<h4>L'agenzia per la sicurezza nazionale Usa sarebbe in grado di violare i sistemi crittografici che proteggono email, sistemi bancari e database medici</h4> Datagate, nuovo atto. Lo scenario svelato dai documenti passati dal whistlebower dell'agenzia per la sicurezza nazionale statunitense, Edward Snowden (attualmente in una localit&#65533;segreta della Russia), si tinge di tinte sempre pi&#65533; fosche. Stando agli ultimi segreti divulgati congiuntamente da&#65533; Guardian, ProPublica e New York Times, infatti, l' Nsa &#65533;&#65533;assieme ad altre agenzie di intelligenze statunitensi e britanniche &#65533; sarebbe in grado di violare sistematicamente la maggior parte dei sistemi crittografici attualmente utilizzati per proteggere i dati relativi a banche, database medici e commercio online. Oltre che, naturalmente, email, ricerche Internet, conversazioni telefoniche e chat di tutto il mondo. I documenti divulgati mostrano che l'Nsa ha investito miliardi di dollari in una campagna clandestina per acquistare supercomputer in grado di scardinare le protezioni, indebolire gli standard crittografici e installare backdoor in vari prodotti software per accedere ai dati prima che venissero criptati. <font color="#000000">&#65533;Molti utenti credono &#65533; o sono stati indotti a credere dalle aziende Internet&#65533;, scrive il Nyt, &#65533;che i loro dati sono al sicuro da occhi indiscreti, e l'Nsa ha tutto l'interesse a mantenere questo tipo di fiducia&#65533;. Ma, a quanto pare, purtroppo non &#65533;cos&#65533; &#65533;L'agenzia &#65533;riuscita a decriptare informazioni altamente protette, inserendoli in un programma supersegreto&#65533;. Nome in codice Bullrun. L'Nsa, inoltre, stando ai documenti, avrebbe collaborato con aziende di tecnologia statunitensi &#65533; i cui nomi non sono stati divulgati &#65533; per inserire una specie di cimici nei loro prodotti hardware e software. In alcuni casi, tali aziende sono state costrette dal governo ad accettare l'ingerenza dell'agenzia per la sicurezza nazionale. Cosa ancora pi&#65533; grave, l'Nsa ha usato la sua influenza &#65533; in fin dei conti, vi lavorano sviluppatori tra i pi&#65533; abili al mondo &#65533; per introdurre debolezze negli standard seguiti dai programmatori di tutto il mondo.

&#65533;un lavor&#65533; sotterraneo che va ancora avanti. Nel budget per il 2013, il direttore dell' Nsa, James R. Clapper, ha scritto che &#65533;l'agenzia per la sicurezza nazionale sta investendo nello sviluppo di straordinarie capacit&#65533;di criptoanalisi per scardinare i metodi crittografici dei nostri avversari e penetrare nel traffico Internet&#65533;. La motivazione ufficiale, naturalmente, &#65533;sempre la stessa: &#65533;Queste tecnologie servono agli Stati Uniti per decifrare i messaggi dei terroristi, spie straniere o altri avversari. Se non ci riuscissimo, saremmo in grave pericolo&#65533;, sostengono i funzionari dell'agenzia. Tant'&#65533;che nelle ultime settimane l'amministrazione Obama ha chiesto alle agenzie di intelligence dettagli sulle comunicazioni del leader di Al Qaeda riguardo all'uso di &#65533;armi chimiche da parte delle autorit&#65533;siriane&#65533;. Peccato, per&#65533; che nel mirino dell'Nsa non ci siano solo terroristi armati. Ma anche centinaia di milioni di cittadini inconsapevoli, per cui il significato della parola privacy va sempre pi&#65533; assottigliandosi.

Gli sforzi pi&#65533; intensi dell'Nsa, dicono i documenti, si sono concentrati sui sistemi di criptazione pi&#65533; utilizzati, tra cui l' Ssl (Secure Sockets Layer) e le Vpn (Virtual Private Networks). E anche le nuove reti 4G per il traffico mobile non sarebbero sfuggite all'occhio indiscreto dell'agenzia. Per almeno tre anni, tra l'altro, anche gli esperti del Gchq, i cugini britannici dell'Nsa, avrebbero sondato le comunicazioni protette di Yahoo!, Google (che ha sempre negato di aver dato l'accesso al governo), Facebook e Hotmail. Com'&#65533;facile comprendere, non si tratta di buone notizie: &#65533;Le tecnologie di criptazione che l'Nsa ha sfruttato per la sorveglianza&#65533;, racconta a Wired.com Christopher Soghoian, analista ed esperto di tecnologia per lo Speech, Privacy and Technology

Project, rendono completamente inutile la protezione dei nostri dati sensibili. Il fatto che l'agenzia abbia deliberatamente introdotto debolezze nei sistemi di protezione se possibile, ancora pi grave. Tanto per fare un esempio, potrebbero essere completamente compromessi gli sforzi che gli attivisti Tor per i diritti umani sono costretti a compiere per proteggere le loro comunicazioni dai regimi.

Il crittografo Bruce Schneier spiega al Guardian qual la strategia operativa dell'Nsa: Fondamentalmente, l'agenzia chiede alle aziende di cambiare alcuni dettagli dei loro prodotti software: rendere un po' meno casuale un generatore di numeri casuali o aggiungere una determinata cifra a una chiave pubblica, per esempio. Saremo tutti destinati a tornare a comunicare via pizzini, dunque? Non ancora detto. Schneier ha suggerito cinque accorgimenti da adottare per restare al sicuro, tra cui l'uso di Tor e software analoghi per rendere anonima la propria presenza sul Web. Non sono completamente a prova di Nsa. Ma almeno avremo cercato di rendere loro la vita un po' pi difficile. </p>