



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Supply Chain Risk Management

Can we Secure the IT Supply Chain in the Age of Globalization?

Marcus H. Sachs
Verizon

marcus.sachs@verizon.com

- **The IT Supply Chain**
- **Certified Pre Owned Consumer Devices**
- **Case Studies**
- **USB Memory as an Attack Vector**
- **Counterfeit Routers**
- **What do we do to solve this problem?**

Four major pipelines for OEM (original equipment manufacturer) products:

1. From country where manufactured to a certified domestic distributor to domestic end user
2. From country where manufactured through a certified distributor in a second country to domestic end user
3. From country of origin to eBay or similar online auction site to end user
4. From country of origin to distributor or retailer with unknown credentials to end user

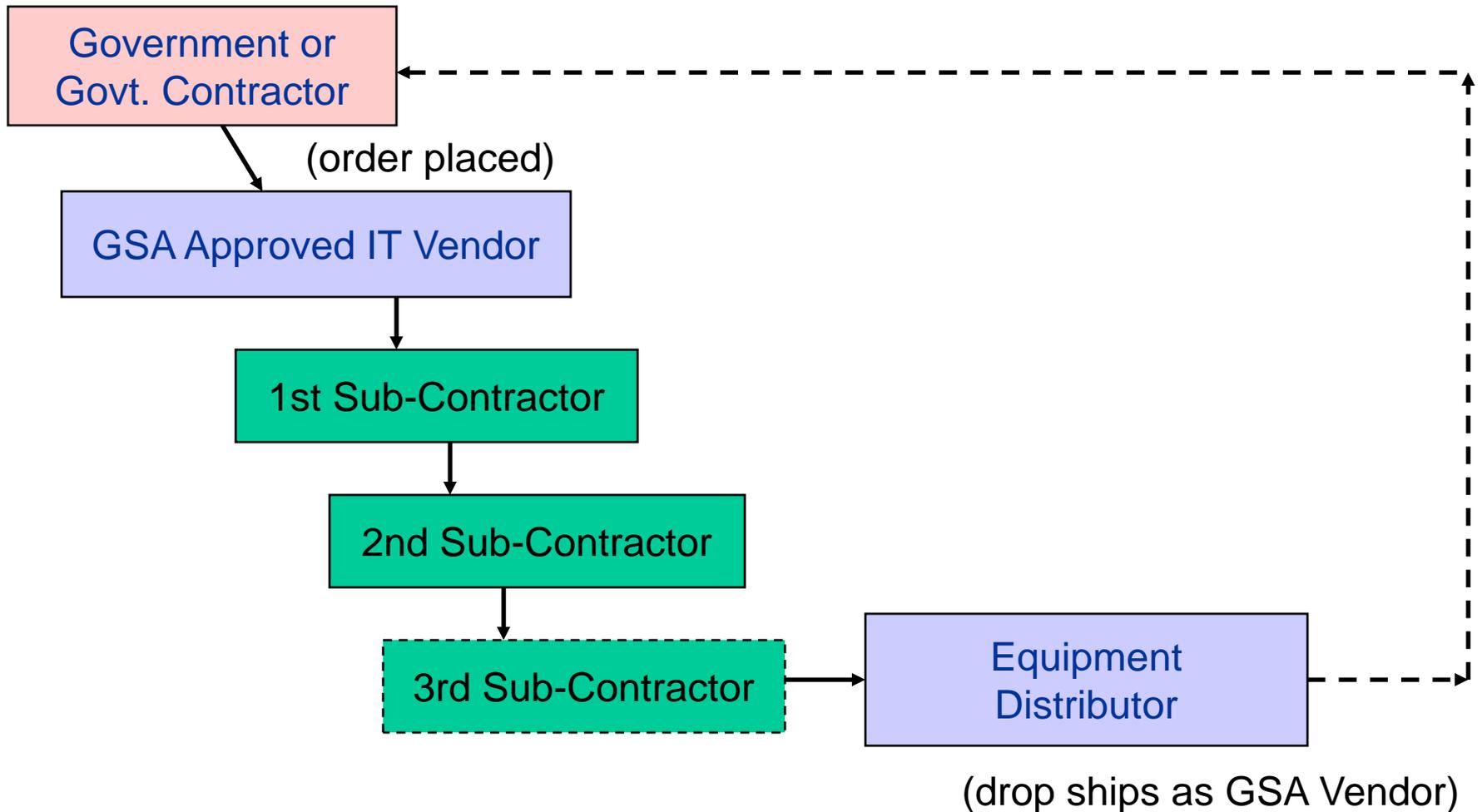
Supply Chain Sources

	Dell	HP	Lenovo
System Design	China, US, Singapore, Taiwan, India	US, India	China, US, Taiwan, Japan
Motherboard Assembly	China	China	China
System Assembly	China, US, Brazil, Ireland, Malaysia	China, Canada, US, Czech Republic, India, Australia	China, Mexico, Hungary, India, Japan, Czech Republic, Brazil
BIOS Design	China, US, India	China, US, India	China, US, Japan

Most use the same BIOS suppliers

BIOS Suppliers	Phoenix, Award, Internal	Phoenix, Award, Softex, AMI, Award, Internal	Phoenix, Award, Insyde, AMI, Internal
-----------------------	--------------------------	--	---------------------------------------

US Government Sub-Contracting Process



Supply Chain Security

- Previously characterized by physical security
 - Theft of items in transit
 - Customs violations at borders
 - Mis-routed or delayed deliveries
 - Incorrect orders, such as wrong quantities or wrong items
 - Bad manufacturing and lack of quality control
- Laws, policies, and standards were developed over time to mitigate the consequences of these risks
- Lots of international agreement on how to protect the physical side of the supply chain

The New Issue is Virtual Security

- In addition to physical security, we now worry about new risks:
 - Theft of intellectual property
 - Import/export of strong encryption
 - Logic bombs and self-modifying code
 - Deliberately hidden back doors for unauthorized remote access
 - Other “value added features” like key loggers
 - Fake or counterfeit products
- Current laws, policies, and standards are immature



Supply System Attacks

- Why send malicious code over the Internet if you can pre-infect computer parts or consumer devices?
- Some recent examples:
 - Fall 2007: hard drives from China arrived on store shelves pre-infected with a virus
 - Christmas 2007: hundreds of digital photo frames, USB memory sticks, GPS devices, and other plug-n-play devices were found to be infected with malware
 - January 2008: FBI announces a multi-year investigation into counterfeit Cisco routers

Certified Pre Owned Consumer Products

When	Who Shipped	What Media	With What
2008-10-09	Cisco	VPN Client CD	Mexican Narco Corridos MP3s
2008-10-08	ASUS	Eee Box's 80GB Hard Drive	W32/Taterf worm - aka W32.Gammima.AG (recycled.exe)
2008-08-19	ASUS	Laptop Recovery DVD	Cracking software, confidential documents, proprietary source code, employee CVs
2008-04-09	Hewlett-Packard	256K / 1GB USB Drives	W32.Fakerecy and W32.SillyFDC
2008-01-23	Insignia (sold via Best Buy)	10.4" NS-DPF10A Digital Photo Frame	Unspecified Virus
2008-01-04	Unspecified	Victory LT-200 MP3 Player	Worm.Win32.Fujack.aa
2007-12-25	ADS (sold via Sam's Club)	8" Digital Photo Frame	Win/32Mocmex.AM
2007-12-13	Unknown Nepalese Vendor	Kingston CF Memory Card	Worm.VBS.Small
2007-09-15	Medion Laptops (via Aldi)	Laptop	Stoned.Angelina Virus
2007-08-??	Seagate	Seagate Maxtor Basics Personal Storage 3200	Virus.Win32.AutoRun.ah
2007-01-29	TomTom	TomTom GO 910 Satnav Unit	win32.Perlovga.A Trojan and TR/Drop.Small.qp
2006-10-18	Apple	30GB Apple Video iPod	RavMonE.exe Virus
2006-10-16	McDonald's Japan	MP3 Player	QQPass Password-stealing Trojan
2005-11-25	I-O Data Device	HDP-U Series Hard Drive	Tompai-A Worm
2005-11-11	Sony BMG	XCP Software	Unspecified Virus
2005-09-01	Creative	5GB Zen Neon MP3 Player	Wullik.B Virus
2001-12-03	Kool Kizz	Atelier Marie (Japanese-language version)	W32/Kriz Virus
199?-??-??	Three Unspecified European PC Gaming Magazines	Cover CD-ROM	CIH Virus

Certified Pre Owned Consumer Products

1991-12-??	Konami Inc.	Spacewrecked Game Disk	Stoned
1991-12-??	Novell	Network Encyclopedia Disk	Stoned-3
1991-11-11	Virtual Reality Lab	Distant Suns Disk	Michelangelo
1991-11-??	Zinc Software	C++ Library Disk	Form
1991-11-??	NTIS Software Distribution	Unspecified	Stoned
1991-11-??	Software Perspectives	Demo Disk	Stoned
1992-01-28	Leading Edge Products Inc.	PC	Michelangelo Virus
1991-10-??	Z-Soft	PC Paintbrush Update Disk	Michelangelo
1991-10-??	Publishing International	PUMPKIN PATCH Screen Saver	Jerusalem
1991-09-??	Cypress Semi-Conductor	MAXPROG, version 2.72C	Stoned
1991-09-01	Sun Microsystems	PCNFS 3.5b	Jerusalem
1991-08-??	European Patent Office	Bulletin Disk	Stoned
1991-07-??	Oracle	Oracle Windows' DDE/Toolbox Demo Disk	Stoned
1990-12-??	LAN Source Technologies Distributing	Modem Protocall One Modem Evaluation	Stoned
1990-11-??	Shimadzu	Photo-detection Detec-tor SPD-M6A Version 2.14	Vienna
1990-11-??	PC Benelux World	Unspecified	Cascade 1704
1990-10-??	DOS-TREND Magazine	Unspecified	Stoned II
1990-10-??	Modular Circuit Technology	Utility Disk	Stoned
1990-07-??	PC Today Magazine	Unspecified	Disk-killer
1990-04-??	Far Side Moon Artdink Inc.	PC	Nambal / Nambal II

A History Lesson: Summer 1982

- Soviet Union was obtaining western technologies for a natural gas pipeline operation in Siberia
- CIA decided to give the Soviets a bit of “extra value” in the software needed to run the pipeline
- Later, pumps and valves were set to run at levels beyond what would be tolerated, resulting in an enormous explosion
 - NORAD and others thought a nuclear bomb had detonated
 - National Security Council was briefed within a few minutes after the explosion by CIA officials
- More about this CIA operation is at:
http://en.wikipedia.org/wiki/Farewell_Dossier



Infected Global Positioning Systems

- Tom-Tom admitted that a batch of GO 910 devices manufactured in a one-week period around October 2006 were shipped with malware
 - `Backdoor.Win32.Small.10` uses the Windows AutoRun feature to run other malicious software pre-installed on the device
 - Included at no extra cost: `Perlovga.a` and `Small.qp`
 - Malware had been detected by popular AV companies since June 2006
- Operating system of the Tom-Tom is based on Linux
- Malware cannot affect an automobile computer, at least not yet



Fall 2007: Hard Drives with a Value-added “Feature”

- **Virus.Win32.AutoRun.ah** was found on Seagate's "Maxtor Basics Personal Storage 3200" drives sold after August 2007
 - Virus hunts for gaming passwords
 - Installed as soon as a user plugs in the drive and double clicks on a corresponding icon
 - Tries to install itself with an autorun.inf file in the root of the external disk drive
- Infected lot made its way to many regions including China, Russia and the Middle East
- Drives were built under contract, not by Seagate itself
 - An internal investigation by the contract manufacturer determined that the virus was accidentally transferred by one of its employees and was not a malicious act



Christmas 2007 – Digital Photo Frames

- On Christmas Day 2007, SANS Internet Storm Center was alerted to a digital photo frame that blue-screened consumer computers when plugged into the USB port
 - Purchased at Sam’s Club, an affiliate of Wal-Mart
 - Contained an autorun.inf file that loaded malicious software
- Over the next several days, dozens more reports of infected photo frames, memory sticks, and other USB devices came in
- All devices were made in China but distributed by US companies
- Most likely cause: improper “digital hygiene” in the various factories where items were tested prior to shipment



March 2008: Pre-Infected Laptops

Posting by a blogger on 3 March 2008

RavMon.exe virus on new Toshiba Satellite laptop

A few days ago I bought a very inexpensive Toshiba Satellite L40-18Z laptop from Comet in the UK. It's a basic laptop running Windows Vista, and it is certainly good enough for web browsing and wordprocessing.

But this particular laptop came with something extra. Despite the security seals being intact, and the OS having never been activated, the laptop came with a file called RavMon.exe on the C: and E: partitions.

RavMon.exe is an insidious virus that spreads on USB keys and drives, so it seems likely that this laptop was infected during the manufacturing process, despite having Symantec Anti-virus installed.

Of course, the first thing I did was remove Symantec and install ZoneAlarm, and ZA's Kaspersky anti-virus engine found RavMon.exe pretty much straight away. Thinking it was a false positive, I sent it to VirusTotal and the results speak for themselves.

VirusTotal Results From Laptop Malware

VirusTotal - Google Chrome
 http://www.virustotal.com/compacto.html

VIRUS TOTAL

File RavMon.exe received on 03.03.2008 20:38:32 (CET)

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.3.4.0	2008.03.03	Win-Trojan/Xema.variant
AntiVir	7.6.0.73	2008.03.03	TR/Agent.Abt.33
Authentium	4.93.8	2008.03.02	W32/Trojan.NAT
Avast	4.7.1098.0	2008.03.02	Win32:Agent-EDN
AVG	7.5.0.516	2008.03.03	Generic3.NKU
BitDefender	7.2	2008.03.03	Trojan.Downloader.Chacent.A
CAT-QuickHeal	9.50	2008.03.03	Trojan.Agent.abt
ClamAV	0.92.1	2008.03.03	Trojan.Agent-3327
DrWeb	4.44.0.09170	2008.03.03	Win32.HLLW.Autoruner.198
eSafe	7.0.15.0	2008.02.28	Suspicious File
eTrust-Vet	31.3.5582	2008.03.03	Win32/Compfault.C
Ewido	4.0	2008.03.03	Trojan.Agent.abt
F-Prot	4.4.2.54	2008.03.02	W32/Trojan.NAT
F-Secure	6.70.13260.0	2008.03.03	W32/Agent.CUTV
Ikarus	T3.1.1.20	2008.03.03	Trojan.Win32.Agent.abt
Kaspersky	7.0.0.125	2008.03.03	Trojan.Win32.Agent.abt
McAfee	5243	2008.03.03	New Malware.eb
Microsoft	1.3301	2008.03.03	Worm:Win32/RJump.F
NOD32v2	2918	2008.03.03	Win32/AutoRun.FQ
Norman	5.80.02	2008.03.03	W32/Agent.CUTV
Panda	9.0.0.4	2008.03.03	Generic Malware
Prevx1	v2	2008.03.03	Generic.Malware
Rising	20.34.02.00	2008.03.03	Trojan.DL.MnLess.n
Sophos	4.27.0	2008.03.03	Troj/QQRob-ADL
Symantec	10	2008.03.03	W32.Nomvar
VBA32	3.12.6.2	2008.02.27	Trojan.Win32.Agent.abt
VirusBuster	4.3.26:9	2008.03.03	Packed/nPack
Webwasher-Gateway	6.6.2	2008.03.03	Trojan.Agent.Abt.33

Additional information

File size: 48640 bytes

MD5: 5557dd0fd5565f12a71c92e6aad7088f

SHA1: 1dd1be78715ff68354967adadc8b6990706caafa

PEid: -

packers: NPack

Prevx info: <http://info.prevx.com/aboutprogramtext.asp?PX5=9AB5F45400BEE2AABE7B0084B4179D0075A088E9>

Speaking of RavMon...



- Apple statement: “We recently discovered that a small number - less than 1% - of the Video iPods available for purchase after September 12, 2006, left our contract manufacturer carrying the Windows RavMonE.exe virus.”
- *How did Microsoft malware get into an Apple factory?!*

April 2008: HP Admits They Have A Problem

SUPPORT COMMUNICATION - SECURITY BULLETIN



Document ID: c01404119

Version: 1

HPSBMA02323 SSRT080032 rev.1 - HP USB Floppy Drive Key (Option) for ProLiant Servers, Local Virus Infection

NOTICE: The information in this Security Bulletin should be acted upon as soon as possible.

Release Date: 2008-04-03

Last Updated: 2008-04-03

Potential Security Impact: Local virus infection.

Source: Hewlett-Packard Company, HP Software Security Response Team

VULNERABILITY SUMMARY

A potential security vulnerability has been identified with two types of optional HP USB Floppy Drive Keys intended for use with certain ProLiant servers. This vulnerability could cause a local 'W32.Fakerecy' or 'W32.SillyFDC' virus infection.

References: ~~CVE-2008-0708~~

SUPPORTED SOFTWARE VERSIONS*: ONLY impacted versions are listed.

Option Part # 442084-B21 HP 256MB USB 2.0 Floppy Drive Key

Option Part # 442085-B21 HP 1GB USB 2.0 Floppy Drive Key

July 2008: USB Thumb Drives

Email sent to US government employees on
July 9, 2008

Please be advised that two USB thumb drives were discovered on the 9th Floor of the Bicentennial Building. One was discovered in the Men's restroom yesterday afternoon. Another was found this morning on a facsimile machine. The drives contain malicious code that automatically and silently executes when the drive is plugged into a system. The code captures certain system information and transmits it out of DOJ.

Malware in Afghanistan

- A Soldier assigned to CJTF-82 (US forces in Afghanistan) discovered a virus on an “out-of-the-package” USB drive
- Investigation revealed a **W32.Nomvar** worm infection
- Further investigation revealed a number of “brand new” USB drives with the worm
- Symantec: *W32.Nomvar is a worm that copies itself to the root of all drives, including removable and shared drives, and downloads potentially malicious files onto the compromised computer*

What is the Difference?



Social Customs

- We are told as children, “don’t pick something up off the street and put it in your mouth!”
 - “You don’t know where that penny has been!”
- So why do we pick up a strange USB key and stick it into our computers?
 - “You don’t know where that USB key has been!”



But Doesn't AutoPlay Fail With USB Memory?

- Windows by default will not automatically run a program on a USB memory device
- But it *will* read and autorun a CD
- So, if you are U3 Technologies what do you do?
 - Make it look like a read-only ISO 9660 volume on an emulated CD-ROM drive, of course!



But if U3 can do that, so can anybody else!

January 2008: FBI Investigates Counterfeit 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 Versus Genuine



So What? As Long As It Works...

- Alliance for Gray Market and Counterfeit Abatement (AGMA) & KPMG White Paper
 - 1 in 10 IT products sold are counterfeit
 - 10% of IT products counterfeit = \$100 billion market
- US Law Enforcement estimates are much higher
 - Customs and Border Protection (CBP)
 - Can only seize registered items
 - Dell Computers not registered
 - No label = no seizure
 - Cannot check every container
 - Federal Bureau of Investigation (FBI)
 - Chinese postal service vs. shipping services
 - Smaller shipments
 - Hardware, software, manuals and labels shipped separately
 - Assembled in United States



What Does It Mean?

- What is the purpose of the counterfeit equipment?
 - For profit, or for espionage?
 - IT Subversion/Supply Chain Attack?
- What is the scope of the counterfeit equipment problem?
 - We know about the routers
 - What about other equipment (PCs, printers, etc.)?
- Potential effect on the critical infrastructure
 - Cause immediate or premature system failure during usage
 - Gain access to otherwise secure systems
 - Weaken cryptographic systems
- Could an adversary gain “intimate access to a target system”?

This is a National Security Policy Issue

- National security policies must conform with international laws and agreements
 - While preserving a nation's rights and freedoms, and while
 - Protecting a nation's self interests and economic goals
- Advances in computer science will always outpace the ability of governments to react with new policies and legislation
- We need forward-looking and flexible laws that can adapt to the new world of globalized supply chains
- Industry has a significant leadership role in solving this issue

Some Possible Outcomes

- Technology solution
 - Coding standards are adopted and enforced that eliminate the ability to produce subversive software
- Political solution
 - Government mandates that all “critical” software programming be performed domestically
- Legal solution
 - Severe fines and penalties are imposed on companies found guilty of importing subverted IT products
- Industry solution
 - Offshore production is closely supervised by trusted citizens

Final Thoughts

- A “policy window” is open right now
 - Chinese lead content in consumer toys
 - Indian “sweat shops” used to manufacture textiles
 - Infected consumer devices
 - FBI investigation into counterfeit routers
- Our challenge is to leverage the policy opportunity
 - Pay close attention to what toy and textile manufacturers do with their supply chains
 - Industry and government should work closely to enable laws that are business-friendly but not overly restrictive
- Globalization will not be reversed, this is how we will conduct business in the 21st Century
 - Now is the time to shape the future

Contact Information

- SANS Internet Storm Center
 - <http://isc.sans.org>
- Certified Pre Owned List
 - <http://www.attrition.org/errata/cpo/>
- Verizon's Open Development Initiative
 - <http://www.verizonwireless-opendevelopment.com/>
- Marcus H. Sachs
 - marcus.sachs@verizon.com
 - marc@sans.org
 - +1 202 515 2463