Osservatorio Nessuno

Spyware in the wild

Nexa Lunch Seminar

Cosa è uno spyware?

Cosa è uno spyware?

- Gli spyware sono software progettati per raccogliere informazioni da un dispositivo senza il consenso dell'utente.

Cosa è uno spyware?

- Gli spyware sono software progettati per raccogliere informazioni da un dispositivo senza il consenso dell'utente.
- Possono essere installati tramite vulnerabilità o tramite azioni inconsapevoli dell'utente.

Cosa è uno spyware?

- Gli spyware sono software progettati per raccogliere informazioni da un dispositivo senza il consenso dell'utente.
- Possono essere installati tramite vulnerabilità o tramite azioni inconsapevoli dell'utente.
- Permettono l'accesso a tutti i dati del dispositivo: chat, chiamate, posizione, file, videocamera, microfono, ecc.

Cosa è uno spyware?

- Gli spyware sono software progettati per raccogliere informazioni da un dispositivo senza il consenso dell'utente.
- Possono essere installati tramite vulnerabilità o tramite azioni inconsapevoli dell'utente.
- Permettono l'accesso a tutti i dati del dispositivo: chat, chiamate, posizione, file, videocamera, microfono, ecc.
- Operano in modo silenzioso e persistente.

Tipi di spyware

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)
- Spyware di Stato (NoviSpy - Serbia)

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)
- Spyware di Stato (NoviSpy - Serbia)
- Stalkerware

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)
- Spyware di Stato (NoviSpy - Serbia)
- Stalkerware
- Controllo parentale e monitoraggio dipendenti

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)
- Spyware di Stato (NoviSpy - Serbia)
- Stalkerware
- Controllo parentale e monitoraggio dipendenti
- Keyloggers

Tipi di spyware

- "Commercial spyware" (Pegasus - NSO Group, Predator - Intellexa, Dante - MementoLabs, Hermit - RCS, Graphite - Paragon Solutions, Spyrtacus - SIO)
- Spyware di Stato (NoviSpy - Serbia)
- Stalkerware
- Controllo parentale e monitoraggio dipendenti
- Keyloggers
- Infostealers

Rispetto ai metodi tradizionali...

Rispetto ai metodi tradizionali...

- Poche/nessuna garanzia giuridica e trasparenza sul loro uso*.

Rispetto ai metodi tradizionali...

- Poche/nessuna garanzia giuridica e trasparenza sul loro uso*.
- Nessuna limitazione di tempo, accede anche a dati passati.

Rispetto ai metodi tradizionali...

- Poche/nessuna garanzia giuridica e trasparenza sul loro uso*.
- Nessuna limitazione di tempo, accede anche a dati passati.
- Nessuna limitazione di categoria di dati, accedere anche a dati super sensibili, o di altri utenti.

Rispetto ai metodi tradizionali...

- Poche/nessuna garanzia giuridica e trasparenza sul loro uso*.
- Nessuna limitazione di tempo, accede anche a dati passati.
- Nessuna limitazione di categoria di dati, accedere anche a dati super sensibili, o di altri utenti.
- Nessuna limitazione di soggetto, accede a chiunque ha contatti con quella persona.

Rispetto ai metodi tradizionali...

- Poche/nessuna garanzia giuridica e trasparenza sul loro uso*.
- Nessuna limitazione di tempo, accede anche a dati passati.
- Nessuna limitazione di categoria di dati, accedere anche a dati super sensibili, o di altri utenti.
- Nessuna limitazione di soggetto, accede a chiunque ha contatti con quella persona.
- L'installazione compromette il dispositivo alterandone l'integrità, per cui le prove ottenute non sono utilizzabili in tribunale.

Vulnerabilità ed Expoits

La maggior parte degli spyware sfruttano vulnerabilità di sicurezza nei sistemi operativi o nelle app mobili. Il componente che sfrutta la vulnerabilità viene chiamato exploit.

Vulnerabilità ed Expoits

La maggior parte degli spyware sfruttano vulnerabilità di sicurezza nei sistemi operativi o nelle app mobili. Il componente che sfrutta la vulnerabilità viene chiamato exploit.

- 0-click: non richiede alcuna interazione da parte della vittima.

Vulnerabilità ed Expoits

La maggior parte degli spyware sfruttano vulnerabilità di sicurezza nei sistemi operativi o nelle app mobili. Il componente che sfrutta la vulnerabilità viene chiamato exploit.

- 0-click: non richiede alcuna interazione da parte della vittima.
- 1-click: necessita di un'azione minima come l'apertura di un link o di un file

Vulnerabilità ed Expoits

La maggior parte degli spyware sfruttano vulnerabilità di sicurezza nei sistemi operativi o nelle app mobili. Il componente che sfrutta la vulnerabilità viene chiamato exploit.

- 0-click: non richiede alcuna interazione da parte della vittima.
- 1-click: necessita di un'azione minima come l'apertura di un link o di un file

L'intera catena può includere più exploit combinati (exploit chain).

Ciclo di vita degli spyware

Ciclo di vita degli spyware

- Gli spyware necessitano di vulnerabilità per funzionare.

Ciclo di vita degli spyware

- Gli spyware necessitano di vulnerabilità per funzionare.
- Stati e aziende produttrici di Spyware non hanno interesse a rendere il software sicuro.

Ciclo di vita degli spyware

- Gli spyware necessitano di vulnerabilità per funzionare.
- Stati e aziende produttrici di Spyware non hanno interesse a rendere il software sicuro.
- Cosa succede se malintenzionati ottengono/scoprono le vulnerabilità? (EquationGroup vs ShadowBroker!)

Ciclo di vita degli spyware

- Gli spyware necessitano di vulnerabilità per funzionare.
- Stati e aziende produttrici di Spyware non hanno interesse a rendere il software sicuro.
- Cosa succede se malintenzionati ottengono/scoprono le vulnerabilità? (EquationGroup vs ShadowBroker!)

Meno sicurezza per tutti :(

Mercato: Dimensione e Numeri

Mercato: Dimensione e Numeri

- Il mercato degli exploit vale diversi miliardi di dollari.

Mercato: Dimensione e Numeri

- Il mercato degli exploit vale diversi miliardi di dollari.
- Centinaia di aziende operanti in diversi stati. Le principali nelle 3I: Italia, India, Israele.

Mercato: Dimensione e Numeri

- Il mercato degli exploit vale diversi miliardi di dollari.
- Centinaia di aziende operanti in diversi stati. Le principali nelle 3I: Italia, India, Israele.
- Secondo rapporti di Citizen Lab e Amnesty Tech, spyware commerciali sono stati utilizzati in oltre 60 paesi.

Mercato: Dimensione e Numeri

- Il mercato degli exploit vale diversi miliardi di dollari.
- Centinaia di aziende operanti in diversi stati. Le principali nelle 3I: Italia, India, Israele.
- Secondo rapporti di Citizen Lab e Amnesty Tech, spyware commerciali sono stati utilizzati in oltre 60 paesi.
- Continue violazioni dei diritti umani per un uso indiscriminato, **Caso Paragon in Italia**.

Mercato: Dimensione e Numeri

- Il mercato degli exploit vale diversi miliardi di dollari.
- Centinaia di aziende operanti in diversi stati. Le principali nelle 3I: Italia, India, Israele.
- Secondo rapporti di Citizen Lab e Amnesty Tech, spyware commerciali sono stati utilizzati in oltre 60 paesi.
- Continue violazioni dei diritti umani per un uso indiscriminato, **Caso Paragon in Italia**.
- Migliaia di vulnerabilità in software che usiamo tutti i giorni.

Come proteggersi?

MVT

MVT

- Tool open source sviluppato da **Amnesty Tech**.

MVT

- Tool open source sviluppato da **Amnesty Tech**.
- Analizza dispositivi iOS e Android alla ricerca di **indicatori di compromissione (IoC)**.

MVT

- Tool open source sviluppato da **Amnesty Tech**.
- Analizza dispositivi iOS e Android alla ricerca di **indicatori di compromissione (IoC)**.
- Verifica la presenza di Spyware conosciuti e pubblici.

MVT

- Tool open source sviluppato da **Amnesty Tech**.
- Analizza dispositivi iOS e Android alla ricerca di **indicatori di compromissione (IoC)**.
- Verifica la presenza di Spyware conosciuti e pubblici.
- Necessita di un PC alla quale connetter il device.

MVT

- Tool open source sviluppato da **Amnesty Tech**.
- Analizza dispositivi iOS e Android alla ricerca di **indicatori di compromissione (IoC)**.
- Verifica la presenza di Spyware conosciuti e pubblici.
- Necessita di un PC alla quale connetter il device.
- Usa ADB su Android e i backup su iOS.

MVT

- Tool open source sviluppato da **Amnesty Tech**.
- Analizza dispositivi iOS e Android alla ricerca di **indicatori di compromissione (IoC)**.
- Verifica la presenza di Spyware conosciuti e pubblici.
- Necessita di un PC alla quale connetter il device.
- Usa ADB su Android e i backup su iOS.
- Pensato per tecnici, difficile da utilizzare e poco user-friendly.

BugBane

- Abbiamo deciso di sviluppare **Bugbane**!

BugBane

- Abbiamo deciso di sviluppare **Bugbane**!
- Applicazione Android per verificare la presenza di spyware.

BugBane

- Abbiamo deciso di sviluppare **Bugbane**!
- Applicazione Android per verificare la presenza di spyware.
- Porting dell'engine MVT su Android.

BugBane

- Abbiamo deciso di sviluppare **Bugbane**!
- Applicazione Android per verificare la presenza di spyware.
- Porting dell'engine MVT su Android.
- Usa **ADB Wireless Debugging**.

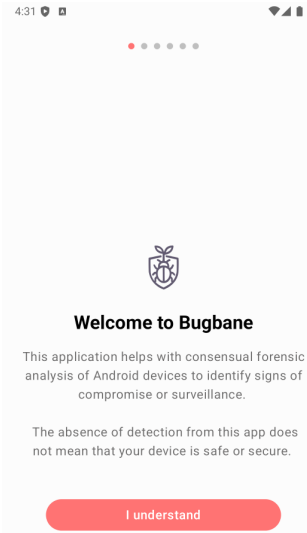
BugBane

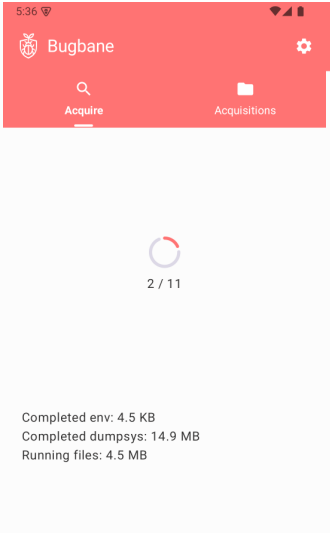
- Abbiamo deciso di sviluppare **Bugbane**!
- Applicazione Android per verificare la presenza di spyware.
- Porting dell'engine MVT su Android.
- Usa **ADB Wireless Debugging**.
- Utilizzabile direttamente sul dispositivo da testare.

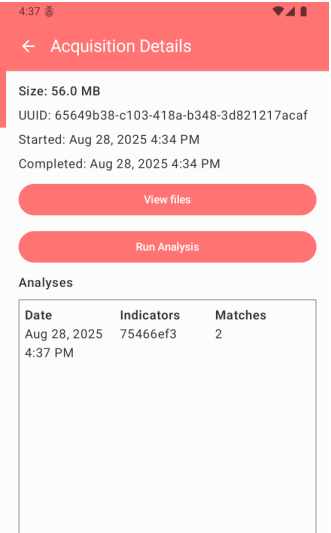
BugBane

- Abbiamo deciso di sviluppare **Bugbane**!
- Applicazione Android per verificare la presenza di spyware.
- Porting dell'engine MVT su Android.
- Usa **ADB Wireless Debugging**.
- Utilizzabile direttamente sul dispositivo da testare.
- Interfaccia moderna e facile da usare.

BugBane


4:31
Welcome to Bugbane
This application helps with consensual forensic analysis of Android devices to identify signs of compromise or surveillance.
The absence of detection from this app does not mean that your device is safe or secure.
I understand


5:36
Bugbane
Acquire
Acquisitions
2 / 11
Completed env: 4.5 KB
Completed dumpsys: 14.9 MB
Running files: 4.5 MB


4:37
Acquisition Details
Size: 56.0 MB
UUID: 65649b38-c103-418a-b348-3d821217acaf
Started: Aug 28, 2025 4:34 PM
Completed: Aug 28, 2025 4:34 PM
View files
Run Analysis
Analyses
Date
Indicators
Matches
Aug 28, 2025 4:37 PM
75466ef3
2

Quindi?

Nel suo report 2025, **EDRi (European Digital Right)** ha chiesto al Parlamento Europeo:

Quindi?

Nel suo report 2025, **EDRi (European Digital Right)** ha chiesto al Parlamento Europeo:

`il divieto totale dello sviluppo, della produzione, della commercializzazione, della vendita, dell'esportazione e dell'uso degli spyware, come unica soluzione accettabile e conforme ai diritti umani.`

Quindi?

Nel suo report 2025, **EDRi (European Digital Right)** ha chiesto al Parlamento Europeo:

`il divieto totale dello sviluppo, della produzione, della commercializzazione, della vendita, dell'esportazione e dell'uso degli spyware, come unica soluzione accettabile e conforme ai diritti umani.`

- Stop alla proliferazione di vulnerabilità ed exploit.

Quindi?

Nel suo report 2025, **EDRi (European Digital Right)** ha chiesto al Parlamento Europeo:

`il divieto totale dello sviluppo, della produzione, della commercializzazione, della vendita, dell'esportazione e dell'uso degli spyware, come unica soluzione accettabile e conforme ai diritti umani.`

- Stop alla proliferazione di vulnerabilità ed exploit.
- Più strumenti di analisi e di verifica delle infezioni.

Altri progetti in cantiere...

Non solo Bugbane

Non solo Bugbane

- Recentemente abbiamo fornito supporto tecnico a giornalisti ed attivisti in Italia. Abbiamo confermato la compromissione e inequivocabili segni di utilizzo degli strumenti dell'azienda Israeliana. Ci siamo coordinati con organizzazioni internazionali e stiamo assistendo nell'analisi tecnica approfondita. I risultati di questa analisi sono stati pubblicati in una serie di articoli.

Non solo Bugbane

- Recentemente abbiamo fornito supporto tecnico a giornalisti ed attivisti in Italia. Abbiamo confermato la compromissione e inequivocabili segni di utilizzo degli strumenti dell'azienda Israeliana. Ci siamo coordinati con organizzazioni internazionali e stiamo assistendo nell'analisi tecnica approfondita. I risultati di questa analisi sono stati pubblicati in una serie di articoli.
- Dal 2021 abbiamo creato l'associazione **Osservatorio Nessuno** per gestire **Exit-Node Tor** in Italia.

Non solo Bugbane

- Recentemente abbiamo fornito supporto tecnico a giornalisti ed attivisti in Italia. Abbiamo confermato la compromissione e inequivocabili segni di utilizzo degli strumenti dell'azienda Israeliana. Ci siamo coordinati con organizzazioni internazionali e stiamo assistendo nell'analisi tecnica approfondita. I risultati di questa analisi sono stati pubblicati in una serie di articoli.
- Dal 2021 abbiamo creato l'associazione **Osservatorio Nessuno** per gestire **Exit-Node Tor** in Italia.
- Abbiamo **comprato una cantina** a Torino, una nostra **subnet ipv4** e facciamo **BGP** dalla cantina.

Non solo Bugbane

- Recentemente abbiamo fornito supporto tecnico a giornalisti ed attivisti in Italia. Abbiamo confermato la compromissione e inequivocabili segni di utilizzo degli strumenti dell'azienda Israeliana. Ci siamo coordinati con organizzazioni internazionali e stiamo assistendo nell'analisi tecnica approfondita. I risultati di questa analisi sono stati pubblicati in una serie di articoli.
- Dal 2021 abbiamo creato l'associazione **Osservatorio Nessuno** per gestire **Exit-Node Tor** in Italia.
- Abbiamo **comprato una cantina** a Torino, una nostra **subnet ipv4** e facciamo **BGP** dalla cantina.
- Durante questo percorso abbiamo implementato un flusso per gestire i nostri server **disk-less** utilizzando **TPM** e progetti open source.

Non solo Bugbane

- Recentemente abbiamo fornito supporto tecnico a giornalisti ed attivisti in Italia. Abbiamo confermato la compromissione e inequivocabili segni di utilizzo degli strumenti dell'azienda Israeliana. Ci siamo coordinati con organizzazioni internazionali e stiamo assistendo nell'analisi tecnica approfondita. I risultati di questa analisi sono stati pubblicati in una serie di articoli.
- Dal 2021 abbiamo creato l'associazione **Osservatorio Nessuno** per gestire **Exit-Node Tor** in Italia.
- Abbiamo **comprato una cantina** a Torino, una nostra **subnet ipv4** e facciamo **BGP** dalla cantina.
- Durante questo percorso abbiamo implementato un flusso per gestire i nostri server **disk-less** utilizzando **TPM** e progetti open source.
- E poi abbiamo sgravato...

Procio.Network

- **Reti riconfigurabili e programmabili**: Ogni CPE e router potrà ospitare interfacce virtuali per testare protocolli alternativi, come modelli di rete peer-to-peer e cifrati, in modo parallelo (test e produzione).

Procio.Network

- **Reti riconfigurabili e programmabili**: Ogni CPE e router potrà ospitare interfacce virtuali per testare protocolli alternativi, come modelli di rete peer-to-peer e cifrati, in modo parallelo (test e produzione).
- **Hardware e software di rete aperti**: costruire uno stack il più possibile aperto, verificabile e riproducibile, dimostrando che soluzioni trasparenti e documentate possono sostituire apparati proprietari a costi nettamente inferiori e con maggiore flessibilità per la ricerca.

Procio.Network

- **Reti riconfigurabili e programmabili**: Ogni CPE e router potrà ospitare interfacce virtuali per testare protocolli alternativi, come modelli di rete peer-to-peer e cifrati, in modo parallelo (test e produzione).
- **Hardware e software di rete aperti**: costruire uno stack il più possibile aperto, verificabile e riproducibile, dimostrando che soluzioni trasparenti e documentate possono sostituire apparati proprietari a costi nettamente inferiori e con maggiore flessibilità per la ricerca.
- **Remote attestation e trasparenza**: ricerca e sviluppo su meccanismi di remote attestation, supply chain transparency e reproducible builds.

Procio.Network

- **Crittografia moderna e privacy**: sperimentazione di applicazioni di crittografia moderna. Tra gli esempi, l'uso di Private Information Retrieval (PIR) per verificare la reputazione di domini o indirizzi IP senza rivelare le richieste degli utenti.

- **Crittografia moderna e privacy**: sperimentazione di applicazioni di crittografia moderna. Tra gli esempi, l'uso di Private Information Retrieval (PIR) per verificare la reputazione di domini o indirizzi IP senza rivelare le richieste degli utenti.
- **Infrastruttura come esperimento sociale**: il progetto è anche un laboratorio sociotecnico, volto a studiare come la gestione comunitaria dell'infrastruttura possa ridefinire la percezione della rete come bene comune.

Procio.Network

- **Crittografia moderna e privacy**: sperimentazione di applicazioni di crittografia moderna. Tra gli esempi, l'uso di Private Information Retrieval (PIR) per verificare la reputazione di domini o indirizzi IP senza rivelare le richieste degli utenti.
- **Infrastruttura come esperimento sociale**: il progetto è anche un laboratorio sociotecnico, volto a studiare come la gestione comunitaria dell'infrastruttura possa ridefinire la percezione della rete come bene comune.
- **Divertirci un casino!**

E ora la polemica...

E ora la polemica...

- Quasi tutti i nostri progetti sarebbero dovuti nascere all'interno dello spazio collettivo della scuola, universita' e ricerca. Oggi la maggior parte degli atenei sono apertamente ostili ed inospitali oltre che cronicamente sottofinanziati.

E ora la polemica...

- Quasi tutti i nostri progetti sarebbero dovuti nascere all'interno dello spazio collettivo della scuola, universita' e ricerca. Oggi la maggior parte degli atenei sono apertamente ostili ed inospitali oltre che cronicamente sottofinanziati.
- Negli ultimi 20 anni e' nato un ecosistema di ONG per i diritti digitali che adesso sono state pesantemente stroncate da Trump. Abbiamo fatto finta di non sapere che le fondamenta dell'ecosistema opensource/libero e' estremamente polarizzato.

E ora la polemica...

- Quasi tutti i nostri progetti sarebbero dovuti nascere all'interno dello spazio collettivo della scuola, universita' e ricerca. Oggi la maggior parte degli atenei sono apertamente ostili ed inospitali oltre che cronicamente sottofinanziati.
- Negli ultimi 20 anni e' nato un ecosistema di ONG per i diritti digitali che adesso sono state pesantemente stroncate da Trump. Abbiamo fatto finta di non sapere che le fondamenta dell'ecosistema opensource/libero e' estremamente polarizzato.
- Le istituzioni "aperte" della rete (RIPE/IETF/W3C/ICANN) sono diventati luoghi ricchi ed escludenti che agiscono sistematicamente per gli interessi politici ed economici di pochi.

E ora la polemica...

- Quasi tutti i nostri progetti sarebbero dovuti nascere all'interno dello spazio collettivo della scuola, universita' e ricerca. Oggi la maggior parte degli atenei sono apertamente ostili ed inospitali oltre che cronicamente sottofinanziati.
- Negli ultimi 20 anni e' nato un ecosistema di ONG per i diritti digitali che adesso sono state pesantemente stroncate da Trump. Abbiamo fatto finta di non sapere che le fondamenta dell'ecosistema opensource/libero e' estremamente polarizzato.
- Le istituzioni "aperte" della rete (RIPE/IETF/W3C/ICANN) sono diventati luoghi ricchi ed escludenti che agiscono sistematicamente per gli interessi politici ed economici di pochi.
- FSF, EFF, CCC, etc stanno vivendo una crisi di identita' e paralisi di fronte ad un mondo in evidente mutamento. Dov'eravamo quando sono arrivati Chat Control, Piracy Shield, etc?

E ora la polemica...

- Quasi tutti i nostri progetti sarebbero dovuti nascere all'interno dello spazio collettivo della scuola, universita' e ricerca. Oggi la maggior parte degli atenei sono apertamente ostili ed inospitali oltre che cronicamente sottofinanziati.
- Negli ultimi 20 anni e' nato un ecosistema di ONG per i diritti digitali che adesso sono state pesantemente stroncate da Trump. Abbiamo fatto finta di non sapere che le fondamenta dell'ecosistema opensource/libero e' estremamente polarizzato.
- Le istituzioni "aperte" della rete (RIPE/IETF/W3C/ICANN) sono diventati luoghi ricchi ed escludenti che agiscono sistematicamente per gli interessi politici ed economici di pochi.
- FSF, EFF, CCC, etc stanno vivendo una crisi di identita' e paralisi di fronte ad un mondo in evidente mutamento. Dov'eravamo quando sono arrivati Chat Control, Piracy Shield, etc?
- Forse abbiamo creduto in un idea, quella della privacy, che si e' rivelata essere l'idea **SBAGLIATA**.

Supporto

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)
- Contribuire al codice dei nostri progetti

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)
- Contribuire al codice dei nostri progetti
- Contribuire al **Tor Project** o progetti simili, c'e' molto spazio per la ricerca... **GSoC**

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)
- Contribuire al codice dei nostri progetti
- Contribuire al **Tor Project** o progetti simili, c'e' molto spazio per la ricerca... **GSoC**
- Mantenere un pezzo dell'infrastruttura: bridge, snowflake, relay intermedi possono essere ospitati in una rete di casa senza conseguenze legali

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)
- Contribuire al codice dei nostri progetti
- Contribuire al **Tor Project** o progetti simili, c'e' molto spazio per la ricerca... **GSoC**
- Mantenere un pezzo dell'infrastruttura: bridge, snowflake, relay intermedi possono essere ospitati in una rete di casa senza conseguenze legali
- Buoni avvocati. O anche non buonissimi, ma che lavorano gratis

Supporto

- **5x1000** o donazioni (accettiamo anche hardware buono!)
- Contribuire al codice dei nostri progetti
- Contribuire al **Tor Project** o progetti simili, c'e' molto spazio per la ricerca... **GSoC**
- Mantenere un pezzo dell'infrastruttura: bridge, snowflake, relay intermedi possono essere ospitati in una rete di casa senza conseguenze legali
- Buoni avvocati. O anche non buonissimi, ma che lavorano gratis
- Attivate una linea di procio.network!

The End

Contatti

- **osservatorionessuno.org**
- **bsky.app/profile/osservatorionessuno.org**
- **mastodon.cisti.org/@0n_odv**
- **github.com/osservatorionessuno**
- **procio.network** (coming soon...)
- **radioblackout.org/shows/stakka-stakka**: ogni due martedì **H18.30**