The RAVE Network Attack

Aaron Campbell
Cedarville University, acampbell@cedarville.edu

Aidan Graef
Cedarville University, aidangraef@cedarville.edu

Jarett Insko
Cedarville University, jarettinsko@cedarville.edu

Alec Mathisen
Cedarville University, alecmathisen@cedarville.edu

School of ENGINEERING and COMPUTER SCIENCE
CEDARVILLE UNIVERSITY

CRYPTIC VECTOR

The RAVE Network Attack

Covert Leave-behind Device

Faculty Advisor: *Prof. Dudenhofer & Prof. Sprague*
Students: *Aaron Campbell, Aidan Graef, Jarett Insko, Alec Mathisen*

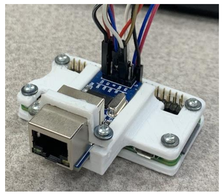
Research & Scholarship SYMPOSIUM

The Device

Hardware:

We used a Raspberry Pi Zero for the device. The Pi Zero has an ARMv7 chip.

- 1GHz core CPU
- 512 MB RAM
- 40-pin GPIO Header



Connection:

The RAVE Device uses an ENC28J60 Ethernet port to connect to the victim network. The port is connected using GPIO pins on the Raspberry Pi 0.

Software:

The OS the RAVE device runs on is Raspbian with minimal additional packages and some custom scripts and cronjobs. This allows us the greatest level of use of the Pi Zero's resources.

Power:

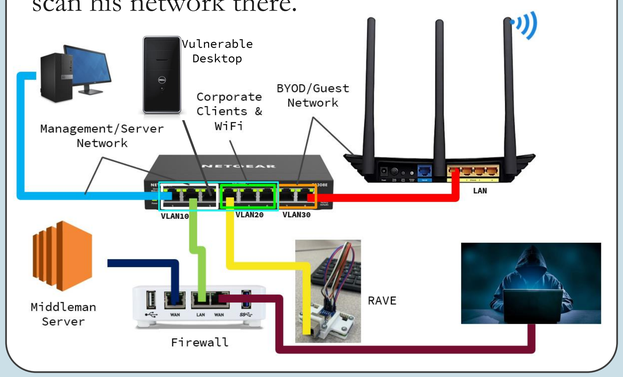
The RAVE device is powered by a 5V micro-USB power adapter. This helps keep the physical device as small as possible.

Abstract

Cyber-attacks are an ever-present threat to our modern, technologically dependent world. This looming shadow of a disaster waiting to happen has led companies to invest heavily into their software resiliency and network defenses. However, many companies, especially small ones, have forgotten the danger of an insider threat, or at least how an insider threat could be emulated. Anything on the inside of a network automatically has a higher level of trust because most companies' defenses have only gone as far as to protect their perimeter and educate their employees. What if an outside attacker was able to gain physical access for just a brief time to the inside of a small business? Say, in a waiting room or consultation? RAVE stands for Remote Attack Vector Engine, and is a device designed to test this flaw. RAVE is a small Raspberry Pi 0, disguised as any common workplace device, that an attacker can plant in a business's network to attack from the inside. By connecting RAVE to an internal ethernet port, a secure reverse OpenVPN connection is automatically created to a Middleman Server over common HTTPS traffic through port 443 and kept persistent. An operator is then able to connect into RAVE through the Middleman Server. The operator can then use tools installed on the device to launch network scans, perform brute force password attacks on network devices and services, take over more devices on the network, and steal data from the company. By using this device, penetration testers can help companies develop better security practices to keep their network safe from infiltration and exploitation.

Simulating an Attack

To demonstrate the usefulness of the RAVE leave-behind device, we created a vulnerable test network that was disconnected from the internet on which we could simulate a network attack. By plugging RAVE into a network switch, we were able to test out our tools to hack into a vulnerable computer, Wi-Fi router, the original switch, and tunnel out of a firewall to the operator computer. We also tested the reverse connection in the real world at a team member's off campus house and were able to scan his network there.



Our Arsenal

MAC Spoofing - MAChanger

Our Ethernet module allows us to change our MAC address to whatever we want, such as a printer, so that RAVE will blend in better on the network.

Password Attacks - Hydra

We can use the RAVE device to conduct password attacks on other machines on the network, such as the router, using Hydra.

Machine Pivoting – Metasploit & Meterpreter

Using Metasploit on the operator computer, RAVE allows us to move control from one infected machine to another, so we can add more computers to the RAVE! Metasploit installs a client known as meterpreter on RAVE which allows us to use Metasploit's full power to exploit other computers.

Reverse Shell Connection – OpenVPN & Cronjobs

The Middle-Man Server is running an OpenVPN server which allows for a discreet connection to RAVE over port 443. This connection is kept alive by a custom cronjob and scripts.

Network Reconnaisance – NMAP & TCPDump

There is also a host of network scanning tools to allow us to capture network traffic and look for vulnerable machines.

How the Attack Works