1.What is the IP of the organization&DNS server/s?\*

* DNS: 172.16.1.10 (local), 8.8.4.4(Public)
* Org. IP Address: 172.16.0.0

2. What is the name of the malicious file/s downloaded by the accountant?\*

* dotnettojs.hta
* 764796-1652561297.exe

3. What is the sha256 hash of the downloaded malicious file/s?\*

* dotnettojs.hta:

SHA-256 : 64adf742707b89faa233c976e63338e5fb75eadd86d7d38139f2b5f4f32c7d72

* 764796-1652561297.exe:

SHA-256 :77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

4. What is the name of the malware/s, according to BitDefender?\*

* dotnettojs.hta: JS : JS:Trojan.Agent.CSOU
* 764796-1652561297.exe : Generic.Ransom.Hive.A.3532D023

5. What is the malware type of the malicious file/s?\*

* dotnettojs.hta : Trojan
* 764796-1652561297.exe : Ransomware

6. What is the malware family of the malicious file/s?\*

* dotnettojs.hta: : Trojan:JS/Agent family
* 764796-1652561297.exe : Hive Ransomware Family

7. What are the used TTP/s according to the MITRE ATT&CK framework for malicious file/s?\*

1- Hive Ransomware TTPs (764796-1652561297.exe );

* Reconnaissance [TA0043]
  + Gather Victim Identity Information [T1589, T1591]:
  + Phishing for Information [T1598]
* Initial Access [TA0001]
  + Phishing [T1566]:
  + Remote Access [T1219]
* Defense Evasion [TA0005]
  + Valid Account [T1078]
* Exfiltration [TA0010]
  + Exfiltration over Web Service [T1567]
* Phishing emails including malicious attachments to gain initial access and then taking control of Remote Desktop Protocol (RDP) to move laterally.
* After compromising the network, it looks for and terminates all the process related to backups, anti-virus, and copying of files to increase the chance of success.
* After encryption the file ends with .hive extension. The attacker leaves a ransom note in each affected directory inside the system which includes all the instruction related how to pay for the decryption software.
* The ransom note which threaten to leak the victim data on tor website “HiveLeaks”.
* Hive Ransomware uses phishing emails including malicious attachments to gain initial access and then taking control of Remote Desktop Protocol (RDP) to move laterally.
* Behavioural Analysis via Sandbox
  + Drops hive.bat and shadow.bat
  + Shell Commands;
    - %SAMPLEPATH%
    - %ComSpec% /c hive.bat >NUL 2>NUL
    - timeout 1
    - %ComSpec% /c shadow.bat >NUL 2>NUL
    - vssadmin.exe delete shadows /all /quiet
  + Processes Terminated;
    - 2120 - "C:\Program Files\Windows Media Player\wmpnetwk.exe"
    - 2108 - C:\Windows\system32\cmd.exe /c hive.bat >NUL 2>NUL
    - 2264 - C:\Windows\system32\cmd.exe /c shadow.bat >NUL 2>NUL
    - 1536 - vssadmin.exe delete shadows /all /quiet
    - 2684 - C:\Windows\system32\vssvc.exe
  + Files Written;
    - C:\Windows\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\UPnP Device Host\upnphost\udhisapi.dll
    - C:\Users\<USER>\Downloads\hive.bat
    - C:\Users\<USER>\Downloads\shadow.bat
    - C:\ProgramData\Microsoft\Windows\Start Menu\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\7-Zip\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Tablet PC\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Adobe\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Adobe\Adobe Download Manager\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Games\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Graphviz 2.38\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Graphviz 2.38\Manuals\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Java\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\LibreOffice 6.4\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Maintenance\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Tablet PC\HOW\_TO\_DECRYPT.txt
    - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\VideoLAN\HOW\_TO\_DECRYPT.txt
    - C:\Users\Default\HOW\_TO\_DECRYPT.txt

2- JS Trojan (dotnettojs.hta)

* Techique: T1059.007, Procedure: S0283
  + Adversaries may abuse various implementations of JavaScript for execution. JavaScript (JS) is a platform-independent scripting language (compiled just-in-time at runtime) commonly associated with scripts in webpages, though JS can be executed in runtime environments outside the browser.
  + Adversaries may abuse various implementations of JavaScript to execute various behaviors. Common uses include hosting malicious scripts on websites as part of a Drive-by Compromise or downloading and executing these script files as secondary payloads. Since these payloads are text-based, it is also very common for adversaries to obfuscate their content as part of Obfuscated Files or Information.

8. What are the payload/s for web application threats?\*

* SQL Injection Payload: ?action=mec\_load\_single\_page&time=2)+AND+(SELECT+7710+FROM+(SELECT(SLEEP(5)))ondl)+AND+(9419%3d9419
* XSS Payload:

%3Cscript%3EaIert(%27xss%27)%3C/script%3E ---- (<script>aIert(‘xss’)</script>)

9. What are the affected product/s for web application threat/s?\*

* Apache/2.2.31 (Ubuntu)
* WordPress Ajax

10. If it exists for web application threats, what are the CVE and CWE number/s of the webapplication threats?\*

* Apache Tomcat Cross-Site Scripting (XSS) ---– CVE-2019-0221 CWE-79
* WordPress 'admin-ajax.php' SQL Injection --------CVE-2007-2821 CWE-89