Exploiting UPnP Protocol for Botnet Propagation and Control

Di Wu[1,2], Binxing Fang[3,4], Xiang Cui[1,2], Chaoge Liu[1]

1 (Institute of Information Engineering, Chinese Academy of Sciences)
2 (School of Cyber Security, University of Chinese Academy of Sciences)
3 (Beijing University of Posts and Telecommunications)
4 (Institute of Electronic and Information Engineering in Dongguan UESTC)

wudi6@iie.ac.cn

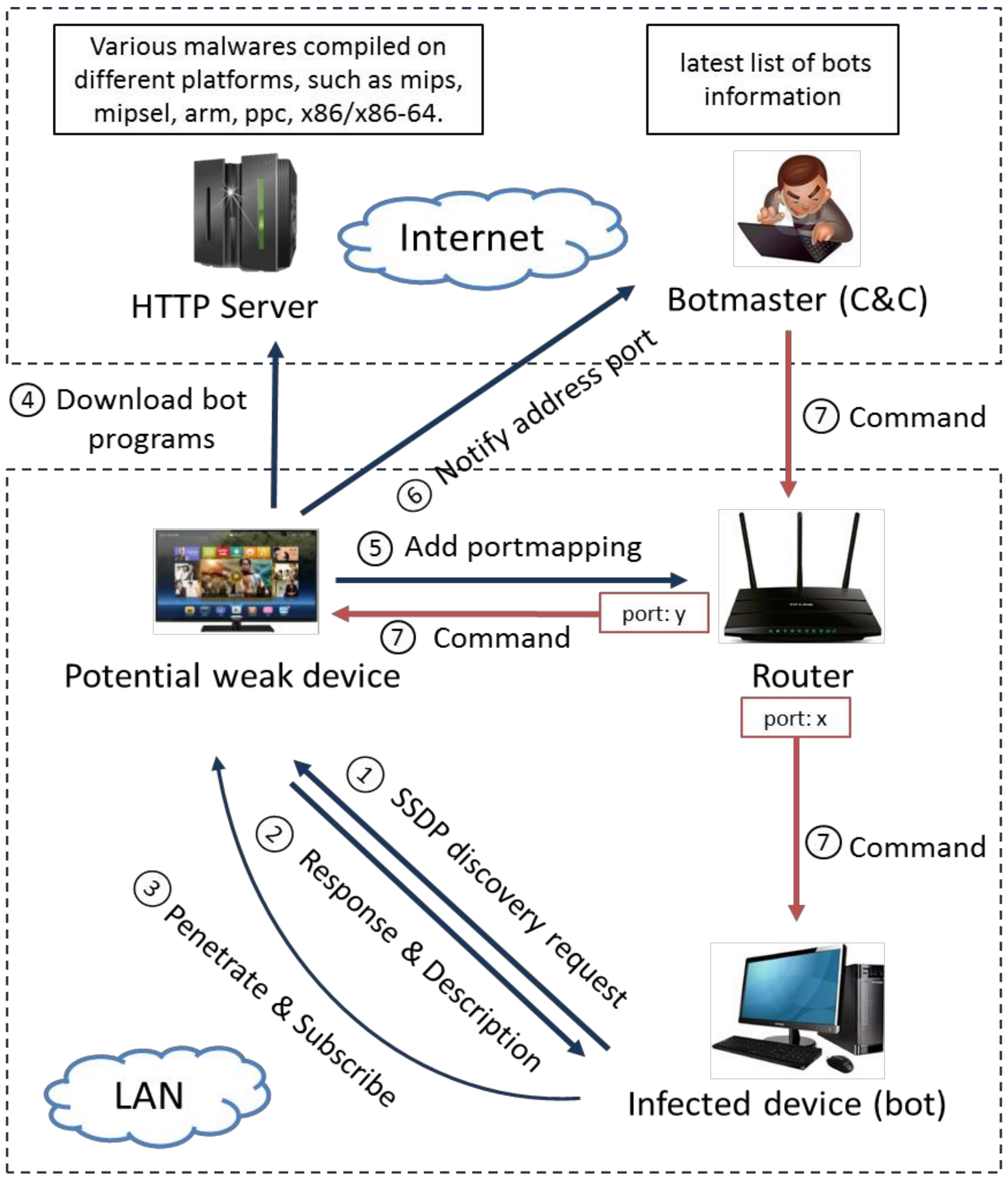
ABSTRACT

- To date, most research workers in the IoT security field focus on analyzing the weakness of devices from communication, configuration, backdoor and system vulnerability. However, with the increase of devices and protocol types, large-scale controlling is becoming more difficult.
- To change this situation, we studied the communication technology among devices and determined that the Universal Plug and Play (UPnP) protocol has the ability to identify IoT devices and distribute commands.
- Consequently, we propose an UPnP-based botnet, implementing bot propagation and control by exploiting the UPnP protocol. Moreover, we set up a re-infection mechanism to enhance the resilience. In general, the botnet, which has good accuracy in device discovery and status monitoring, is efficient and stable.

DESIGN

A. Scan ("①" and "②")

- In order to discover potential weak UPnP devices, the bot on the LAN first sends several SSDP discovery requests with different "ST" field to "239.255.255.250:1900" by multicast. The "ST" field in request packet is used to refer the type of search target. By setting this value, bot can scan devices in the specified range initially.
- If the response is received, it means that there are interested targets alive. The "Location" field in response packet gives the URL of device description, and bot will get the description file through it. The description is stored in XML format and usually includes more detail information about the device. These parameters can help the bot to further determine whether the target is vulnerable.



B. Infection ("③" and "④")

- Once bot has determined the target, the next step is trying to penetrate it with the included exploit code and password dictionary. In case of success, target will connect to the server of botmaster and download appropriate bot programs.
- Since the resilience of malware in most such devices is not strong, to solve this issue, we can choose a reliable device on the LAN like PC to be a "subscriber" and establish a re-infection mechanism. Each UPnP device has some state variables to show the running status, when they changed, device will multicast the events.
- We can choose a major event that is able to indicate whether the target is active or not as a reference, and let subscriber use GENA protocol to monitoring it through the "eventSubURL". The target will be deemed invalid if the subscriber has not received the event signal for a long time, and then subscriber will re-infect it and notify the C&C of its state. Through the mechanism of mutual supervision, we can increase the overall survival on the LAN.

Specification	Device-Type	Service-Type	Variable Name
Home Automation	BinaryLight	SwitchPower	Target
AV	MediaRenderer	RenderingControl	LastChange
Printer	Printer	PrintBasic	JobId

C. Control ("⑤", "⑥" and "⑦")

- In order to take control of devices, we can let the botmaster to access to bots besides polling commands from the botmaster. Due to the weakness in authentication, infected device can use AddPortMapping SOAP action to request a Port Mapping to forward from the IGD WAN interface to bots, and then bot will notify the C&C server of its address port.
- In this way, botmaster can transmit commands to bots through specified ports on the router. Compared to the way of polling commands from the botmaster, this control method will be more flexible.

Preliminary Results

- According to the official standardized documents, we chose and verified some type of devices and their representative required properties for propagating and subscribing bots(the table above).
- We realized major construct operations in embedded Linux devices by using lib files of miniupnp, such as sending control commands to the router and adding a designated port mapping. Experiments show that many routers exist such UPnP security problems, which proves that our approach is feasible in practice.

Contributions

- We improve the accuracy and efficiency of target discovery in the IoT.
- We enhance the resilience of botnet by mutual monitoring among bots.
- We propose a C&C channel from the botmaster to bots.

Acknowledgment

This work is supported by the Industry-University-Research Cooperation Project of Guangdong Province (No. 2016B090921001).