Come bloccano internet

Sappiamo perché i governi bloccano internet, totalmente o parzialmente (per spegnere il dissenso; impedire la sua organizzazione; ridurre l'accesso o la circolazione di informazioni sgradite, ecc); sappiamo che negli ultimi anni lo hanno fatto sempre più spesso (182 casi nel 2021 in 34 Paesi contro i 159 del 2020). Ma non sappiamo molto di come avvengano effettivamente tali blocchi. Eppure anche il come è importante, per un motivo molto semplice: "l'assenza di comprensione tecnica ha un impatto nella nostra capacità di combatterli".

Una tassonomia dei blocchi internet

Così scrive un rapporto appena uscito dell'Ong Access Now che analizza le differenze tecniche dei vari tipi di blocchi della Rete tracciando una "tassonomia degli internet shutdown".
Ma prima di tutto una definizione. Per internet shutdown si intende, scrive Access Now, "la sospensione intenzionale di internet o di comunicazioni elettroniche, al fine di rendere le stesse inaccessibili o di fatto inutilizzabili, per una popolazione specifica o in una località, spesso per esercitare controllo sul flusso di informazioni".

Non solo. Siccome cresce la pressione internazionale contro questa forma di "punizione collettiva" (e aggiungo io, siccome un blocco totale ha costi economici non indifferenti) i

governi stanno ricorrendo sempre di più a forme mirate, geograficamente o a livello di servizio/app specifiche. Ad esempio, c'è una mobilitazione di piazza antigovernativa? Si sospende il traffico dati mobile della zona, e via dicendo.

Ora il report identifica 8 tipi di shutdown, che vi riassumo qui di seguito (in un difficile equilibrismo tra tecnicismi, divulgazione e sintesi, dato che il report è dettagliato e rivolto a un pubblico tecnico):

1) Blocco fondamentale dell'infrastruttura

Quando l'interruzione nasce da un danneggiamento all'infrastruttura fisica. Esempio: quando nel 2015-2016 gli hacker di Sandworm (considerati legati all'intelligence russa) hanno provocato un blackout elettrico in Ucraina, hanno anche causato un'interruzione nelle reti di comunicazione. O quando nel 2018 è andato a fuoco un centro tecnico di Orange in Costa d'Avorio dei cavi sottomarini sono stati distrutti col risultato di rendere il servizio inaccessibile per settimane. Per Orange si trattò di sabotaggio.
Vantaggi per chi lo fa: efficace; offre plausible deniablity (negazione plausibile: è stato un incidente, non volevamo mica censurare nessuno!); ma può essere alla portata anche di attori non statali.
Come affrontarlo: comunicazioni satellitari, radio, altre infrastrutture.

2) Routing

La manipolazione del network routing. L'informazione sul routing è alterata in punti chiave dell'infrastruttura di rete, come ai gateways internazionali, per non far passare il traffico ad altre infrastrutture, determinando uno shutdown. Non funziona bene su sezioni localizzate del network, e di solito è implementata per nazioni intere o grandi aree geografiche.
Vantaggi: un modo semplice di chiudere la connettività

internet internazionale per un Paese. Ma ha lo svantaggio che i cambiamenti nel routing devono propagarsi e ci vuole del tempo.
Come affrontarlo: comunicazioni satellitari, radio, altre infrastrutture.

3) Manipolazione del sistema dei nomi di dominio (DNS)

Si usa la manipolazione dei DNS (il sistema che regola la traduzione dei domini in indirizzi IP) e in particolare dei domain name servers di un Paese per dirigere il traffico verso domini specifici (ad esempio WhatsApp) via dai server dell'azienda e mandarlo invece a server sotto il controllo del governo o che nemmeno esistono, causando un blocco del servizio. Perché sia efficace serve il controllo (da parte del governo) o la collaborazione degli internet service providers (ISP). Inoltre alcuni meccanismi usati per implementare questo tipo di blocco sono facili da aggirare da parte degli utenti. In realtà questo tipo di manipolazione è molto complessa e con varie sfumature, per cui rimando al rapporto, che va molto in dettaglio.
Esempi: L'Iran anni addietro aveva bloccato Facebook Messenger in questo modo. Il Pakistan l'ha usata per bloccare alcuni social media durante le proteste del 2017. E la manipolazione dei DNS è stata usata per bloccare 25 siti in Catalogna in occasione del referendum del 2017 sull'indipendenza.
Vantaggi: facile da implementare contro social o piattaforme "hostate su un piccolo set di domini DNS".
Come affrontarla: a seconda della tipologia si possono usare server DNS non sotto il controllo delle autorità; e/o una VPN. Per proteggersi da attacchi di questo tipo può aiutare anche l'uso di una funzione DNS avanzata, nota come DNSSEC, "che aggiunge un livello di fiducia al DNS fornendo un servizio di autenticazione".

4) Filtraggio (Filtering)

Usa particolari apparecchiature (filtering appliances), adottate anche a livello corporate, per bloccare l'accesso a specifiche piattaforme, come Facebook, Twitter ecc. È un meccanismo usato spesso da Cina, Iran, Arabia Saudita. In genere tali apparecchiature sono già messe in piedi per filtrare siti criminali e poi sono estese ad altri.
Sono implementate a livello di backbone, dorsali internet (se il governo controlla le infrastrutture telco in un Paese), o a livello di ogni singolo ISP del Paese (e in tal caso il filtraggio non sarà omogeneo).
Esempi: il Brasile ha bloccato Whatsapp in questo modo nel 2015.
Vantaggi: nasce come tecnologia con vari scopi commerciali; ha effetto immediato; può essere molto granulare, anche sulla base della localizzazione degli utenti. Quando l'utente prova a collegarsi a un sito bloccato, può vedere un avviso che dice che è bloccato ma anche un messaggio di errore.
Come affrontarlo: si possono usare VPN per aggirarlo (se non sono a loro volta bloccate)

5) Ispezione profonda dei pacchetti (Deep packet inspection o DPI)

Si tratta ancora di device di filtraggio in grado anche di valutare i contenuti del traffico e anche qua possono essere implementati a livello di backbone o da ogni singolo ISP. Sono strumenti che possono essere usati in un'ottica di sorveglianza ma anche di censura. Il Paese che forse più l'ha usata in questa maniera è la Cina.
Esempi: come segnalato dall'osservatorio anti-censura OONI (che ha collaborato al report di Access Now), Cuba ha usato questa tecnologia per bloccare Skype. L'Iran l'ha usata nel 2018 per bloccare Instagram.
Vantaggi: è una tecnologia potente con vari utilizzi, da quelli commerciali alla censura e sorveglianza. Anche questa può essere molto granulare.

Come affrontarla: con alcuni meccanismi per nascondere la comunicazione in un protocollo (obfuscation proxies).

6) Attacco attraverso un'infrastruttura non autorizzata (rogue)

Avviene quando l'attaccante introduce un meccanismo (in genere temporaneo) nell'infrastruttura o in un segmento di rete, così da clonare l'infrastruttura legittima a cui si connetterà l'utente. Che in quel modo, senza accorgersene, affida le comunicazioni all'operatore del nodo illegittimo. In genere si utilizza su reti cellulari e WI-Fi.
Esempi: nel 2016 durante una protesta in North Dakota i partecipanti hanno riferito di chiamate disconnesse e altri problemi al segnale mobile.
Vantaggi: permette di identificare i partecipanti a una protesta o a una attività in un certo luogo.
Come gestirlo: Bisogna smettere di usare il sistema di comunicazione intercettato dai nodi non autorizzati.

7) Attacco di negazione del servizio – Denial of Service (DoS)

I suoi autori usano attacchi di negazione distribuita del servizio o DDoS (Distributed Denial of Service) e altri attacchi DoS (Denial of Service) per prendere di mira le comunicazioni di una piattaforma specifica, o anche le comunicazioni internet di un intero Paese, come accadde nel 2016 quando il gruppo dietro la botnet Mirai attaccò le telco e infrastrutture della Liberia (collegata a internet solo da un cavo sottomarino). L'offerta criminale di questi servizi, che possono essere acquistati da altri, è ampia e ben organizzata.
Esempi: i DDoS che si sono visti in Ucraina.
Vantaggi: plausible deniability (non sono stato io ma questo gruppo di scappati di casa); ma d'altro canto si tratta di uno strumento che possono usare anche attori non-statali; gli utenti non possono fare nulla per aggirare o risolvere il

problema, se non lo risolve il fornitore del servizio sotto attacco.
Come mitigarli: la mitigazione va fatta prima usando dei servizi di protezioni dai DoS.

8) Throttling (limitazione)

È l'atto di limitare volutamente, senza bloccare del tutto, il flusso di dati attraverso una rete di comunicazione. Così sembra che il servizio o la piattaforma in questione siano disponibili, ma di fatto sono inutilizzabili. Ci sono vari meccanismi tecnici per farlo, e la comunicazione può essere limitata sulla base del protocollo, origine, destinazione ecc. È difficile distinguere se la causa sia voluta o dovuta ad altro.
Esempi: l'Iran col traffico HTTPS prima delle elezioni.
Vantaggi: plausible deniability; permette alcuni usi essenziali: spinge utenti via dai canali cifrati.
Come affrontarlo: se il throttling riguarda solo siti e servizi basati su uno specifico protocollo, si possono usare sistemi come VPN ecc. Altrimenti se tutto il traffico è limitato, è più difficile aggirarlo.

Il report, dopo aver classificato le diverse tipologie di shutdown, prosegue ad analizzare l'impatto di questi blocchi: quante persone hanno riguardato? Hanno impedito attività economiche? Servizi di emergenza? L'accesso a informazione indipendente? Comunicazioni interpersonali? Era facile migrare a una piattaforma equivalente? E quanto le persone si affidavano alla tecnologia/piattaforma bloccata? E infine, come si possono individuare e attribuire le diverse cause all'origine di questi blocchi?
Nella riconfigurazione di internet che sta avvenendo in questi ultimi tempi (o che alcuni vorrebbero far avvenire) anche le questioni tecniche assumono una forte connotazione di attualità politica. Non che ne siano mai state prive