Sr. No.	Activity
1	Fill incident response interview question list on site project
2	Log analysis
3	Areas to look for
4	Traffic insepection using wireshark
5	Inspect prefetch folder
6	Anaylze passkey
7	Check registry entry for 'run' file
8	FInd malware fingerprint using memory analysis
9	Inspect all DNS queries made from the target system
10	Nslookup all the Ip address identified to which the malware is trying to connect
11	Inspect all 3-way handshakes using TCP streams
12	Reversing firmware using binwalk
13	MD5 signature analysis
14	Analyze malware using Hex Editor Neo
15	Configure snort for analyzing targetedports for the attack
16	To detect the type of packer or compiler employed to build an application
17	Check for all HTTP/HTTPs port traffic in wireshark
18	Use virustotal to scan the signature of well known malware
19	Check user profile data
20	Inspect open ports
21	Examine running processes
22	Identify malware using volatility framework
23	Inspect exported DDLs files for running suspicious process
24	Inspect DOS commands with doskey
25	Identify available shares on the system
26	Check web browser download folder
27	Check browser for malicious addons
28	Analyze browser cookie files

29	Run automated tools
40	Check if the suspicious files are self-extracting executables or not
31	Open suspicious files in notepad++ for further analysis
32	Check if any suspicious file makes TCP connection with any foreign address
33	Find ISP and other information of suspicious foreign address
34	Check for the startup programs
35	Upload suspicious file on online malware analysis sandbox
36	Navigate to suspected domain
37	Create encrtypted/encoded backdoors
38	Identify malware author's developer e
39	Identify for the details section of the r
40	Check for leak information about the
41	Identify micro and mini activities of Po
42	Identify how and from where malware
43	Identify how many infections are bein
44	Identify which malware delivery mech
45	Identify the naming convention of all t
46	Identify sites that are compromised to
47	Identify for language ID when a versio
48	Identify for leaked assert path and ex
49	Identify the C&C server used, IPs, Se
50	Identify searching patterns and exten
51	Identify malware code samples with p
52	Identify malware compilation time and
53	Check registry entry for 'run' file.
54	Inspect traffic using Wireshark, espec
55	Inspect all DNS queries to identify po
56	Identify the main characteristics of ma
57	Identify malware attributes such as fu
58	Perform malware execution in the saf

Tools
Manual 1) Field interview questions – spreadsheet 2) Field notes – spreadsheet
1) Manual 2) Installed products by vendors (IDS/IPS/Firewall/Proxy etc.)
N/A
Wireshark
Manual
Manual
Manual
WinHex
Wireshark
1) Windows Command Prompt 2) Windows Poweshell
Wireshark
Binwalk
md5sum
Hex Editor Neo
snort
PEiD
Wireshark
https://www.virustotal.com/
Manual
1) Nmap 2) Manual
1) Process Explorer 2) Tcpview 3) Autorun 4) Windows shell prompt – 'tasklst'
Volatility framework
DLLExport viewer
Windows shell command – doskey
Windows shell command – net share
Manual
Manual
1) Galleta 2) Mozilla cookies view

1) TDSSkiller from Kaspersky 2) Malwarebytes antimalware
Manual
Manual
Netstat
whois tools (Online tools)robtex
Start > Run > msconfig > Startup
1) malwr.com 2) anubis.iseclab.org
1) Manual 2) Burpsuite
1) Empyre Framework 2) Veil Framework

nvironment intensively.
nalware stub via property information
third-party libraries installed paths. C
owershell scripts.
stubs are being downloaded.
g downloaded to infect victim's mach
anism is used.
the files being downloaded by the ma
host the malware on them. Identify
n resource is compiled to a library. T
ternal blog references. Some librarie
rvers.
sion lists when malware is searching
reviously used malware in the past.
d date.

cially for all HTTP/HTTPS outgoing tr
ssible exfiltration activities.
alware sample including size, type, c
nctionalities, inner workings, strings,
fe environment and perform runtime

How to do
Ask for the incident response interview question sheet and fill the relevent data in it. It looks professional and it also help to plan your investigation.
Check for the below areas from where we can find the source of alert1) User may complain/alert about suspicious activities going on in his/her system2) Proxy logs & alerts3) Firewall logs4) SIEM logs & alerts (IDS/IPS etc.)5) End point protection alerts (Macfee/Sophos/Symentic etc.)
These are the below ares which are too look for malware analysis1) User profile2) Registry run keys3) Prefetch folders4) Browser history and caches
1) See info field for any malicous activit name2) See info field for any unknown service name3) Analyze port specific traffic using belowfilter:tcp.port==4434) Analyze TCP stream after that4) Check all HTTP POST reqeust which may click and send system screenshot to some domains in background maliciously - Filename may contain .jpg extension within POST request.5) Navigate to the path of the screenshot which is being
1) Inspect prefetch folder for suspicious file traces.
1) use attrib -s -h -r -a * command in C drive first.2) analyze C:/RECYCLER folder3) Hunt all isntances for the malware detection using manual method or 'search' feature of windows OS.4) Remove identified malware
1) Navigate to HKCU\Software\Microsoft\Windows\CurrentVersion\RunHKLM\Software\Microsoft\Windows\CurrentVersion\
1) Open malware in WinHex2) Find any unique signature which can help later on to analyze malware further using internet resources.
1) Find DNS entries for Domain Name System(Query)2) Find DNS entries for Domain Name System(Resposne)Filter: dns
1) Run following commandnslookup X.X.X.X2) If domain is registred then find the relevent information
1) Find SYN-SYN/ACK-ACK and PSH-PSH/ACK-ACK conversation.2) Right click on packet and select the option "Follow TCP Stream".3) Right click on packet and select the option "Follow UDP Stream".4) Analyze the result.
1) use binwalk tool in Kali for signature detection and othe information too.
1) Use mdfsum chintan.exe command to calcualte the hash value.2) Do it same for the original build of that software and compare it.3) Google mdf signature hash value.
1) Open mawlare in hex editor neo2) Try to find mawlare traces (signature, company, induvidual name,
1) Installa and configure snort2) Create a rules set for snort3) Run the snort4) Analyze the result by reading log file
1) Open physical build exe file in PEid tool.
1) Run wireshark with active interface2) Type “http” in the filter and analyze each request carefully.3) Identifiy suspicous URL requests.4) Send those URL to virustotal.com in two form a. Give homepage of the URL b. Give the exact location of the URL taken from wireshark5) Analyze the result.
1) Open suspicious file on www.virustotal.com and analyze the result.
1) Gather user profile's data from below location.
1) Run nmap on localhost to determine open ports and servicesnmap -sV localhost2) run netstat command with -ano and -anb option in windows command shell and analyze the result.3) Corelate open ports with
1) Run process explorer tool. Go to Tools tab and select image verification/verify images. Detect for unknown suspicious vendor file running process. Also inspect all pink and red marked running process.2) Inspect all red and pink marked running process.3) Send doubtful files to virustotal.com and analyze the reuslt.4) Run tcpview to identify current process state along with port number and service.5) run 'tasklist' command for analyzing
1) Run following commands in order to analyze the operating system's state. a. plist: Gives comprehensive list of running processes b netsscan/conscan: Displays connections in memory and tries to tie with the process. c. psxview: Try to identify hidden processes d. malfind: Look certain malicious charactristics of specified Process
In order to inspect the previously given dos commands on windows systems, give 'doskey/history' command.
In order to inspect drive/folder sharing give dos command as 'net share'
Check all web broswer's default download folder or custom download folder location. Analyze files with
Check all browsers in order to inspect any installed malicious unnecessary addons.
Analyze cookie files with virustotal and winhex tools.

Run these tools. Save log file. Take Pocs by visitng particular folder. Scan those suspicious files with www.virustotal.com. Save result as pocs. Qurantine files with scanners. If not removed, then remove manually
Double click on the file and analyze in the same folder for number of new files generated after double clicking the original build.
Sometimes applications such as VBS, BAT may have self replicating and extracting code. Those should be analysed manually.
Many times malicious script runs services.exe service located at C:\Windows\Win\Services.exe -i . It creates TCP connection to the outerworld which needs to be analysed using netstat command.
Find ISP and location of suspicious foreign address via whois tools for further investigation.
Check if any malicious programs placed in startup entries or not.
Analyse below things1) String analysis2) Behavioural analysis3) Network analysis (To which domains this suspicious files interacts with)4) Number of registry entries created5) Number of various files created in sub
Find any juicy information which can help to solve your analysis case. Also try to find other evidences which can strongly emphasize your investigation.
Use both frameworks to create your encrypted payloads in order to bypass the signatures. Never submit those payloads to virustotoal.com and any other websites to scan.

. This may contain misleading data too.
ross-validate/check this information on public references to find sites/forums/blogs that mentic

ine. (Attackers try to brute-force their infections on victim's machine in case if one doesn't wo

lware stub and link it with any historical ATPs.
CMS, version, country and other properties of the website. This helps determine whether ATF
'his may contain OS artefacts taken directly from the Visual Studio.
s used the "assert()" mechanism to help the developers debug unexpected conditions.

juicy information before the exfiltration process starts.
Try to determine ATP campaign.

affic.

ompiler, cryptographic hash.
API calls, and other metadata.
nonitoring to collect artefacts such as processes it interacts with, file systems, registry activitie

groups have found any zero-day in any particular CMS to compromise the server and hos

st malware stubs on it.