NUOVO PROGETTO/BLOG SULLA DIFFUSIONE DI MANUALI/VIDEO DI TERRORISMO ANTI-POLITICO

Ricevo e pubblico:

http://terrorismoegoarca.torpress2sarn7xw.onion/

http://terrorismoegoarca.torpress2sarn7xw.onion/2019/05/21/introduzione/

Introduzione

Presentiamo un nuovo progetto che si rifà al terrorismo, di un certo tipo, specifico, è che non ha che fare con la politica. Questo "concetto" è già stato espresso varie volte su blog o riviste affini, per quello che pensiamo del terrorismo. Parliamo in questo caso della corrente Terroristica Misantropica Attiva, di quella Eco-estremistica, del Nichilismo Terrorista, degli Individualisti amorali e asociali, di tutta quella "specie", che è odiata e temuta, perchè toglie fiato alla pace, non solo quella "sociale", ma anche quella della morale di oggi giorno. Pubblicheremo su questo blog, solo ed esclusivamente, manuali/video sugli ordigni esplosivi, quelli incendiari, le formule chimiche per produrre sostanze detonanti, ma anche manuali sulla sopravvivenza urbana e non, sulle tecniche clandestine per procurarsi documenti falsi o altro ancora… Sotto mettiamo il nostro contatto elettronico a disposizione, per eventuali interesse in materiale affine al contesto, più alcune tecniche elettroniche per riuscire ad usare meglio Tor o Tails, dato che il nostro blog usa determinate tecniche di sicurezza (naturalmente non tutto è perfetto e c'è sempre da migliorarsi)

cultoabaddon@secmail.pro

_____

https://darkwhite666.blogspot.com/2016/11/tor-e-tracciabile-come-eliminare-lo.html

TOR E’ Tracciabile? Come Eliminare Lo State File (Entry Guard Relays)

Quello che TOR fa è semplicemente nascondere la tua posizione, la comunicazione invece non è crittografata.
Invece di intraprendere un percorso diretto (dalla sorgente alla destinazione cercata), le comunicazioni che utilizzano la rete TOR prendono un percorso casuale attraverso molti relays che ne coprono le tracce.
Quindi, nessun attaccante situato in un dato punto del “percorso”, può dire da dove vengono i dati e dove arrivano.
Una connessione TOR di solito passa attraverso 3 Relays con l’ultimo che stabilisce la connessione effettiva alla destinazione finale cercata.
Dunque l’ultimo Exit Relays è quello che stabilisce la connessione effettiva al server di destinazione.
Quello che invece TOR non fa e non può fare è crittografare il traffico tra un Exit Relays e il server di destinazione, qualsiasi Exit Relays è in grado di intercettare il traffico che lo attraversa.
Ad esempio, nel 2007, un ricercatore di sicurezza intercettò migliaia di messaggi di posta elettronica privati □□inviati da ambasciate straniere e gruppi per i diritti umani in tutto il mondo per spiare le connessioni in uscita di un Exit Relay.
Per proteggersi da tali attacchi si dovrebbe utilizzare la crittografia “end-to-end”.
Una buona soluzione è ovviamente la distribuzione Linux chiamata Whonix (sistema operativo) che include molti strumenti che consentono di utilizzare sistemi di crittografia

durante la navigazione, l'invio di e-mail, chat, etc
Whonix che comprende due macchine virtuali (Workstation e un TOR Gateway) però non maschera l'utilizzo di TOR.
TOR cerca di nascondere i siti visitati anonimizzando l'IP ma chi di dovere (tipo un provider) sa che lo state utilizzando (non che di per sè sia illegale ma viene meno la privacy).

Infatti se non si utilizza una configurazione apposita, il vostro provider o amministratore di rete può dimostrare facilmente che vi state collegando ad un server TOR e non ad un normale sito web.
In altre parole, a meno di utilizzare un tunnel proxy / SSH / VPN configurati con TOR, il server di destinazione a cui ci si sta collegando attraverso TOR può sapere da dove proviene la vostra connessione, consultando le liste pubbliche di Exit Relays (ad esempio, utilizzando il TOR Bulk Exit List Tool di TOR Project).
Quindi, a meno che non si stia utilizzando configurazioni opzionali per impedire ciò, la soluzione ideale è Whonix che rende "uguali" tutti gli utenti quindi non è possibile identificare chi transita da un dato Exit Relay.

MAN IN THE MIDDLE E CERTIFICATI SSL
Pericolosi attacchi sono quelli detti "man in the middle".
Con questi attacchi, il malintenzionato fa credere a due utenti/due client/due server che stanno dialogando tramite una connessione privata, quando invece l'intera conversazione è controllato da lui stesso.
Con TOR, l'Exit Relays può agire come man in the middle.
Anche in questo caso, per proteggersi da tali attacchi si dovrebbe utilizzare la crittografia "end-to-end" verificando anche l'autenticità del server.
Di solito, questo viene avviene automaticamente attraverso i certificati SSL.
Se si riceve un messaggio di eccezione di protezione come questo di sotto, si potrebbe essere vittima di un attacco man

in the middle.
Messaggio che non andrebbe ignorato, a meno che non si disponga di un altro modo affidabile di verifica dei certificati del sito web.

Ad esempio, nel 2011, Comodo, una delle principali società di certificati SSL, ha riferito che un account utente con autorità di registrazione (della filiale) era stato compromesso.
E' stato poi utilizzato per creare un nuovo account utente che ha emesso le richieste di firma per 9 certificati (7 domini): mail.google.com, login.live.com, www.google.com, login.yahoo.com (3 certificati), skype.com, addons.mozilla.org.
Poi, nel 2011, anche DigiNotar, una società olandese di certificati SSL, si vide alcuni certificati compromessi mesi prima (se non 2 anni prima).
Questo lascia ancora aperta la possibilità di un attacco man in the middle, anche quando il browser utilizza una connessione HTTPS.
Strumenti che forniscono una certa sicurezza di connessione sono Monkeysphere, Convergence e gli hidden services di TOR.
Da un lato, prevedendo l'anonimato, TOR rende più difficile eseguire un attacco di tipo man in the middle destinato ad una persona specifica.
Ma paradossalmente questo tipo di attacchi sono resi possibili utilizzando i già citati exit relays, tramite attacchi mirati ad un server specifico.
Proprio per questi motivi crittografare i messaggi è molto importante (GPG, Kgpg e Mozilla Thunderbird con TorBirdy ed Enigmail con un GPG add-on).

PERSISTENT TOR ENTRY GUARD RELAYS
TOR non può proteggerci contro la correlazione end-to-end (riferita al traffico), in cui un aggressore cerca di monitorare il vostro traffico (in altre parole i Persistent

TOR Entry Guard Relays possono rendervi tracciabili).
Persistent TOR Entry Guard è usato per motivi di sicurezza da TOR, Whonix, TOR Browser (TBB) ma in alcune situazioni è più sicuro non usare il Guard Relay.
Infatti il Guard Relay raccolto dal vostro client TOR può rendere il vostro TOR attaccabile per via del fingerprint (impronte) in diversi punti di accesso, deanonimizzando la vostra connessione.
Se utilizzo TOR da casa lascio appunto un'impronta (state file), lo stesso succede utilizzandolo da un altro luogo.
Il client utilizzando la stessa Entry Guard (anche se da un'altra posizione "fisica", cioè da un altro luogo) dà la sicurezza che i messaggi provengono dalla stessa persona che era collegata a quello specifico Guard Relay da casa (e poi in un dato luogo al di fuori di essa).
Questa tecnica è simile al tracciamento degli utenti tramite gli indirizzi MAC.

Detto in parole povere il problema è il file "state" dove sono inseriti in sequenza una serie di "Guard" usati per inviare e ricevere dati da TOR. Il primo è quello da cui ci si collega normalmente, poi ce ne sono altri predisposti per altre funzioni. Ogni "state" file ha una sequenza univoca e quindi è automaticamente tracciabile, anche utilizzando una VPN, modificando l'IP o utilizzando Whonix. Cioè ci si collega a TOR utilizzando gli stessi percorsi. Pur usando distinte identità, esse sarebbero comunque collegate al medesimo soggetto grazie allo state file.

CANCELLARE LO STATE FILE Questo problema viene risolto cancellando di tanto in tanto lo state file o utilizzando Tails (che per ogni riavvio genera uno state file diverso, rendendo impossibile il tracciamento). Per cancellare lo state file, andare nella cartella TOR Browser (con TOR non avviato), poi schiacciare su Data, TOR e poi eliminate il file "State". Fatto ciò, potete avviare TOR e navigare.