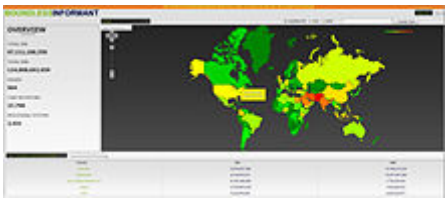
PRISM (programma di sorveglianza)

Da Wikipedia, l'enciclopedia libera.

PRISM è un programma di sorveglianza elettronica, cyberwarfare e Signal Intelligence, classificato come di massima segretezza, usato per la gestione di informazioni raccolte attraverso Internet e altri fornitori di servizi elettronici e telematici. È stato posto in attività dalla National Security Agency (NSA) fin dal 2007.[1] PRISM è il nome in codice scelto dal governo statunitense per US-984XN, ispirandosi al prisma ottico ("un mezzo trasparente alla luce che ha la capacità di alterare la visione della realtà osservata attraverso di esso").[2] I documenti pubblicati da Edward Snowden (ex impiegato di una società informatica che lavora per la NSA) nel giugno 2013 descrivono il programma PRISM come abilitato alla sorveglianza in profondità su comunicazioni dal vivo di gran parte del traffico Internet mondiale e delle informazioni memorizzate. I dati ottenibili comprendono quindi email, chat, chat vocali e videochat, video, foto, conversazioni VoIP, trasferimento di file, notifiche d'accesso e dettagli relativi a siti di reti sociali. Per ottenere ciò, PRISM si serve della collaborazione di vari fra i maggiori service provider, tra cui i principali sono Google, Facebook, Microsoft, Skype, Apple, Yahoo, AOL e altri;[3][4] inoltre, esso sfrutta le caratteristiche di routing tipiche della Rete: in particolare, il fatto che il percorso seguito dai pacchetti IP durante le connessioni non sia necessariamente il più breve ma piuttosto quello più economico. Grazie a tali caratteristiche di routing gran parte del traffico mondiale delle comunicazioni fra utenti e server posti in nazioni diverse (ad esempio un utente italiano che si collega a un sito web cinese) passa per gli Stati Uniti o per ISP statunitensi, circostanza che permette a PRISM di immagazzinare ancor più dati.[5] Il 14 giugno, in un'intervista, Snowden ha dichiarato che la NSA, per ampliare l'area coperta dalle intercettazioni, svolge abitualmente attacchi contro le dorsali Internet mirando ai router più importanti, sia di paesi amici (come gli stati europei), sia di provider cinesi.[6] Nello stesso periodo Snowden dichiarò pure che la NSA aveva svolto azioni del genere su reti cinesi in decine di migliaia di attacchi.[7] L'unica contromisura veramente efficace che i cittadini possono usare per difendersi da PRISM è, secondo Snowden, l'uso di sistemi di crittografia forte (come PGP, Tor e mezzi simili).[8]

Logo del programma PRISM


Mappa della raccolta dati dell'NSA

L'operatività del programma si basa sulle previsioni normative contenute nella sezione 702 del *Foreign Intelligence Surveillance Act* (FISA), una legge promulgata nel 1978 ma più volte modificata (ad esempio, dallo USA PATRIOT Act concepito nel 2001) e prorogata (l'ultima volta da Barack Obama nel dicembre 2013), durante gli anni successivi agli attentati dell'11 settembre 2001.

Il 2 agosto 2013 un articolo del Süddeutsche Zeitung rivela che le operazioni di PRISM non si limitano al solo spionaggio. Da alcuni documenti di cui la testata è in possesso risulta che i maggiori ISP europei e no:

1. svolgono veri e propri attacchi informatici a reti private;
2. alterano attivamente il traffico utente allo scopo di sfruttare vulnerabilità (tramite exploit) e installare trojan su determinati computer, compromettono così sistemi informatici onde ottenerne controllo completo al pc delle vittime.

Gli ISP coinvolti vengono definiti "la Crème de la Crème" di Internet, in quanto da soli hanno il controllo quasi totale sul traffico Internet mondiale.[9] [10]

Indice

Risposta delle presunte società coinvolte

Gli articoli del *Washington Post* e del *Guardian* riportano che i dati raccolti da PRISM provenivano direttamente dai server degli Internet Service Provider.[1]

Dirigenti aziendali di diverse società individuate nei documenti trapelati hanno comunicato al *The Guardian* che non erano a conoscenza del programma PRISM e, in particolare, hanno anche negato di rendere disponibili su vasta scala tali informazioni al governo, come riportato dai quotidiani.[11]

Elenco delle società, ordinate per data in cui si sono unite al progetto PRISM

Note

1. (EN) Barton Gellman e Laura Poitras, *US Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, in *The Washington Post*, 6 giugno 2013. URL consultato l'11 giugno 2013.
2. ^ (EN) *Prisms - definition of Prisms*, su *Free Online Dictionary*.
   «A medium that misrepresents whatever is seen through it».
3. ^ (EN) *NSA leaks hint Microsoft may have lied about Skype security*, su *Russia Today*.
4. ^ (EN) *NSA leak fallout: LIVE UPDATES*, su *Russia Today*.
5. ^ (EN) *'How little rights you have:' Anonymous leaks more PRISM-related NSA docs*, su *RT.com*.
6. ^ (EN) *Edward Snowden claims US hacks Chinese targets. The US has perpetrated hacking attacks on "hundreds" of targets in Hong Kong and mainland China since 2009, the former CIA analyst Edward Snowden has claimed.*, su *telegraph.co.uk*.
   «We hack network backbones – like huge internet routers, basically – that give us access to the communications of hundreds of thousands of computers without having to hack every single one," Edward Snowden su Telegraph».
7. ^ (EN) *Snowden's asset: NSA hacking exposer knows secrets China wants*, su *RT.com*.
8. ^ (EN) *Edward Snowden's live Q&A: eight things we learned*, in *The Guardian*.
   «Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.».

9. **^** (EN) *Telecom giants give GCHQ unlimited access to networks, develop own spyware – Snowden leaks*, su *RT.com*.
«...Such software could come in a form of Trojan viruses installed on targeted computers, the reports say, stating that the companies' involvement in data collection is much larger and more complicated than previously thought... (...Tale software può apparire sotto forma di virus trojans installati sui computer dell'obiettivo, dice il report, affermando che il coinvolgimento delle aziende nella raccolta dati è molto più vasto e complicato di quanto precedentemente pensato...)».
10. **^** (DE) *Internet-Überwachung: Snowden enthüllt Namen der spähenden Telekomfirmen*, in *Süddeutsche Zeitung*.
«...Bislang geheime Powerpoint-Folien, die der SZ vorliegen, zeigen, was der britische Geheimdienst GCHQ alles kann: Installation von Trojanern, Desinformation, Angriffe auf Netzwerke. .... und welche privaten Internetanbieter beim Ausspähen behilflich sind. Es ist die Crème de la Crème der Branche, mit Macht über große Teile der weltweiten Internetstruktur... (Dalle presentazioni Powerpoint, che il Süddeutsche Zeitung ha ricevuto, emerge che il GCHQ britannico può tutto: Installazione di Virus Trojan, Disinformazione, Attacco alle Reti. ... viene poi rivelato quali ISP privati collaborano allo spionaggio. Sono la "Crème de la Crème" dell'industria, controllano la maggior parte dell'infrastruttura globale di Internet)».
11. **^** (EN) Cyrus Farivar, *New Leak Shows Feds Can Access User Accounts for Google, Facebook and More - Secret Slides Reveal Massive Government Spying, Tech Companies Dispute Reports*, Ars Technica, 6 giugno 2013. URL consultato il 12 giugno 2013.

Voci correlate

- Divulgazioni sulla sorveglianza di massa del 2013
- National Security Agency
- Cyberwarfare
- SORM
- SIGINT
- Spionaggio industriale
- Bullrun
- Echelon
- Sniffing
- Man in the middle
- Replay attack
- Tempora
- Unit 8200

Altri progetti

- Wikimedia Commons (https://commons.wikimedia.org/wiki/?uselang=it) contiene immagini o altri file su **PRISM (https://commons.wikimedia.org/wiki/Category:PRISM_(surveillance_program)?uselang=it)**

Collegamenti esterni

- "The NSA Files (http://www.guardian.co.uk/world/the-nsa-files)." *The Guardian*
- prism-break.org (https://prism-break.org/) Una lista di contromisure per l'autodifesa degli utenti dallo spionaggio di PRISM, scritta dalla FSF