Mini NCAC Challenge

This is condensed version of the NCAC challenge. It should take a little less than 3 hours to complete as opposed to 50 hours. Thus, a lot of the data will be reducted and hints/pointers will be given.

The data can be downloaded here.

Instructions / Indicators

The FBI called to inform you they noticed traffic from your company to a known bad APT drop site. Details were sketchy and sparse as usual; however, the FBI indicated that it observed a file “d.7z” being transferred. No analysis of the contents of the file was conducted (or they didn’t care to share).

Although there is no evidence the attackers used email as a delivery vector, the FBI indicated this particular adversary regularly uses career-type themes to target job seekers and HR personnel. Previously observed email Subjects were:

“Your CV has been updated”
“Take career to your level next”
“Tried of grind”
“opportunity waits”

No other information is available at this time.

Question 1

Q: The file "d.7z" was retrieved from this external IP address.

Question 2

Q: In aQddition to d.7z these three other zip files were stored to an external source at about the same time

Question 3

Q: This exe file was retrieved from the same IP address

Question 4

Q: A user downloaded an executable while browsing a career themed watering hole with related to the malicious IP. The domain of that website is:

Question 5

Q: The name of the malicious executable is

Question 6

Q: This external IP address is also associated with the domain mentioned above

Question 7

Q: The hash of the file is

Question 8

Q: The executable is a strain of this Remote Access Tool

Question 9

Q: The user also downloaded two script that would automate ftp tasks. The scripts are named name ___.txt

Question 10

Q: The adversary IP Address 60.235.12.64, performed some reconnaissance on SICCO INC before the attack. Based on the blog ____ is the leading APT detection software developed by SICCO, Inc:

Question 11

Q: Sicco Inc. launched a partnership with this company in order to develop the Vortex product.

Question 12

Q: The president & owner of that company is named

Question 13

Q: Several Sicco Inc employees received an email atttachment which Diggler claims he never sent. The name of that attachment is:

Question 14

Q: There were 4 recipients to the mysterious attachments. Their email addresses are:

Question 15

Q: A legitimate email from Dirk Diggler (dirkdiggler853) would normally come from this email server

Question 16

Q: The spoofed message from Diggler came from this mail server
Hint: The email containing only the pdf attachment and a vague message sounds spoofeed. Check the email headers.

Question 17

Q: The attachment in encoded in:

Question 18

Q: The pdf says:

Question 19

Q: The hash of the file is:

Question 20

Q: This employee actually downloaded the pdf attachment

Question 21

Q: The adversary (203.57.206.173) downloaded a series tools on this user's machine

Question 22

Q: The adversary's tools were stored in this folder: C:\Windows____\

Question 23

Q: During the Adversary's command and control sessions, they used this Helpdesk password to run the psexec process

Question 24

Q: The adversary dumps system/user passwords in this file:

Question 25

Q: The adversary exfiltrated this employee's emails by first consolidating them in a file called _____.pst

Question 26

Q: The employee in questions is: