# Incident Response Report Form

**Privileged and Confidential Attorney-Client Communication/Work Product**

## INCIDENT IDENTIFICATION INFORMATION

| | |
|---|---|
| Date and Time of Notification: 03/02/2023 15:48 | |
| Incident Detector’s Information: | |
| Name: Nitin Bhanderi | Date and Time Detected: 03/02/2023 15:48 |
| Title: service control manager | Location: system log |
| Phone/Contact Info: 6353719479 | System or Application: system |

## INCIDENT SUMMARY

**Type of Incident Detected:**

☐ Denial of Service
☐ Unauthorized Access
☐ Malicious Code
☐ Unplanned Downtime
☐ Unauthorized Use
[✓ ☐ Other]

**Description of Incident:** Background Intelligent Transfer Service (BITS) is used by programmers and system administrators to download files from or  upload files to HTTP web servers and SMB file shares.

**Names and Contact Information of Others Involved:No involment**

## INCIDENT NOTIFICATION – OTHERS

☐ IS Leadership
☐ Security Incident Response Team
☐ Administration
☐ Other:
[✓ ☐ System or Application Owner]
☐ Public Affairs
☐ Human Resources
☐ System or Application Vendor
☐ Legal Counsel

## ACTIONS

**Identification Measures (Incident Verified, Assessed, Options Evaluated): the problem has been identified through system logs and found something suspicious with BITS service where the administrator's involvement is negative.**

**Log information:**

**Level:information**

**Source:service control manager**

**Event id:7040**

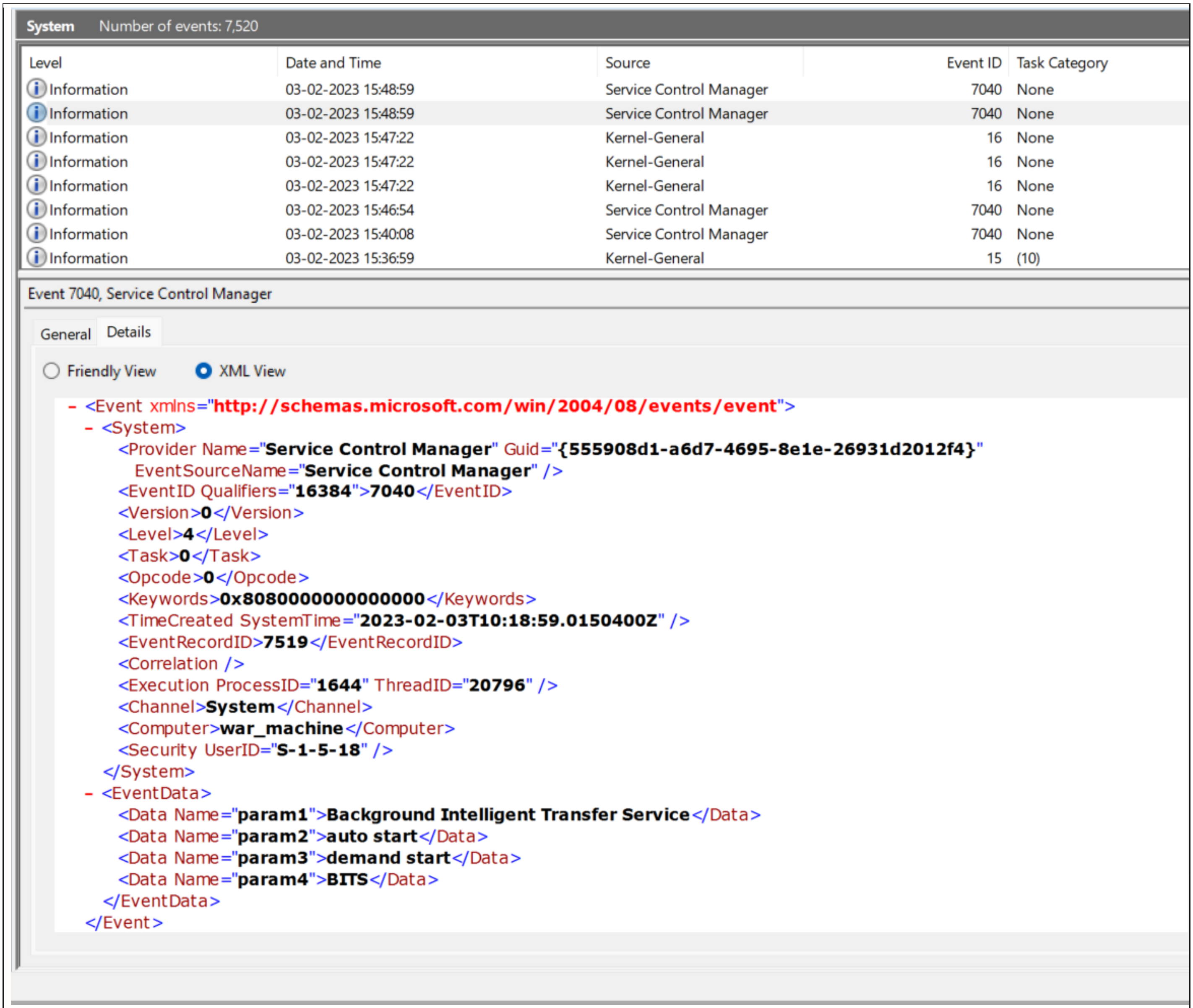
**Containment Measures:**

**Stop the BITS service's**

**Delete the files those are found to be malicious in our system**

**Interrupt the established lines of  communication**

**Evidence Collected (Systems Logs, etc.):**



**System** Number of events: 7,520

| Level | Date and Time | Source | Event ID | Task Category |
|---|---|---|---|---|
| Information | 03-02-2023 15:48:59 | Service Control Manager | 7040 | None |
| Information | 03-02-2023 15:48:59 | Service Control Manager | 7040 | None |
| Information | 03-02-2023 15:47:22 | Kernel-General | 16 | None |
| Information | 03-02-2023 15:47:22 | Kernel-General | 16 | None |
| Information | 03-02-2023 15:47:22 | Kernel-General | 16 | None |
| Information | 03-02-2023 15:46:54 | Service Control Manager | 7040 | None |
| Information | 03-02-2023 15:40:08 | Service Control Manager | 7040 | None |
| Information | 03-02-2023 15:36:59 | Kernel-General | 15 | (10) |

Event 7040, Service Control Manager

○ Friendly View ● XML View

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Service Control Manager" Guid="{555908d1-a6d7-4695-8e1e-26931d2012f4}"
        EventSourceName="Service Control Manager" />
      <EventID Qualifiers="16384">7040</EventID>
      <Version>0</Version>
      <Level>4</Level>
      <Task>0</Task>
      <Opcode>0</Opcode>
      <Keywords>0x8080000000000000</Keywords>
      <TimeCreated SystemTime="2023-02-03T10:18:59.0150400Z" />
      <EventRecordID>7519</EventRecordID>
      <Correlation />
      <Execution ProcessID="1644" ThreadID="20796" />
      <Channel>System</Channel>
      <Computer>war_machine</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <EventData>
      <Data Name="param1">Background Intelligent Transfer Service</Data>
      <Data Name="param2">auto start</Data>
      <Data Name="param3">demand start</Data>
      <Data Name="param4">BITS</Data>
    </EventData>
  </Event>
```

**Eradication Measures:**

**Scan the devices before connecting  to the system**

**Unplug the external peripheral device's**

**Block the external device's ports**

**Recovery Measures:**

**Clone the files**

**Data backup**

**Upload the files cloud**

**Other Mitigation Actions:**

**Scan the device before connecting**

**Enable the antivirus and ids,ips,firewalls**

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

# Sample Security Incident Response Report Form

**Privileged and Confidential Attorney-Client Communication/Work Product**

## EVALUATION

**How Well Did Work Force Members Respond?**

The team found suspicious logs within no time and informed higher authority immediately

**Were the Documented Procedures Followed? Were They Adequate?**

yes, the documented procedures were sufficent to solve the issue and they were Adequate

**What Information Was Needed Sooner?**

service identification

**Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?**

yes

**What Could Work Force Members Do Differently the Next Time an Incident Occurs?**

Always being vigilant

**What Corrective Actions Can Prevent Similar Incidents in the Future?**

constant monitoring on ports,firewalls,ids and ips

**What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?**

Perform the incident detection process frequently

**Other Conclusions or Recommendations:**

Do not provide the access to untrusted external devices

## FOLLOW-UP

**Reviewed By:**

☐ Security Officer

☐ Privacy Officer

☐ IS Department/Team

☐ Other

**Recommended Actions Carried Out:**

**Initial Report Completed By:**

**Follow-Up Completed By:**

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.