



The WorldWide WarDrive:

The Myths, The Misconceptions, The Truth, The Future

Chris Hurley aka Roamer

History

- I was talking with The Watcher on the Netstumbler Forums and found out we live relatively close to each other.
- We thought it would be fun to try to coordinate a WarDrive to cover the entire city of Baltimore and started a thread on the Netstumbler Forums to see if there was any interest.
- Renderman decided to do a coordinated drive in his area.
- Blackwave and Mentat had discussed a similar idea in the past.



History

- I posted the idea on the DefCon Forums to see if there was any more interest. There was.
- That coordinated drive of Baltimore quickly evolved into the WorldWide WarDrive.



The Myths

Myths are the false impressions about the WorldWide WarDrive and WarDriving in general that have been thrust upon the general public by the media and the uninformed (not mutually exclusive).





The myth that the WorldWide WarDrive is a covert organization run by shady individuals out to provide terrorists with information has been propagated by several different media organizations.



“The group that runs the www.worldwidewardrive.org Web site leaves its own identity secret but does offer numerous links to other like-minded organizations as well as giving a somewhat cryptic e-mail address, roamer@worldwidewardrive.org, for those interested in organizing their own local efforts.

Wardrive appears to be an offshoot of warchalking, another tactic intended to disclose unsecured wireless networks.”

Source: Wardrive attempts to find unsecured wireless networks

by Ephraim Schwartz http://www.infoworld.com/article/02/10/24/021024hnwardrive8_1.html

Using a handle or online identity is “an act of hiding your identity”

Many individuals use an online name or handle. My real name is all over the WWWD site.

There appears to be no description of the WWWD members

There are no “members” of the WWWD. The individual organizers’ sites often have information about themselves.

A link from a for profit security company is on the WWWD site.

This is just not true. The for profit issue is even addressed in the WWWD FAQ:

"Can I hire you to secure my access point for me?

No"



WWWD participants “warchalk” the access points discovered during the worldwide wardrive

*The WWWD FAQ also specifically addresses warchalking:
"Do you "WarChalk" the APs you find?
No. I think WarChalking is stupid."*

*Neither I nor anyone I know has actually
SEEN a chalked AP.*

WarDriving is an “offshoot” of warchalking.

*Certainly one was "derived" from the other. He just had it
backwards.*





There is a prevalent myth that the Information Security Industry has a hard time locking down access points and securing wireless networks



War driving bedevils security types partly because it is so cheap and easy to do. Drivers amble around with a directional antenna sometimes fashioned from a coffee or potato-chip can. Their software of choice, called NetStumbler, comes free on the Web and detects the low-level radio waves coming out of wireless-network access points.

Source: Hackers target wireless networks Worldwide 'war drive' set for Saturday by William M. Bulkeley
<http://www.msnbc.com/news/824622.asp?cp1=1>



The media has also pushed the myth that the WWWD is an attempt to provide people with information on how to get free internet access.

People with knowledge of the location of an unprotected wireless network can also use it for free Web surfing, to send out e-mail messages or spam anonymously.

Anyone who wants to access a network without authorization isn't going to look to online sources to find access points.

It would be faster to just find one outside.

Participants make chalk marks on sidewalks or building fronts to signal the availability of access points.

Knowing such locations permits people with laptops to avoid paying for Internet access.



This has already been exposed as a myth. This just doesn't happen





WARChALKING IS A MYTH!!

Do you warchalk?
You have already voted on this poll.

Yes		0	0%
No		48	100.00%
Total:		48 votes	100%

The Misconceptions

Misconceptions are the false impressions that those within the hacking community, the security industry, and some Law Enforcement Organizations have about the WorldWide WarDrive and WarDriving in general.





A common misconception is that the WWWD is an attempt to propagate FUD and scare Security Professionals and Network Administrators



According to an article that ran at net-security.org IT managers should be wary of Aug 31st (Kickoff of first WWWD)

IT managers have no reason to fear the WWWD. Our goals clearly state that we make no attempt to access ANY networks.

“Hackers armed with laptops” are looking for unprotected networks

We are making a statistical analysis of ALL access points, not just the “unprotected” networks



Some within the hacking and wireless communities have the misconception that the WWWD is a marketing tool to sell products or services.



The WWWD data is being used to:

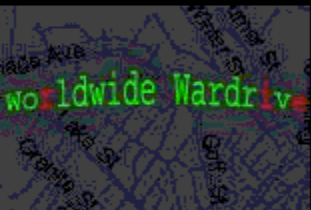
- 1) Contact people for the purpose of selling their services
- 2) Show to potential customers to point out how "insecure" everyone is
- 3) The WWWD did not respond to these accusations when confronted with them.

1) We sell nothing. Period. We provide FREE information on the site on how to "secure" their APs.

2) See point 1. We have no customers nor do we have any potential customers.

3) I was given only 36 hours from the time these accusations were mailed to me until this email was sent to the kismet list.





There is a misconception that during the WWWD wireless networks are more likely to be attacked/compromised.

This one was prevalent from the start of the first WWWD. SANS was probably my favorite offender here.

From SANS NewsBites, 11 September 2002:

--9 September 2002 Wardriving Reveals Lack of LAN Security A week-long worldwide wardrive revealed that many wireless LANs (local area networks) don't employ even basic security. A New Jersey-based company is selling complete wardriving kits. A consultant for the company observed that wardriving is legal and has legitimate uses.

[Editor's Note (Murray): it is legal to look in your neighbor's open window but nice people do not do it. There is no more corrupting idea than the current one that that which is legal is, ipso facto, ethical.]





The Canadian Security Intelligence Service was very concerned about the first WorldWide WarDrive.

=====
FOR IMMEDIATE **RELEASE**
=====

Hackers and geeks worldwide will be inaugurating the first international wardriving day, Saturday August 31st, 2002.

"Wardriving" is a cousin of "war dialing," a term popularized in the 1983 movie "War Games.". War dialing used software to dial many phone numbers automatically, looking for tones which indicated a modem. Wardriving, also known as "net stumbling," is a new variant, focused on discovering wireless computer networks.

This is a "high-tech" hobby, where participants armed with laptops, wireless networking gear, global positioning units and vehicles compete to find as many "wireless" networks in their regions as possible. There are literally tens of thousands of wireless networks operating throughout the world.

Hundreds have already been mapped in Calgary and Edmonton, let alone other communities throughout Alberta.

While there are no prizes, no rules and definitely no glamour, this activity is constructive in that it raises awareness with regards to: privacy, security (or alternatively a complete lack of security), and the growing number of wireless networks sending information over, around and through an area.

On Saturday, August 31st, participants will depart from Edmonton and Calgary converging on Red Deer, Alberta. At which point, we will plan a wardriving route, which we will then use to map Red Deer upon departure.

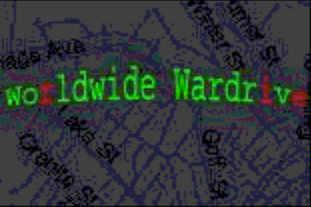
Meeting time & location:

10 AM

White Spot

6701 - 50th Avenue, Red Deer, AB

We would be pleased to include media representatives for participation as passengers, or competitors. We can provide transportation or setup instructions as appropriate. Space is obviously limited, so contact us ASAP.



“3. A computer enthusiast from Edmonton issues a press release on 21 August 2002, stating that he was arranging a war-driving exercise in Red Deer, Alberta, on 31 August 2003 as a component of the internationally scheduled event...”

“4. Wireless technology makes it easier for“ attackers “to search for data and invade the privacy of networks users since computer networks have no physical boundaries.”

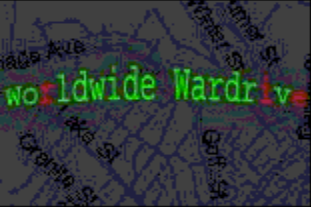
Luckily, the CSIS ended up educating themselves. It was quickly discovered that the WWWD had no untoward intentions



The Truth

The WorldWide WarDrive is an effort by security professionals and hobbyists to generate awareness of the need by individual users and companies to secure their access points. The goal of the WorldWide WarDrive (or WWWD) is to provide a statistical analysis of the many access points that are currently deployed.

We feel that many end users are not aware that the factory or "default" settings on Access Points do not take any security measures into account. By providing these statistics we hope that end users will become aware of the need to take simple measures to secure their access points.



The First WorldWide WarDrive

The First WorldWide WarDrive took place between 31 August and 7 September 2002. Approximately 100 people participated in 22 areas. 6 Countries and 2 Continents were represented.



The First WorldWide WarDrive

CATEGORY	TOTAL	PERCENT
TOTAL APs FOUND	9374	100
WEP Enabled	2825	30.13
No WEP Enabled	6549	69.86
Default SSID	2768	29.53
Default SSID and No WEP	2497	26.64
Unique SSIDs	3672	39.17
Most Common SSID	1778	18.97
Second Most Common SSID	623	6.65



The Second WorldWide WarDrive

CATEGORY	TOTAL	PERCENT	PERCENT CHANGE
TOTAL APs FOUND	24958	100	+62.5
WEP Enabled	6970	27.92	-2.21
No WEP Enabled	17988	72.07	+2.21
Default SSID	8802	35.27	+5.74
Default SSID and No WEP	7847	31.44	+4.8
Most Common SSID	5310	21.28	+2.31
Second Most Common SSID	2048	8.21	+1.56



The Third WorldWide WarDrive



The Third WorldWide Wardrive took place from June 28 – July 5 2003. Approximately 300 people in 52 areas participated. 11 countries and 4 continents were represented.

The Third WorldWide WarDrive

Results will be released at DefCon 11

CATEGORY	TOTAL	PERCENT	PERCENT CHANGE
TOTAL APs FOUND	88122	100	+71.68
WEP Enabled	28427	32.26	+4.34
No WEP Enabled	59695	67.74	-4.34
Default SSID	24525	27.83	-7.44
Default SSID and No WEP	21822	24.76	-6.68



The Combined Results from
All Three WorldWide WarDrives
will be released at DefCon 11

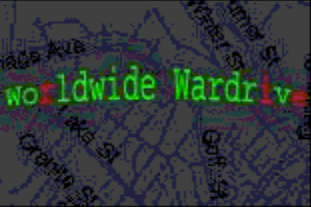
CATEGORY	TOTAL	PERCENT
TOTAL APs FOUND	113529	100
WEP Enabled	35654	31.41
No WEP Enabled	77875	68.59
Default SSID	32938	29.01
Default SSID and No WEP	29276	25.78



The WWWD Coin

These 30 contributors are the inaugural class of WWWD coin recipients.

Blackwave	Maui	Agent Green
AirFoot	Ffrf	Renderman
WiGLE	DaClyde	Mentat
Deadtech	Vtosearch	Mother
DT	Dragorn	Marius
Korben	BKS	Converge
Fred	Borg Man	Pete Shipley
Medic	Shmoo	Novillo
Thorn	Mr. White	JimmyPopAli
Rambopfc	C-mag	Sparafina



Conclusion..aka The Future

WWWD Stat generator will be released by the Church of WiFi.

WWWD will be an annual event.

Data upload/stat generation will be an automated (and instant) process.

