

## ▶ **Wardialing: Practical Advice to Understand Your Exposure**

---

A Perspective on Practical Security February 1999  
by Cheng Tang & Jonathan Gossels

© Copyright 1999 SystemExperts Corporation. All rights reserved.

## ► Wardialing: Practical Advice to Understand Your Exposure

---

### Abstract

“Wardialing” is the automated process hackers use to find computers accessible via telephone lines. It is one of the earliest and remains one of the most pervasive forms of electronic intrusion, predating Internet-based attacks. There have been well-publicized reports of hackers finding and exploiting valuable corporate and governmental resources and data using wardialing techniques. Unfortunately, most organizations have never adequately protected themselves from this simple form of penetration. The reality is that anyone with a \$1,000 PC using freely available wardialer software is capable of exploiting your organization with just a phone call.

This white paper explores the tools and a technique commonly used by hackers, identifies ways to recognize the signatures such tools leave behind, and recommends practical measures you can take to reduce your exposure from wardialing attack.

### Inside

- What is Wardialing?
- Wardialing tools
- Wardialing process
- Configuring your Wardialer
- Classification Methodology
- Establishing ground rules
- Interpreting your results
- Protecting yourself

### What is Wardialing?

Wardialing is the automated process used to find computing and telephone resources. Essentially, it is simply calling a large range of telephone numbers. A software program, called a *wardialer* systematically analyzes each telephone call. Historically, “hackers” used wardialing to find Telephone Company (telco) and corporate access numbers for free, albeit illegal, long distance telephone calls. Wardialing has matured since then, and now publicly available hacker software is much better at identifying vulnerable computers than making free phone calls.

Wardialing is difficult to defend against because most organizations set up their telephone systems with availability and ease of use as their top priorities, not security. Customary business etiquette amplifies what would otherwise be minor exposures. For example, a hacker wardialing into an organization can deduce a lot, even if he fails to connect to a computer. Suppose the hacker reaches a person who answers the phone, “Company XYZ NT Help Desk, how may I help you?” That information tells the hacker two important things: 1) that he is probing numbers within an IT department which will likely hit computers within nearby ranges and 2) that he has confirmed important numbers to tie up in order to slow down the company’s response when he launches an attack.

In much of the world, wardialing is an illegal, punishable crime. In mainstream America, hackers like this are usually treated as nuisances, but in some criminal cases wardialing has been characterized as fraud. Not surprisingly, hackers have developed ways to avoid detection and have numerous tools and processes for this purpose.

There are, however, legitimate uses for wardialing including remote access diagnostics, routine telephone ring tests, and independent penetration testing. Since a critical first step in achieving good IT security is to understand what potential exploits exist, wardialing your own organization is a beneficial activity. The rest of this paper will focus on how to set up wardialing for your organization, as well as how to defend against would-be wardialing hackers.

### Wardialing Tools

Wardialing can be performed using basic tools. Inexpensive computers can drive a modem to quickly scan an organization’s telephones. The threat can literally come from any source. Here is a list of the minimum tools needed to perform wardialing:

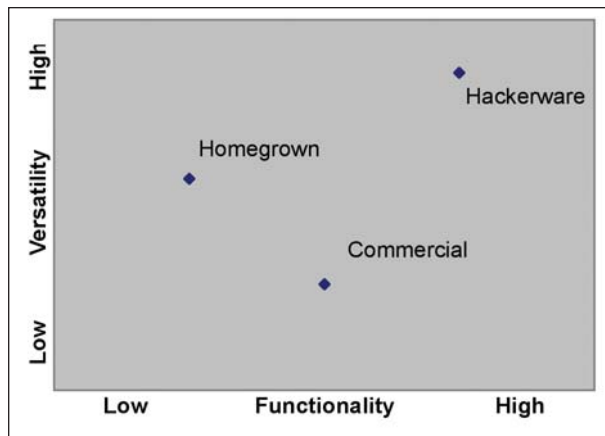
- Computer
- Modem
- Telephone line
- Wardialer software

## ► Wardialing: Practical Advice to Understand Your Exposure

In diagnostic wardialing, it is important to establish ground rules and emergency contact numbers. In case of problems, these rules and contacts can be used to prevent disruptions due to telephone calls. We discuss how to arrange these escalation activities later in the paper.

As for the basic equipment needed in wardialing, using better equipment yields better results. A standards-based modem assures the best chance for successfully negotiating a modem session. A better computer or more telephone lines can be used to accelerate the dialing process.

The most important tool is the wardialer software itself. The two best known tools are THC-SCAN (The Hacker's Choice) and ToneLoc (Tone Locator). Unfortunately, all wardialers suffer from the same major deficiencies that we will discuss later in the *Wardialing Process* section of this paper. A wardialer is a software program that systematically dials and attempts to negotiate a carrier with target phone numbers. There are three general classes of software that perform wardialing-like functionality. They are commercial, homegrown, and hackerware, see Figure 1. Commercial wardialing software is generally geared for specific modem pools or remote access solutions. For example, Shiva and USR use special tools and scripts to verify their equipment works properly. Homegrown software consists of utilities created by network administrators and used by network operation centers to quickly check if they can get a phone number to pick up an incoming call. The most powerful and versatile wardialing tools are created by the underground hacker community. As a matter of fact, network administrators and commercial environments often use hackerware as a valuable diagnostic tool.



**Figure 1: Versatility versus Functionality of Wardialing Software:** as software matures, homegrown tends to be more versatile, where commercial tends to be more functional.

Note: In selecting hackerware, remember what you are dealing with and take appropriate precautions. Hackers sometimes bury call-back schemes into their tools. Before using any hackerware be sure to carefully review the software's behavior or source code. Use it initially in a controlled environment where you can observe and record the data flows. For example, unexpected outgoing email [likely containing private information gathered from your system] is a sure sign of trouble.

### Wardialing Process

The first objective of wardialing is to compile an accurate inventory of each telephone number in your organization. Determining exactly how many and what kinds of equipment helps in the assessment of vulnerabilities and helps to better secure critical systems. For this reason, the 'dial inventory' developed during wardialing must be as complete and accurate as possible. Three steps are involved in creating such an assessment of your exposure:

1. calling numbers
2. detecting resources
3. classifying answering devices

## ► Wardialing: Practical Advice to Understand Your Exposure

Remember in the previous section when we noted that all wardialers have the same types of deficiencies? Well, these deficiencies challenge the creation of an accurate and complete dial inventory. One of the biggest deficiencies is false negatives. A “false negative” is a condition where the wardialer reports no carrier, when in fact a carrier is present. This phenomenon occurs when the two modem/systems fail to negotiate a valid session. Unless the sending and receiving modems are properly configured to recognize each other (some of the configuration specifics are shown in Table 1 of the following section), a connection will not occur. Modem negotiation failure is a common occurrence and causes simple automated wardialers to under-report dial exposures. They fail to classify all telephone resources, for example, analog modems cannot detect ISDN equipment, and they tend to report a significant number of these false negatives. One of the challenges of any wardialing exercise is to reduce such inaccuracies. It is imperative for any wardialing effort of business critical systems to eliminate the false negatives reported by all wardialing programs.

The final step in the wardialing process is classifying the dial inventory. Classification methodology is used to identify exploitable telephone resources. Typically, tools are used after a wardialer has created a dial inventory. Tools include terminal emulators, remote control software, and password crackers. Depending on the response a wardialer is able to obtain from the initial call, the appropriate tools can be selected to determine exactly what type of system is answering.

Hackers and professional organizations tend to put together dialing programs and classification methodologies in the same few ways. Here are three methods for conducting wardialing:

Basic Wardialing Sweep (BWS): unattended wardialing software automatically dials a range of numbers and recognizes a set of known carrier signals.

1. Multiple Wardialing Sweep (MWS): a series of Basic Wardialing Sweeps are conducted using a range of configuration parameters and

conditions. Most common of these are separate sweeps for fax machines or specific carrier tones.

2. Attended Wardialing Sweep (AWS): attended, one-pass or multi-pass semi-automated dialing of a range of numbers with an expert listening to the negotiation tones to identify anomalous behavior and unknown devices. Examples of devices that are difficult for a BWS or MWS to detect are: voice, voicemail, and ISDN equipment.

The only sure way to produce a complete and accurate dial inventory is through an Attended Wardialing Sweep; have an expert listen to the modem negotiation tones and manually correct the false negatives reported by the wardialing tools. This is because the human ear can quickly and accurately recognize a variety of tones that the software fails to correctly characterize.

Most hackers and professionals tend to run BWS and MWS, respectively. Unfortunately, these techniques overlook significant vulnerabilities. If possible, use AWS in your organization’s scanning policy.

Most security consulting firms and organizations perform assessments via Basic Wardialer Sweeps. The primary benefit of a BWS is that it can run unattended and any exposures it finds are likely to be accurate. However, major BWS weaknesses are:

- Can only identify what the modem is set to recognize (cannot be set to detect “all carriers”)
- Does not detect non-carrier telephone resources such as voice, voicemail, and televideo
- Cannot detect ISDN equipment
- Has long timeout periods for non-carrier answers
- Reports false negatives.

To address some of these problems, some organizations perform MWS. Multiple sweeps are tuned so that some settings are altered, for example, fax recognition or software flow control. MWS are also performed at different times of the day and on different days of the week. This approach yields more carrier responses, fewer busy responses, and fewer false negatives. However, the cost of MWS is more phone calls and overlapping and possibly conflicting results.

## ▶ Wardialing: Practical Advice to Understand Your Exposure

AWS alleviates most of the problems in BWS and MWS. An expert can detect unknown behavior that often confuses wardialing software. Although AWS has the disadvantage of being semi-manual, the benefits often outweigh the costs of extra labor. When accuracy and quality are paramount, AWS is superior to BWS and MWS.

### Configuration Variables

One of the hardest things to get right in wardialing is the configuration of the wardialer software itself. This stems from the modem-to-modem session negotiation (the loud squeaking noises). The numerous standards, as well as the slow phase-out

of older protocols and equipment, lead to numerous settings that must be synchronized. The possible parameter combinations can be practically infinite (see the table below).

Higher-end modems tend to be smarter about negotiating a session. They can also identify voice, data, and fax machines, which are helpful in the classification of telephone resources. Unfortunately, special hardware and expert-listening still work best to identify other telephone resources, such as, voicemail, PBX tones, ISDN equipment, and video-conferencing equipment.

The table below provides some helpful guidelines to configuring wardialer software.

Check	Why	Comments
Country	Different countries have different telephone characteristics	Ringing tones can confuse modems. Adjust according to tones for a particular country.
Data compression	Turn it off, if possible	v.42bis and MNP are used in for data compression
Detection level	Use the appropriate level	Wardialers can be configured to detect various characteristics: voice, fax, carriers, tones, voicemail!
Error control	Turn on, if possible	v.42 and MNP are used for error control
Fax recognition	Fax machines use different protocols to negotiate a connection.	Faxmodems need to be "switched" to fax-mode or data-mode.
Flow control	Use hardware flow control, if possible	Some software emulations cause problems.
Modem Command set*	Make sure the modem accepts standard Hayes AT commands, or the wardialer is properly configured with init-strings	Use Hayes Optima, Hayes Accura, and USR Courier "high-end" modems
Modulation	Answering modems may not work with different standards	2400 and 9600 baud (V.23bis and V.32) seem to be supported by most older and all newer modems.
PBX or switch	Your PBX or local switch may or may not support certain dialing features: tone vs. pulse	This is especially true in different countries. Check what your local loop provides.
Phone services	Voicemail, call forwarding, call waiting	All of these features create unrecognizable dialtones for your modem.
Serial port*	Set to appropriate speed	Most com ports can support 115200 baud, but are default set to 9600. Adjust according to UART.
Timeout*	Enough time needs to be allocated per phone number scanned	S7 register in modem and wardialing timeout values need to be checked and adjusted accordingly.

\* Modem command set, serial port, and timeout are critical to identifying modems in wardialing

Table 1: Hardware Configuration

## ► Wardialing: Practical Advice to Understand Your Exposure

Configuration of the wardialer should be as broad as possible. Unfortunately, the least common denominator will not produce complete and accurate results. Using an AWS to identify false negatives can aid in creating the dial inventory.

### Classification

Once a dial inventory database has been compiled from wardialing, the next step is to classify the resources. Most carriers will not be recognized by the BWS or MWS, so it is necessary that these be logged and redialed during an AWS to determine the nature of the hardware on the other end of the phone line. Unfortunately, since there are so many

different types of answering devices, there is no authoritative classification software available. Instead, classification is based on experience and leg-work in researching unusual tones encountered.

Classification is accomplished through a series of tests performed to infer the nature of the remote device. The tests should be arranged in probability order so the common types of devices are discovered by the earliest tests. Finally, if none of the tests succeed, you can infer that the link is being used for some proprietary protocol.

Table 2 shown below summarizes a typical classification strategy.

Step	How to do	Comments
If protocol negotiated, re-dial with terminal emulator	Capture all information	Systems usually identify themselves, few have banners to prevent unauthorized access
Test for fax machines	Set fax-modem to fax-mode	Fax protocol usually is a carrier tone with a periodic beep.
Test for standard protocols and well-known proprietary systems	Examples: NT RAS, PcAnywhere, PPP, SLIP	
Test for ISDN equipment	Configure originating modem for callback and ISDN modem negotiation	Necessary for ISDN equipment.
If all fail, then classify as "unknown carrier"		Proprietary or obscure protocol may be in use. Although this may seem low-risk, it is dependent on the criticality of the system. Market feed or company-to-company data poses a business-critical function, and may still be compromised given enough time and resources. Insider knowledge can easily exploit this vulnerability.

**Table 2: Classification Strategy**

## ► Wardialing: Practical Advice to Understand Your Exposure

---

The primary classification tool is a terminal emulator, such as HyperTerm, but anything capable of emulating VT100, ANSI, or TTY is suitable. The terminal emulator can be used to capture data return by the system, such as a login prompt, or router information. The data received can be characterized and proper tools selected to exploit specific system vulnerabilities.

Usually, most exercises are done “blind” – no information aside from the target phone numbers is given. Although all remote access points represent potential vulnerabilities, there is a point of diminishing returns in wardialing. At some point, an internal investigation (or audit) is more effective at classifying the discovered resources. For example, it is easier to locate and see what type of device is present than to try to infer it by blind wardialing. Non-responses (no login banner) may require remote control software, such as PCAnywhere, LapLink, or Procomm Plus. However, systematically attempting the numerous proprietary remote control options may be prohibitively time-intensive.

### Establishing Ground Rules

Since we are focused on wardialing to protect businesses, there are many legal, as well as policy-based ground rules that need to be established before undertaking wide-scale wardialing. Some of the more important ground rules to establish are listed below:

- Confirmation of comprehensive contact information (testers and resource owners)
- Internal authorization as well as telephone company authorization, where appropriate
- Notification and escalation plan (in case dialing becomes too disruptive)
- Agreement on time and dates for dialing
- Identification and exclusion of business critical systems (e.g., don't dial trading systems when the market is open)
- Confirmation of range of telephone numbers to be dialed

Finally, a feedback and checkpoint system should be created. In case a critical exposure is discovered, a responsive feedback system can aid in closing or monitoring the security hole as quickly as possible.

Many organizations have explicit policies that prohibit the use of modems without appropriate authorization and compensating controls. When a modem is discovered in these firms, the results are clear; either the modem had been approved or not. Many other organizations do not have clear policies limiting modem usage. In these organizations, the results of the wardialing exercise can serve as the jumping off point to begin an analysis of the business need for each modem detected. Non critical modems should be removed and alternative secure connectivity provided.

### How to Interpret Your Results

To aid in your wardialing, we provide the following practical advice below:

- Automate the data collection process – use a database to collect information.
- A phone number that is constantly busy has a greater chance of being a modem and/or critical resource.
- Classify carriers as soon as possible. Unauthorized equipment may be shut-off, hidden, or removed if wardialing is detected.
- Wardialing is inherently statistical. Carriers and non-carrier responses change, depending upon schedule and usage. For example, busy numbers are not always busy, with enough persistence, eventually a detection can be made.

### Conclusions and How to Protect Yourself

Wardialing is a simple, but insidious threat to large organizations. With the proliferation of remote access points, every telephone is potentially a vulnerability. We recommend an Attended Wardialing Sweep to ensure the highest integrity of results. An expert using good tools can recognize and find all computers set up for remote dial-in while the war-

## ▶ Wardialing: Practical Advice to Understand Your Exposure

dialing software alone cannot. Here are some recommendations for establishing an effective wardialing process:

- ▶ Schedule regular and routine wardialing
- ▶ Set up a process to assess and to secure critical exposures
- ▶ Establish and publish a remote access policy for employees
- ▶ Train employees to recognize social engineering tactics
- ▶ Wardialing attacks usually go undetected. Know your exposure before you find out about them in the headlines

There are many Internet sites, as well as sources for wardialing software. Below is a list of some available wardialers, phone “phreaking” tools, tone-generators, and utilities. **CAUTION:** Take special precaution when downloading and evaluating these tools. As we have noted before, most of these are hackerware and should be treated as potentially high-risk software. With the proliferation of such

tools and processes, it is plain to see the threat of wardialing into the vital resources of any organization.

A-Dial	Assault dialer	Autoscan
BASTap	Bbeep	BlueDial
Carrier	CATCALL	Code Thief Deluxe
CyberPhreak	Deluxe Fone-Code Hacker	Demon Dialer
Dialer	Dialing Demon	Doo Tools
DTMF_d	Fear’s Phreaker Tools	GunBelt
HyperTerm	LapLink	Mhunter
OkiPad	PBX Scanner	PCAnywhere
PhoneSweep	PhoneTag	PhreakMaster
Procomm Plus	Professor Falken’s Phreak Tools	Scavenger-Dialer
Super Dial	THC-scan	The Little Operator
ToneLoc	Ultra-Dial	VrACK
WildDialer	X-DialeR	Zhacker

**Table 3: Wardialing Tools**