LETTERA ACCOMPAGNATORIA DISCIPLINARE TECNICO

Premessa

Il presente documento espone i principi ai quali si devono conformare gli strumenti e le procedure d'uso di strumenti informatici a fini investigativi, chiamati nel documento "captatori" o "captatori informatici".

L'obiettivo è assicurare l'aderenza ai principi costituzionali degli strumenti e dei procedimenti che ne fanno uso, in continuità per quanto possibile con la prassi e con le buone pratiche già in atto nella dimensione non digitale. Definiamo:

- **captatori** gli strumenti che, implementando anche criteri di *privacy by design*, assicurino il rispetto di detti principi
- **trojan** gli strumenti di uso generico che sfruttano vettori infettivi e che non assicurano il rispetto di diritti costituzionali.

Principi

Il primo principio è che si deve assicurare che ogni funzione di un captatore possa essere effettivamente mappata ad una corrispondente azione di polizia giudiziaria. Le funzioni attivate di un captatore devono poter essere disciplinate applicando l'equivalente legge che già decreta le azioni di polizia giudiziaria tradizionale. Ad esempio un'intercettazione telematica può essere, a tutti gli effetti, paragonata ad una intercettazione telematica effettuata tramite apposito apparato e, come tale, deve fornire le stesse identiche garanzie. Lo stesso dicasi, ad esempio, per funzioni meno invasive, come per esempio i dati di posizionamento forniti da programma elettronico che dovrebbero essere equivalenti ad una operazione di pedinamento, ecc..

Il secondo principio è quello per il quale un software captatore che contenga codice in grado di fornire all'autorità giudiziaria dati sensibili e personali sui cittadini debba, necessariamente, essere verificato a priori e verificabile a posteriori in ogni sua funzione.

Il cittadino deve essere messo nelle condizioni di esercitare (ma non abusare di) il proprio diritto di difesa e avere conferma di quanto operato dal captatore in questione e che i dati rilevati non possano in alcun modo essere stati né inoculati né modificati ad hoc da parte sia del captatore stesso sia da parte di terzi sfruttando il captatore.

il terzo principio è assicurare la integrità del procedimento utilizzato mediante la tracciabilità e verificabilità delle azioni compiute dagli operatori, della adeguatezza degli operatori stessi ed il rispetto del previsto iter autorizzativo e dispositivo.

Il quarto principio è quello della rintracciabilità. Si rende necessario creare un registro che permetta di tracciare tutte le istanze di captatore che siano state utilizzate legalmente. In questo modo sarà possibile sia evitare che più autorità giudiziarie tentino di sorvegliare i medesimi obiettivi sia verificare le autorizzazioni concesse per ogni singolo captatore e se le stesse sono state rispettate.

Il quinto principio è che l'installazione di un software a fini investigativi in un sistema elettronico non debba, in nessun modo abbassare il livello di sicurezza del sistema in cui è stato installato, rischiando che il sistema possa poi essere compromesso da altre parti in causa vanificando, di fatto, anche tutta l'attività investigativa effettuata.

DISCIPLINARE TECNICO CAPTATORE INFORMATICO

Questa la bozza proposta di disciplinare tecnico relativo alla proposta di legga, da impiegare come base per la regolamentazione ministeriale.

Requisiti Tecnici

Sono in seguito evidenziati i principali requisiti tecnici/funzionali del captatore informatico.

1. Il captatore deve disporre delle seguenti funzioni base (obbligatorie):
1. Il sistema fornito deve essere fornito di, minimo, tre moduli:
1. **Un sistema di gestione**: tramite tale sistema sarà possibile creare nuovi captatori, gestire i captatori già creati e target inviati agli obiettivi, gestire in automatico tutte le comunicazioni all'ente preposto alla conservazione del registro dei captatori, gestire le chiavi crittografiche di comunicazione, verificare che un captatore disponga delle sole funzioni autorizzate, verificare un binario già istanziato, creare il supporto per il deposito del captatore creato nel fascicolo di indagine.
1. **Un modulo captatore**: Il modulo captatore è la componente software che, posizionata nei dispositivi informatici degli obiettivi autorizzati, opera l'acquisizione delle informazioni. Il modulo captatore può essere disponibile per varie piattaforme software eterogenee fra loro, ma deve mantenere senza eccezione alcuna l'aderenza ai requisiti tecnici definiti nel presente documento.
1. **Un sistema di comunicazione**: Il sistema potrà disporre sia di un proprio sistema di raccolta dei dati catturati dal modulo captatore, in tal caso dovrà fornire tutte le garanzie necessarie per tracciare gli accessi ai dati e verificare la loro inalterabilità, o può appoggiarsi ad un sistema terzo di monitoring center certificato.
1. **Un sistema di inoculazione**: Il sistema di inoculazione, avente lo scopo di installare il captatore sui dispositivi dell'obbiettivo autorizzato, deve essere estensivamente documentato per indicare il suo funzionamento in modalità attiva o passiva, definendo con precisione tutti i passaggi da questo effettuati per la sua operatività. Il sistema di inoculazione deve, al pari degli altri moduli, fornire un log di tutta la sua operatività, con particolare dettaglio per qualunque azione che vada a modificare, creare o cancellare informazioni sul dispositivo dell'obbiettivo autorizzato.
1. **Un sistema di registrazione**: Tutte le operazioni effettuate sul sistema di gestione, dai captatori installati e dagli utenti che accedono ai dati devono essere registrate e salvate in maniera inalterabile da parte di chiunque, sia utilizzatori sia software house che abbiano sviluppato il software. Al fine di fornire tutte le necessarie garanzie, si richiede che siano usati firme digitali e meccanismi di timestamping crittografico, e che il log contenga tutti i passi compiuti per istanziare il captatore, le autorizzazioni fornite, gli identificativi degli utenti autorizzati ad operare nonché tutte le operazioni effettuate da questi attraverso il centro di controllo.
1. **Un sistema di controllo dei log**: Il sistema di controllo dei log deve essere disponibile come modulo software separato dalla piattaforma, accessibile liberamente e pubblicamente senza autorizzazione alcuna, distribuito dal sito internet del produttore del software. Il sistema di controllo dei log, software e relativa documentazione d'uso, deve consentire la validazione dell'integrità dei log di operatività di un captatore oltre ad

esportare in un formato intelligibile tutte le operatività del captatore. I codici sorgenti e le relative istruzioni di trasformazione in codice binario utilizzabile su un computer, devono essere anch'esse pubblicate sul sito del produttore.

1. Il sistema deve rispettare, in tutte le sue componenti, i requisiti minimi definiti dallo standard ISO/IEC IS-15408 (Common Criteria) EAL2

Requisiti di Certificazione

Il processo di certificazione si rende necessario per verificare che tutti i captatori utilizzati all'interno del territorio italiano siano aderenti alle norme di legge e rispondano ai requisiti e ai principi richiesti.

Il processo di certificazione richiede, nel dettaglio:

1. Il sistema dovrà garantire, per tutte le componenti software, la possibilità di riprodurre una copia esatta dei codici binari a partire da una specifica versione/edizione dei codici sorgenti attraverso metodiche di "build riproducibili", già impiegate per la garanzia del software nell'ambito dei sistemi di gestione di lotterie e giochi a premi

1. Il sistema dovrà dichiarare tutte le funzioni messe a disposizione dal captatore all'Autorità Giudiziaria

1. Il sistema dovrà disporre di un metodo che permetta di identificare, in maniera univoca, gli agenti di polizia giudiziaria autorizzati sia ad amministrarlo sia ad operare sui captatori. Il sistema deve inoltre registrare ogni accesso effettuato per la manutenzione dello stesso da parte della software house che lo ha creato e di chi ha autorizzato tale accesso

Il produttore dovrà:

1. effettuare il processo di certificazione almeno 1 volta l'anno

1. depositare i codici sorgenti almeno 1 volta ogni 6 mesi, includendo tutte le versioni rilasciate
1. *Le modalità di esecuzione della verifica del processo di certificazione dovranno garantire la tutela della riservatezza delle metodiche funzionali e dei segreti industriali. In considerazione delle specifiche esigenze di tutela di segreti industriali, tipicamente inferiori al 2% dell'intera base di codice sorgente, il produttore potrà indicare quali porzioni di codici siano da assoggettare ad ulteriori forme di tutela, che comunque non si*

applicheranno nei confronti dell'ente certificatore, ma esclusivamente nei riguardi delle parti che in modo indipendente volessero ripetere il processo di certificazione.

1. comunicare tempestivamente ogni singola versione software rilasciata, e i relativi elementi di identificazione univoci

1. comunicare all'ente preposto gli identificativi univoci e i relativi dati anagrafici degli utilizzatori di tutti centri di controllo attivati su base trimestrale

1. fornire tutta la documentazione, le automazioni, gli strumenti necessari ad effettuare il processo di certificazione, ovvero ad analizzare il rispetto dei requisiti tecnici e funzionali obbligatori

Enti di certificazione

L'ente preposto alla esecuzione della certificazione per l'Italia è l'Isticom (Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione) e del suo specifico Centro di Valutazione (CE.VA.) abilitato a condurre valutazione secondo lo "Schema Nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione, ai fini della tutela delle informazioni classificate, concernenti la sicurezza interna ed esterna dello Stato" www.isticom.it/index.php/ceva .

Custodia Codici Sorgenti

Al fine di garantire una separazione dei compiti e di una maggior riservatezza dei segreti industriali si consideri l'opportunità di consentire il deposito dei codici sorgenti, della documentazione completa e di tutte le informazioni necessarie ad effettuare un processo di certificazione presso soggetto terzo indicato dal produttore a scelta fra uno dei soggetti abilitati/accreditati dall'ente certificatore (es: TUV Italia).

Registro dei captatori

Il registro dei captatori e di tutte le loro versioni rilasciate dai produttori e istanziate dagli operatori di giustizia e installate sui dispositivi obiettivo d'indagine sarà detenuto e manutenuto dall'ente di certificazione che lo metterà a disposizione delle forze di pubblica sicurezza, dei servizi di informazione e alle parti che si trovassero oggetto di impiego di un captatore informatico.

L'esigenza di mantenere l'impronta anche dei captatori installati è dovuta in considerazione del fatto che i captatori possano impiegare tecniche di polimorfismo o offuscamento per migliorare le proprie capacità di occultamento ai software anti-malware e antivirus, e che quindi la versione "instanziata" dal sistema di gestione sia un file diverso da quello "installato" sul sistema obiettivo.

Il gestore di tale registro vedrà la copertura dei costi relativi al mantenimento della infrastruttura informatica come quota percentuale dei costi esposti a produttori e alle parti nei processi di certificazione.

Le richieste di informazioni, possibili solo da parte degli avvocati difensori di indagati che sono stati oggetto di verifica tramite captatore, non avranno carattere di onerosità per i richiedenti e dovranno essere espletate entro 30 giorni dalla richiesta.

Processo di generazione, uso e gestione dei captatori

Nel caso si ravvisi l'impossibilità di operare tramite metodi tradizionali e si renda necessario l'utilizzo di un captatore informatico sarà necessario procedere con i seguenti passi:

1. L'amministratore del centro di controllo della Procura competente sulle indagini effettuerà un'operazione di "richiesta di captatore" per tramite della piattaforma di gestione. A tal fine sarà necessario fornire:
1. Numero del procedimento penale
1. Nome del magistrato competente
1. Elenco dei dispositivi per i quali viene richiesto il captatore, comprensivo di tuti i dati identificativo possibili e del tipo di architettura (es. Sistema operativo, tipo di hardware).

1. Il sistema di controllo provvederà a creare i documenti necessari per la raccolta delle dovute autorizzazioni, secondo il seguente quadro sinottico:

Funzione captatore informatico	**Equivalente indagine reale**
Intercettazione traffico voce	Intercettazione telefonica
Intercettazione telematica	Intercettazione telematica
Registrazione audio/video	Intercettazione ambientale
Registrazione e-mail	Intercettazione di corrispondenza
Dati di posizionamento	Pedinamento

Ricerca di file sul dispositivo	Perquisizione
Acquisizione di file sul dispositivo	Sequestro

1. Una volta che tutte le autorizzazioni saranno debitamente firmate l'autorizzazione inserirà le medesime all'interno del sistema di controllo.

1. Il sistema di controllo a questo punto provvederà a:
1. Verificare le autorizzazioni. In nessun caso sarà possibile istanziare un captatore con una funzione per la quale non ci sia una precisa autorizzazione. Nel caso il numero di autorizzazione immesse nel sistema sia un sottoinsieme di quelle per le quali era stata fatta la richiesta al punto 1, il sistema di controllo istanzierà uno o più captatori solo per le funzioni autorizzate.
1. Istanziare un captatore per ogni dispositivo di cui al punto 1.c. Ad ogni captatore sarà assegnato un ID univoco composto dall'ID del centro di controllo e da un numero progressivo.
1. Comunicherà in automatico al registro dei captatori gli ID di tutti i captatori istanziati e delle autorizzazioni fornite per le singole funzioni.
1. Salverà una copia di ogni captatore su un supporto non alterabile che sarà allegato al fascicolo.

Al fine di evitare che tali file possano essere oggetto di una fuoriuscita non autorizzata di informazioni a causa dei molteplici soggetti sostanzialmente abilitati all'accesso del fascicolo, è ammesso che questo sia salvato in forma crittografata. Le chiavi di accesso sono conservate presso il registro dei captatori e presso il sistema di gestione che lo ha generato e/o operato, accessibili secondo le modalità indicate nella sezione "**Verifica autonoma del captatore**"

Una volta installato il captatore nei dispositivi obiettivo, i dati potranno essere raccolti o tramite il centro di controllo o tramite terzo monitoring center certificato. In entrambi i casi si richiede che i sistemi salvino e conservino i dati con le dovute garanzie. Per ogni accesso il sistema provvederà a:

1. Riconoscere in maniera univoca l'Agente di P.G. operante
1. Registrare tutte le attività svolte sia direttamente effettuare da operatore autorizzato, sia effettuate autonomamente dal software in qualunque dei suoi sistemi e moduli in relazione a tale captatore.

Terminata l'indagine il sistema provvederà a:

1. Creare un supporto inalterabile con la copia dei log relativi a tutte operazioni svolte
1. Creare un supporto inalterabile con tutto il materiale rilevato ritenuto di interesse all'indagine

1. Effettuare una disinstallazione del captatore dai dispositivi ove sia stato installato. Nel caso in cui un dispositivo non possa consentire una disinstallazione, sarà necessario istanziare un programma ad hoc, da allegare al fascicolo, che permetta di effettuare una disinstallazione off-line ritardata
1. Aggiornare in automatico il registro dei captatori evidenziando quali siano stati disinstallati e quali possano essere ancora attivi
1. Chiudere l'indagine e quindi inibire la possibilità che eventuali captatori ancora sul campo, possano comunicare con il sistema di controllo o ricevere da esso ulteriori comandi.

Verifica del captatore

In questa sezione le diverse modalità con cui verificare il captatore e il suo operato.

Verifica del captatore presso centro di controllo

Una volta che la parte riceva accesso al fascicolo è suo diritto richiedere una verifica della regolarità del/i captatore/i utilizzati. A tal fine sarà data possibilità alla parte di visionare la verifica del captatore da parte del sistema di controllo.

Essa si svolgerà nel seguente modo:

1. L'amministratore effettuerà una login sul sistema di controllo
1. Sarà inserito nello stesso il supporto inalterabile precedentemente generato nella fase di creazione del captatore
1. Il sistema verificherà quindi che:
1. La copia del captatore sia identica a quella contenuta nei propri archivi
1. Che le funzioni inserite nel modulo captatore siano quelle effettivamente autorizzate
1. Che la comunicazione al registro dei captatori sia effettivamente stata effettuata
1. Che la comunicazione di cessazione di utilizzo sia effettivamente stata effettuata
1. Che i log depositati siano congrui con le copie negli archivi

In nessun caso la parte, o un suo consulente tecnico, potrà effettuare alcuna operazione sul sistema di controllo, tuttavia potrà osservare l'esecuzione in sequenza di tali operazioni e ottenere verbale di verifica.

Verifica autonoma del captatore

Al fine di garantire la più ampia possibilità di verifica indipendente, a partire dal captatore allegato al fascicolo, le parti hanno diritto di richiedere l'accesso in formato non crittografato al captatore nei suoi files sia instanziati che installati.

In considerazione della natura di riservatezza del captatore, la parte che volesse accedere ai file del captatore allegato al fascicolo in formato non crittografato, dovrà siglare un accordo di riservatezza con il produttore, assumendosi la responsabilità di non divulgare lo stesso.
Il produttore si impegna entro 20 giorni a siglature tale accordo di riservatezza con la parte richiedente, sulla base di un modello contrattuale standard allegato al processo di certificazione.
Il registro dei captatori e/o l'ente presso cui viene operato il sistema di controllo, previa esibizione dell'accordo di riservatezza siglato dalle parti con il produttore, fornirà la chiave crittografica di decifratura e le istruzioni tecniche-operative per ottenere l'accesso al captatore allegato al fascicolo.

Verifica dei log allegati al fascicolo

Una volta che la parte riceva accesso al fascicolo è suo diritto verificare in modo indipendente, attraverso gli strumenti messi a disposizione pubblicamente e gratuitamente dal produttore, che il log allegato al fascicolo:

- Rispetti i requisiti di integrità
- Sia completo, ovvero includa tutte le fasi di operatività del captatore, dalla generazione dell'istanza specifica, a tutte le azioni effettuate sino alla sua disinstallazione.

Tali passaggi devono poter essere eseguiti senza competenze tecniche specifiche, tuttavia qualunque operatività tecnica eseguita nella operazione di verifica deve essere registrata in un ulteriore log apposito, tale da consentire a uno specialista di validarne minuziosamente il funzionamento.

Verifica della validità del captatore

Una volta che la parte riceva accesso al fascicolo è suo diritto verificare in modo indipendente, attraverso richiesta effettuata al detentore e manutentore del registro dei captatori, che il captatore utilizzato:

- Sia un captatore certificato
- Quale sia la versione/edizione software comunicata dal produttore al registro dei captatori
- Quando la versione/edizione software è stata comunicata dal produttore al registro dei captatori
- Quale sia la procura che lo ha istanziato e quando tale operazione è stata fatta
- Quando l'istanza specifica è stata comunicata dalla procura al registro dei captatori

Verifica del processo di certificazione

Le parti potranno richiedere all'ente certificatore di verificare in modo indipendente il processo di certificazione per l'esatta versione e istanza utilizzata del captatore.
La verifica del processo di certificazione eseguita in modo indipendente comporterà per la parte richiedente i costi burocratici, operativi e strumentali necessari alla ripetizione del processo.

La verifica del processo di certificazione, dovrà consentire la riproduzione esatta dell'istanza del captatore in formato binario e tale istanza deve risultare identica a quella già depositata all'interno del fascicolo (cd. Reproducible Build).

E' necessario che l'intero processo di certificazione consenta di riprodurre le esatte condizioni necessarie a riprodurre sia la versione rilasciata dal produttore che la versione istanziata dalla procura che la versione installata sul/i dispositivo/i oggetto d'indagine allegati al fascicolo.

Il produttore dovrà fornire come prestazione obbligatoria remunerata, su richieste delle parti coinvolte in un caso che veda l'utilizzo di un captatore da questi certificato, la messa a disposizione di personale tecnico e/o documentazione atta a spiegare il funzionamento del sistema. La tariffa che il produttore potrà esporre non potrà essere superiore alla tariffa media praticata dai consulenti tecnici d'ufficio nei confronti delle procure, per consulenze inerenti il c.d computer forensics.

Nel caso la verifica del processo di certificazione dovesse fallire per motivi attribuibili al produttore e inquadrabili nelle fattispecie di dolo, colpa grave o negligenza:

1. questi dovrà sostenere in luogo delle parti richiedenti i costi necessari all'attività di verifica svolta.
1. tutte le fonti di prova e/o elementi investigativi acquisiti a mezzo del captatore che non ha passato con successo la verifica del processo di certificazione dovranno essere immediatamente eliminati dal fascicolo
1. il produttore sarà sanzionato con un'ammenda pari al 50% delle spettanze pagata da istituzioni pubbliche nell'ultimo anno

Il produttore dovrà fornire come prestazione obbligatoria remunerata, su richieste delle parti coinvolte in un caso che veda l'utilizzo di un captatore da questi certificato, la messa a disposizione di personale tecnico e/o documentazione atta a spiegare il funzionamento del sistema. La tariffa che il produttore potrà esporre non potrà essere superiore alla tariffa media praticata dai consulenti tecnici d'ufficio nei confronti delle procure, per consulenze inerenti il c.d computer forensics.