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

organization: 192.168.1.10, Server172.16.1.10

1. What is the name of the malicious file/s downloaded by the accountant?

764796-1652561297.exe

1. What is the sha256 hash of the downloaded malicious file/s?

sha256: 77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

1. What is the name of the malware/s, according to BitDefender?

BitDefender: Generic.Ransom.Hive.A.3532D023

1. What is the malware type of the malicious file/s?

Type: Ransomware

1. What is the malware family of the malicious file/s?

Family: Register-hive

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

Impact/Data Encrypted for Impact/ <https://attack.mitre.org/tactics/TA0040/>

Persistence/T1543-Create or Modify System Process: Launch Agent/S0235 CrossRAT/https://attack.mitre.org/software/S0235/

1. What are the payload/s for web application threats?

XSS: %3Cscript%3EaIert(%27xss%27)%3C/script%3E (encoded)

SQL Injection: wp-admin/admin-ajax.php?action=mec\_load\_single\_page&time=2)+AND+(SELECT+7710+FROM+ (SELECT(SLEEP(5)))ondl)+AND+(9419%3d9419

1. What are the affected product/s for web application threat/s?

Register.hive files,

WordPress

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

**CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')**

This attack includes a GET request to WordPress Modern Events Calendar Lite SQL Injection attack. The Modern Events Calendar Lite WordPress plugin before 6.1.5 does not sanitize and escape the time parameter before using it in a SQL statement in the mec\_load\_single\_page AJAX action, available to unauthenticated users, leading to an unauthenticated SQL injection issue. Furthermore, this vulnerability is marked as CVE-2021-24946.