This page contains dynamic content -- Highest Possible Classification isTOP SECRET//SI/TKSecurity BannerTerms of Use

1. Intelink
2. Blogs
3. Bookmarks
4. eChirp
5. Inteldocs
6. Intellipedia
7. Search
    1. Enterprise Search
    2. Enterprise Catalog
    3. Map
    4. People
    5. Recent Intel
    6.
    7. Search Support
8. More
    1. Community
    2. Gallery
    3. IC Connect
    4. IC PKI
    5. IntelShare
    6. iStory
    7. iVideo
    8. Living Intelligence
    9. Maps
    10. Messenger
    11. Passport
    12. RSS Reader
    13. Tapioca
    14. URL Shortener

1. Help
    1. Intellipedia Help
    2.
    3. Submit a Ticket
    4. ISMC Watch
    5. About Intelink

(U) Supply Chain Cyber Threats

TOP SECRET//SI//NOFORN

Jump to: navigation, search

Contents

[hide]

[edit] (U) Background

(U) A supply chain cyber threat is a defect, exploited vulnerability, or remote exploitation capability that is embedded into a product by an adversary by virtue of access to product's design or production.

(U//FOUO) Creators and supervisors of the supply chain take many precautions to prevent lapses in security. Malicious actors are targeting the global supply chain as a means to infiltrate global computer networks, including the United States. Global supply chains have procedures in place to prevent the loss/tampering of products en route to a final destination. Unfortunately, there are ways malicious actors can use the supply chain to their advantage and alter products before they ever become a part of the supply chain.

[edit] (U) Vulnerabilities

(U) This section details a variety of supply chain vulnerabilities that exist in traditional desktop and laptop systems.

[edit] (U) PC Power Supply

(U) The PC power supply is well positioned for remote exploitation. Power supplies are distributed as sealed metal containers, they contain a co-processor that executes its own program, and it interfaces to both the power line and the computer's electronics. Thus the power supply is well positioned for exploitation by an adversary.

(U) Power supplies can be signed through coded messages sent through RF or through the power line itself. A power supply could be set to shut down, self-destruct, damage the computer's motherboard (through the introduction of higher-than-expected voltage), or even start a fire or explosion.

(U) Power supplies are frequently changed by manufacturers during a production run, making it difficult to determine if a power supply was substituted in the supply chain or in the field. They have standard sizes and connectors, and are frequently replaced in the field when they fail. It would be very difficult to detect a targeted power supply substitution.

[edit] (U) Network Interface Cards (NICs)

(U) Network Interface Cards (NICs) such as ethernet interfaces are well-positioned to plant malware and exfiltrate information from a PC in a manner that is invisible to the operating system or other host-based defenses.

(U) Modern NICs have a co-processor that runs its own firmware. Frequently this firmware can be updated in the field, allowing for the insertion of malicious code by an adversary. The NIC has DMA access to the computer's physical memory---it can read or write protected memory belonging to the kernel or to any user-level process.

[edit] (U) RAID Controllers

(U) Disk controllers, and especially RAID controllers, are well-positioned as an attack point against PCs.

(U) Disk controllers frequently have their own co-processors and firmware that can be updated in the field. The standard disk controller receives requests from the host computer, executs the request on the disk, and then transfers information from the disk to main memory (or vice-versa). As a result, disk controllers have unrestricted read/write access to the computer's memory.

(U) A disk controller can plant malware in an operating system binary on the disk, or inject the malware directly into the computer's memory. Better than a root kit, the controller can tell the difference between a request to read a file for execution vs. reading it for anti-virus---so the malware oculd be inserted when the program is run, but not when it is scanned. The controller could also execute its own search algorithms, as the disk controller has unrestricted access to the computer's hard drives. When data is found the controller could inject a process into the computer's memory for the purpose of sending the data to another host.

[edit] (U) Graphics Coprocessor Units (GPUs)

(U) GPUs are another location where code can be loaded and execute autonomously of the CPU. Today's GPUs typically have a dozen or more execution units. Each individual unit is slower than the computer's primary CPU, but the combination of them all together is faster than the host CPU. Typically there is a lot of bandwidth inside the GPU but limited bandwidth from the GPU to the host memory.

(U) GPUs are equipped with firmware that can be updated in the field. Malware operating on the GPU could preserve the functionality of the GPU while scanning the system for sensitive information. Unlike malware running elsewhere with the computer, malware within then GPU would be well positioned to scan the computer's screen for sensitive information. This information could then be exfiltrated using traditional means.

[edit] (U) Firmware

(U) Malicious software has been found in mouse drivers which interface between operating systems and hardware made by Razer USA. This malicious software tricked users into downloading and installing malware onto their computers.[1]

[edit] (U) Reporting

[edit] (U) Recent

click column headers to sort

Agency ↓	Feed ↓
Open Source	Failed to load RSS feed from [redacted]
CIA	Failed to load RSS feed from [redacted]
DIA	Failed to load RSS feed from [redacted]
NSA	Failed to load RSS feed from [redacted]
State Department	Failed to load RSS feed from [redacted]

[edit] (U) CIA

(S//NF) CIA assesses that tampering with hardware circuitry may ultimately be an equally as dangerous as a software threat.[2] According to experts, as advanced systems like aircraft, missiles, and radar have become increasingly dependent on their computing capabilities, the specter of computer hardware subversion causing weapons to fail in times of crisis, or secretly corrupting crucial data, is a growing concern. Computer chips are increasingly complex and subtle modifications made in design or manufacturing processes could be made impossible to detect with the practical means currently available. United States now lacks the capacity to produce the computer chips needed for classified systems, and therefore relies on foreign vendors to support the demand.[3]. The Institute for Defense Analyses identified Critical Network Routers and Transport Layer Switches that could affect the integrity of the entire USG communications information architecture.[4],

[edit] (U) DIA

(S//NF) DIA Supply Chain Threat Analysis Team assesses with moderate confidence that the Commercial Off the Shelf (COTS) components such as application and terminal servers, routers, switches, and distribution consoles used by the Trusted Thin Client are vulnerable to the global supply chain threat.[5] See also Potential Supply-Chain Threats to the DISN Core.[6] The best opportunity for subversion of SCADA supply chain would involve recruiting an insider.[7] The threat against BMD networks will likely employ insiders, supply chain, or SCADA.[8]

(S//NF) The increasing role of international companies and foreign individuals involved in U.S. IT supply chains and services will increase the potential for persistent, stealthy subversion particularly by foreign intelligence and military services but also by international terrorist and criminal groups and even companies engaged in industrial espionage.[9] Risks to the GIG will continue to rise commensurate with growing threats to telecommunications supply chains.[10]

(S//NF) Supply chain concerns will be exacerbated as U.S. providers of cybersecurity products and services are acquired by foreign firms. The Committee on Foreign Investment in the United States (CFIUS) works to identify such concerns and mitigate them as necessary, but the Committee's reach is limited. The CFIUS process depends almost entirely on voluntary filings by companies involved in foreign acquisitions. As a result, CFIUS examines a relatively small percentage of such transactions and acquisitions of smaller firms that are developing emerging security technologies may escape the Committee's notice.[11] Supply chain threats even provide foreign intelligence services potential access to DIA systems.[12]

[edit] (U) FBI

(U) In 2008, the FBI conducted Operation Cisco Raider which has led to 15 criminal cases involving counterfeit products bought in part by military agencies, contractors, and electric power companies in the United States.[13]. In 2011, FBI assesses with high confidencethat the state-sponsored and criminal threat to supply chain integrity is a high cyber threat.[14]

[edit] (U) CYBERCOM

(U)In 2010 Huawei Technologies, ZTE, and Meadville Holdings Limited are among the many Chinese based companies that could pose a threat to the GIG in Chinese Companies and United States Supply Chain Vulnerabilities.[15]

[edit] (U) Other Links

- (U) Air-Gapped Network Threats
- (U) DoD Supply Chain Risk Management Threat Analysis Center
- (U) The Supply Chain Threat Assessment Team A-Space Workspace

[edit] (U) References

1. ↑ (U) McMillan, R; 21 September 2009; Gaming Mouse-maker Razer hit with Infected Firmware.
2. ↑ (U//FOUO) Central Intelligence Agency - Cyber Threat Intelligence Highlights 22OCT09.
3. ↑ (U) Markoff, J., Old Tricks Threatens the Newest Weapons The New York Times, 10/27/2009.
4. ↑ (U) IDA; Document D-3222 Log: H 05-002122/1; January 2006; USG Integrated Circuit Supply Chain Threat Opportunity Study; pg. 14.
5. ↑ (U) Cyberthreat to SecureOffice Trusted Thin Client; DIA-06-1003-001. Prepared by [redacted], CTA-6B, 31DEC09.
6. ↑ (S//NF) DIA, S-1566-07/CCO-5, Potential Supply-Chain Threats to the DISN Core.28 November 2007.
7. ↑ DIA; Defense Intelligence Study; 9 September 2009; DIA-08-1101-021 Information Operations Capstone Threat Assessment, Volume 10: Computer Network Operations; p 31.
8. ↑ (U//FOUO) DIA; Defense Intelligence Assessment; 30 September 2009; DIA-06-0909-045 Cyberthreat to Ballistic Missile Defense Programs.
9. ↑ (S) DIA; Defense Analysis Report; TS-1593-08/CCO-5; 24 Nov 2008; Global: The Global Cyberthreat Environment Through 2028.
10. ↑ (S//NF) DIA; Defense Intelligence Report; 13 December 2010; DIA-06-1012-121.A; Telecommunications and Supply Chain Threats; A Systems Primer.
11. ↑ (S) DIA; Defense Analysis Report; TS-1593-08/CCO-5; 24 Nov 2008; Global: The Global Cyberthreat Environment Through 2028.
12. ↑ (S//NF) DIA; DAC-6 Special Report; 30 November 2010; Supply Chain Threat Analysis.
13. ↑ (U) Markoff, John; New York Times; 9 May 2008; FBI Says The Military Had Bogus Computer Gear

14. ↑ (S//NF) FBI; Technology Cyber Intelligence Unit; Intelligence Bulletin; 27 June 2011; Supply Chain Poisoning: A Threat to the Integrity of Trusted Software
15. ↑ (TS//SI//NF) USCYBERCOM; 26 August 2010; J2 Bulletin 10-064; Chinese Companies and United States Supply Chain Vulnerabilities.

Retrieved from "http[redacted]"
Categories: Cyber Threat Assessments | Supply Chain

TOP SECRET//SI//NOFORN

- This page has been accessed 757 times.
- 2 watching users
- This page was last modified 18:26, 19 October 2012 by [redacted]. Most recent editors [redacted] [redacted].

- Main Page
- Recent changes
- Help
- Random Article
- Sandbox
- Guidelines
- Recent files
- Top categories

interaction

- Featured articles
- Announcements
- Collaboration requests
- Tutorial
- Bulletin Board
- Metrics
- Acronyms
- People Finder

social software tools

Toolbox

- Privacy policy
- About Intellipedia
- Disclaimers

linipedweb7j

Use of this U.S. Government system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution.
Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse actions.

This page contains dynamic content -- Highest Possible Classification isTOP SECRET//SI/TKSecurity