1-
172.16.1.10
8.8.4.4

2-764796-1652561297.exe dotnettojs.hta

3-
1) 77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

2) 64adf742707b89faa233c976e63338e5fb75eadd86d7d38139f2b5f4f32c7d72

4-
Generic.Ransom.Hive.A.3532D023
JS:Trojan.Agent.CSOU

5-
Ransomware
Trojan

6-
Hive ransomware
Cactus torch

7-

Tactics

1)Execution (ID: TA0041)
2)Discovery (ID: TA0032)
3)Impact (ID: TA0034)

Techniques

1)Command and Scripting Interpreter (ID: T1059) (Tactics = Execution)
1.1)Windows Command Shell (ID: T1059.003) (Tactics = Execution)
2)Query Registry (ID: T1012) (Tactics = Discovery)
3)System Information Discovery (ID: T1082) (Tactics = Discovery)
4)Inhibit System Recovery (ID: T1490) (Tactics = Impact)

Procedures

1)Starts CMD.EXE for commands execution (2) (Techniques = Command and Scripting Interpreter) (Tactics = Execution)
2.1)Checks supported languages (3) (Techniques = Query Registry) (Tactics = Discovery)
2.2)Checks supported languages (31) (Techniques = Query Registry) (Tactics = Discovery)
2.3)Reads the computer name (1) (Techniques = Query Registry) (Tactics = Discovery)

2.4)Reads the computer name (1) (Techniques = Query Registry) (Tactics = Discovery)
3.1)Checks supported languages (3) (Techniques = System Information Discovery) (Tactics = Discovery)
3.2)Reads the computer name (1) (Techniques = System Information Discovery) (Tactics = Discovery)
4)Deletes shadow copies (1) (Techniques = Inhibit System Recovery) (Tactics = Impact)

8-
1) SQL Injection :/page876475/wp-admin/admin-ajax.php?action=mec_load_single_page&time=2)+AND+(SELECT+7710+FROM+(SELECT(SLEEP(5)))ondl)+AND+(9419%3d9419
2) XSS :
/page451444/printenv.shtml?%3Cscript%3EaIert(%27xss%27)%3C/script%3E

9-
1) Apache Tomcat
2) WordPress Woocommerce

10-
Xss CVE : Cve-2019-0221
SQL Injection : Cve-2022-0783