

McAfee Security 2009

Comprehensive & Easy to Use! The Only Solution You Need, McAfee.

www.McAfee.com/au

Firewall Security

Fully qualified security experts. Informed assessment & advice.

www.ClassicBlue.com.au

New Business IT Advice

ds3 provides true Partnership in IT Private, SME and Corporate services

www.ds3.com.au

SAS Business Intelligence

Fast. Simple. Consistent. Accurate. SAS Software. Free Info Kit

www.Sas.com/australia

Computer Security

Get Nokia VPN and Firewalls for both Large and Small Businesses.

www.nokiaforbusiness.com

Avoid Email Threats

Complimentary Strategy Guide Top Tips for 2008

www.Computerworld.com.au

Internet Security Tools

Free Internet Security Scan. Winner of Best Anti-Spyware,

Rated 5 Stars

www.PCTools.com

Free eBook & Whitepaper

Data Center Network Leader Shares Security Insight - Free Resources

Brocade.com

Norton Internet Security™

Faster, stronger protection against online threats. Download now!

www.Norton.com

PGP Hard Disk Encryption

Leading Enterprise Solution Free Buyer's Guide

www.pgpssoftware.com.au



Cryptome DVDs are offered by Cryptome. Donate \$25 for two DVDs of the Cryptome 12-years collection of 46,000 files from June 1996 to June 2008 (~6.7 GB). Click Paypal or mail check/MO made out to John Young, 251 West 89th Street, New York, NY 10024. The collection includes all files of cryptome.org, jya.com, cartome.org, eyeball-series.org and iraq-kill-maim.org, and [23,000 \(updated\)](http://23,000) pages of counter-intelligence dossiers declassified by the US Army Information and Security Command, dating from 1945 to 1985. The DVDs will be sent anywhere worldwide without extra cost.

Google™

Search

Web
 cryptome
 jya.com
 eyeball-series.org
 cryptome.cn

18 October 2008. Thanks to Robert Eringer.

And now the Manchurian microchip

Robert Eringer

October 18, 2008 7:13 AM

The geniuses at Homeland Security who brought you hare-brained procedures at airports (which inconvenience travelers without snagging terrorists) have decreed that October is National Cyber Security Awareness Month. This means The Investigator -- at the risk of compromising national insecurities -- would be remiss not to make you aware of the hottest topic in U.S. counterintelligence circles: rogue microchips. This threat emanates from China (PRC) -- and it is hugely significant.

The myth: Chinese intelligence services have concealed a microchip in every computer everywhere, programmed to "call home" if and when activated.

The reality: It may actually be true.

All computers on the market today -- be they Dell, Toshiba, Sony, Apple or especially IBM -- are assembled with components manufactured inside the PRC. Each component produced by the Chinese, according to a reliable source within the intelligence community, is secretly equipped with a hidden microchip that can be activated any time by China's military intelligence services, the PLA.

"It is there, deep inside your computer, if they decide to call it up," the security chief of a multinational corporation told The Investigator. "It is capable of providing Chinese intelligence with everything stored on your system -- on everyone's system -- from e-mail to documents. I call it Call Home Technology. It doesn't mean to say they're sucking data from everyone's computer today, it means the Chinese think ahead -- and they now have the potential to do it when it suits their purposes."

Discussed theoretically in high-tech security circles as "Trojan Horse on a Chip" or "The Manchurian Chip," Call Home Technology came to light after the Defense Advanced Research Projects Agency (DARPA) launched a security program in December 2007 called Trust in Integrated Circuits. DARPA awarded almost \$25 million in contracts to six companies and university research labs to test foreign-made microchips for hardware Trojans, back doors and kill switches -- techie-speak for bugs and gremlins -- with a view toward microchip verification.

Raytheon, a defense contractor, was granted almost half of these funds for hardware and software testing.

Its findings, which are classified, have apparently sent shockwaves through the counterintelligence community.

"It is the hottest topic concerning the FBI and the Pentagon," a retired intelligence official told The Investigator. "They don't know quite what to do about it. The Chinese have even been able to hack into the computer system that handles our Intercontinental Ballistic Missile system."

Another senior intelligence source told The Investigator, "Our military is aware of this and has had to take some protective measures. The problem includes defective chips that don't reach military specs -- as well as probable Trojans."

A little context: In 2005 the Lenovo Group in China paid \$1.75 billion for IBM's PC unit, even though that unit had lost \$965 million the previous four years. Three congressmen, including the chairman of the House Armed Services Committee, tried to block this sale because of national security concerns, to no avail. (The PRC embassy in Washington, D.C., maintains a large lobbying presence to influence congressmen and their staffs through direct contact.)

In June 2007, a Pentagon computer network utilized by the U.S. defense secretary's office was hacked into -- and traced directly back to the Chinese PLA.

A report presented to Congress late last year characterized PRC espionage as "the single greatest risk to the security of American technologies." Almost simultaneously, Jonathan Evans, director-general of MI5, Britain's domestic security and counterintelligence service, sent a confidential letter to CEOs and security chiefs at 300 UK companies to warn that they were under attack by "Chinese state organizations" whose purpose, said Mr. Evans, was to defeat their computer security systems and steal confidential commercial information.

The Chinese had specifically targeted Rolls-Royce and Shell Oil.

The key to unlocking computer secrets through rogue microchips is uncovering (or stealing) source codes, without which such microchips would be useless. This is why Chinese espionage is so heavily focused upon the U.S. computer industry.

Four main computer operating systems exist. Two of them, Unix and Linux, utilize open-source codes. Apple's operating system is Unix-based.

Which leaves only Microsoft as the source code worth cracking. But in early 2004, Microsoft announced that its security had been breached and that its source code was "lost or stolen."

"As technology evolves, each new program has a new source code," a computer forensics expert told *The Investigator*. "So the Chinese would need ongoing access to new Microsoft source codes for maintaining their ability to activate any microchips they may have installed, along with the expertise to utilize new hardware technology."

No surprise then that the FBI expends much of its counterintelligence resources these days on Chinese high-tech espionage within the United States. Timothy Berezney, while still serving as assistant director of the FBI's Counterintelligence Division, told *USA Today*, "Foreign collectors don't wait until something is classified -- they're targeting it at the research and development stage." Mr. Berezney now heads Raytheon's Intelligence and Information Systems division.

The PRC's intelligence services use tourists, exchange students and trade show attendees to gather strategic data, mostly from open sources. They have also created over 3,500 front companies in the United States -- including several based in Palo Alto to focus on computer technology.

Back in 2005, when the Chinese espionage problem was thought to be focused on military technology, then-FBI counterintelligence operations chief Dave Szady said, "I think the problem is huge, and it's something we're just getting our arms around." Little did he know just how huge, as it currently applies to computer network security.

The FBI is reported to have arrested more than 25 Chinese nationals and Chinese-Americans on suspicion of conspiracy to commit espionage between 2004 and 2006. *The Investigator* endeavored to update this figure, but was told by FBI spokesman William Carter, "We do not track cases by ethnicity."

Excuse us for asking. We may be losing secrets, but at least the dignity of our political correctness remains intact.

Oh, and Homeland Security snagged comic icon Jerry Lewis, 82, trying to board a plane in Las Vegas with a gun -- no joke.

*If you have a story idea for *The Investigator*, contact him at reringer@newspress.com. State if your query is confidential.*
