soloreti.com

LA FASE STATICA E DINAMICA DELL'ACQUISIZIONE DATI

Le problematiche ad esse sottese

soloreti.com

- Supporto fisico
- Copia da remoto
- Registrazione da remoto

DOVE RISIEDE IL DATO?

- memorie esterne: ad es. dischi rigidi esterni, cd-dvd, pen drive usb, memorie ext di telefoni smartphone, memorie ext di macchine fotografiche digitali
- memorie interne: ad es. HDD, SSD e sistemi RAID, RAM dump su calcolatori accesi, NVRAM di smartphone o tablet

STATICO: SU SUPPORTO FISICO

- Copia di documento pubblicato su web: ad es. copia di pagina web presso un provider
- Copia di documenti su cartelle condivise in rete
- Copia di documenti residenti su dispositivi (PC, etc) durante una intercettazione

IBRIDO: COPIA DA REMOTO

- registrazione di dati che altrimenti di norma non sarebbero salvati dal sistema, programma o app: tipico esempio le chiamate e/o le conferenze audio-video

NETWORKING: REGISTRAZIONE DA REMOTO

QUESITI

- In che categoria sistemiamo il c.d. «captatore» ?
- Come cataloghiamo invece i dati risultanti da un'intercettazione ?

- Integro
- Parzialmente danneggiato
- Gravemente danneggiato

«STATO DI SALUTE» DEL SUPPORTO

- Integro e indicizzato
- Integro ma non indicizzato
- Danneggiato

«STATO DI SALUTE» DEL DATO SUL SUPPORTO

- Integro, correttamente incapsulato
- Danneggiato, ad es. per interruzione di comunicazione

«STATO DI SALUTE» DEL DATO IN RETE

- Le registrazioni dei dati in network locali/geografiche e/o in internet non sono da ritenersi necessariamente «fase dinamica»
- Si può avere interattività, ad esempio nel caso delle comunicazioni in tempo reale;
- Possiamo però anche avere una mera trasmissione o ricezione di un file

«DINAMICITÀ» DEL DATO IN RETE

- Ricordiamoci che l'apertura di un file produce comunque degli effetti sul sistema da cui consultiamo il file. Anche il caricamento di un semplice font in passato è stato sufficiente per ottenere il controllo del kernel sul sistema operativo ospite.
- Il kernel di un sistema operativo prende le richieste dai vari software e le invia alla CPU e alle altre periferiche.
- Potendo controllare il kernel si è in grado di ottenere il controllo pressochè totale del sistema operativo.

«STATICITÀ» DEL DATO SU SUPPORTO

DATI CANCELLATI

- Trattasi del dato integro ma non indicizzato
- Può trovarsi sia nel c.d. «slack space» ovvero cluster liberi in spazio allocato, sia nello spazio non allocato
- La rilevanza di tale dato nelle Ind. Prel. è a discrezione degli organi inquirenti

QUESITO

- Che cosa succede, ai fini della ripetibilità, quando il supporto è parzialmente danneggiato e invece il dato è integro ? Tipico esempio il disco rigido che presenta vari settori danneggiati
- Sempre ai fini della ripetibilità, come ci si comporta con la copia della memoria RAM qualora contenga dati di interesse ?

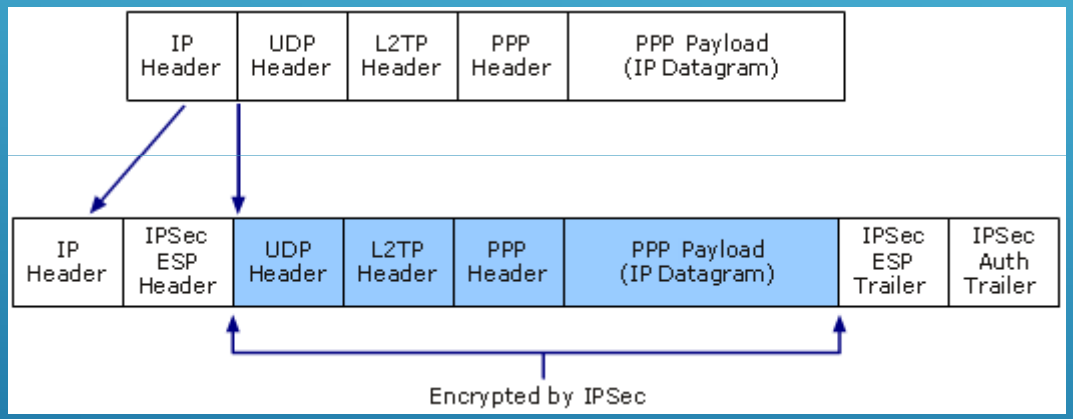
soloreti.com

- I collegamenti aziendali fra sedi e fra dipendenti dotati di dispositivi portatili e sedi
- I meccanismi di autenticazione da remoto (es. email) e ormai anche lo scambio stesso di email fra client e server
- Lo scambio di dati verso e da spazio disco in Cloud, e i relativi meccanismi di autenticazione
- Lo stesso schema che contiene i files su dispositivi portatili, quindi l'intero contenuto di essi, è sempre più spesso completamente criptato

CRITTOGRAFIA NELLE INDAGINI

CRITTOGRAFIA IN RETE

- Lo standard industriale più diffuso rimane IPSEC. PPTP è ancora usato ma considerato insicuro per mission-critical



soloreti.com

- Standard industriale: crittografia asimmetrica con chiavi pubbliche e private; (RSA, DH, DSS etc) altro uso tipico è quello dei certificati digitali per la verifica di autenticità
- Standard normativo fra cittadini e P.A. : D. Lgs. 82/2005 (Cod. Amm. Digitale): «certificatori» (autorità di certificazione, PKI), firma digitale.
- Algoritmo di cifratura più usato: SHA2
- Essenziale per datare e certificare l'attività del C.T.

CRITTOGRAFIA NELL'ATTIVITÀ DEL C.T.

RECUPERO DEL DATO CRIPTATO

- L'attività presenta buoni margini di fattibilità con vari dispositivi
- Un primo problema può sorgere ove il soggetto indagato (anche privato) deliberatamente predisponga strumenti avanzati di crittografia per proteggere i propri dati. Le tecniche di hacking possono aiutare
- Un secondo problema deriva da alcuni dei nuovi dispositivi immessi sul mercato, per i quali al momento delle indagini non si è ancora trovata alcuna vulnerabilità

soloreti.com

- Il solo elemento di unità del c.d. «captatore» è l'interfaccia utente, da cui si controllano, consultano e catalogano i dati eventualmente acquisiti
- Tale interfaccia funziona quindi da elemento di raccordo per una serie piuttosto nutrita di singoli programmi e sottoprogrammi
- I programmi sono suddivisi per sistema operativo o sistema informativo da violare

IL COSIDDETTO «CAPTATORE»

- Una prima parte del programma si occupa del «delivery». Si determina se il trojan possa essere direttamente installato sul dispositivo o se è richiesta una ulteriore azione da parte dell'utente
- Nel secondo caso si propone all'utente un aggiornamento di sistema, ovvero si invia una email contenente codice malevolo, etc.
- Una volta «consegnato» il pacco all'utente, entra in azione la seconda parte del programma, la quale si occupa dell'installazione

ESEMPIO SOFTWARE DI HACKING PER SISTEMA OPERATIVO

LIMITI DELLE TECNICHE DI HACKING

- Non è solo vero che il sistema è nelle mani di chi ha effettuato l'operazione di hacking: il sistema diventa spesso in balia dello hack, quindi dell'espediente di cui ci si è serviti.
- Non è affatto infrequente che i team di hackers, i quali curano gli aggiornamenti a tali programmi, si servano di trojan o virus di terze parti senza magari avere il tempo sufficiente di modificarli (vista ad esempio la urgenza di una indagine). In tal caso si può verificare una infezione non solo del dispositivo del malcapitato indagato (si pensi a una penna usb) ma anche di tutti i dispositivi con cui esso è venuto a contatto, o con cui è collegato in rete.

RIPETIBILITÀ

- E' un concetto che tecnicamente è applicabile solo al dato in sé, giuridicamente invece sembra applicabile anche alla rappresentazione del dato, anche quando esso non si presenti più nella sua forma originale, posto che si fornisca della alterazione una spiegazione plausibile, e posto che la alterazione non modifichi la rappresentazione stessa.
- Rimane ovvio comunque che la forza processuale di un reperto informatico sarà più alta tanto più alto sia l'indice di ripetibilità dell'accertamento, in ognuna delle sue fasi.
- Ricordiamoci che esistono accertamenti irripetibili in cui possono esserci, tecnicamente, una o più fasi che invece sono ripetibili. Ciò, se non rileva ai fini giuridico-procedurali, rileva invece eccome ai fini, ad esempio, di una controperizia.

- Promemoria per gli studi professionali di Avvocati in Italia: siamo assolutamente indietro per quanto riguarda la sicurezza «forensically sounding» del perimetro aziendale, sia sulle PMI sia sulla grande industria. Ciò si traduce in una grande opportunità di business per i professionisti coinvolti.
- Tali accorgimenti consentirebbero, se adottati, di limitare enormemente l'impatto di eventuali incursioni di sedicenti «captatori», autorizzati e non, in ambito di rete aziendale perlomeno: quindi di limitare l'eventuale danno derivante dall'incursione.

GRAZIE