1.What is the IP of the organization&DNS server/s?
*
2. What is the name of the malicious file/s downloaded by the accountant?
*
3. What is the sha256 hash of the downloaded malicious file/s?
*
4. What is the name of the malware/s, according to BitDefender?
*
5. What is the malware type of the malicious file/s?
*
6. What is the malware family of the malicious file/s?
*
7. What are the used TTP/s according to the MITRE ATT&CK framework for malicious file/s?
*
8. What are the payload/s for web application threats?
*
9. What are the affected product/s for web application threat/s?
*
10. If it exists for web application threats, what are the CVE and CWE number/s of the webapplication threats?
*