
The Art of Wardialing

Fall Internet World 99



Cheng Tang
Consultant



SYSTEM EXPERTS



My Office	703 648 9012
Main Office	888 749 9800
Fax	703 648 9014

Cheng.Tang@SystemExperts.com
www.SystemExperts.com

What We Do

- System Management Architectures, Strategies & Technology Selection
- Security Architecture & Encryption Strategy
- Ecommerce & World Wide Web Design
- Network Penetration Analysis, Internet Exposure Profiles, Wardialing, and “Tiger Team Attacks”
- High Availability Design, Planning, Training, and Implementation
- Security, Network, & Operations Policy Development



Purpose and Setting Expectations

- Special issue of “Consumer Reports(tm)” on Wardialers and Wardialing
- History & Education
- Current Industry Practices
- Chart, Ratings, and Comparisons
- What Do You Need?



Wardialing 101

- Our Working Definition: An automated process to classify telephone resources.
- Another Definition [from The Hackers Handbook]: Phreaking systems for phun and profit.
- Historically, wardialing is the *first*, and oldest form of widespread illegal computer crime. Originally used to avoid long distance telephone charges, it quickly became the popular form of breaking into random business/governmental facilities, and now is the most pervasive, vulnerable method for attacking Internet and Intranet systems.



Why Wardialing is so threatening

- Telnet-like access to “secure systems”
- Remote control software
- Faxes or other analog phone lines
- ISDN modems
- Privacy
- Teleconference/televideo
- Voicemail/Pagers
- Denial of Service (turrets, Help Desk)
- Social Engineering
- Routers with a modem
- Dial-up servers
- Proprietary leased lines to databases or data feeds
- New acquisitions/mergers



The Art of Wardialing

- “How long does it take to find the vulnerabilities in my telephone system?”
- Some Industry answers:
 - Typical Contractor: “One week!”
 - Internal IT Department: “Eh...about a week?”
 - Realistically: “Depends on what you have.”
- You don’t know what you have.

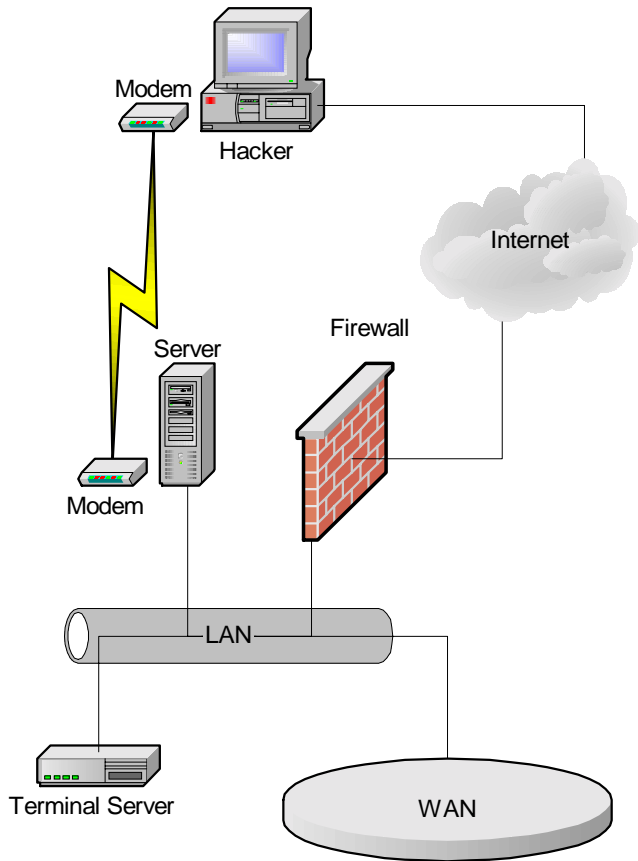


The Art of Wardialing

- How do I actually analyze my telephone exchange?
- Some Industry answers:
 - Typically: “We use a sophisticated suite of linked computers and modems, using custom tailored software for this purpose.”
 - Translation: “A couple of PC’s, a bunch of old 9600 baud modems, and ToneLoc.
 - Realistic: “The scary thing, this works pretty well.”
- You can do better.



The Science of Wardialing



- Path of least resistance
- Likely scenarios:
 - Install sniffer
 - Launch external attacks
 - Find WAN/partner connections



The Science of Wardialing

Check	Why	Comments
Country	Different countries have different telephone characteristics	Ringing tones can confuse modems. Adjust according to guard tones for a particular country.
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.
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.
Fax recognition	Fax machines use different protocols to negotiate a connection.	Faxmodems need to be "switched" to fax-mode or data-mode.
Phone services	Voicemail, call forwarding, call waiting	All of these features create unrecognizable dialtones for your modem. Modems do not recognize DTMF other than "vanilla", for example, unanswered voicemail creates a rapid DTMF.
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
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.
Data compression	Turn it off, if possible	v.42bis and MNP are used in for data compression
Flow control	Use hardware flow control, if possible	Some software emulations cause problems.
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
Serial port	Set to appropriate speed	Most com ports can support 115200 baud, but are default set to 9600. Adjust according to UART.



Criteria for Resource Allocation

- Basic Wardialing Sweep (BWS)
- Multiple Wardialing Sweep (MWS)
- Attended Wardialing Sweep (AWS)
- Quality versus Time
- False Positives
- Identifying ALL resources

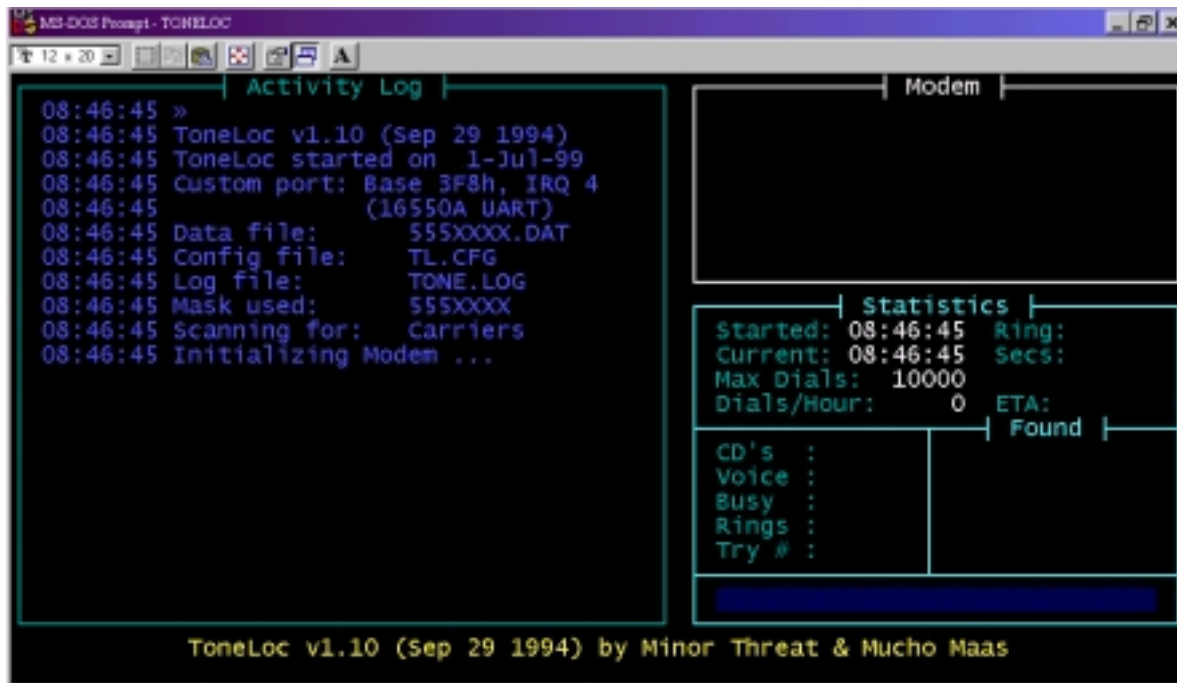


Wardialers

- Commercial
 - equipment-specific, but fairly powerful
 - a few new general-purpose
- Homegrown
 - fairly versatile, but little classification
- Hackerware
 - most powerful tools



Wardialers



```
MS-DOS Prompt - TONELOC
12 * 20
Activity Log
08:46:45 »
08:46:45 ToneLoc v1.10 (Sep 29 1994)
08:46:45 ToneLoc started on 1-Jul-99
08:46:45 Custom port: Base 3F8h, IRQ 4
08:46:45 (16550A UART)
08:46:45 Data file: 555XXXX.DAT
08:46:45 Config file: TL.CFG
08:46:45 Log file: TONE.LOG
08:46:45 Mask used: 555XXXX
08:46:45 Scanning for: Carriers
08:46:45 Initializing Modem ...

Modem

Statistics
Started: 08:46:45 Ring:
Current: 08:46:45 Secs:
Max Dials: 10000
Dials/Hour: 0 ETA:

Found
CD's :
Voice :
Busy :
Rings :
Try # :

ToneLoc v1.10 (Sep 29 1994) by Minor Threat & Mucho Maas
```



Wardialing How-To

- Set ground rules
 - scheduling, escalation plan
- Contact legal and telephone regarding liability
- Pass 1 Dial & construct a database of numbers
 - voice, vmb, tones, carriers, busy
- Pass 2 Classify Unknowns & Exploit Vulnerabilities
 - telnet-like prompts, NT RAS, PCAnywhere(tm)
- Be organized



What We are Seeing

- Statistics
 - carriers
 - 2-5% hits on normal ranges
 - 20-60% have simple or no passwords/banners
 - Findings:
 - databases & other critical servers
 - routers/telco
 - personal/remote control software
 - terminal servers & dial-up hardware
-



What We are Hearing

- Frustration...
 - Current wardialing software generates false positives...although you may not know it
 - Usually, software requires several “passes” or sweeps to find specific types of vulnerable devices
 - No automated way to classify carriers
 - No Intrusion Detection
 - Social engineering on the rise
 - Internet Vulnerabilities are just the front door
 - International Exchanges worse than National
-



Common Problems

- No banners
- Low quality passwords
- No policy (procedures, controls/auditing)
- New acquisitions/mergers have lower security standards
- Susceptible to PIN guessing & bombing attacks
- PBX tones/third party dialing



The Challenge

- Buy-in at the employee level for new policies/procedures
- New methodology for sysadmins
- Regular AWS
 - baselining
 - full sweeps
 - random sampling over the year
- Vetting wardialers & tools



Oh, By the Way

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



Oh, By the Way

- Whitepaper

- Links:

<http://www.paranoia.com/~mthreat>

<http://www.escape.com/~evian/>

