



FBI Fears Chinese Hackers and/or Government Agents Have Back Door Into US Government & Military Computer Networks

Some months ago, my contacts in the defense industry had alerted me to a startling development that has escalated to the point of near-panic in nearly all corners of Government security and **IT infrastructure**. The very-real concern, being investigated by the FBI, is that either the Chinese government or Chinese hackers (or both) have had the benefit of undetectable back-doors into highly secure government and military **computer networks** for months, perhaps years. The cause: a high-number of counterfeit Cisco routers and switches installed in nearly all government networks that experienced upgrades and/or new units within the past 18 months.

News of the counterfeit Cisco equipment has been in the mainstream for some time:
Co llaborative Current Event: Counterfeit Cisco Network Hardware Imported From China Seized
Chinese Counterfeit Cisco Network Routers Targeted In North America
Counterfeit Cisco Gear Showing Up In US

But the US government has been attempting to avoid these issues by only using higher-end Cisco partners/suppliers for the gear. However, the highly-competitive lowest-bid environment of government procurement has inspired several vendors to look for cheap alternatives for hardware... resulting in a catastrophic meltdown of security.

A few weeks ago, my sources have been providing information on a scathing investigation summary by the FBI. They've indicated that a critical Powerpoint document has been quietly circulating after a few internal presentations. While the **Powerpoint presentation** has been labeled unclassified, it is an official FBI publication and has been hard to track down. Thanks to key clues provided last week by two sources (both of which do not have the **presentation**, but have seen it), specific searches on the content of the document have turned up an online source, and I've provided all pages of the document below, along with the link to the discovered

As you can see, the FBI is concerned about critical **infrastructure** damage, AND, the potential of access to secure government systems. Many online IT circles have been speculating that the counterfeit hardware will provide backdoor capabilities and access into compromised networks for the originators of the equipment. In fact, some areas of speculation regarding the counterfeit Cisco equipment has focused on the possibility that the hardware is being manufactured expressly to deploy exploitable **systems** far and wide into the wild. The rationale being that the likely "wholesale" price of the counterfeit routers and switches are so low and profit margins likely very thin, that the only real advantage may be gained from downstream system exploits in the future.

The threat is real. Compromised hardware of potentially hostile foreign origin sits within secure networks of the US government, military, and intelligence services. And as you now see, the FBI has been concerned about it.

Graphic file export of the FBI's **Powerpoint** document slides.



FBI Criminal Investigation: Cisco Routers

The overall classification of this presentation is
UNCLASSIFIED

Section Chief Raul Roldan
Supervisory Special Agent Inez Miyamoto
Intelligence Analyst Tini Leon

January 11, 2008

- **FBI Criminal Investigation**
- **Supply Chain**
- **Critical Infrastructure Threats**
- **Government Procurement Problems**
- **FBI Coordination**
- **Intelligence Gap**



FBI Criminal Investigation

Cisco Routers

- Routers
 - Models: 1000 and 2000 Series
- Switches
 - Models: WS-C2950-24, WS-X4418-GB (for CAT4000series)
- GigaBit Interface Converter (GBIC)
 - Models: WS-G5483, WS-G5487
- WAN Interface Card (WIC)
 - Models: VWIC-1MFT-E1, VWIC-2MFT-G703, WIC-1DSU-T1-V2

Counterfeit Products

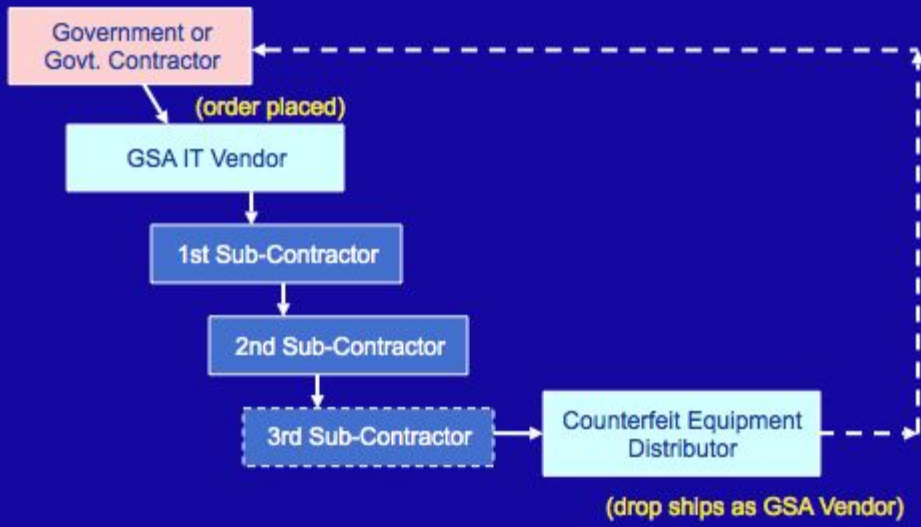


- **Counterfeit**
 - 1721 Router
 - \$234.00
- **Genuine**
 - 1721 Router
 - \$1,375.00

Cisco Identified Problems



- **Problems**
 - Low manufacturing standards
 - Higher failure rate
 - Duplicate MAC addresses of routers and switches can shut down an entire network
- **Examples**
 - In 2002, duplicate MAC addresses shut down an end user's network in Pittsburgh
 - In 2004, a government agency conducted a network upgrade to its North American weather communication system—it failed upon installation
 - Cisco 1721 router installed in a network caught fire due to a faulty power supply

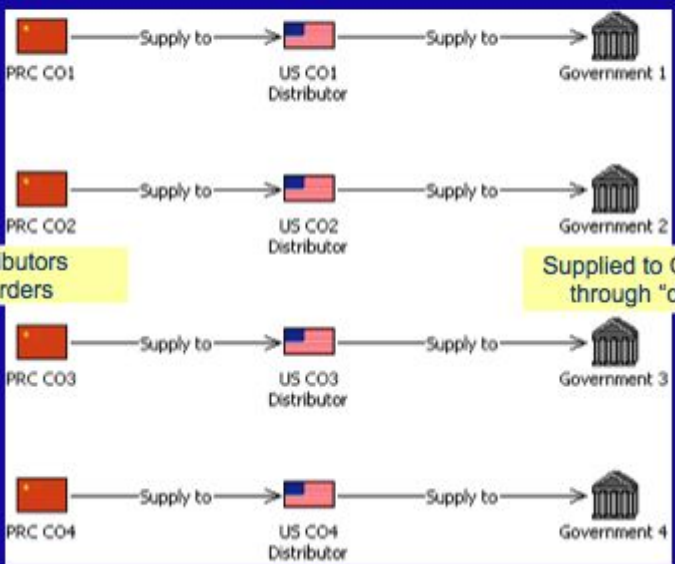


Supply Chain

PR CHINA



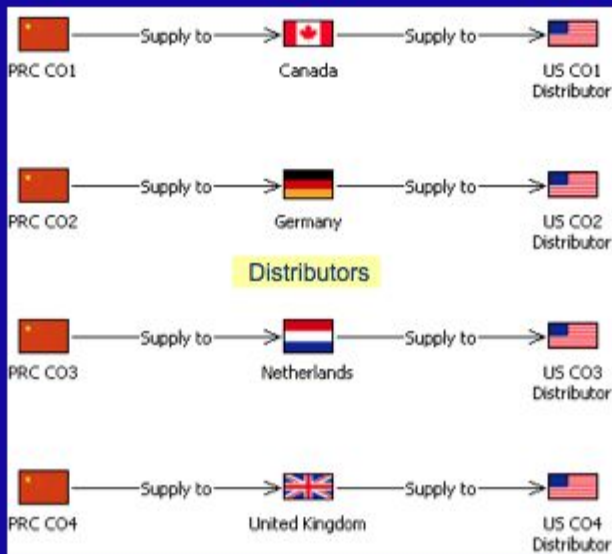
Supply Chain 1 – Directly from PRC



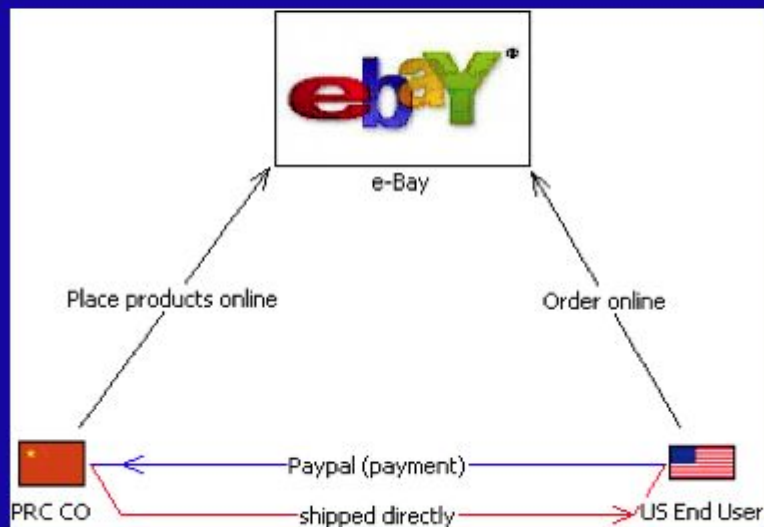
U.S. Distributors places orders

Supplied to Government through "drop ship"

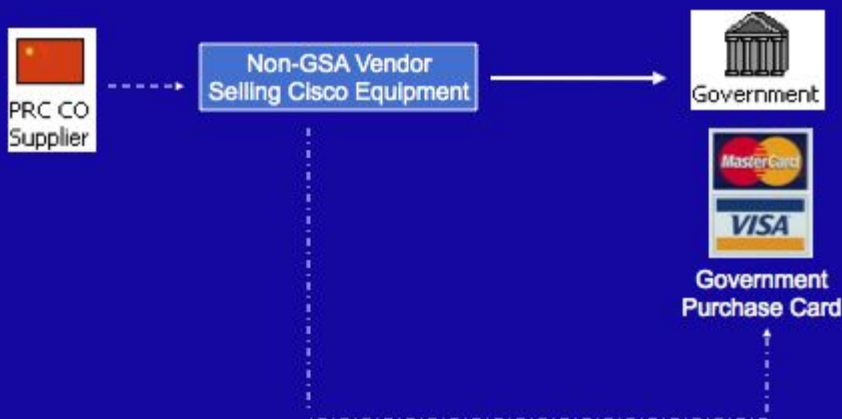
Through Foreign Country



Supply Chain 3 – ebay



Government Credit Card



Open Source Examples



- Supply Chain 1 – Directly from PRC
 - eGlobe Solutions Inc.
 - Syren Technology
 - Navy Project
 - MortgageIT
- Supply Chain 3 – ebay
 - Todd Richard
- Supply Chain 4 – Government Purchase Card
 - FBI



(Authorized Cisco Vendor)

Source: <http://www.usdoj.gov/ao/invest/evls/evl2006/invsong.html>

eGlobe Solutions Inc.



- **May 2003 – July 2005**
 - \$788,000 counterfeit equipment
- **November 2006 Indicted**
 - Conspiracy, Mail Fraud, and Counterfeit Trademark
- **Sold to**
 - U.S. Naval Academy
 - U.S. Naval Air Warfare Center
 - U.S. Naval Undersea Warfare Center
 - U.S. Air Base (Spangdahelm, Germany)
 - Bonneville Power Administration
 - General Services Administration
 - Raytheon (Defense Contractor)



Source: <http://ftp://www.usdoj.gov/cead/bul/relnews/January/NOV2002/0300104Edman.html>

Syren Technology



- August 2002 – July 2004
- December 2007 Indicted
 - Trafficking in counterfeit Cisco products
- Sold to
 - Marine Corps
 - Air Force
 - Federal Aviation Administration
 - FBI
 - Defense Contractors
 - Universities and Financial Institutions



(Won bid for US Navy Project)

U.S. Navy



(Unauthorized Cisco reseller)



Sub-contractor

(Ships counterfeit to U.S. Navy)

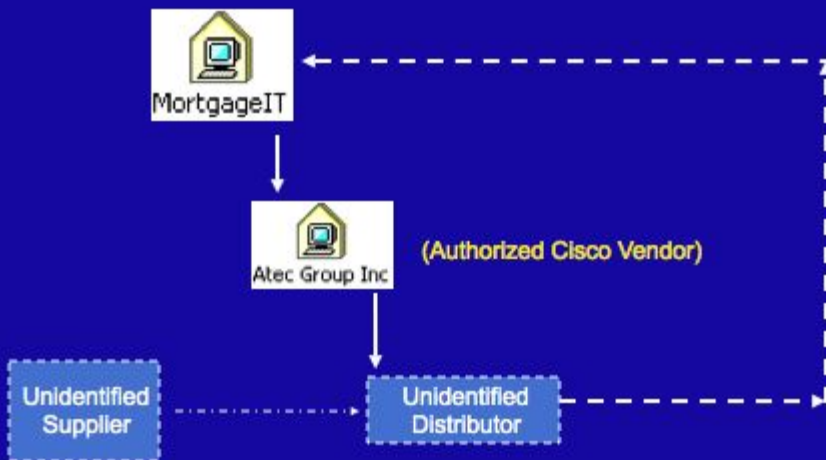
Source: <http://www.govexec.com/daily/ed/03070203091.htm>

U.S. Navy Project



- \$250,111 counterfeit Cisco equipment
- Lockheed Martin
 - Did not use GSA IT Vendor or authorized Cisco reseller
 - Discovered duplicate serial numbers Cisco switches

Non-government Example

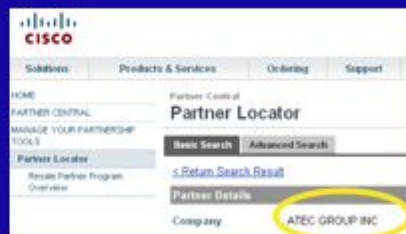


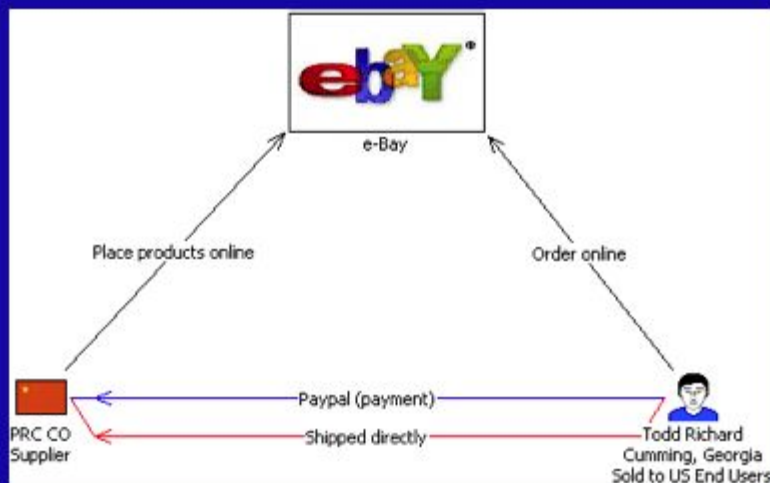
Source: <http://www.nth-akworld.com/news/2008/10/2008counterfeit.html>

MortgageIT: Non-government Example



- Discovered WICs were faulty during routers upgrade
 - 30 counterfeit WAN Interface Cards (WIC)
- Atec Group Inc.
 - Authorized reseller selling counterfeit
 - Cisco
 - Microsoft
 - Symantec





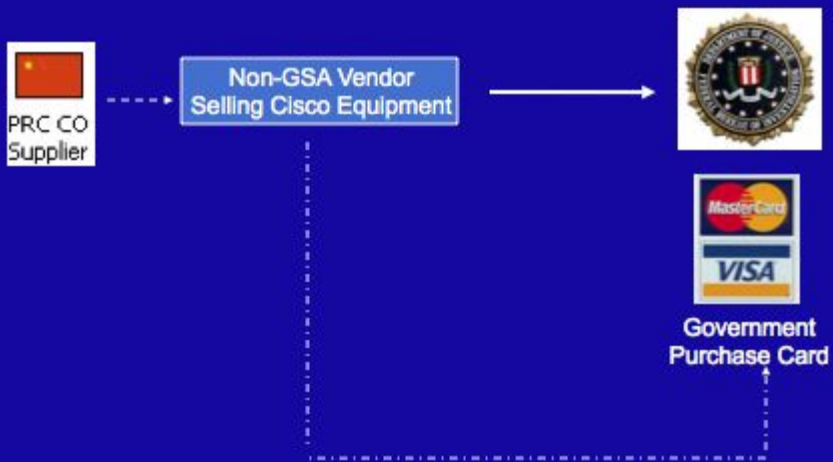
Source: <http://www.cybercrime.gov/toddRichardPlea.pdf>

Todd Richard



- **Between 2003 – 2007**
 - \$1,000,000 counterfeit equipment
- **October 2007 Indicted**
 - Trafficking in counterfeit Cisco trademarks
- **Separate shipments**
 - Counterfeit equipment, labels, boxes, and manuals

Government Credit Card



Critical Infrastructure Threat

- **Alliance for Gray Market and Counterfeit Abatement (AGMA) & KPMG White Paper**
 - 1 in 10 IT products sold are counterfeit
 - 10% IT products counterfeit
 - \$100 billion

Source: KPMG/International, "Measuring the Rate of Counterfeiting in the Information Technology Industry," 2003

Scope of the Problem



- **Law Enforcement estimates much higher**
 - **Customs and Border Protection (CBP)**
 - Only seize registered items
 - Dell Computers not registered
 - No label = no seizure
 - Cannot check every container
 - **FBI**
 - Chinese postal service vs. shipping services
 - Smaller shipments
 - Hardware, software, manuals and labels shipped separately
 - Assembled in United States



Government Procurement Problem



Government Procurement



- **Most government agencies use enterprise information system**
 - Coordinate business process
 - Standard data structure
 - Standard equipment
- **Cisco routers used in enterprise information systems**

- Cisco has 80% market share



Government Procurement



- Government searches for lowest price
- Contract language allows for
 - Subcontracts
 - 2 to 3 levels of sub-contractors
 - “Blind drop” or “drop ship”
 - Non-OEM purchase
 - Smaller businesses
- No vetting of vendors by Cisco or GSA
 - If done by government, usually only background check

- **No Direct Sales**
 - Cisco has 5 major distributors
 - 2 distributors sell to government via GSA
 - Comstor.net (200+ vendors)
 - Immix Group (not awarded yet - ? vendors)
- **Exceptions**
 - Highly specialized equipment sales
 - Intelligence community agencies
 - Large telecom providers

Problems with Cisco



- **Cisco's solution:**
 - Use Cisco Gold/Silver Partners
 - Training/support designation given by Cisco

- **Government's Problem:**
 - **Gold/Silver Partners**
 - purchased counterfeit
 - sold counterfeit to government and defense contractors
 - **Cisco's Brand Protection does NOT coordinate with Cisco's Government Sales**



FBI Effort to Combat Problem

- **3 Case Coordination Meetings (2006-2007)**

- Immigration & Customs Enforcement (ICE)
- Customs & Border Protection (CBP)
- Defense Criminal Investigative Service (DCIS)
- Department of Interior (DOI)
- Environmental Protection Agency (EPA)
- Department of State (DOS)
- Department of Defense (DOD)
- Local Police Departments

FBI Coordination



- **General Services Administration (GSA)**
 - Ongoing coordination
 - 03/2007, GSA attended FBI Case Coordination Meeting (Dallas)
 - 07/2007, GSA-FBI-DCIS Coordination Meeting (Seattle)
 - GSA Actions
 - Letters of supply
 - Policy review - ongoing
 - Expansion of investigation to address all counterfeit IT equipment
 - Supporting FBI investigations

- **Department of Defense – multiple investigations**
 - Defense Criminal Investigative Service (DCIS)
 - Naval Criminal Investigative Service
 - Air Force Office of Special Investigations
 - Army Criminal Investigative Service
- **All services concerned with critical infrastructure protection**
 - DCIS-FBI Counterfeit IT Equipment Working Group

US-China Joint Liaison Group



- **Co-chaired by US DOJ and Chinese Ministry of Public Security (MPS)**
 - **Facilitate cross-border criminal enforcement operations**
 - **Intellectual Property Criminal Enforcement Working Group**
 - Submitted requests for investigation
 - Example: Summer Solstice (Microsoft software investigation)

- Canada
- Germany
- United Kingdom



Intelligence Gap

- **Purpose of counterfeit:**
 - For profit or state sponsored?
- **Scope of counterfeit equipment problem:**
 - Routers?
 - Other IT equipment (PCs, printers, etc.)?
- **Effect on the critical infrastructure?**

The Threat



- **IT Subversion/Supply Chain Attack**
 - Cause immediate or premature system failure during usage
 - Gain access to otherwise secure systems
 - Weaken cryptographic systems
- **Requires “intimate access to target system”**