1-
192.168.1.10
172.16.1.10
8.8.4.4

2-764796-1652561297.exe ad0hgkeeb.dll encryptor_win32.exe 00007509.exe

3-
1) 77a398c870ad4904d06d455c9249e7864ac92dda877e288e5718b3c8d9fc6618

2) b591dc8c24be6c3a41e5b7270100a396c98accd62b54ff73c134373f16857cf6

4-
Generic.Ransom.Hive.A.3532D023

5-Ransomware

6-Trojan

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
2) Html injection

9-
1) Microsoft ASP .NET Framework 2.0.50727.42
2) Chrome/97.0.4692.71

10-
Html injection CVE : CVE-2006-7192
SQL Injection : CVE-2022-0292 CWE-358 - Improperly Implemented Security Check for Standard