



webroot[®]
SOFTWARE

eCrime: Is the Hype around Spyware Justified?

Stuart Jones
EMEA Product Evangelist





webroot™

Spy Sweeper™

Enterprise

Agenda

Privacy. Protection. Peace of mind.

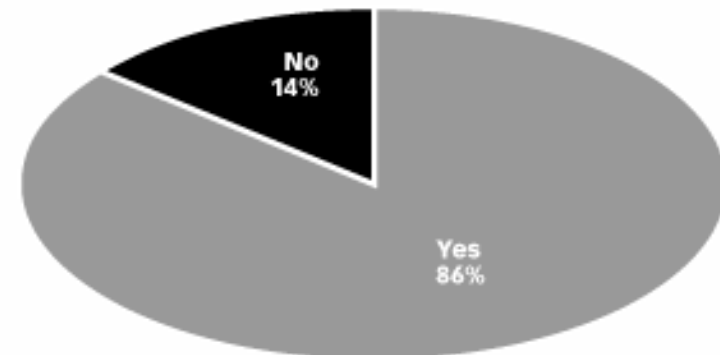
- What is Spyware is it a Mystery?
- How do we get Infected?
- What is the Impact to your Business?
- What should we be asking of our Vendor(s)?
- How do I determine if my Organisation has a Spyware Issue?

The Mystery (Misery) of Spyware

Privacy. Protection. Peace of mind.

- Users are not sure about what spyware is, how it got on their computers, or how to get rid of it.
- The one thing most people are sure about is that they don't like it.
- More than 86% of those who report having been infected with spyware believe they have experienced a monetary loss, a productivity loss or some other inconvenience.
- People *hate* spyware — even if they don't understand exactly what it is

US Adult Internet Users Who Believe that Spyware on Their Computers Has Caused Them to Suffer a Monetary Loss, 2005 (as a % of respondents)



Note: n=1,630; both spyware and adware assist in gathering information about a person or organization and send it to other interested parties. The difference is that you agree to download adware in exchange for free software or other offers. Spyware is downloaded without your consent or awareness that it is on your computer collecting information about you
Source: Ponemon Institute commissioned by Unisys Corporation, May 2005

065580 ©2005 eMarketer, Inc.

www.eMarketer.com

What is Spyware?

Privacy. Protection. Peace of mind.

- Spyware and Other Potentially Unwanted Technologies are “technologies... that impair the user’s control over... changes that affect their user experience, privacy, or system security.” *

- Degrading user experience:
 - Using (*stealing*) system resources
 - Showing unwanted advertisements/content (pornography)
 - Redirecting user through false search results and other hijacks

- Harvesting user information
 - Login/password info
 - Account information
 - Surfing habits
 - Shopping habits
 - Computer files



*ASC Definitions and Supporting Documents, July 2005



webroot™

Spy Sweeper™

Enterprise

Defining Spyware

Privacy. Protection. Peace of mind.

System Monitors

Trojans

Adware

Cookies



webroot™

Spy Sweeper™

Enterprise

Cookies

Privacy. Protection. Peace of mind.

Cookies

Text files used to gather limited information about a user's activities or to identify a user. They can also store sensitive personal information such as passwords and user names.

- Cookies are NOT executable files
- Some organizations don't consider them a threat
- Some websites do not work properly if cookies are not allowed
- Most browsers now have built in support to completely disallow the use of cookies, or to delete them when the browser is closed



webroot™

Spy Sweeper™

Enterprise

Adware

Privacy. Protection. Peace of mind.



Adware

Adware's primary function is to serve advertisements to the user, in some way directing them to towards products for sale.

It can present itself in many forms:

- Browser Helper Objects
- Browser-ad overwrites
- Homepage Hijackers
- Pop-ups/Pop-unders
- Search Hijackers
- Desktop Hijackers



webroot™

Spy Sweeper™

Enterprise

Trojan Horses

Privacy. Protection. Peace of mind.

Trojans

Trojan Horses are named such because the user usually thinks that they're getting something that they want, while they're really just getting something very nasty.

1. **Trojan Downloader:** After install, the Trojan contacts a remote host or site and then it installs packages or affiliates from the remote host.
2. **Trojan Backdoor:** contacts a remote site. opens up the computer to be further compromised by way of this remote contact.
3. **Trojan Bot:** A Trojan Bot is a program that compromises the system so that it can be controlled sending spam, or transferring sensitive information on command



webroot™

Spy Sweeper™

Enterprise

Keyloggers/System Monitors

Privacy. Protection. Peace of mind.

System Monitors

Covertly or overtly records system processes and/or user actions

Makes those records available for retrieval and review at a later time

- Time of power on
- Login information
- Email passwords
- Financial account information
- Credit card numbers
- Social security numbers
- Screenshots
- Phone numbers
- Addresses
- Keystrokes
- Webcam photos
- Sound
- Time of power off

Keyloggers and System Monitors are used by thieves to steal identity information and account information.

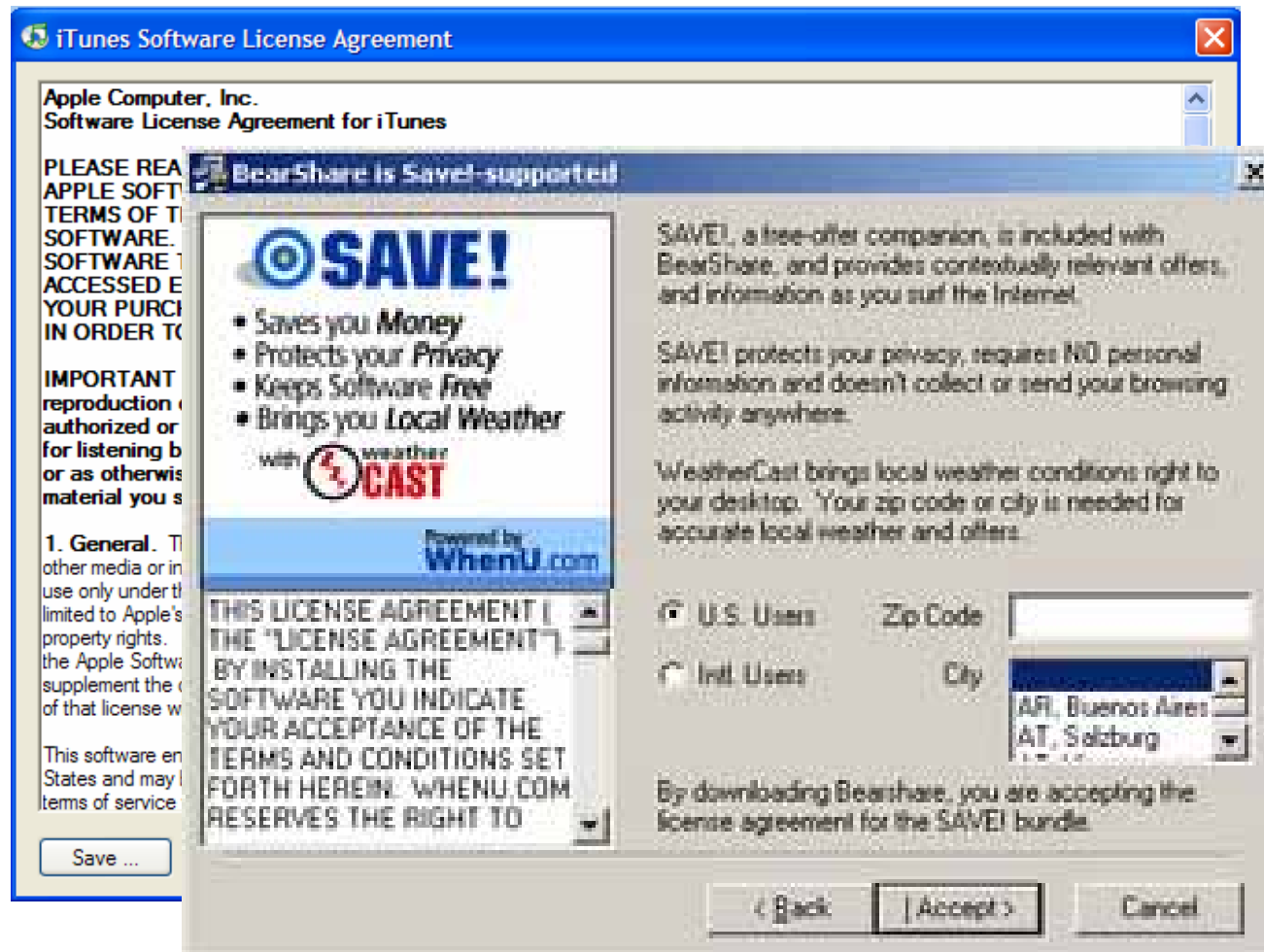


How do we get Infected?



How do we get Spyware?

Privacy. Protection. Peace of mind.



Spyware Propagation

Privacy. Protection. Peace of mind.

Drive-By websites:

- A computer user may unwittingly surf to a website with malicious code designed to take advantage of various browser exploits
- A recent, widely-known example of this was the www.google.com site
- When the user arrived there, up to 49 different exploits were waiting for them
 - Even a system with the most current level of OS security patches can be infected
 - Most often, though, users are not up to date on security patches

Peer-to-Peer Network Search Results:

New and sophisticated applications will propagate on P2P networks.

- A user will search for an application or file and an infected peer will detect the search and offer a virtually-named, or renamed file that is actually some form of spyware. When the file is downloaded and executed, the user's system becomes infected.

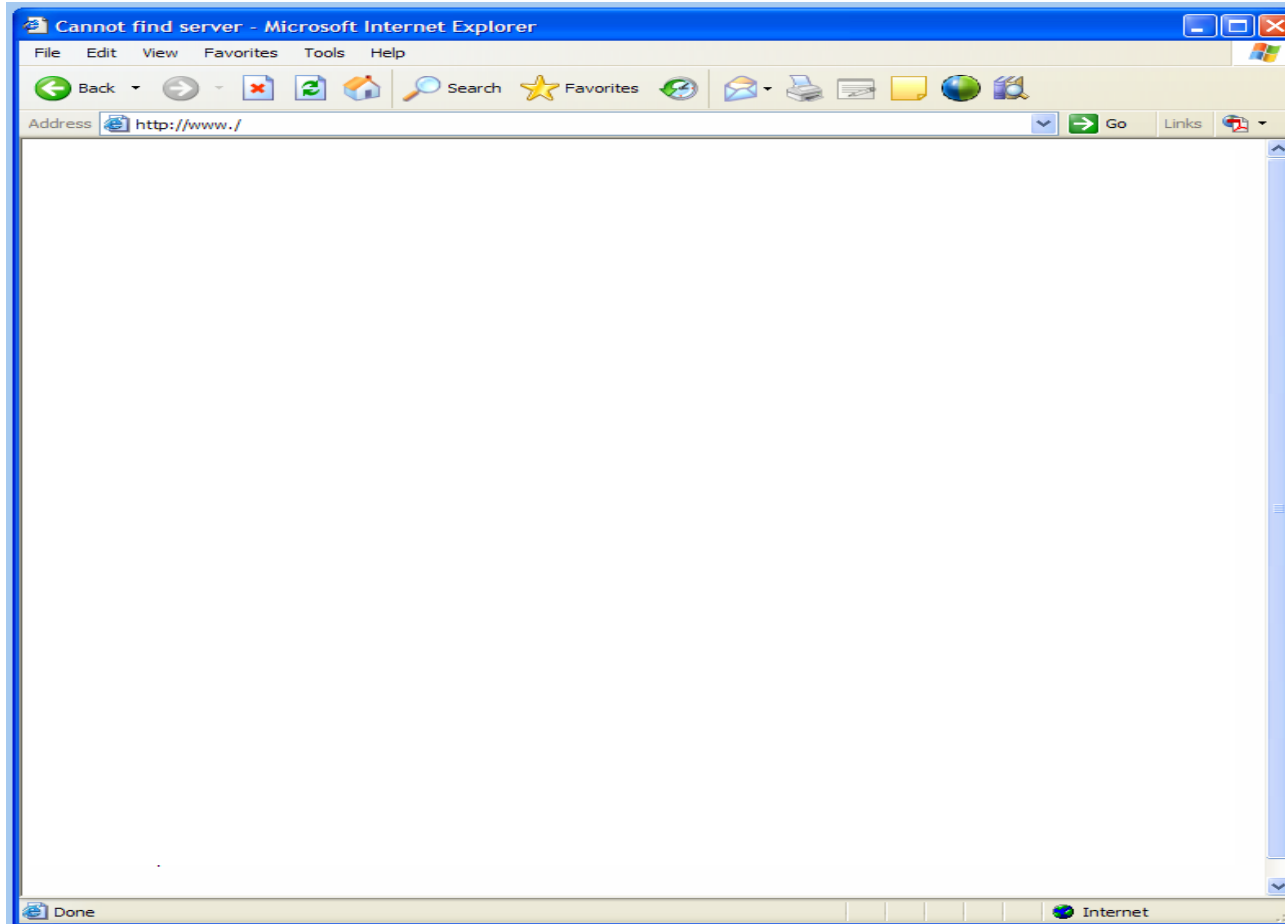
Evolving Spyware and Distribution Techniques

Privacy. Protection. Peace of mind.

- Evolving distribution and obfuscation methods
 - Rootkit-like behavior continues to increase
 - Re-emergence of phishing Trojans
 - New phishing Trojans include code updates implementing rootkit-like functionality and advanced obfuscation procedures
 - The top threats this quarter displayed the continued use of packing and encryption algorithms
- Keyloggers are becoming more aggressive
 - Continue to use kernel-level drivers
 - Use process blocking techniques to actively stop anti-spyware programs from running
- Adware programs have become more aggressive
 - Adopting sophisticated techniques used by malicious spyware writers to evade detection and removal
 - Many of these programs continue to download adware programs onto a machine without the user's consent.
 - Often will download a toolbar, advertisements and hijacks browser settings without consent

Infection... you think it's not a problem!

Privacy. Protection. Peace of mind.

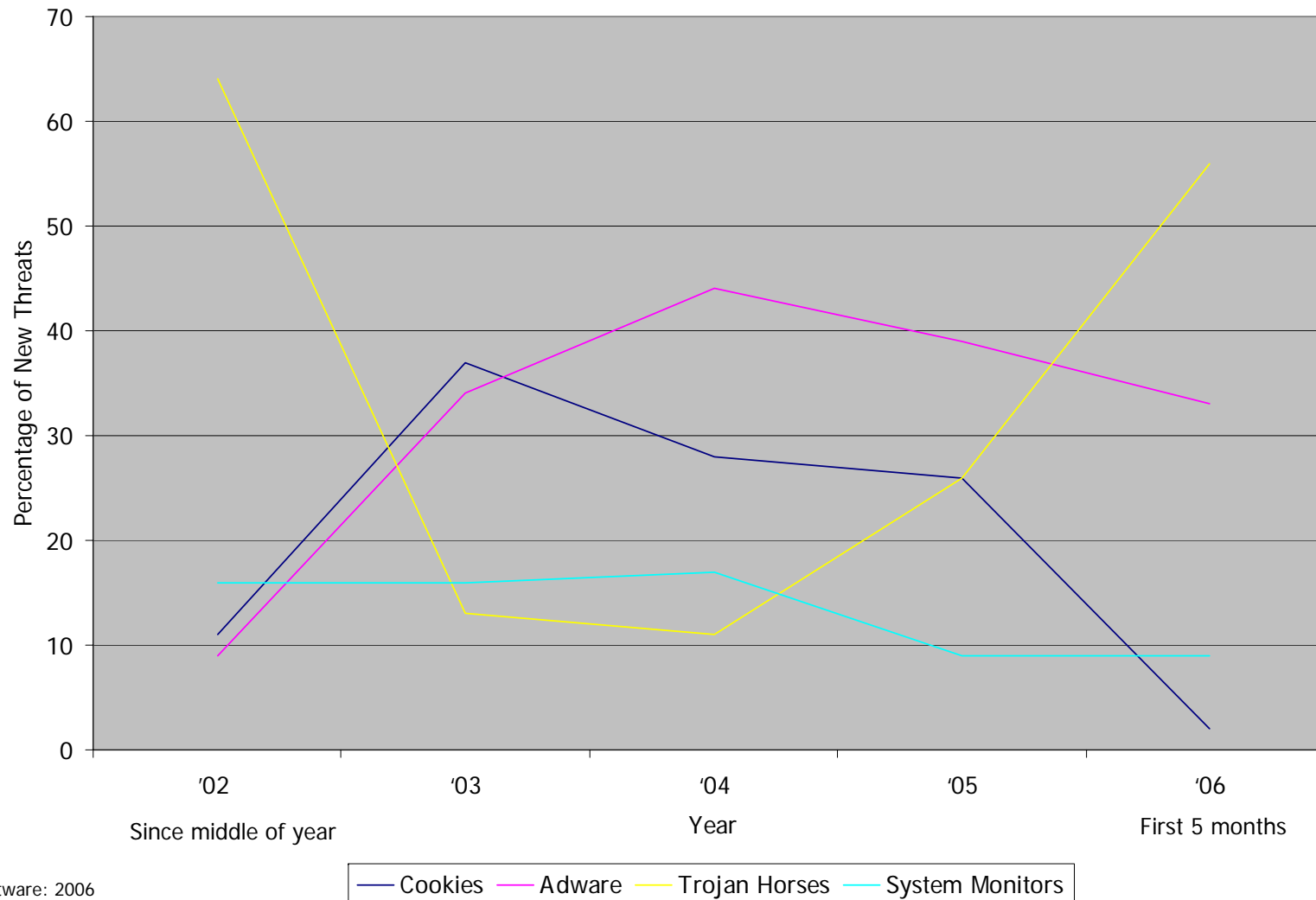


A Web Browser Highly Infected By Browser Helper Objects, Hijackers, and Other Various Types of Spyware



Threat Trends

Privacy. Protection. Peace of mind.



Threat Trends

Privacy. Protection. Peace of mind.

- Spyware is getting more sophisticated and the threat continues to grow in complexity and maliciousness – with a recent rash of spies using rootkit capabilities to hide deep within a user's PC and avoid detection
 - Disguised as legitimate traffic using legitimate ports
 - Self-modifying code at time of installation and/or run-time
 - Obscured processes and file names
 - Process monitoring to prevent removal
- Number of known spyware distribution sites have quadrupled this year - over 400,000 sites in total, and rising
- Over 141,000* traces of Spyware

Staying ahead of spyware requires commitment and leadership in research.

* As of beginning July 2006



What is the Impact to your business?



The Pain

Privacy. Protection. Peace of mind.

- Incidents of spyware will continue to rise driven by monetary gain potential – e-crime activity is on the rise
- Strain on the Help Desk and corporate IT
 - 20% - 50% of all enterprise Help Desk calls involve Spyware
 - About one-third of all Windows crashes due to Spyware*
 - Typical rebuild time is 2-3 hours per PC
- Reduced desktop & network performance and functionality
 - Consumes valuable network bandwidth to transmit data back to network spyware agents
 - Premature requirement for desktop upgrade
- Severely impacts employee productivity
 - How long will users put up with spyware issues before calling help desk?
 - Lost Employee productivity due to desktop downtime



•Source: Microsoft -- data from Windows error reporting tool, which sends data back to Microsoft when an application crashes

The Risk

Privacy. Protection. Peace of mind.

- Average 13 percent of enterprise PCs are infected with malicious spyware, including Trojans and System Monitors
- Access proprietary corporate information
 - Compromised passwords, admin privileges, applications
 - Intellectual Property
 - Sensitive customer data
 - Employee & company financial information
 - Litigation data, etc.
- Direct Implications to Compliance
 - Sarbanes Oxley, FDIC, Gramm-Leech-Bliley (GLB) – Adoption of prevention
 - EMEA Italy -Testo Unico compliances is now in place
 - EMEA – Basel II





webroot™

Spy Sweeper™

Enterprise

Can you afford to be in the News?

Privacy. Protection. Peace of mind.

Choice Point identity theft	145,000 individuals affected
Ransom - A Threatens to delete or encrypt files	When activated will delete files every 30s unless a ransom is paid
Sumitomo Bank keystroke logger	£220m compromised
Israeli Trojan horse	High-profile companies indicted -- confidential data stolen
Card Systems systems hacked	40m individuals affected
Rebery Trojan captures, names, CC No's, log-ins, 1000's passwords, social security No's.	Distributed through "teens7.com" Steals data sent to central FTP server. In 109 countries in over 10,000 pc's
Sony BMG The use of rootkits in their digital rights management software, bundled with various music CDs	File obfuscation techniques, allow spyware to avoid detection and removal
UK – HealthCare , patient records stolen Drive-By methods	30,000 Records. Only discovered when data was sold to Scotland Yard undercover police officers.

Security Institutions state that only 1/5th of high-profile companies make incidents public. €38B was compromised in FY05



**What should we be asking of our
Vendor(s)?**





webroot™

Spy Sweeper™

Enterprise

Questions

Privacy. Protection. Peace of mind.

- How Proactive are you in finding the threats
 - Is it your primary focus?
 - How frequent do you release new definitions?
 - Do you prevent & remove threats?
- Will it work with my environment
 - How do you handle false positives?
- Easy of use and deployment
 - Can I use my existing software deployment package?
 - Is it a gateway or desktop solution?
- Centrally Managed
 - Multiple policies can be created?
 - Automated updates of software and policies to clients?
- Reporting
- Support



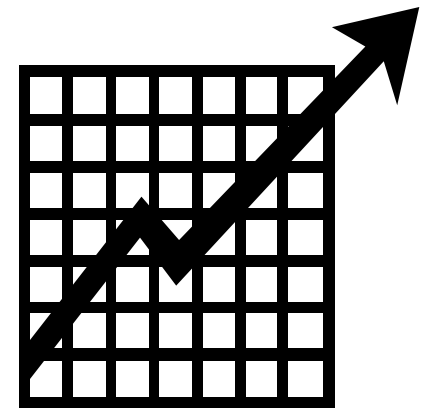
**How do I determine if my
Organisation has a Spyware Issue?**



The Anti-Spyware Market

Privacy. Protection. Peace of mind.

- Anti-spyware was the fastest-growing segment of the Secure Content Management (SCM) market in 2004, reaching **€90M**.
 - From 2003 – 2005, the anti-spyware market increased by **204.4%**
- Anti-spyware will increase from **€90M** in 2004 to **€620M** in 2009
 - Representing a compound annual growth rate (CAGR) of **45.9%**
- The entire SCM market as a whole is only expected to grow at a CAGR of **18.7%**



*IDC: WW Secure Content Management 2005-2009 Forecast Update

Which one are you?

Privacy. Protection. Peace of mind.

Company	X	Y	Z
Total No of PC's	11,500	12,900	12,000
Total No of PC's Audited	996	9,578	2,287
Total No of Threats Found			
System Monitors	3	125	0
Trojan Horses	15	91	0
Adware	720	1,208	29
System Cookies	32,768	413,993	68,225

Can you guess which result is associated to an Energy, Defence or Financial Company?

Ask Webroot for your free Spy Audit,
can you afford not to?



Conclusion



5 Ways to keep **YOU** safe from e-crime

Privacy. Protection. Peace of mind.

1. Firewall, URL & Email Filtering etc.
2. Security Updates
3. Anti-virus
4. Anti-spyware
5. **Be paranoid!**

**Don't let someone else find the loopholes
in your security system**



webroot[®]
SOFTWARE

Thank You

Stuart Jones
EMEA Product Evangelist



ware