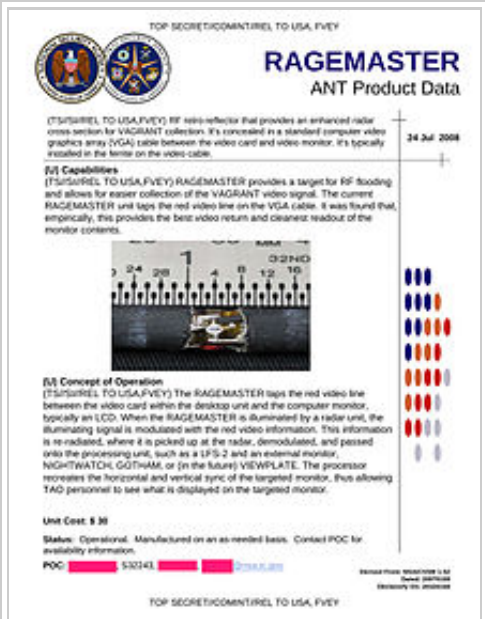
NSA ANT catalog

From Wikipedia, the free encyclopedia

The **NSA ANT catalog** is a 50 page document listing technology available to the United States National Security Agency (NSA) Tailored Access Operations (TAO) by the ANT division to aid in cyber surveillance. According to *Der Spiegel*, "The list reads like a mail-order catalog, one from which other NSA employees can order technologies from the ANT division for tapping their targets' data."[1][2][3][4][5][6][7][8][9] The document was created in 2008.[10]



NSA ANT product data for RAGEMASTER

Security researcher Jacob Appelbaum gave a speech at the Chaos Communications Congress in Hamburg, Germany, in which he detailed techniques that he claims the NSA uses in its surveillance efforts in the US and internationally.[11]

The price of the items in the catalog ranges from free (typically for software) to US$250,000.[1]

Contents

- 1 Background
- 2 Capabilities list
- 3 References
- 4 External links

Background

In 2013, *Der Spiegel* published an article, co-written by Jacob Appelbaum, Judith Horchert and Christian Stöcker, that exposed the NSA "toolbox". Their source of the document was not disclosed, but came from a news agency such as *The Washington Post* or *The Guardian* which are in possession of documents leaked by former NSA contractor Edward Snowden.[12]

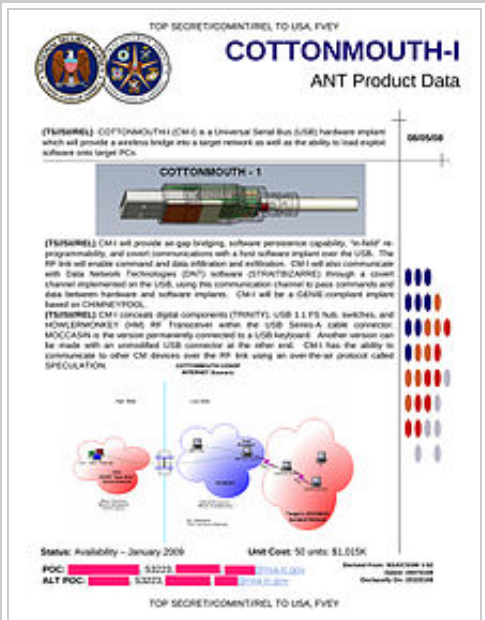
Exploits described in the document are mostly targeted at devices manufactured by US companies, including Apple,[13] Cisco, Dell, Juniper Networks, Maxtor, Seagate, and Western Digital, although there is nothing in the document that suggests that the companies were complicit.[1][14] After *Der Spiegel* revealed that NSA has the ability to inject software onto iPhones using an ANT product called DROPOUTJEEP, Apple issued a statement denying any prior knowledge of the NSA spyware and stated that they would take steps to protect their customers from security attacks "regardless of who's behind them".[15] Cisco has mustered their Cisco Product Security Incident Response Team (PSIRT) to investigate the hack vulnerability.[16]

Capabilities list

The NSA ANT document contains codeword references to hardware and software surveillance technology available to the NSA.[17]

- ANGRYMONK: Technology that can infiltrates the firmware of hard drives manufactured by Maxtor, Samsung, Seagate, and Western Digital[18]
- BULLDOZER: Technology that creates a hidden wireless bridge allowing NSA personnel to remotely control a system wirelessly[14]
- CANDYGRAM: A $40,000 tripwire device that emulates a GSM cellphone tower.

- COTTONMOUTH: A family of modified USB and Ethernet connectors that can be used to install Trojan horse software and work as wireless bridges, providing covert remote access to the target machine.[19] COTTONMOUTH-I is a USB plug that uses TRINITY as digital core and HOWLERMONKEY as RF transceiver. Cost in 2008 was slightly above $1M for 50 units. COTTONMOUTH-II is deployed in a USB socket (rather than plug), and costs only $200K per 50 units, but requires further integration in the target machine to turn into a deployed system. COTTONMOUTH-III is a stacked Ethernet and USB plug costing approximately $1.25M for 50 units.
- CTX4000: Continuous wave radar device that can ""illuminate" a target system for recovery of "off net" information[20]
- DEITYBOUNCE: Technology that installs software on Dell PowerEdge servers by via the motherboard BIOS
- DROPOUTJEEP:"A software implant for the Apple iPhone that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device. SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control and data exfiltration can occur over SMS messaging or a GPRS data connection. All communications with the implant will be covert and encrypted."[8]
- FEEDTROUGH: Software that can penetrate Juniper Networks firewalls allowing other NSA-deployed software to be installed on mainframe computers[1][9][21]

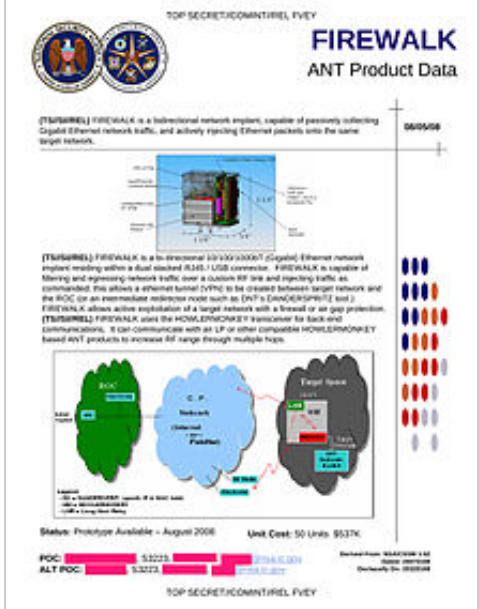


COTTONMOUTH-I

- FIREWALK: A device that looks identical to a standard RJ45 socket that allows data to be injected, or monitored and transmitted via radio technology[22] using the HOWLERMONKEY RF transceiver. It can for instance create a VPN to the target computer. Cost in 2008: $537K for 50 units.
- FOXACID: Technology that can install spyware using a "quantum insert" capable of infecting spyware at a packet level
- GINSU: Technology that uses a PCI bus device in a computer, and can reinstall itself upon system boot-up[14]
- GOPHERSET: GSM software that uses a phone's SIM card's API (SIM Toolkit or STK) to control the phone through remotely-sent commands[23]
- GOURMETTROUGH: User-configurable persistence implant for certain Juniper Networks firewalls[20]
- HEADWATER: Persistent backdoor technology that can install spyware using a "quantum insert" capable of infecting spyware at a packet level on Huawei routers[20]

- HOWLERMONKEY: A RF transceiver that makes it possible (in conjunction with digital processors and various implanting methods) to extract data from systems or allow them to be controlled remotely
- HALLUXWATER: Back door exploit for Huawei Eudemon firewalls[20]
- IRONCHEF: Technology that can "infect" networks by installing itself in a computer I/O BIOS.[14]
- JETPLOW: Firmware that can be implant to create a permanent backdoor in a Cisco PIX series and ASA firewalls[20]
- LOUDAUTO: $30 audio-based RF retro-reflector listening device[20]

- MAESTRO-II: a multi-chip module approximately the size of a dime that serves as the hardware core of several other products. The module contains a 66 Mhz ARM7 processor, 4 MB of flash, 8 MB of RAM, and a FPGA with 500,000 gates. Unit cost: $3-4K (in 2008). It replaces the previous generation modules which were based on the HC12 microcontroller.
- MONKEYCALENDAR: Software that transmits a mobile phone's location by hidden text message
- MONTANA: A collection of tools, including SIERRAMONTANA, SCHOOLMONTANA and STUCCOMONTANA, designed to compromise Juniper Networks routers running the JUNOS operating system[14]
- NIGHTSTAND: Portable system that wirelessly installs Microsoft Windows exploits from a distance of up to eight miles[20]
- NIGHTWATCH: Portable computer used to reconstruct and display video data from VAGRANT signals; used in conjunction with a radar source like the CTX4000 to illuminate the target in order to receive data from it
- PICASSO: Software that can collect mobile phone location date, call metadata, access the phone's microphone to eavesdrop on nearby conversations[23]
- PHOTOANGLO: A joint NSA/GCHQ project to develop a radar system to replace CTX4000[20]



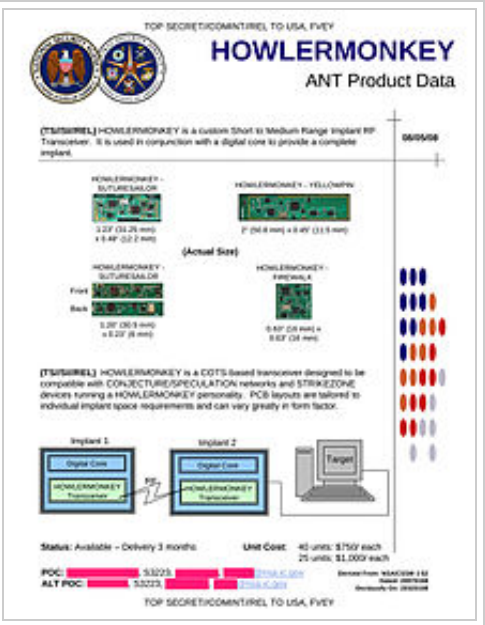
FIREWALK

- RAGEMASTER: A $30 device that can intercept video between a desktop computer video card's VGA output and a monitor; only sends out the red-color signal, but is powered by a remote radar and responds by modulating the VGA red signal in the RF signal it sends back; this method of transmission is codenamed VAGRANT. RAGEMASTER is usually installed/concealed in the ferrite choke of the target cable. Several receiver/demodulating devices are available, e.g. NIGHTWATCH.
- SCHOOLMONTANA: Software that makes DNT implants persistent on JUNOS-based firewalls[20]
- SIERRAMONTANA: Software that makes DNT implants persistent on JUNOS-based firewalls[20]
- STUCCOMONTANA: Software that makes DNT implants persistent on JUNOS-based firewalls[20]
- SOMBERKNAVE: Software that can be implanted on a Windows XP system allowing it to be remotely controlled from NSA headquarters
- SOUFFLETROUGH: BIOS injection software that can compromise Juniper Networks SSG300 and SSG500 series firewalls[20]

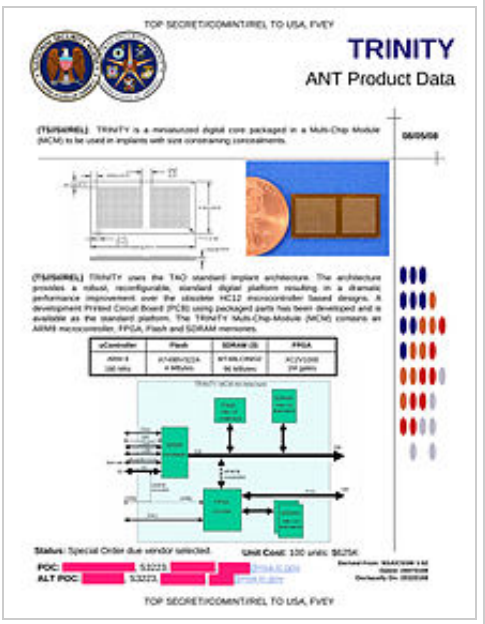
- SPARROW II: A small computer intended to be used for WLAN collection, including from UAVs. Hardware: IBM Power PC 405GPR processor, 64 MB SDRAM, 16 MB of built-inflash, 4 mini PCI slots, CompactFlash slot, and 802.11 B/G hardware. Running Linux 2.4 and the BLINDDATE software suite.

Unit price (2008): $6K

- SURLYSPAWN: Keystroke monitor technology that can be used on remote computers that are not internet connected
- SWAP: Technology that can reflash the BIOS of multiprocessor systems that run FreeBSD, Linux, Solaris, or Windows
- TOTEGHOSTLY: Software that can be implanted on a Windows mobile phone allowing full remote control
- TRINITY: A more recent and more powerful multi-chip module using a 180 Mhz ARM9 processor, 4 MB of flash, 96 MB of SDRAM, and a FPGA with 1 million gates. Smaller than a penny. Estimated cost (2008) $625K for 100 units.
- WATERWITCH: A portable "finishing tool" that allows the operator to find the precise location of a nearby mobile phones



HOWLERMONKEY

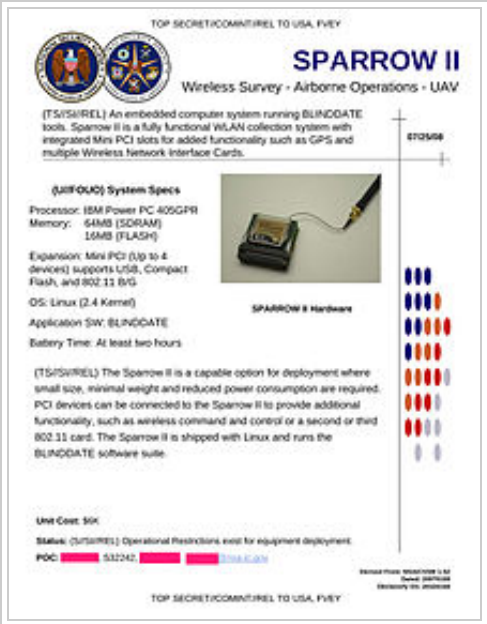


TRINITY

References

1. ^ *a b c d* Applebaum, Jacob and Stöcker, Christian (December 29, 2013). "Shopping for Spy Gear: Catalog Advertises NSA Toolbox" (http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html). *Der Spiegel*. Retrieved January 1, 2014.
2. ^ Hathaway, Jay (December 30, 2013). "The NSA has nearly complete backdoor access to Apple's iPhone" (http://www.dailydot.com/politics/nsa-backdoor-iphone-access-camera-mic-appelbaum/). *Daily Dot*. Retrieved January 1, 2014.
3. ^ Condliffe, Jamie (December 31, 2013). "The NSA Has Crazy Good Backdoor Access to iPhones" (http://gizmodo.com/the-nsa-has-crazy-good-backdoor-access-to-iphones-1492117035). *Gizmodo*. Retrieved January 1, 2014.
4. ^ Edwards, Jim (December 30, 2013). "DOCUMENTS: NSA Has 'A 100% Success Rate' Putting Spyware On iPhones" (http://www.businessinsider.com/nsa-spyware-backdoor-on-iphone-2013-12#ixzz2p9j67gXN). *Business Insider*. Retrieved January 1, 2014.
5. ^ "De l'interception de colis à l'espionnage de l'écran, inventaire des outils de la NSA" (http://www.lemonde.fr/technologies/article/2013/12/30/de-l-interception-de-colis-a-l-espionnage-du-moniteur-inventaire-des-outils-de-la-nsa_4341385_651865.html). *Le Monde*. December 30, 2013. Retrieved January 1, 2014.
6. ^ Satter, Raphael (December 30, 2013). "Privacy Advocate Exposes NSA Spy Gear at Gathering" (http://abcnews.go.com/International/wireStory/hacker-pulls-curtain-back-nsa-spy-gear-21372219). *ABC News*. Retrieved January 1, 2014.
7. ^ Hardawar, Devindra (December 31, 2013). "The iPhone has reportedly been fully hacked by the NSA since 2008 (Update: Apple denies working with NSA)" (http://venturebeat.com/2013/12/31/the-iphone-has-reportedly-been-fully-hacked-by-the-nsa-since-2008/). *Venture Beat*. Retrieved January 1, 2014.

8. ^ *a b* Kain, Erik (December 30, 2013). "The NSA Reportedly Has Total Access To The Apple iPhone" (http://www.forbes.com/sites/erikkain/2013/12/30/the-nsa-reportedly-has-total-access-to-your-iphone/). *Forbes*. Retrieved January 1, 2014.
9. ^ *a b* Zetter, Kim (December 30, 2013). "NSA Hackers Get the 'Ungettable' With Rich Catalog of Custom Tools" (http://www.wired.com/threatlevel/2013/12/nsa-hacking-catalogue/). *Wired*. Retrieved January 1, 2014.
10. ^ Lawler, Richard (December 31, 2013). "Leaked documents detail 2008 NSA program to hack and remote control iPhones" (http://www.engadget.com/2013/12/31/nsa-drououtjeep-iphone-hack-details/). *Engadget*. Retrieved January 1, 2014.
11. ^ Mick, Jason (December 31, 2013). "Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years" (http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm). *Daily Tech*. Retrieved January 1, 2014.
12. ^ Kirk, Jeremy (December 30, 2013). "The NSA intercepts computer deliveries to plant spyware" (http://www.computerworld.com/s/article/print/9245064/The_NSA_intercepts_computer_deliveries_to_plant_spyware). *Computer World*. Retrieved January 1, 2014.
13. ^ Campbell, Mickey (December 30, 2013). "NSA worked on iPhone spyware to remotely monitor users, leaked documents show" (http://appleinsider.com/articles/13/12/30/nsa-worked-on-iphone-spyware-to-remotely-monitor-users-leaked-documents-show). *Apple Insider*. Retrieved January 1, 2014.
14. ^ *a b c d e* Gallagher, Sean (December 31, 2013). "Your USB cable, the spy: Inside the NSA's catalog of surveillance magic" (http://arstechnica.com/information-technology/2013/12/inside-the-nsas-leaked-catalog-of-surveillance-magic/). *Ars Technica*. Retrieved January 1, 2014.
15. ^ Hughes, Neil (December 31, 2013). "Apple says it was unaware of NSA's iPhone spying, vows to defend customers' privacy" (http://appleinsider.com/articles/13/12/31/apple-says-it-was-unaware-of-nsas-iphone-spying-vows-to-defend-customers-privacy). *Apple Insider*. Retrieved January 1, 2014.
16. ^ Brandon, Russell (December 30, 2013). "The NSA's elite hackers can hijack your Wi-Fi from 8 miles away" (http://www.theverge.com/2013/12/30/5256636/nsa-tailored-access-jacob-appelbaum-speech-30c3). *The Verge*. Retrieved January 1, 2014.
17. ^ Elmer-DeWitt, Philip (December 31, 2013). "Apple, Jacob Appelbaum and the National Security Agency" (http://tech.fortune.cnn.com/2013/12/31/apple-nsa-appelbaum-spiegel/). *Fortune*. Retrieved January 1, 2014.
18. ^ Meyer, David (December 29, 2013). "NSA's backdoor catalog exposed: Targets include Juniper, Cisco, Samsung, Huawei" (http://gigaom.com/2013/12/29/nsas-backdoor-catalog-exposed-targets-include-juniper-cisco-samsung-and-huawei/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+OmMalik+%28GigaOM%3A+Tech%29). *Gigaom*. Retrieved January 1, 2014.



SPARROW II

19. ^ http://allthingsd.com/20131230/you-wont-believe-all-the-crazy-hardware-the-nsa-uses-for-spying/
20. ^ *a b c d e f g h i j k l* "NSA's ANT Division Catalog of Exploits for Nearly Every Major Software/Hardware/Firmware" (http://leaksource.wordpress.com/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/). *LeakSource*. December 30, 2013. Retrieved January 2, 2014.
21. ^ Whitwam, Ryan (December 30, 2013). "The NSA regularly intercepts laptop shipments to implant malware, report says" (http://www.extremetech.com/computing/173721-the-nsa-regularly-intercepts-laptop-shipments-to-implant-malware-report-says). *Extreme Tech*. Retrieved January 1, 2014.
22. ^ Thomson, Iain (December 31, 2013). "How the NSA hacks PCs, phones, routers, hard disks 'at speed of light': Spy tech catalog leaks" (http://www.theregister.co.uk/Print/2013/12/31/nsa_weapons_catalogue_promises_pwnage_at_the_speed_of_light/). *The Register*. Retrieved January 1, 2014.
23. ^ *a b* Estes, Adam Clark (December 31, 2013). "A Peek Inside The NSA's Spy Gear Catalogue" (http://www.gizmodo.com.au/2014/01/a-peek-inside-the-nsas-spy-gear-catalog/). *Gizmodo* Australia. Retrieved January 1, 2014.

External links

- Jacob Appelbaum video that exposes NSA surveillance technology (http://www.youtube.com/watch?v=b0w36GAyZIA&feature=youtu.be)
- Der Spiegel Interactive Document: NSA's ANT Division Catalog of Exploits (http://www.spiegel.de/international/world/a-941262.html)

Retrieved from "http://en.wikipedia.org/w/index.php?title=NSA_ANT_catalog&oldid=590900480"
Categories: National Security Agency | Mass surveillance | Edward Snowden | National Security Agency operations

---