

Tailored Access Operations

The **Office of Tailored Access Operations (TAO)**, now **Computer Network Operations**,^[1] is a cyber-warfare intelligence-gathering unit of the National Security Agency (NSA). It has been active since at least circa 1998.^{[2][3]} TAO identifies, monitors, infiltrates, and gathers intelligence on computer systems being used by entities foreign to the United States.^{[4][5][6][7]}

TAO is reportedly "now the largest and arguably the most important component of the NSA's huge Signals Intelligence Directorate (SID)^[8] (SIGINT), consisting of more than 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers".^[2]

A document leaked by former NSA contractor Edward Snowden describing the unit's work says TAO has software templates allowing it to break into commonly used hardware, including "routers, switches, and firewalls from multiple product vendor lines".^[9] According to *The Washington Post*, TAO engineers prefer to tap networks rather than isolated computers, because there are typically many devices on a single network.^[9]



A reference to Tailored Access Operations in an XKeyscore slide

Contents

Organization

Virtual locations

NSA ANT catalog

QUANTUM attacks

Known targets and collaborations

See also

References

External links

Organization

TAO's headquarters are termed the *Remote Operations Center* (ROC) and are based at the NSA headquarters at Fort Meade, Maryland. TAO also has expanded to NSA Hawaii (Wahiawa, Oahu), NSA Georgia (Fort Gordon, Georgia), NSA Texas (San Antonio, Texas), and NSA Colorado (Buckley Air Force Base, Denver).^[2]

Since 2013, the head of TAO is Rob Joyce, a 25-plus year employee who previously worked in the NSA's Information Assurance Directorate (IAD). In January 2016, Joyce had a rare public appearance when he gave a presentation at the Usenix's Enigma conference.^[10]

In the **Remote Operations Center**, 600 employees gather information from around the world.^{[11][12]}

- Data Network Technologies Branch: develops automated spyware
- Telecommunications Network Technologies Branch: improve network and computer hacking methods^[13]
- Mission Infrastructure Technologies Branch: operates the software provided above^[14]
- Access Technologies Operations Branch: Reportedly includes personnel seconded by the CIA and the FBI, who perform what are described as "off-net operations", which means they arrange for CIA agents to surreptitiously

plant eavesdropping devices on computers and telecommunications systems overseas so that TAO's hackers may remotely access them from Fort Meade.^[2] Specially equipped submarines, currently the USS Jimmy Carter,^[15] are used to wiretap fibre optic cables around the globe.

Virtual locations

Details on a program titled QUANTUMSQUIRREL indicate NSA ability to masquerade as any routable IPv4 or IPv6 host. This enables an NSA computer to generate false geographical location and personal identification credentials when accessing the Internet utilizing QUANTUMSQUIRREL.^[16]

NSA ANT catalog

The NSA ANT catalog is a 50-page classified document listing technology available to the United States National Security Agency (NSA) Tailored Access Operations (TAO) by the Advanced Network Technology (ANT) Division to aid in cyber surveillance. Most devices are described as already operational and available to US nationals and members of the Five Eyes alliance. According to *Der Spiegel*, which released the catalog to the public on December 30, 2013, "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." The document was created in 2008.^[17] Security researcher Jacob Appelbaum gave a speech at the Chaos Communications Congress in Hamburg, Germany, in which he detailed techniques that the simultaneously published *Der Spiegel* article he coauthored disclosed from the catalog.^[17]



QUANTUMSQUIRREL image from an NSA presentation explaining the QUANTUMSQUIRREL IP host spoofing ability

QUANTUM attacks


The TAO has developed an attack suite they call QUANTUM. It relies on a compromised router that duplicates internet traffic, typically HTTP requests, so that they go both to the intended target and to an NSA site (indirectly). The NSA site runs FOXACID software which sends back exploits that load in the background in the target web browser before the intended destination has had a chance to respond (it's unclear if the compromised router facilitates this race on the return trip). Prior to the development of this technology, FOXACID software made spear-phishing attacks the NSA referred to as spam. If the browser is exploitable, further permanent "implants" (rootkits etc.) are deployed in the target computer, e.g. OLYMPUSFIRE for Windows, which give complete remote access to the infected machine.^[18] This type of attack is part of the man-in-the-middle attack family, though more specifically it is called man-on-the-side attack. It is difficult to pull off without controlling some of the Internet backbone.^[19]



Lolcat image from an NSA presentation explaining in part the naming of the QUANTUM program

There are numerous services that FOXACID can exploit this way. The names of some FOXACID modules are given below:^[20]

- alibabaForumUser
- doubleclickID
- rocketmail
- hi5
- HotmailID
- Linkedin

- # QUANTUMTEORY
- 
- (TS/SU/REL) Extremely powerful CNE/CND/CNA network effects are enabled by integrating our passive and active systems:
 - Redirecting connections (QUANTUMSTRT)
 - Redirecting targets for exploitation (QUANTUMSERT)
 - Taking control of IRC bots (QUANTUMBOT)
 - Compromising file uploads/downloads (QUANTUMCOPPER)
 - (TS/SU/REL) QUANTUMTEORY dynamically injects packets into a target's network session to achieve CNE/CND/CNA network effects.
 - **Detect:** TurlinBot passive sensors detect target traffic & tip TurlinBot command-control.
 - **Decide:** TurlinBot mission logic constructs response & forwards to TAO node.
 - **Inject:** TAO node injects response into Internet towards target.
 - (TS/SU/REL) The propagation delay from tip-to-target determines the success rate of the network effect. **Less Latency = More Success!**
- THE GREAT WALL, CHINA, 2013

NSA's QUANTUMTHEORY
overview slide with various
codenames for specific types of
attack and integration with other
NSA systems

QUANTUM attacks launched from NSA sites can be too slow for some combinations of targets and services as they essentially try to exploit a race condition, i.e. the NSA server is trying to beat the legitimate server with its response.^[24] As of mid-2011, the NSA was prototyping a capability codenamed QFIRE, which involved embedding their exploit-dispensing servers in virtual machines (running on VMware ESX) hosted closer to the target, in the so-called Special Collection Sites (SCS) network worldwide. The goal of QFIRE was to lower the latency of the spoofed response, thus increasing the probability of success.^{[25][26][27]}

QUANTUMCOOKIE is a more complex form of attack which can be used against Tor users.^[31]

Known targets and collaborations

- According to a 2013 article in *Foreign Policy*, "TAO has become increasingly accomplished at its mission, thanks in part to the high-level cooperation it secretly receives from the 'big three' American telecom companies (AT&T, Verizon and Sprint), most of the large US-based Internet service providers, and many of the top computer security software manufacturers and consulting companies."^[37] A 2012 TAO budget document claims that these companies, on TAO's behest, "insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint

communications devices used by targets".^[37] A number of US companies, including Cisco and Dell, have subsequently made public statements denying that they insert such back doors into their products.^[38] Microsoft provides advance warning to the NSA of vulnerabilities it knows about, before fixes or information about these vulnerabilities is available to the public; this enables TAO to execute so-called zero-day attacks.^[39] A Microsoft official who declined to be identified in the press confirmed that this is indeed the case, but said that Microsoft can't be held responsible for how the NSA uses this advance information.^[40]

See also

- Advanced persistent threat
- Bullrun (decryption program)
- Computer and Internet Protocol Address Verifier (CIPAV)
- Cyberwarfare
- Cyberwarfare in the United States
- DigiNotar
- Equation Group
- FinFisher
- Hacking (disambiguation)
- Magic Lantern (software)
- MiniPanzer and MegaPanzer
- NSA ANT catalog
- PLA Unit 61398
- Stuxnet
- Syrian Electronic Army
- WARRIOR PRIDE

References

1. Ellen Nakashima (1 December 2017). "NSA employee who worked on hacking tools at home pleads guilty to spy charge" (https://www.washingtonpost.com/world/national-security/nsa-employee-who-worked-on-hacking-tools-at-home-pleads-guilty-to-spy-charge/2017/12/01/ec4d6738-d6d9-11e7-b62d-d9345ced896d_story.html). *WashingtonPost.com*. Retrieved 4 December 2017.
2. Aid, Matthew M. (10 June 2013). "Inside the NSA's Ultra-Secret China Hacking Group" (<https://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group/>). *Foreign Policy*. Retrieved 11 June 2013.
3. Paterson, Andrea (30 August 2013). "The NSA has its own team of elite hackers" (https://www.washingtonpost.com/blogs/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/?tid=d_pulse). *The Washington Post*. Retrieved 31 August 2013.
4. Kingsbury, Alex (June 19, 2009). "The Secret History of the National Security Agency" (<https://www.usnews.com/opinion/articles/2009/06/19/the-secret-history-of-the-national-security-agency>). *U.S. News & World Report*. Retrieved 22 May 2013.
5. Kingsbury, Alex; Anna Mulrine (November 18, 2009). "U.S. is Striking Back in the Global Cyberwar" (<https://www.usnews.com/news/articles/2009/11/18/us-is-striking-back-in-the-global-cyberwar>). *U.S. News & World Report*. Retrieved 22 May 2013.
6. Riley, Michael (May 23, 2013). "How the U.S. Government Hacks the World" (<http://www.businessweek.com/articles/2013-05-23/how-the-u-dot-s-dot-government-hacks-the-world>). *Bloomberg Businessweek*. Retrieved 23 May 2013.
7. Aid, Matthew M. (8 June 2010). *The Secret Sentry: The Untold History of the National Security Agency* (https://books.google.com/books?id=x_K2rb-OShMC&pg=PA311). Bloomsbury USA. p. 311. ISBN 978-1-60819-096-6. Retrieved 22 May 2013.
8. FOIA #70809 (released 2014-09-19) (<https://www.aclu.org/files/assets/eo12333/NSA/Signals%20Intelligence%20Directorate%20%28SID%29%20Management%20Directive%20422%20United%20States%20SIGINT%20System%20Mission%20Delegation.pdf>)

9. Barton Gellman; Ellen Nakashima (August 30, 2013). "U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show" (https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html). *The Washington Post*. Retrieved 7 September 2013. "Much more often, an implant is coded entirely in software by an NSA group called, Tailored Access Operations (TAO). As its name suggests, TAO builds attack tools that are custom-fitted to their targets. The NSA unit's software engineers would rather tap into networks than individual computers because there are usually many devices on each network. Tailored Access Operations has software templates to break into common brands and models of "routers, switches, and firewalls from multiple product vendor lines," according to one document describing its work."
10. The Register: NSA's top hacking boss explains how to protect your network from his attack squads (https://www.theregister.co.uk/2016/01/28/nsas_top_hacking_boss_explains_how_to_protect_your_network_from_his_minions?page=1), January 28, 2016
11. "Secret NSA hackers from TAO Office have been pwning China for nearly 15 years" (<https://web.archive.org/web/20140125123015/http://blogs.computerworld.com/cybercrime-and-hacking/22321/secret-nsa-hackers-tao-office-have-been-pwning-china-nearly-15-years>). Computerworld. 2013-06-11. Archived from the original (<http://blogs.computerworld.com/cybercrime-and-hacking/22321/secret-nsa-hackers-tao-office-have-been-pwning-china-nearly-15-years>) on 2014-01-25. Retrieved 2014-01-27.
12. Rothkopf, David. "Inside the NSA's Ultra-Secret China Hacking Group" (https://foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group). *Foreign Policy*. Retrieved 2014-01-27.
13. "Hintergrund: Die Speerspitze des amerikanischen Hackings - News Ausland: Amerika" (<http://www.tagesanzeiger.ch/ausland/amerika/Die-Speerspitze-des-amerikanischen-Hackings/story/30196342>). *tagesanzeiger.ch*. Retrieved 2014-01-27.
14. WebCite query result (<https://www.webcitation.org/6HwJORJVg?url=http://www.acus.org/natosource/inside-nsas-ultra-secret-hacking-group>)
15. noahmax (2005-02-21). "Jimmy Carter: Super Spy?" (<http://defensetech.org/2005/02/21/jimmy-carter-super-spy/>). Defense Tech. Retrieved 2014-01-27.
16. "The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics" (<https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/>). *firstlook.org*. 2014-07-16. Retrieved 2014-07-16.
17. This section copied from NSA ANT catalog; see there for sources
18. "Quantumtheory: Wie die NSA weltweit Rechner hackt" (<http://www.spiegel.de/netzwelt/netzpolitik/quantumtheory-wie-die-nsa-weltweit-rechner-hackt-a-941149.html>). *Der Spiegel*. 2013-12-30. Retrieved 2014-01-18.
19. Bruce Schneier (2013-10-07). "How the NSA Attacks Tor/Firefox Users With QUANTUM and FOXACID" (https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html). *Schneier.com*. Retrieved 2014-01-18.
20. Fotostrecke (2013-12-30). "NSA-Dokumente: So knackt der Geheimdienst Internetkonten" (<http://www.spiegel.de/fotostrecke/nsa-dokumente-so-knackt-der-geheimdienst-internetkonten-fotostrecke-105326-11.html>). *Der Spiegel*. Retrieved 2014-01-18.
21. "NSA-Dokumente: So knackt der Geheimdienst Internetkonten" (<http://www.spiegel.de/fotostrecke/nsa-dokumente-so-knackt-der-geheimdienst-internetkonten-fotostrecke-105326-12.html>). *Der Spiegel*. 2013-12-30. Retrieved 2014-01-18.
22. Gallagher, Sean (August 1, 2013). "NSA's Internet taps can find systems to hack, track VPNs and Word docs" (<https://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/>). Retrieved August 8, 2013.
23. "Inside TAO: Targeting Mexico" (<http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html>). *Der Spiegel*. 2013-12-29. Retrieved 2014-01-18.
24. Fotostrecke (2013-12-30). "QFIRE - die "Vorwärtsverteidigung" der NSA" (<http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigung-der-nsa-fotostrecke-105358-14.html>). *Der Spiegel*. Retrieved 2014-01-18.
25. "QFIRE - die "Vorwärtsverteidigung" der NSA" (<http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigung-der-nsa-fotostrecke-105358-8.html>). *Der Spiegel*. 2013-12-30. Retrieved 2014-01-18.
26. "QFIRE - die "Vorwärtsverteidigung" der NSA" (<http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigung-der-nsa-fotostrecke-105358-9.html>). *Der Spiegel*. 2013-12-30. Retrieved 2014-01-18.
27. "QFIRE - die "Vorwärtsverteidigung" der NSA" (<http://www.spiegel.de/fotostrecke/qfire-die-vorwaertsverteidigung-der-nsa-fotostrecke-105358-11.html>). *Der Spiegel*. 2013-12-30. Retrieved 2014-01-18.

28. [""Chaos Computer Club CCC Presentation" at 28:34" \(https://www.youtube.com/watch?v=b0w36GAyZIA#t=28m34s\)](https://www.youtube.com/watch?v=b0w36GAyZIA#t=28m34s).
29. Thomson, Iain (2013-12-31). "How the NSA hacks PCs, phones, routers, hard disks 'at speed of light': Spy tech catalog leaks" (https://www.theregister.co.uk/2013/12/31/nsa_weapons_catalogue_promises_pwnage_at_the_speed_of_light). *The Register*. London. Retrieved 2014-08-15.
30. Mick, Jason (2013-12-31). "Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years" (<https://web.archive.org/web/20140824193107/http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm>). *DailyTech*. Archived from the original (<http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm>) on 2014-08-24. Retrieved 2014-08-15.
31. Weaver, Nicholas (2013-03-28). "Our Government Has Weaponized the Internet. Here's How They Did It" (<https://www.wired.com/opinion/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/>). *Wired*. Retrieved 2014-01-18.
32. "Inside TAO: The NSA's Shadow Network" (<http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html>). *Der Spiegel*. 2013-12-29. Retrieved 2014-01-27.
33. Gallagher, Sean (2013-11-12). "Quantum of pwnness: How NSA and GCHQ hacked OPEC and others" (<https://arstechnica.com/information-technology/2013/11/quantum-of-pwnness-how-nsa-and-gchq-hacked-opec-and-others/>). *Ars Technica*. Retrieved 2014-01-18.
34. "British spies reportedly spoofed LinkedIn, Slashdot to target network engineers" (<https://web.archive.org/web/20140115014135/http://www.networkworld.com/news/2013/111113-british-spies-reportedly-spoofed-linkedin-275807.html>). *Network World*. 2013-11-11. Archived from the original (<http://www.networkworld.com/news/2013/111113-british-spies-reportedly-spoofed-linkedin-275807.html>) on 2014-01-15. Retrieved 2014-01-18.
35. "Läs dokumenten om Sverige från Edward Snowden - Uppdrag Granskning" (<http://www.svt.se/ug/las-dokumenten-om-sverige-fran-edward-snowden>). *SVT.se*. Retrieved 2014-01-18.
36. "What You Wanted to Know" (<http://s3.documentcloud.org/documents/894386/legal-issues-uk-regarding-sweden-and-quantum.pdf>) (PDF). *documentcloud.org*. Retrieved 2015-10-03.
37. Matthew M. Aid, (October 15, 2013) "The NSA's New Code Breakers" (https://foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers?page=0,0) Archived (https://web.archive.org/web/20141110194220/http://www.foreignpolicy.com/articles/2013/10/15/the_nsa_s_new_codebreakers?page=0,0) 2014-11-10 at the *Wayback Machine*", *Foreign Policy*
38. Farber, Dan (2013-12-29). "NSA reportedly planted spyware on electronics equipment | Security & Privacy" (http://news.cnet.com/8301-1009_3-57616334-83/nsa-reportedly-planted-spyware-on-electronics-equipment/). *CNET News*. Retrieved 2014-01-18.
39. Schneier, Bruce (2013-10-04). "How the NSA Thinks About Secrecy and Risk" (<https://www.theatlantic.com/technology/archive/2013/10/how-the-nsa-thinks-about-secrecy-and-risk/280258/>). *The Atlantic*. Retrieved 2014-01-18.
40. Riley, Michael (2013-06-14). "U.S. Agencies Said to Swap Data With Thousands of Firms" (<https://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html>). *Bloomberg*. Retrieved 2014-01-18.

External links

- [Inside TAO: Documents Reveal Top NSA Hacking Unit \(http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html\)](http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html)
- [NSA 'hacking unit' infiltrates computers around the world – report \(https://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao\)](https://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao)
- [NSA Tailored Access Operations \(http://williamsarkin.wordpress.com/2013/09/03/nsa-tailored-access-operations/\)](http://williamsarkin.wordpress.com/2013/09/03/nsa-tailored-access-operations/)
- <https://www.wired.com/threatlevel/2013/09/nsa-router-hacking/>
- <https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html>

Retrieved from "https://en.wikipedia.org/w/index.php?title=Tailored_Access_Operations&oldid=861317173"

This page was last edited on 26 September 2018, at 15:40 (UTC).

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.