Contents

Introduction ........................................................................................................................................ 3
The Importance of Rogue Device Detection ..................................................................................... 3
Types of Rogue Devices .................................................................................................................. 3
Rogue Device Discovery .................................................................................................................. 5
Automated Actions After Rogue Device Detection ........................................................................ 7
Summary .......................................................................................................................................... 8
Introduction

This document has been created to explain the mechanisms used by ForeScout CounterACT™ to detect rogue devices that are connected to a network. In addition, this document will clarify how CounterACT identifies unauthorized network devices such as switches, routers, and rogue wireless access points (WAPs).

The Importance of Rogue Device Detection

Rogue device detection is becoming a major concern in a number of different industries. The market has already seen a number of major retail banks investigating how they profile and detect rogue devices on their network; this will only expand to be a major initiative over the next 18 months. This has been driven by a number of high profile cases in the UK and African retail banking sector recently. Rogue devices have been accessing banking networks and stealing assets.

The fundamental problem that allows rogue devices to occur is the fact that the vast majority of all enterprises do not have complete visibility of devices on their network. This lack of real time visibility removes the ability to put in place any effective strategy regarding device management, BYOD, or data loss prevention (DLP).

Whether it is PCI compliance for retail organisations, electronic patient records in the health sector, or connecting to the new PSN network in the UK public sector, each situation requires the IT manager to understand all devices that are connected to the network and be able to control their access to the network.

When you consider all of the devices connected to your network — PCs and laptops, VOIP phones, “bring your own device” (BYOD) tablets, smartphones and more — how many do you think you have at any moment? It’s a fundamental question that needs to be answered. The larger your network, the greater the potential risk that a rogue device can disrupt your network or steal your data. All it takes is one rogue device to wreak havoc. What is the economic cost to your company when operations come to a halt because "the network is down"?

Types of Rogue Devices

How do we define a rogue device? There is no one definition that is clearly accepted in the industry. One broad definition is any device that is already “owned” by an attacker, meaning that he can directly or remotely control what that devices does on a network. The attacker may have gained control of the endpoint by sending an email to a user that looked legitimate but contained an application that took control of the user’s computer when the user clicked a link in the email. Or the attacker gained control with a piece of malware that came into the network via a thumb drive, or from a data transfer.

A second type of rogue device is one that is actually (physically) owned by the attacker. The attacker may have figured out how to penetrate your network with his own laptop or device. Once on your network, the attacker can operate invisibly with all the tools he needs.

Below are few other types of rogue devices:

**Wireless Access Points — WAPs**

A rogue wireless access point (WAP) not only makes your network more porous, but it also circumvents your access controls. Why do rogue WAP’s pose such an inherent risk? By design, a WAP is a network bridge that is used to connect two disparate networks — a wireless network to a wired network. Wireless networks are inherently less secure than wired networks. With traditional wired networks, data flows over physical and often protected circuits. Whereas with wireless networks, data is transmitted using radio signals. This has several security implications. First, these signals can be intercepted, making data susceptible to eavesdropping. Second, a rogue WAP can open your network to unauthorized connections that are difficult to detect.
The following is an example of a WAP that sits on a network without using an IP address making it invisible on most networks:

![Image of Pwn Plug Elite]

**Product:** Pwn Plug Elite

**Manufacturer’s Description:**
“The industry’s first enterprise-class penetration testing drop box. Through its innovative, patent-pending design, the Pwn Plug covers the entire spectrum of a full-scale pentesting engagement, from physical-layer to application-layer.”

- Includes 4G/GSM cellular, Wireless (802.11b/g/n), high-gain Bluetooth, & USB-Ethernet adapters
- Fully-automated NAC/802.1X/RADIUS bypass!
- Out-of-band SSH access over 4G/GSM cell networks!
- Text-to-Bash: text in bash commands via SMS!
- Simple web-based administration with “Pwnix UI”
- One-click Evil AP, stealth mode, & passive recon
- Maintains persistent, covert, encrypted SSH access to your target network [Details]
- Tunnels through application-aware firewalls & IPS
- Supports HTTP proxies, SSH-VPN, & OpenVPN
- Sends email/SMS alerts when SSH tunnels are activated
- Preloaded with Debian 6, Metasploit, SET, Fast-Track, w3af, Kismet, Aircrack, SSLstrip, nmap, Hydra, dsniff, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools, & more!
- Unpingable and no listening ports in stealth mode
- Includes 16GB SDHC card for extra storage
- Includes stealthy decal stickers
BYOD Smartphones and Tablets

Consumer oriented devices like smartphones and tablets are also connecting to corporate networks and creating unique risks and challenges. These devices are quickly overwhelming IT managers with increased administrative burdens. Since they are consumer devices, they lack integration with the company’s IT management platforms. As a result, BYOD devices may pose a risk to your network and to your company’s data.

Windows, Mac, Linux, and Virtual Machines (VMs)

Endpoint computing devices such as Windows, Mac, Linux or virtual machines might not be what most people would consider “rogue devices”, but if we look at the ability of an attacker to compromise an endpoint because it is non-compliant with the organization's security policies, that is a security gap that needs to be addressed. These out-compliance endpoints on your network are the low hanging fruit that the attacker goes after to gain access to the network. Why should a hacker use his best tools when he can use a quick exploit that should have been patched in the endpoint’s operating system 3 months ago?

Organizations have embraced virtualization as an effective way to reduce IT operating expenses, but the risk associated with rogue VMs are significant and often overlooked. Detecting rogue, unmanaged or non-compliant VMs is all the more challenging with virtualization creating a greater lack of visibility into the environment. A physical server can have dozens or hundreds of VMs on it, and VMs can also move around from one physical machine to another, based on load, to meet business and service-level requirements. This movement between physical servers increases the possibility of untrusted VMs communicating with sensitive VMs on the same virtual switch. Also, when a virtual machine is not required, it can be stored offline as an image in rest state. When the image is moved back into production, it may be non-compliant with the current security policy. As more VMs are added, simply tracking them becomes difficult, and the number of rogue VMs increases because they can be operating with obsolete security policies or without the latest software updates as they come in and out of service.

Rogue Device Discovery

Gaps in endpoint visibility are gaps in your security, so the first order of business is to obtain complete visibility into who and what is on your network. Once you can see the endpoints, then you can control the endpoints by remediating them, quarantining them, or just taking away their access the network altogether. If you cannot see the endpoint, you cannot manage the device.

ForeScout CounterACT provides complete visibility to everything on your network. It uses multiple techniques to quickly discover and identify endpoints and other devices such as the ones listed above. Some are primary discovery techniques built into the product, and some are secondary discovery techniques that rely on queries of external systems. CounterACT leverages the knowledge gained from other systems (e.g. databases, inventory systems, directories, next generation firewalls, etc.) through its large number of integrations that are collectively known as ControlFabric™ technologies.

The following is a brief description of CounterACT’s discovery and inspection techniques in terms of passive and active discovery and inspection, specific device interrogation, and data collected from integration with third-party products.

Passive Discovery

Passive discovery allows CounterACT to detect devices communicating across your network without any need for CounterACT to be connected inline of the data path. This is a key technology that allows CounterACT to detect endpoints that are connecting to remote network segments. With passive monitoring, CounterACT monitors traffic on your network and discovers devices through the following techniques:

- Passive authentication monitoring
- Passive Nmap
- DHCP & ARP request monitoring
- Ingesting information from HTTP user agents and passive banners
**Active Discovery**

ForeScout CounterACT also employs active discovery techniques through the network infrastructure and authentication services by querying these units/services via SNMP, CLI, or domain administrator credentials as follows:

- **Firewalls, Routers, Switches, Remote Access VPN**
  CounterACT integrates with network devices and queries information on these devices, such as ARP and CAM tables, to gain information about endpoints that are connected to these devices. CounterACT can integrate with VPN gateway servers to monitor and inspect remotely connected hosts for compliance by finding the endpoint location and then performing active inspections as discussed below.

- **LDAP, RADIUS & 802.1X**
  In addition to passively monitoring authentication traffic to discover the type of device that is connecting to your network, CounterACT integrates with multiple authentication services to actively determine the authentication status of every device on the network. CounterACT integrates with authentication services including LDAP and Active Directory to augment endpoint security profiles so it can apply its contextual based security decisions or actions against a company’s security policy.

- **NAT Device Detection**
  CounterACT includes a proprietary NAT detection analysis engine that accurately identifies when an unknown network device, like a rogue WAP, is connected to the network. Once CounterACT discovers such a device, CounterACT can notify the administrator and/or block the device from the network.

Once an endpoint has been discovered, CounterACT is able to actively inspect the endpoint without the need for an agent. This is a major differentiator between CounterACT and most other NAC products which require endpoint agents to inspect the endpoint. CounterACT is able to actively inspect endpoints by using domain credentials on corporate-owned devices and a secure tunnelling mechanism known as SecureConnector on BYOD devices. CounterACT can actively inspect endpoints both initially upon network entry and on a continuous basis to learn details about the host state and any vulnerabilities that might be present. Active inspection techniques include the following:

- **External Scan**
  For non-Windows devices, ForeScout CounterACT can run an active Nmap scan against endpoints to gather detailed information with respect to the operating system, vendor, services, applications, processes, and available files (where applicable). As an example, you might not allow Android devices on your network, and so every Android operating system that CounterACT discovers via this technique is by definition a rogue device.

- **Active Banners**
  CounterACT actively collects banner data to identify an operating system by opening a connection and reading the banner or response sent by the application. Many email, FTP, and web servers will respond to a telnet connection with the name and version of the software. This aids in fingerprinting the operating system and application software.

ForeScout CounterACT continuously monitors endpoints after they have connected to your network. Through this, CounterACT discovers endpoint changes that might be undesirable, as well as suspicious and/or malicious behaviour, with the following:

- **Tracking Changes**
  CounterACT identifies changes on endpoints such as: applications installed, host names, operating systems, shared folders, switches, users, Windows services, and new TCP/IP ports. CounterACT’s unique combination of endpoint discovery and inspection techniques are used to track endpoint changes making CounterACT instrumental in continuously monitoring endpoints while they are connected to the network.

- **Behavior Changes and Spoof Detection**
  CounterACT can be configured to use both its event driven response to tracked changes and ForeScout’s patented ActiveResponse™ threat detection engine to detect changes in endpoint behavior. For example, when a printer starts to behave like an endpoint by trying to connect to a server; this behavior change could be a tell-tale sign that an intruder is on your network because he spoofed the printer’s MAC address.
Automated Actions After Rogue Device Detection

CounterACT automatically neutralizes the threat of rogue devices by blocking, isolating, or remediating the rogue device. Here are some security policies that are examples of how CounterACT can be configured to mitigate rogue devices.

Figure 1: CounterACT policy to block a rogue endpoint from the network, and send a Syslog message to a 3rd party security system.

Figure 2: CounterACT policy to quarantine a rogue endpoint from the network with a virtual firewall (vFW).

Figure 3: CounterACT policy to add a rogue endpoint to the Remediation VLAN.
In addition to these actions, once a rogue device has been detected, CounterACT can send notifications to the CounterACT administrator and/or the end-user of the device.

Summary

A rogue device on a network significantly raises the risk of damaging an organization’s reputation and profitability. ForeScout CounterACT manages rogue devices by using multiple technologies to learn about everything on your network with continuous endpoint visibility, automated actions (as noted in the above section), and integration with your IT security infrastructure through ForeScout ControlFabric.

CounterACT also provides an extensive range of information about endpoint threats, and about users connected to them, to increase situational awareness with real-time and trend reports on threat activity across your network. CounterACT can also use its visibility and automated network actions to manage when a domain user requires a personal device to have network access by initiating an easy-to-use guest registration.