INCIDENT RESPONSE REPORT

Incident ID: SOC-IR-20250703-001
Date/Time Detected: 2025-07-03 05:06:14
Reported By: Splunk SIEM

Summary of Incident

A malware detection event involving a **Worm Infection Attempt** was triggered on user account **bob** from the IP address 203.0.113.77, a public IP. This is a **High Severity** threat based on the organization's alerting policy. Similar threats such as Ransomware and Rootkits were also detected in other user accounts.

User Involved

- **Username:** bob
- **IP Address:** 203.0.113.77
- **Device/Host:** SOC-simulated
- **Location:** Unknown (Public IP)

Log Evidence

Example log event from Splunk:

2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt

Severity: High

Impact Assessment

- Indicates a potential compromise of the user device.
- Threat type suggests a risk of self-replicating malware spreading through internal systems.

Recommended Response Actions

- Immediately isolate the device associated with 203.0.113.77
- Perform a full malware scan
- Reimage the affected system if necessary
- Reset user bob's credentials
- Review login and file access history for lateral movement

Communication Plan

- Notify IT Security Manager via incident ticket and email
- Log the event in the SOC daily report
- Notify affected user with guidance and support steps

Status:

Under investigation