will use is called MetaCap and its purpose is to extract metadata from a PCAP file. Go to the PCAPs view (pictured below) and choose the dump_honeypot.pcap file by clicking on the "Details" button to the left of the filename.



Details	Filename	Description	Length	Modified	Source	Campaign	Status	Favorite	Store ID
🗎	dump_honeypot.pcap		5823	2014-10-30 03:45:06	STIRC		New	★	🗎
🗎	dump_sandbox.pcap		2329710	2014-10-30 03:45:02	STIRC		New	★	🗎

Figure 18 CRITs PCAP view

After clicking on the details button, you will see details about the PCAP including a hash of the PCAP contents and the filename.



PCAP Details	
ID	5451ec82ad951d03d50db6ab
Filename	dump_honeypot.pcap
Created	2014-10-30 03:45:06.484000
Length	5823
MD5	f84168e8aca4b0acb1aa141bc9a110f0
Description	None
Status	New
Sectors	
Sources	STIRC (1): 2014-10-30
Releasability	

Figure 19 CRITs dump_honeypot.pcap view

Go to the "Analysis" tab and click on the MetaCap service.

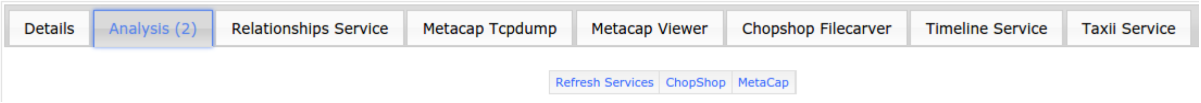
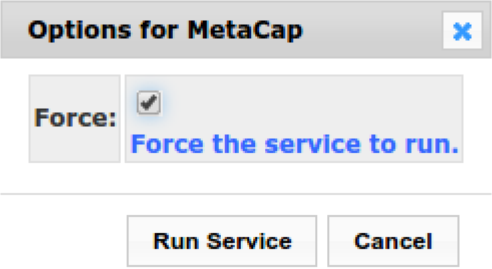


Figure 20 CRITs metacap analysis view

Both the MetaCap and the ChopShop service mentioned below use the ChopShop Protocol Analysis Framework. Due to a bug in this framework you will have to invoke the service several times before it runs successfully. During our tests we had to run it at most 23 times before it ran without displaying an error message, but this number can of course vary. Use the "Force" option for each subsequent run, as pictured below.

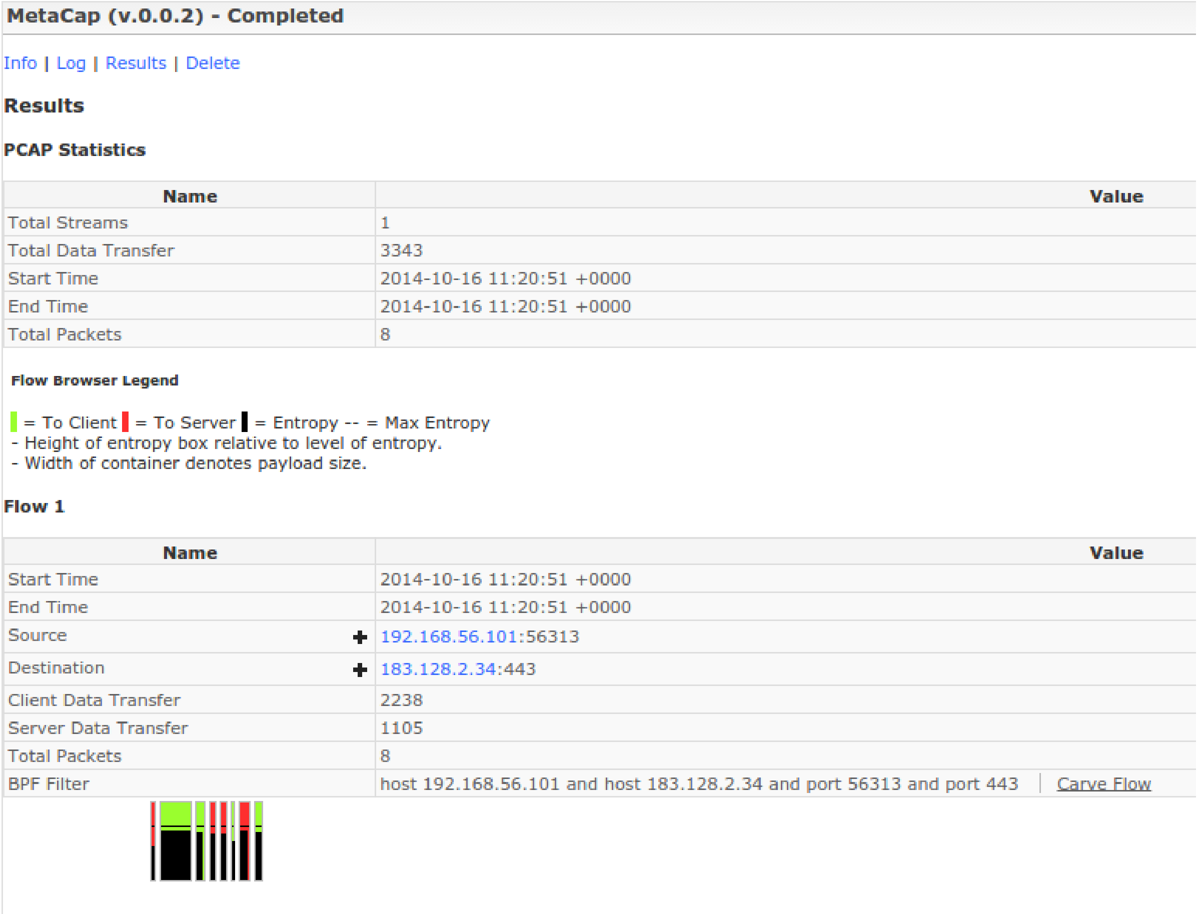


Options for MetaCap

Force: ☑ Force the service to run.

Figure 21 CRITs metacap options dialog

The above remarks also apply to the ChopShop service[5].



MetaCap (v.0.0.2) - Completed

Info | Log | Results | Delete

Results

PCAP Statistics

Name	Value
Total Streams	1
Total Data Transfer	3343
Start Time	2014-10-16 11:20:51 +0000
End Time	2014-10-16 11:20:51 +0000
Total Packets	8

Flow Browser Legend

🟩 = To Client 🟥 = To Server ▮ = Entropy -- = Max Entropy
- Height of entropy box relative to level of entropy.
- Width of container denotes payload size.

Flow 1

Name	Value
Start Time	2014-10-16 11:20:51 +0000
End Time	2014-10-16 11:20:51 +0000
Source +	192.168.56.101:56313
Destination +	183.128.2.34:443
Client Data Transfer	2238
Server Data Transfer	1105
Total Packets	8
BPF Filter	host 192.168.56.101 and host 183.128.2.34 and port 56313 and port 443 | Carve Flow

Figure 22 CRITs metacap results view

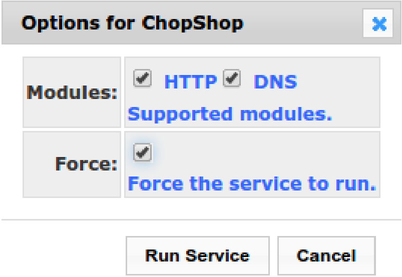
From the results of the MetaCap (presented above) you can easily create CRITs Indicators and corresponding IP Address objects for IP values in the packet headers in the PCAP by clicking on the plus sign displayed next to highlighted values. This will create two distinct data objects in CRITs: an Indicator and the IP Address observable to which that Indicator will refer. If you only wanted to create an IP Address then you would have to do it manually, using the <Shift+i> keyboard shortcut.

Click on the plus sign next to the second IP Address (183.128.2.34). This corresponds to the malicious mail server we identified earlier. In this case CRITs will not actually create a new IP Address object

[5] This bug is described at https://github.com/crits/crits_services/issues/53

because we have already added that IP Address manually. Instead the system will create a relationship between the Indicator and the existing IP Address.

Next, select the ChopShop service and run it. You should choose both the “HTTP” and “DNS” options, as pictured below.



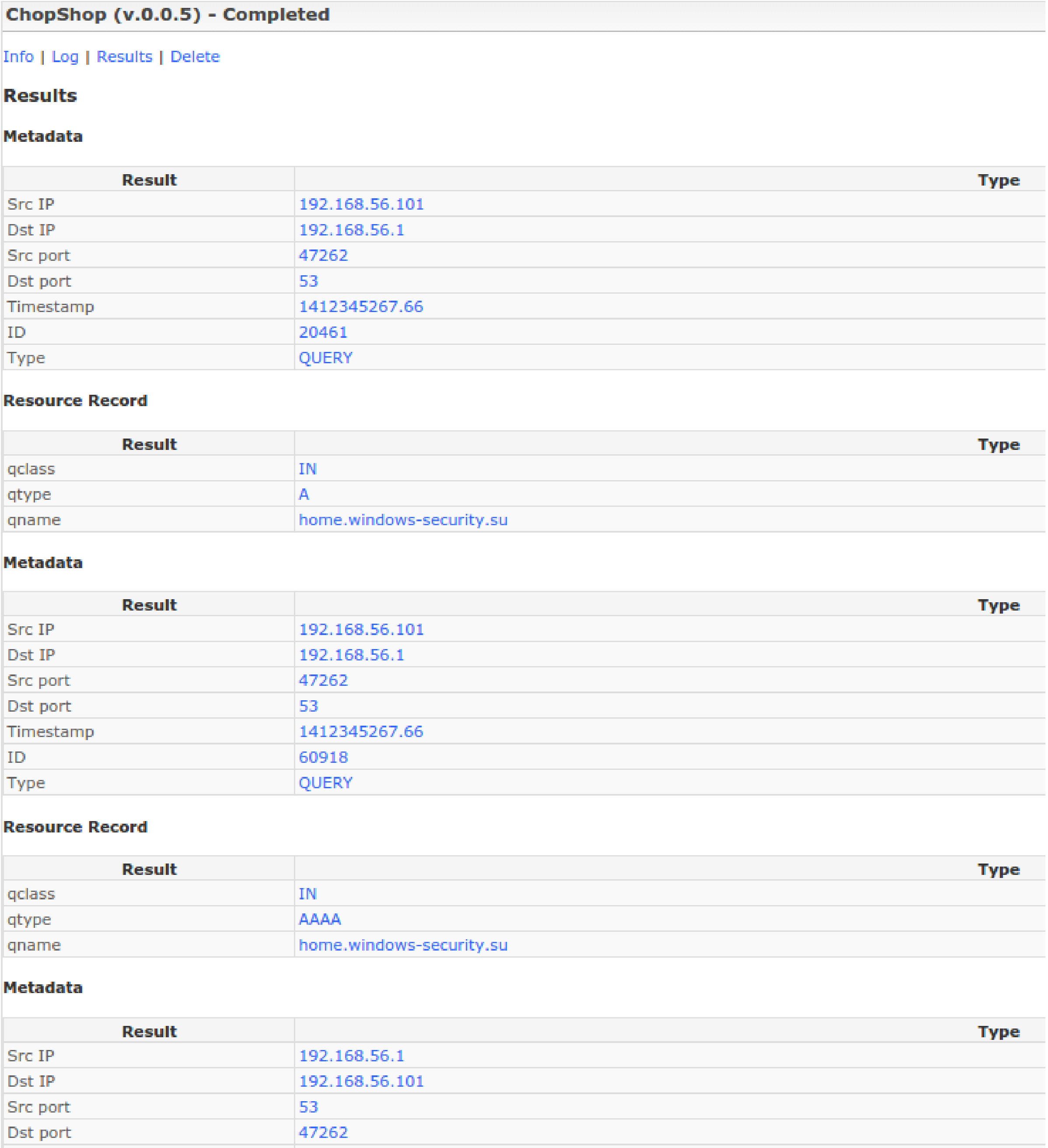
Options for ChopShop

Modules: ☑ HTTP ☑ DNS
Supported modules.

Force: ☑
Force the service to run.

Figure 23 CRITs ChopShop options dialog

This will show additional information about the HTTP and DNS sessions found in the PCAP file, as pictured below.



ChopShop (v.0.0.5) - Completed

Info | Log | Results | Delete

Results

Metadata

Result	Type
Src IP	192.168.56.101
Dst IP	192.168.56.1
Src port	47262
Dst port	53
Timestamp	1412345267.66
ID	20461
Type	QUERY

Resource Record

Result	Type
qclass	IN
qtype	A
qname	home.windows-security.su

Metadata

Result	Type
Src IP	192.168.56.101
Dst IP	192.168.56.1
Src port	47262
Dst port	53
Timestamp	1412345267.66
ID	60918
Type	QUERY

Resource Record

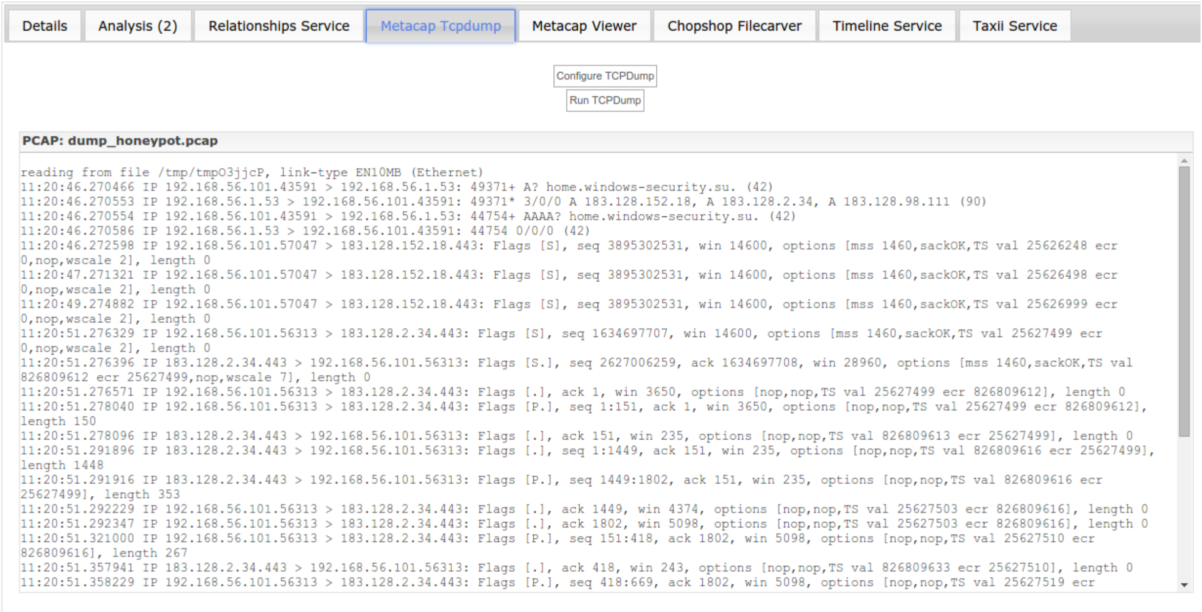
Result	Type
qclass	IN
qtype	AAAA
qname	home.windows-security.su

Metadata

Result	Type
Src IP	192.168.56.1
Dst IP	192.168.56.101
Src port	53
Dst port	47262

Figure 24 ChopShop results view

From this screen you can see all of the DNS queries (and their results) along with the HTTP sessions that were established. All of the malware traffic was made via HTTPS and therefore is not shown here. However, you can view all of the captured packets by using the “MetaCap Tcpdump” tab and clicking on “Run TCPDump”. The result is pictured below.

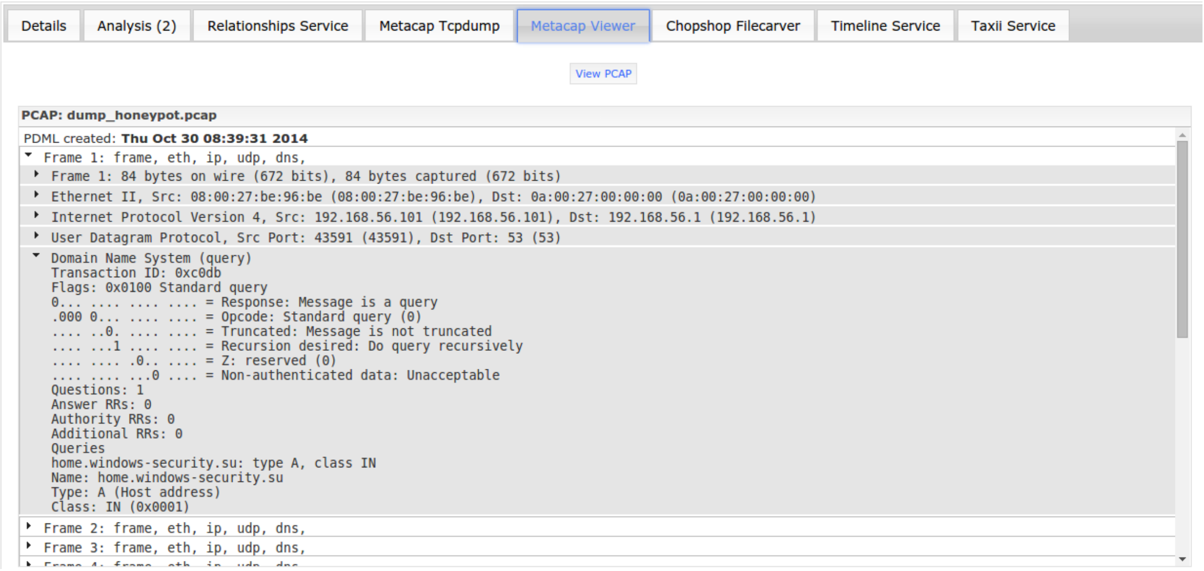


PCAP: dump_honeypot.pcap

```
reading from file /tmp/tmpO3jjcP, link-type EN10MB (Ethernet)
11:20:46.270466 IP 192.168.56.101.43591 > 192.168.56.1.53: 49371+ A? home.windows-security.su. (42)
11:20:46.270553 IP 192.168.56.1.53 > 192.168.56.101.43591: 49371* 3/0/0 A 183.128.152.18, A 183.128.2.34, A 183.128.98.111 (90)
11:20:46.270554 IP 192.168.56.101.43591 > 192.168.56.1.53: 44754+ AAAA? home.windows-security.su. (42)
11:20:46.270586 IP 192.168.56.1.53 > 192.168.56.101.43591: 44754 0/0/0 (42)
11:20:46.272598 IP 192.168.56.101.57047 > 183.128.152.18.443: Flags [S], seq 3895302531, win 14600, options [mss 1460,sackOK,TS val 25626248 ecr
0,nop,wscale 2], length 0
11:20:47.271321 IP 192.168.56.101.57047 > 183.128.152.18.443: Flags [S], seq 3895302531, win 14600, options [mss 1460,sackOK,TS val 25626498 ecr
0,nop,wscale 2], length 0
11:20:49.274882 IP 192.168.56.101.57047 > 183.128.152.18.443: Flags [S], seq 3895302531, win 14600, options [mss 1460,sackOK,TS val 25626999 ecr
0,nop,wscale 2], length 0
11:20:51.276329 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [S], seq 1634697707, win 14600, options [mss 1460,sackOK,TS val 25627499 ecr
0,nop,wscale 2], length 0
11:20:51.276396 IP 183.128.2.34.443 > 192.168.56.101.56313: Flags [S.], seq 2627006259, ack 1634697708, win 28960, options [mss 1460,sackOK,TS val
826809612 ecr 25627499,nop,wscale 7], length 0
11:20:51.276571 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [.], ack 1, win 3650, options [nop,nop,TS val 25627499 ecr 826809612], length 0
11:20:51.278040 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [P.], seq 1:151, ack 1, win 3650, options [nop,nop,TS val 25627499 ecr 826809612],
length 150
11:20:51.278096 IP 183.128.2.34.443 > 192.168.56.101.56313: Flags [.], ack 151, win 235, options [nop,nop,TS val 826809613 ecr 25627499], length 0
11:20:51.291896 IP 183.128.2.34.443 > 192.168.56.101.56313: Flags [.], seq 1:1449, ack 151, win 235, options [nop,nop,TS val 826809616 ecr 25627499],
length 1448
11:20:51.291916 IP 183.128.2.34.443 > 192.168.56.101.56313: Flags [P.], seq 1449:1802, ack 151, win 235, options [nop,nop,TS val 826809616 ecr
25627499], length 353
11:20:51.292229 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [.], ack 1449, win 4374, options [nop,nop,TS val 25627503 ecr 826809616], length 0
11:20:51.292347 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [.], ack 1802, win 5098, options [nop,nop,TS val 25627503 ecr 826809616], length 0
11:20:51.321000 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [P.], seq 151:418, ack 1802, win 5098, options [nop,nop,TS val 25627510 ecr
826809616], length 267
11:20:51.357941 IP 183.128.2.34.443 > 192.168.56.101.56313: Flags [.], ack 418, win 243, options [nop,nop,TS val 826809633 ecr 25627510], length 0
11:20:51.358229 IP 192.168.56.101.56313 > 183.128.2.34.443: Flags [P.], seq 418:669, ack 1802, win 5098, options [nop,nop,TS val 25627519 ecr
```

Figure 25 CRITs metacap tcpdump tab view

If you want a structured, Wireshark-like view of the traffic, just go to the “MetaCap Viewer” tab and click on the “View PCAP” button:



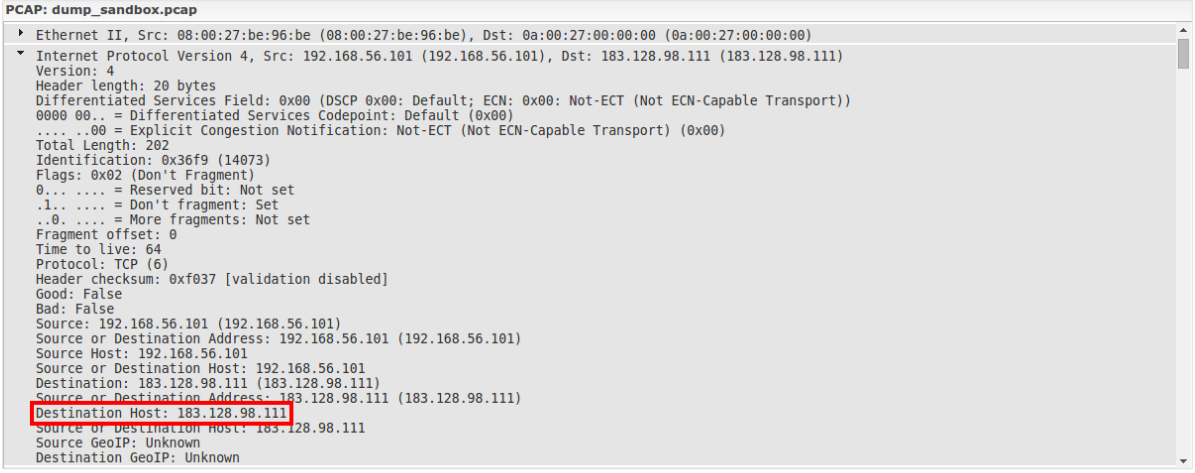
PCAP: dump_honeypot.pcap

PDML created: **Thu Oct 30 08:39:31 2014**

```
▾ Frame 1: frame, eth, ip, udp, dns,
  ▸ Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits)
  ▸ Ethernet II, Src: 08:00:27:be:96:be (08:00:27:be:96:be), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
  ▸ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 192.168.56.1 (192.168.56.1)
  ▸ User Datagram Protocol, Src Port: 43591 (43591), Dst Port: 53 (53)
  ▾ Domain Name System (query)
    Transaction ID: 0xc0db
    Flags: 0x0100 Standard query
    0... .... .... .... = Response: Message is a query
    .000 0... .... .... = Opcode: Standard query (0)
    .... ..0. .... .... = Truncated: Message is not truncated
    .... ...1 .... .... = Recursion desired: Do query recursively
    .... .... .0.. .... = Z: reserved (0)
    .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    Queries
    home.windows-security.su: type A, class IN
    Name: home.windows-security.su
    Type: A (Host address)
    Class: IN (0x0001)
▸ Frame 2: frame, eth, ip, udp, dns,
▸ Frame 3: frame, eth, ip, udp, dns,
```

Figure 26 CRITs dump_honeypot.pcap metacap viewer tab view

Now try to extract the same information from the second PCAP (dump_sandbox.pcap). As you identify additional connections (e.g. the previously mentioned HTTPS connections), remember to create appropriate relationships for them. In the case of this exercise there aren’t any IP addresses that we did not cover yet. You can see the details of the HTTPS connection below.



```
PCAP: dump_sandbox.pcap
▸ Ethernet II, Src: 08:00:27:be:96:be (08:00:27:be:96:be), Dst: 0a:00:27:00:00:00 (0a:00:27:00:00:00)
▾ Internet Protocol Version 4, Src: 192.168.56.101 (192.168.56.101), Dst: 183.128.98.111 (183.128.98.111)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    0000 00.. = Differentiated Services Codepoint: Default (0x00)
    .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 202
    Identification: 0x36f9 (14073)
    Flags: 0x02 (Don't Fragment)
    0... .... = Reserved bit: Not set
    .1.. .... = Don't fragment: Set
    ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xf037 [validation disabled]
    Good: False
    Bad: False
    Source: 192.168.56.101 (192.168.56.101)
    Source or Destination Address: 192.168.56.101 (192.168.56.101)
    Source Host: 192.168.56.101
    Source or Destination Host: 192.168.56.101
    Destination: 183.128.98.111 (183.128.98.111)
    Source or Destination Address: 183.128.98.111 (183.128.98.111)
    Destination Host: 183.128.98.111
    Source or Destination Host: 183.128.98.111
    Source GeoIP: Unknown
    Destination GeoIP: Unknown
```

Figure 27 CRITs dump_sandbox.pcap metacap viewer tab view

3.4 Task 4: Visualize relationships

All the information that you have extracted from the data you loaded can be easily visualized using the relationship service. This will allow you to see connections between the different elements of a campaign. If you created appropriate relationships between the files and extracted objects, you should now be able to freely browse that information using “Relationship service” tab.

First, navigate to the initial e-mail message. You can do this by going to the E-mail view using the Navigation Menu. Then select the “Relationship Service” tab. The relationship graph you see should be similar to the one pictured below.

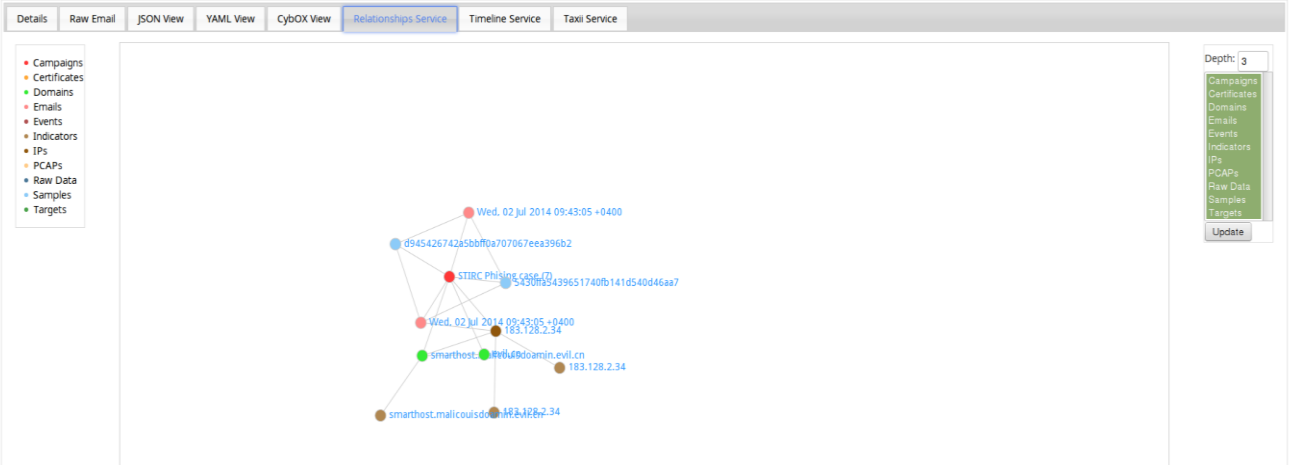


Figure 28 CRITs e-mail "relationships service" tab view (Depth 3)

If you created every object correctly you should see connections between the e-mail, the domain and the PCAP files (labelled using the hash of their contents). Notice that the same malicious e-mail server IP address is used to label two different nodes in the graph: an Indicator and an IP object. You can distinguish them by the colour scheme described in the legend in the upper-left corner.

Now change the “Depth” value in the upper right corner to “1” and click on “Update”. You should see now a smaller graph that includes only immediate connections to the e-mail (e.g. the PCAP files are now filtered out of the view). The new graph is shown below:

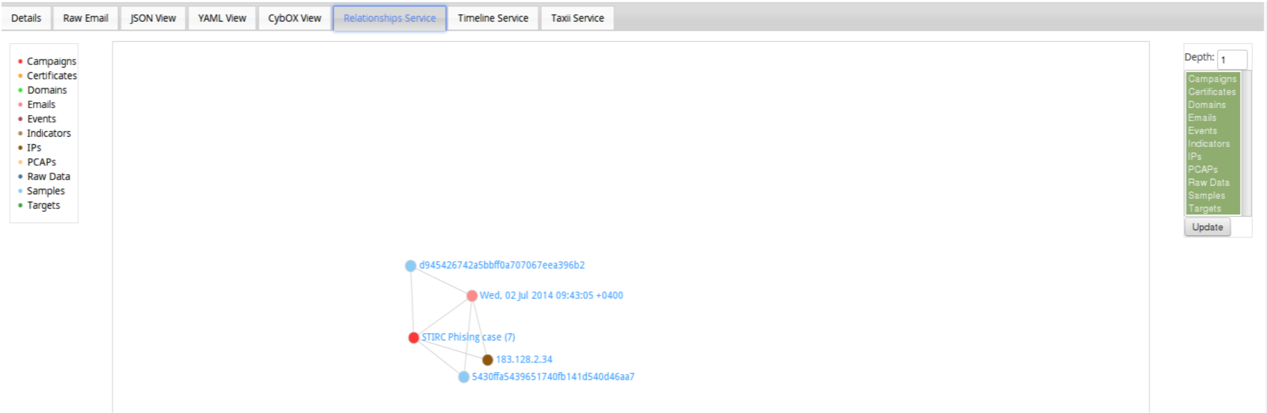


Figure 29 CRITs e-mail "relationships service" tab view (Depth 1)

Next, navigate to the PCAP files to visualize the same relationships from a different perspective. You can do this by going to the PCAPs view (using the Navigation Menu) and, again, going to the "Relationship Service" tab. You will see the relationships pictured for the dump_honeypot.pcap file.

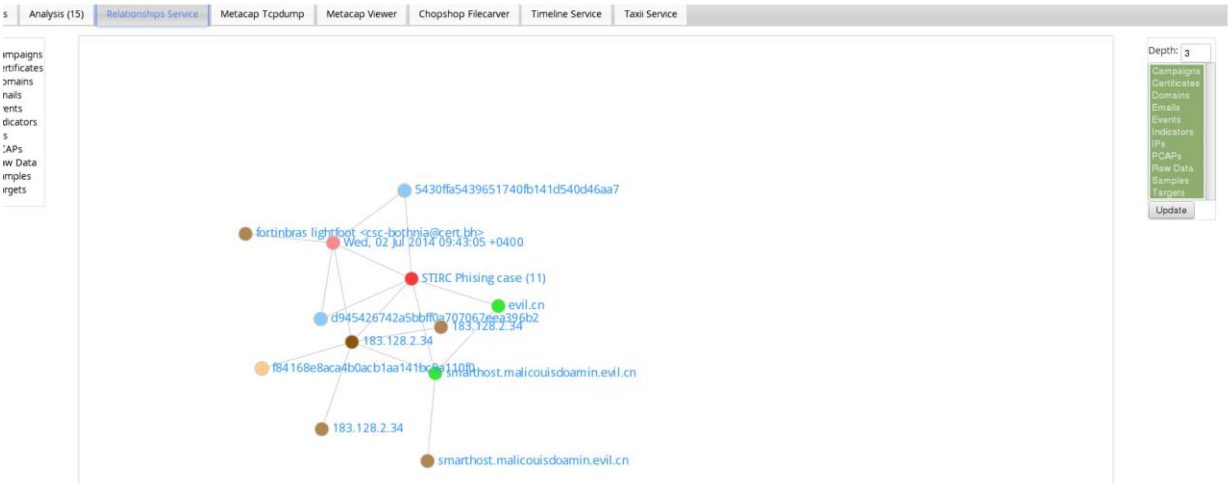

Analysis (15)
Relationships Service
Metacap Tcpdump
Metacap Viewer
Chopshop Filecarver
Timeline Service
Taxii Service
Depth: 3
Update
5430ffa5439651740fb141d540d46aa7
fortinbras lightfoot <csc-bothnia@cert.bh>
Wed, 02 Jul 2014 09:43:05 +0400
STIRC Phising case (11)
evil.cn
d945426742a5bbff0a707067eea396b2
183.128.2.34
183.128.2.34
f84168e8aca4b0acb1aa141bc9a110f0
smarthost.malicouisdoamin.evil.cn
183.128.2.34
smarthost.malicouisdoamin.evil.cn

Figure 30 CRITs PCAP "relationships service" tab view (Depth 3)

You could also filter the graph by adjusting the "Depth" and/or selecting objects types of interest using the box in the upper right corner of the view. If you change the depth to 1, this time you will not see the e-mail message. Then select everything except "Indicators" from the box below "Depth". The result should be similar to the one pictured below:

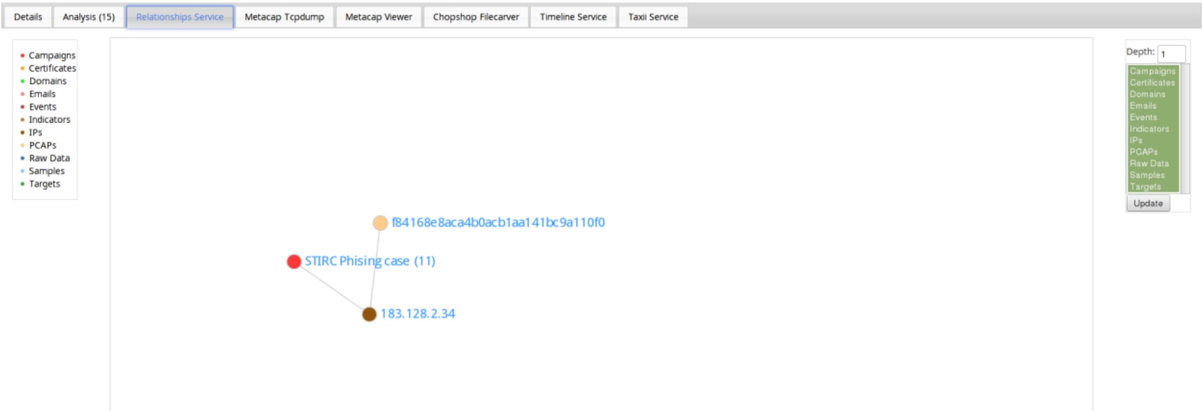


Figure 31 CRITs PCAP "relationships service" tab view (Depth 1)

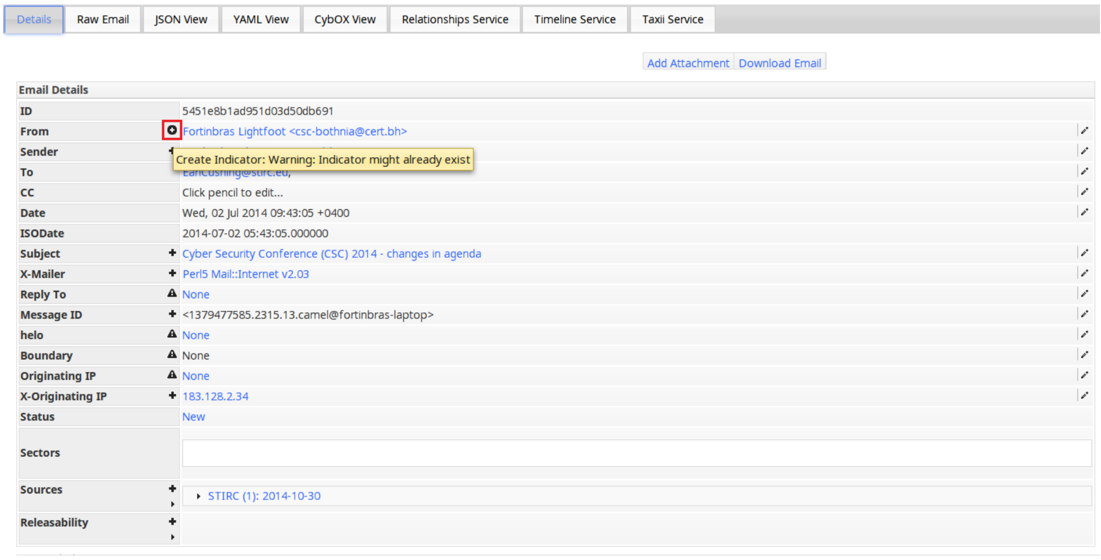
As you can see, the Indicator is also present, but as a kind of “invisible” node, coloured white and unlabelled.

3.5 Task 5: Create indicators

This task, although consisting of simple steps, requires forethought. You must decide which indicators to use for preventive actions, for example to update firewall ACLs. We have already created some indicators from the IP addresses found in the e-mail message, but now let’s consider something a little more complex.

In this task we will consider everything which could reasonably be used as an Indicator in our scenario. You will need to decide what you want to use as a basis for a block, whether it’s a DNS name, an IP address, or even an X-Mailer header. CRITs includes flexible set of Indicator types, as we will see.

For now, don’t worry about precisely which CRITs indicator types to use and instead consider what information is most useful to associate with the campaign. Remember to think through the implications for each candidate indicator. As you’ve seen before, CRITs helps you with the indicator selection task by placing a “plus” sign next to some fields, for example, values in a parsed e-mail message, and IP addresses extracted from PCAP files. This sign is highlighted in the sample screenshot below.



Email Details		
ID		5451e8b1ad951d03d50db691
From	⊕	Fortinbras Lightfoot <csc-bothnia@cert.bh>
Sender	+	
To		EarlCushing@stirc.eu,
CC		Click pencil to edit...
Date		Wed, 02 Jul 2014 09:43:05 +0400
ISODate		2014-07-02 05:43:05.000000
Subject	+	Cyber Security Conference (CSC) 2014 - changes in agenda
X-Mailer	+	Perl5 Mail::Internet v2.03
Reply To	⚠	None
Message ID	+	<1379477585.2315.13.camel@fortinbras-laptop>
helo	⚠	None
Boundary	⚠	None
Originating IP	⚠	None
X-Originating IP	+	183.128.2.34
Status		New
Sectors		
Sources	+	STIRC (1): 2014-10-30
Releasability	+	

Create Indicator: Warning: Indicator might already exist

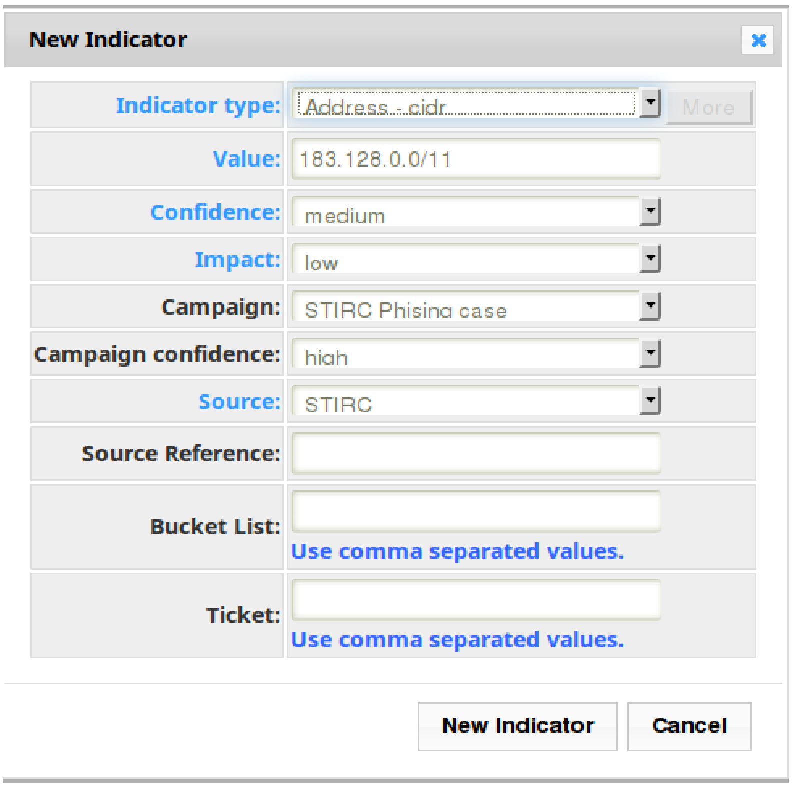
Figure 32 CRITs e-mail details view

The first option available to us is to create an Indicator from the sender email address. Unfortunately, this address is spoofed - it clearly belongs to one of the conference organisers. Hence, it would be pointless to create such an indicator. The same applies to the “From” email address. Analysing the e-mail further, the Subject is also rather generic and might later be used in a normal (i.e. non-phishing) email.

In contrast, X-Mailer seems to be a rather good choice. It looks like only phishing and mailing spam can come with this header. With additional investigation using your mail server you could determine whether this is the case. Hence, we can create an Indicator from it. The next question we will need to answer is what to do with it. We will cover the actions available to us in the next task. For now just click on the plus sign to the left of the X-Mailer value.

A domain that you have added in the second task (smarthost.malicouisdoamin.evil.cn) can also be an indicator, and it can be used to blackhole or sinkhole[6] the C&C domain. We will deal with the actions in the next task.

It is often useful to consider additional context information when deciding on the indicator to use for blocking. For example, for an IP address, you can check the history of the ASN that the IP address originated from, using the bhp.he website (http://bgp.he.net/AS4134) or other reputation service. If the ASN announces bogons[7], it may be worth blocking all of the traffic originating from or directed at that ASN rather than just blocking traffic for the specific IP address. In order to do that you can use "i" shortcut and select "Address - CIDR" as the "Indicator type" (remember to click on "More" before selecting options from the list). The dialog box is pictured below. You can also add the Indicator by clicking on the plus sign to the left of the "Indicators" item in the Navigation Menu.



New Indicator

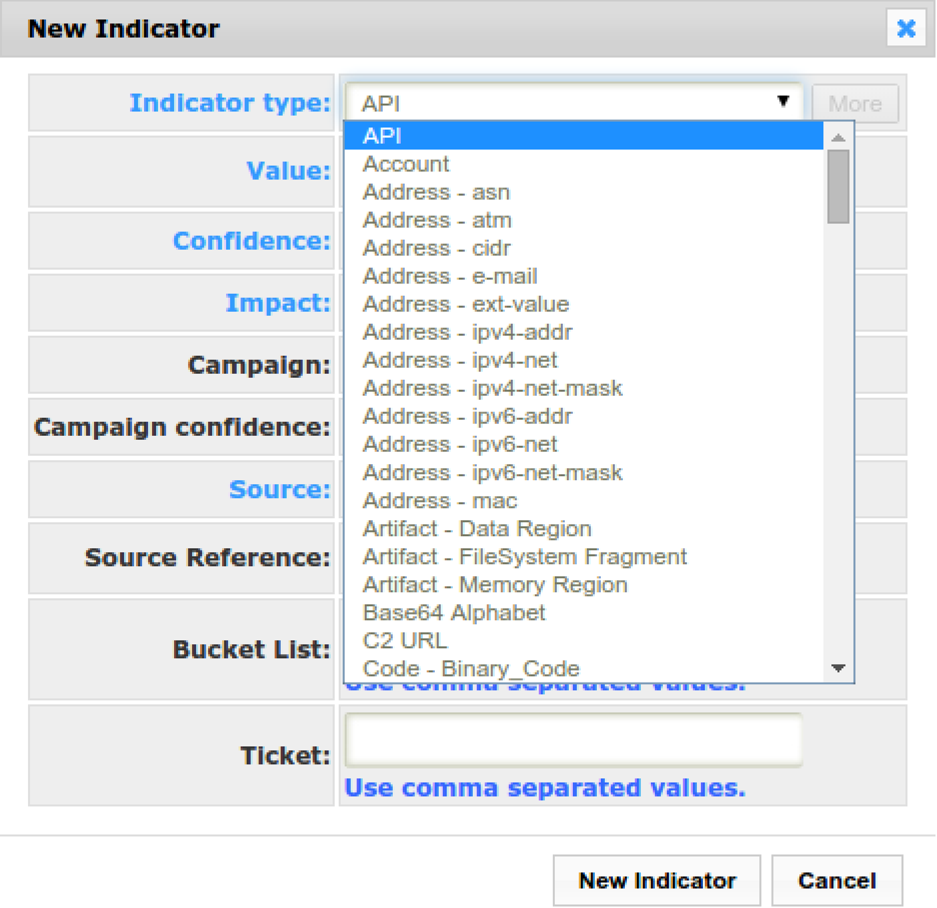
Indicator type:	Address - cidr
Value:	183.128.0.0/11
Confidence:	medium
Impact:	low
Campaign:	STIRC Phising case
Campaign confidence:	high
Source:	STIRC
Source Reference:	
Bucket List:	Use comma separated values.
Ticket:	Use comma separated values.

Figure 33 CRITs Add new indicator window

Although in this exercise we don't explore this, it is important to note that you can also store host-based indicators that have been derived from a malware sample. A wide range of different types of indicators are available in the "Add indicator" dialog box, as we show below:

[6] http://en.wikipedia.org/wiki/Black_hole_%28networking%29

[7] http://www.team-cymru.org/Services/Bogons/



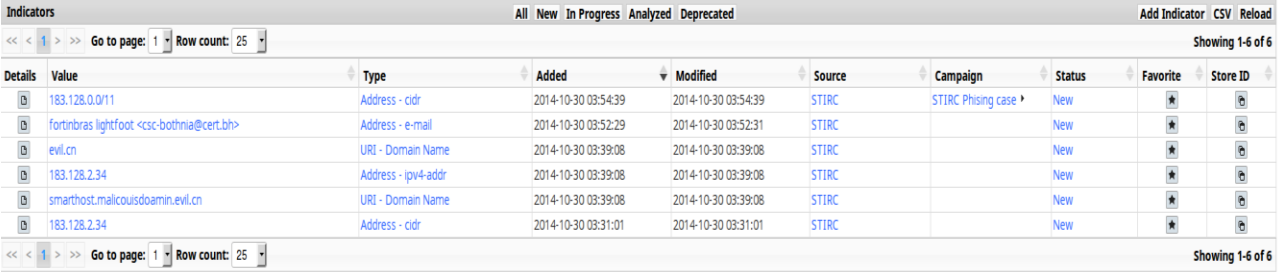
New Indicator

Indicator type:	API
Value:	
Confidence:	
Impact:	
Campaign:	
Campaign confidence:	
Source:	
Source Reference:	
Bucket List:	
Ticket:	Use comma separated values.

Figure 34 CRITs Add new indicator window

We have covered all the indicators available in this exercise. However, in the future, consider reviewing the list above to identify indicator types that may apply to the campaign that you are currently analysing.

Now click on any of the indicators in the Indicators view. You can go to that view (pictured below) using the Navigation Menu.



Details	Value	Type	Added	Modified	Source	Campaign	Status	Favorite	Store ID
	183.128.0.0/11	Address - cidr	2014-10-30 03:54:39	2014-10-30 03:54:39	STIRC	STIRC Phising case	New	★	
	fortinbras lightfoot <csc-bothnia@cert.bh>	Address - e-mail	2014-10-30 03:52:29	2014-10-30 03:52:31	STIRC		New	★	
	evil.cn	URI - Domain Name	2014-10-30 03:39:08	2014-10-30 03:39:08	STIRC		New	★	
	183.128.2.34	Address - ipv4-addr	2014-10-30 03:39:08	2014-10-30 03:39:08	STIRC		New	★	
	smarthost.malicouisdoamin.evil.cn	URI - Domain Name	2014-10-30 03:39:08	2014-10-30 03:39:08	STIRC		New	★	
	183.128.2.34	Address - cidr	2014-10-30 03:31:01	2014-10-30 03:31:01	STIRC		New	★	

Figure 35 CRITs Indicators view

In this view, you can assign “Confidence” and “Impact” values for all of the indicators you have identified. This is crucial for prioritizing the actions you will take. You can use the Confidence value to describe how confident you are that the indicator is effective for flagging malicious activity. It can be assigned one of following values, according to the CRITs documentation[8]:

[8] https://github.com/crits/crits/wiki/Indicators

- Unknown - the default value.
- Benign - it has been determined this Indicator is nothing to be worried about.
- Low - this is something to look out for, but it doesn't need immediate attention.
- Medium - this is something to look out for and attend to as soon as possible.
- High - this is really bad and everyone needs to drop what they are doing to respond.

However, we propose the following, different characterization of the available “Confidence” values. Confidence, intuitively, should be viewed as a measure of how sure you are that this indicator is good. The values below are of course only one of the possible interpretations.

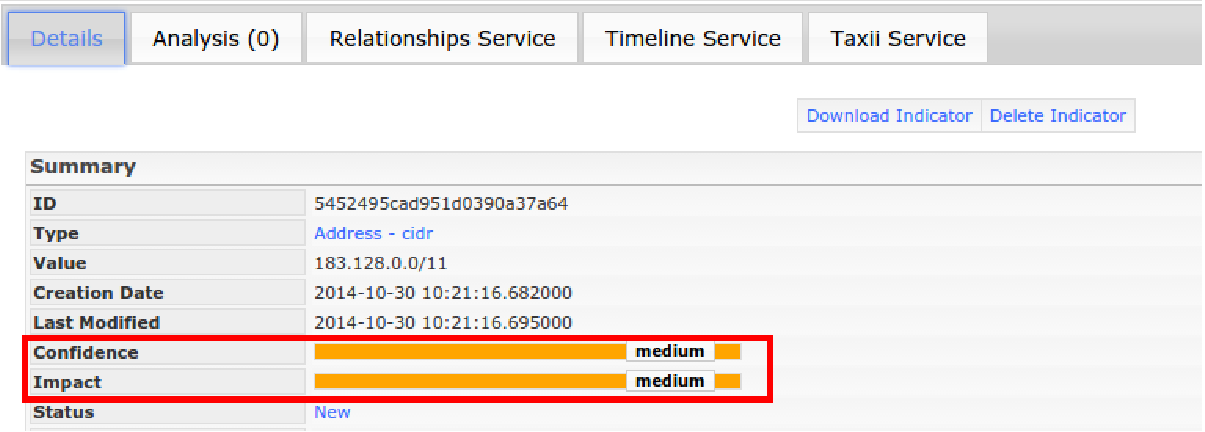
- Unknown - use this value only if you received information from external sources that you cannot verify, and there are no other means of independent verification. For example, in the case when an organization or researcher that you do not know contacts you about a domain connected with a campaign that you study.
- Benign - use only when an indicator has been clearly demonstrated as not corresponding to the malicious activity being analysed. You can also remove such an Indicator to not mess up the view.
- Low - use if you know that the source of this indicator (whether it is a person or an automated tool) has not been consistently reliable in the past, but it is likely that this is an actual indicator. For example, you might mark an indicator that lacks information on how it was derived as “low” confidence when you have no previous experience with the source.
- Medium - use if the source of this information has made some invalidated assumptions, but is using a widely accepted reasoning and/or generalization to derive the indicator. See below for an example. You can also use this for trusted external sources, where you can expect that the information is correct based on experience.
- High - reserve this for an Indicator that you are sure about because you understand exactly how the indicator was derived. For example, you might mark a C&C IP address as “high confidence” when you know it was derived directly from a PCAP file containing malicious traffic.

Impact uses the same values as described above. Impact, intuitively, should measure how much priority you should give to mitigating threats using this indicator. The higher the impact, the more severe the threat. We propose the following interpretation of the values for “Impact”. This is, of course, only one of many possible interpretations.

- Unknown - use only if the impact is hard to estimate. An example would be a domain received from external sources that you did not see included in the campaign that you are analysing.
- Benign - use only if you decide to not take any actions regarding this Indicator. This is different from the previous value, where you did not know if any action is needed. You can also remove such an indicator, but you may consider keeping it for the informational purposes.
- Low - does not require immediate action. Action may be taken later when security team resources are not otherwise committed. This can be because it is really hard to implement this Indicator in your current infrastructure and you are sure that the threat is mitigated via other sources. An example of this would be a specific header in the C&C HTTP response. Maybe you do not have a network device that allows you to inspect HTTP directly and you have already blocked the domain and IP address.
- Medium - it has to be taken up just after the security team finishes their current tasks. An example of this is provided below.
- High - these are the indicators that require immediate action. Only use “high” in cases where the intention is to order the security team to drop everything to address an imminent threat.

An example of this would be an IP address for a host that is actively attacking your network and has to be blocked.

Below there is an example of the Confidence and Impact values defined for the CIDR block indicator we defined earlier for the malicious AS routing traffic from the malicious e-mail server.



Summary	
ID	5452495cad951d0390a37a64
Type	Address - cidr
Value	183.128.0.0/11
Creation Date	2014-10-30 10:21:16.682000
Last Modified	2014-10-30 10:21:16.695000
Confidence	medium
Impact	medium
Status	New

Figure 36 CRITs Indicator details view

This example provides a good illustration of both the “Impact” and “Confidence” attributes. The “Impact” is set to “medium”, because blocking an AS does not have to be immediate. You want to block the offending IP Address right away, but the preventive action of blocking the entire AS can be lower on the priority list. The “Confidence” is set to “medium” because we just assumed that the IP comes from the malicious AS. This was inferred from the fact that the offender came from this AS and that the AS announces bogons. So, this AS may be linked to this campaign, however it is also possible that the attacker simply used a proxy. Hence, we set “Confidence” to “medium”.

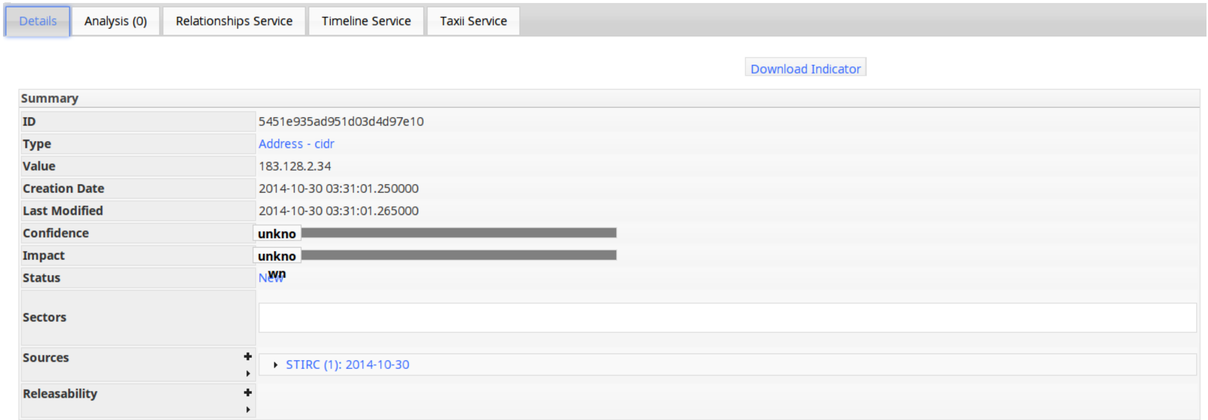
You can change “Confidence” or “Impact” by using the sliders that are on their values. Sliding to the right increases the appropriate level, while sliding to the left decreases it.

You now have actionable information and are prepared to define and take defensive actions, and log them in CRITs. This will be the purpose of your next task.

3.6 Task 6: Apply indicators and log their status

Indicators chosen in the previous tasks have to be applied. While CRITs helps you both with creating the indicators and logging actions performed using these indicators, it does not help you with actually applying them. That part is up to you. Here we will only demonstrate how you can log your actions.

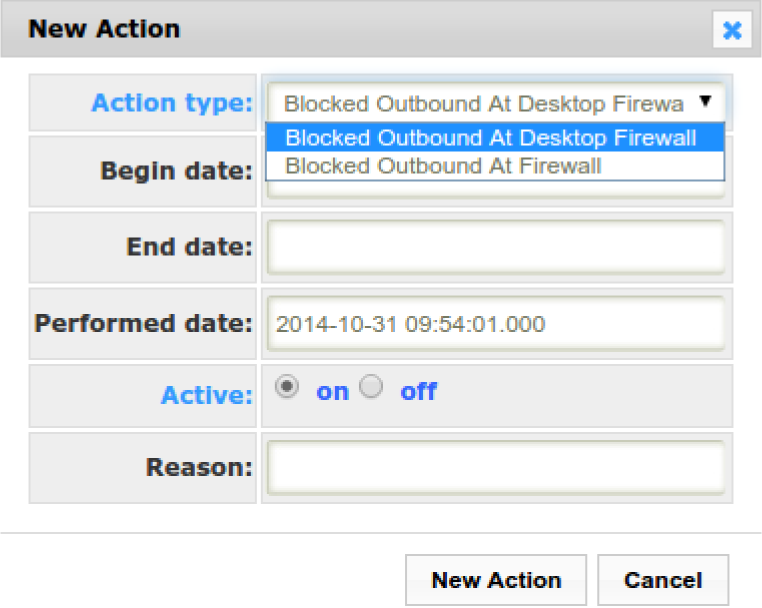
First, open a view on any one of your IP indicators. You will see a number of tables, including the “Actions” table just below the indicator details, as pictured below:



Summary	
ID	5451e935ad951d03d4d97e10
Type	Address - cidr
Value	183.128.2.34
Creation Date	2014-10-30 03:31:01.250000
Last Modified	2014-10-30 03:31:01.265000
Confidence	unkno
Impact	unkno
Status	New
Sectors	
Sources	STIRC (1): 2014-10-30
Releasability	

Figure 37 CRITs IP indicator view

This table will allow you to add descriptions of the actions performed on the specified indicators. Click on the plus symbol next to the table header. You should see a dialog box like the one pictured below:


New Action
Blocked Outbound At Desktop Firewall
Blocked Outbound At Firewall
New Action
Cancel

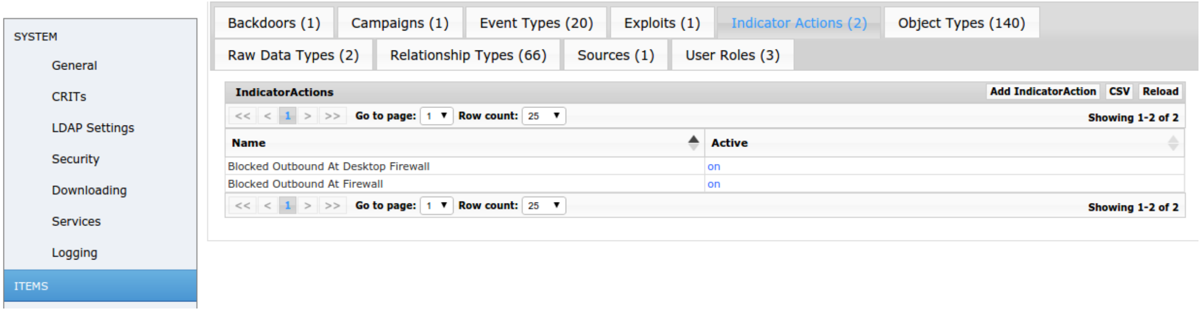
Action type:	Blocked Outbound At Desktop Firewa
Begin date:	
End date:	
Performed date:	2014-10-31 09:54:01.000
Active:	● on ○ off
Reason:	

Figure 38 CRITs Indicator new action window

In the standard CRITs installation there are only two actions available:

- Blocked Outbound At Desktop Firewall,
- Blocked Outbound At Firewall.

You can see these actions and add new ones in the “Items” view of the “CRITs Control Panel” by going to the “Indicator Actions” tab, as pictured below. You will have to do this while logged in as an administrator.



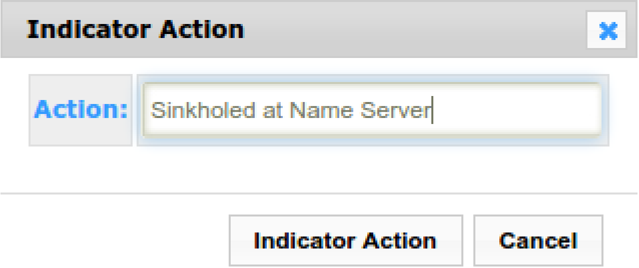
IndicatorActions

Showing 1-2 of 2

Name	Active
Blocked Outbound At Desktop Firewall	on
Blocked Outbound At Firewall	on

Figure 39 CRITs Control panel items view

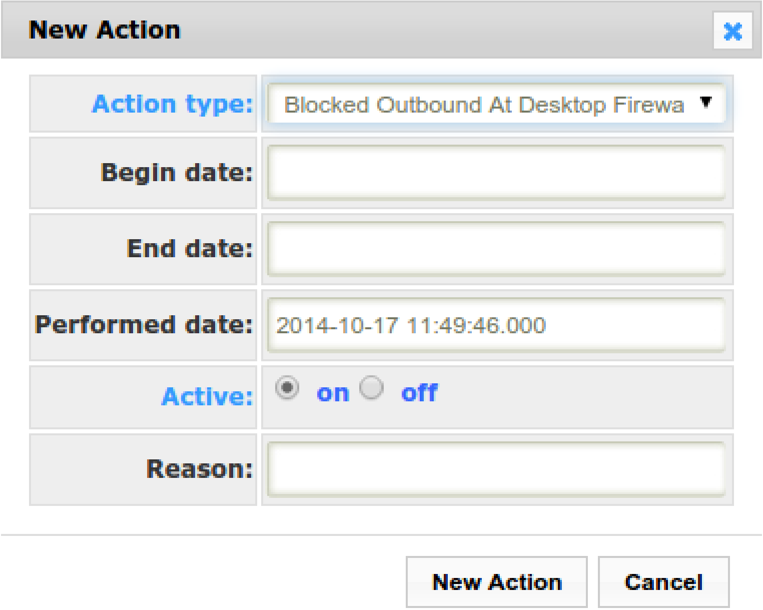
Click on the “Add Indicator Action”. You have to provide the Action name, like “Sinkholed at Name Server” or “Blackholed at Name Server”, like pictured below. By customizing these actions you can tailor them to your network configuration.



Action: Sinkholed at Name Server

Figure 40 CRITs Indicator action window

Try to add a new action to one of the indicators. Go back to the IP indicator view and click on the plus sign next to the “Actions” table. You can see that there are several fields for information about the actions taken.



Action type:	Blocked Outbound At Desktop Firewa ▼
Begin date:	
End date:	
Performed date:	2014-10-17 11:49:46.000
Active:	● on ○ off
Reason:	

Figure 41 CRITs IP indicator new action window

The “Begin date” and “End date” specify the time period during which the defensive measure will be active. “Performed date” in most cases will be the same as the “Begin date”, but in some network environments it may require some time before the measure becomes active. For example when you try to sinkhole a domain, its TTL may make it impossible to sinkhole right away. You may have to wait up to a day before the sinkhole is capturing all of the connections. In such a case these fields will have different values. “Active” is self-explanatory, flagging whether the measure is currently active. After some time you can turn the action off, if you think that it is no longer needed. All of this dates and the “Active” settings are purely informational and used to log your actions.

“Reason” is also a self-explanatory field and is not mandatory. In some cases, for example, blocking an IP address at a firewall, the reason for an action can be inferred from various other information that is already present in CRITs.

Now that you are familiar with how CRITs handles action logging you can go through the list of indicators you created in the previous task and assign actions to them. Remember that you do not have to limit yourself to existing action types - any new action can be easily added by the administrator.

First, consider the domain name that was used for the C&C server. The most obvious choice is to sinkhole it. This can be done by changing a DNS server configuration so that it will return a different, predefined response for all queries that ask for home.windows-security.su. You can also blackhole it (i.e. return the NXDOMAIN response).

Second, consider the IP addresses. Again there is an obvious choice: block them at the firewall. However, there is also a less obvious choice that would require a lot of additional work. You can redirect the traffic to a specially crafted honeypot server. In this way you will deceive the attackers and learn their objective by closely monitoring the honeypot environment.

The X-Mailer header value could be used as the basis for blocking incoming mail at the SMTP server. However, it would probably be more appropriate to mark messages with this header as spam. This can be done using the appropriate spam filter configuration in your local mail system.

Finally, we consider last of our indicators, the ASN associated with the mail server. There are a few ways to tackle this problem. First, you can of course just block all of the communication with this AS. In some cases this approach may be problematic since users will not have access to any web servers hosted in this AS, including legitimate ones. In our particular case this is a Chinese AS that announces bogons, so it’s unlikely blocking the AS will elicit complaints from users.

There is another, somewhat less popular, approach. You can choose to tarpit[9] the AS, giving you more time to act and possibly reducing data leakage. In cases where a limited set of users have to access the AS for some reason, but you want to rate limit traffic to this AS, this can prove to be very successful, even if it is unpopular. You can also redirect all of the traffic incoming from the AS to a segregated honeypot server. However, like the previous case, this can be time consuming and assumes you have the resources to monitor the honeypot for attempted attacks.

4 Conclusions

During the course of this exercise you learned how to leverage CRITs to visualize relationships among different elements of a campaign. Of course, this will be even more useful once you have begun to populate CRITs with information from multiple campaigns. As the information you manage

[9] Tarpitting is a group of techniques used to purposely delay the incoming connections. The idea is that the delayed connections will prove less effective for spammers and computer worms. The delay can be implemented at the IP level, TCP level or at the SMTP level.

becomes richer it will enable you to identify relationships among campaigns, highlighting common IP addresses, domain names and malware samples.

You have also learned how to extract indicators from incident data, develop mitigation actions, and track those actions. The hope is that by taking a more structured approach to indicator management you will ultimately be better equipped to secure your network.

5 Tools

Name	Version	URL	System	Category
CRITS	3.1.0	http://crits.github.io/	GNU/Linux	Threat Intel
Virtualbox		http://www.virtualbox.org	GNU/Linux	Utils

6 References

1	http://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375
	https://www.enisa.europa.eu/activities/cert/support/data-sharing

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu