# Incident Report

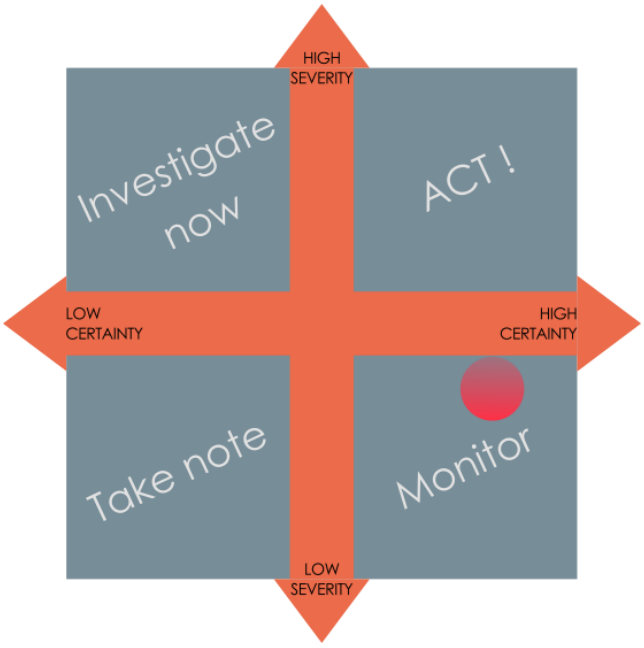
**Codice report**: IRLM_002 **Tipologia**: Port Scan

**Reprting time:** 24/09/2015, 17:00

**Incident time**: 24/09/2015 between14:30 and 14:35

**Analyst**: Mark Reynolds **Reviewer**: Martin Dean

**Action matrix**:



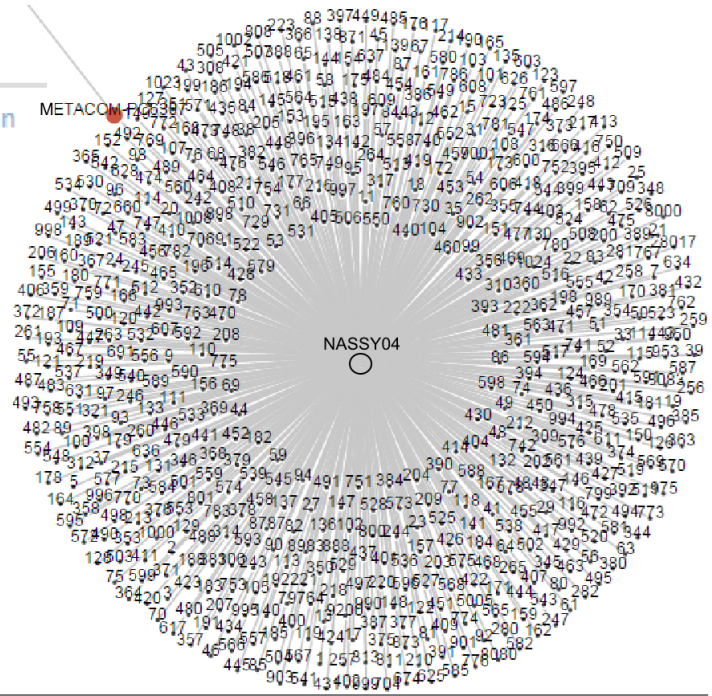

**Analysis**: aramis has detected that the machine METACOM-RS6703 (IP: 172.16.102.23) has performed a Port Scan on the server NASSY04 (IP: 172.16.2.19) contacting 1288 different ports in less than 8 minutes.

| DATE | ADS | TYPE |
|---|---|---|
| Sep 24, 2015 14:31:38 | aramis-demo | Port Scan |

| IP SOURCE | IP DESTINATION |
|---|---|
| 172.16.102.23 | 172.16.2.19 |

MESSAGE

172.16.102.23 scanned at least 17 unique ports of host 172.16.2.19 in 0m1s




Sep 24, 2015 14:30 - 14:32

# Incident Report

**Further details**: this kind of attack is typically associated with discovery activities that attackers usually carry out prior to a proper attack.

In this case, we have noticed 674 HTTP-GET requests, of which 180 were successful. Of those 674 connections, some connections appear to be legitimate, while others indicate a cross-site scripting activity. The attackers tried first to login on the application by using common user/password combinations and then by injecting malicious code into the HTTP Header.

In the same lapse, we noticed a connection on port 993 (IMAP) to the IP 185.49.207.253/254, which appears to be registered to a company named Critical Case.

**Suggested Actions**: we advise checking the logs generated from the applications installed on the server and verify that no access has been granted.