February 2021

DETECT ROGUE IoT BASED ON THE BEHAVIOUR ANALYSIS OF DEVICE WORKFLOW PATTERNS

HP INC

Detect rogue IoT based on the behaviour analysis of device workflow patterns

Abstract

Considering various business workflows or deployment scope, printer manufacturers provide various solutions/configurations to counter misuse of resources, document security, along with ease of use. It is a challenge to track/flag a compromised device.

Existing malicious activity detection approaches use either signature-based detection or require a prior knowledge of specific IoC (indicators of compromise) characteristics or behaviours from manual identification based on network anomalies or SIEM (Security Information and Event Management) logs, etc. The proposed idea contributes to extended detection and response (XDR) within ecosystem of deployment. Solution is to keep monitoring all outgoing network traffic within the host, uniquely assess their integrity with user job flow data and classify any malicious activity with more precision, alert device user and admin through SIEM for actionable security response.

Problem Statement

One of the aspects to exploit an IoT device would be to use it as a launchpad or source to penetrate to other unpatched resources of a network. An attack may vary from scanning network assets for a specific port, to target vulnerabilities of enterprise services like SMB (Server Message Block), SMTP, DNS, DHCP, LDAP, etc.

Printer firmware has very limited user interventions, fixed functional workflows and behaves as a client and generates outbound network traffic to access many network or enterprise services like LDAP, DNS, DHCP, SMB, etc.

Typically, in any enterprise network the devices (printers) generating the outbound network traffic to services or resources within the intranet are usually configured to whitelist such network traffic. Due to some security weakness in enterprise perimeter defences and vulnerability in the device (printer), the attacker would be successful in making the printer a pivot point for the cyber-attacks. Once the printer is in control of the attacker there is no solution exists today to find out if the network traffic generated from the printer is 'valid or not' based on the legitimate or malicious user action, because there is no connection with the user actions and outbound network traffic.

Proposed Solution

The proposed solution is to further enhance malicious activity detection using a traffic inspection module, monitoring the device (printer) generated outbound network traffic and classify them to legitimate or a malicious activity with the help of an Agent and Controller. Once classified as a malicious activity, controller to flag the security incident.

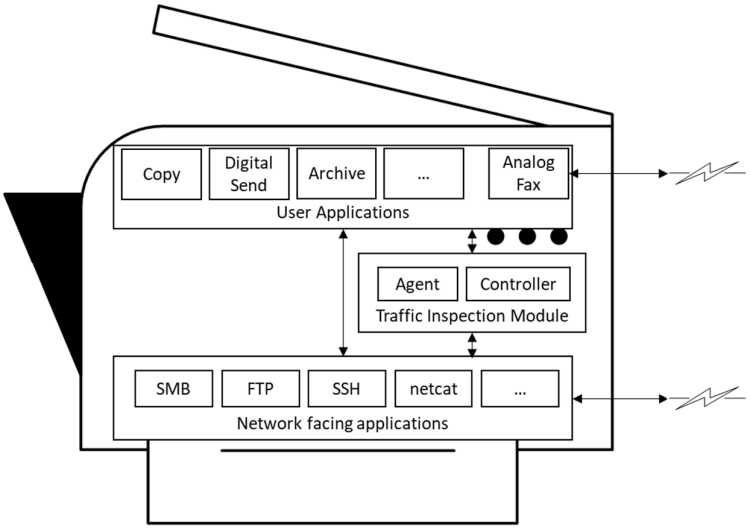

Figure-1: Traffic Inspection module with an Agent and Controller monitoring malicious network activity

Traffic Inspection module is a firmware component which consist of Agent and Controller. Agent has access to

1. Collect Job records such as User Job-ID, scan Job Token, timestamps, process ID of associated network service, etc for every job user initiates on the device (printer)
2. Monitors all network services that could potentially relate to outgoing network traffic
3. allowed processes (discovery queries, network ports, etc) and device profile, i.e known functional workflows (SMB, SNMP, DHCP, LDAP, Kerberos, etc)

For every outbound network query, Agent to forward the above information to Controller.

Controller takes the data from the agent, processes the outbound network traffic to validate whether a process or workflow is approved or not. If allowed, it further verifies whether the outbound network query has all the job records (user job-ID, scan job token, timestamps, process ID of associated network service, etc.) needed to uniquely qualify it to be permitted to continue with the job, if not the device (printer) should assert and notifies the user for potential security incident. Once incident occurs device shall be disconnected from the enterprise network and user intervention is required to bring back the device to normal state. This helps in preventing the device (printer) as pivot for launching cyber-attacks on the enterprise network.

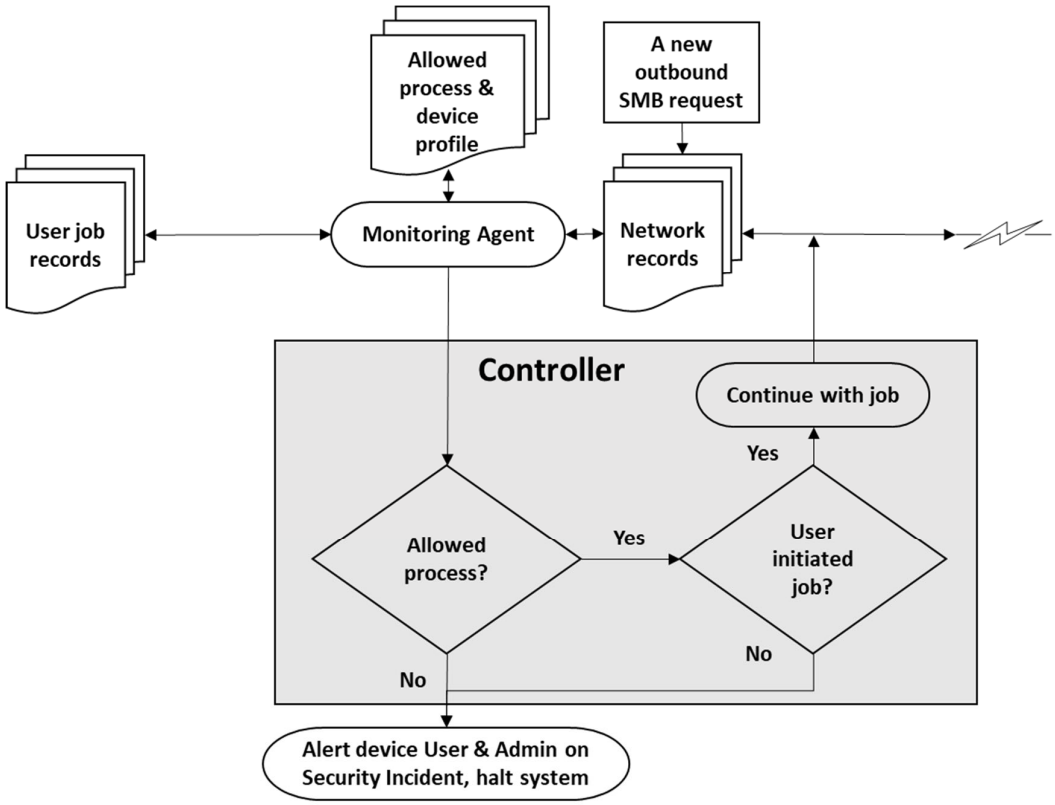

Figure-2: Logical flow of how agent and controller work in case of a printer

As in Figure-3, a security alert message is shown on the control panel before a system reset self-recovery event. Syslog messages are sent from the device for the configuration changes and Protection events.

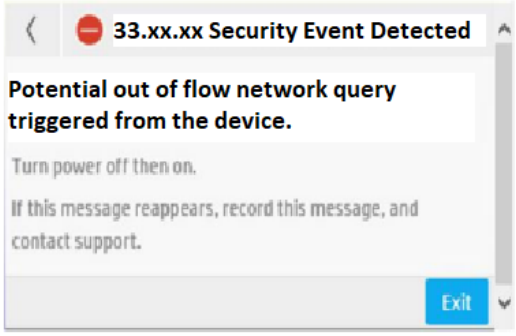

Figure-3: Security Alert for device User

Example-1: Assuming a case where printer firmware with existing solutions is compromised and used as a launchpad for network resource penetration through SMB. In the case of an SFP printer, if any SMB query goes out, it must be immediately flagged as a security incident. And in the case of an MFP, SMB queries could arise in the following cases

a. Digital Send Jobs
b. Copy/Email/Fax archive

For an MFP, an SMB query gets triggered either due to a user-initiated scan job or from an incoming Fax job, and no other job triggers it. But if the same device is compromised, there is possibility of

triggering SMB queries independently with the help of exploitation tools like Eternal Blue, Double Pulsar, etc.

Illustration of how Traffic Inspection Module assess malicious traffic from a printer.

1. A new outbound SMB request triggered by a printer gets the attention of the Traffic Inspection Module.
2. Network records and User Job records are collected by the Agent and forwarded to the controller to get authenticity validated.
3. Controller module assesses the network traffic with device profile and user job records (Scan Pipeline job ticketing entries or archive request entries for an incoming Fax job) to uniquely identify outgoing SMB request to be legitimate or malicious and takes a decision accordingly.

Example-2: Consider a Linux based printer firmware which is compromised. Attacker triggers a netcat query from the printer to another resource within user network. Outbound request of netcat connection for opening-up a blind shell to a remote resource is typically not the core functionality of a printer, the above-mentioned proposed solution triggers Security Incident alert.

This way proposed solution is extendable to other network service like SSH, SMTP, LDAP, etc. to uniquely identify malicious traffic that get triggered during real time exploitation.

Advantages

- Enhances device security by preventing cyber-attacks like DDoS, SSRF, etc
- Contributes towards extended detection and response (XDR) approach for detection accuracy and improved security operations.
- Extendable for any IoT.

Prior Solution and its Disadvantages

No known printer firmware solutions around the proposed idea.

Disclosed by Lakshmi Narasimham Akella, Kotapati Vijay Krishna, Azghar Sheik Ali and Sunil M Kumar, HP Inc.