PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5305 di Mercoledì 11 gennaio 2023

Una app israeliana sta destando molti timori fra gli esperti di security

Alcune riviste specializzate hanno dato notizia di una applicazione israeliana, messa a disposizione di specifiche utenze pubbliche, in grado di modificare in tempo reale le immagini video, catturati da impianti di videosorveglianza. Di cosa si tratta?

Alcune software house israeliane sono ormai diventate famose nel mondo per avere sviluppato degli applicativi particolarmente invasivi. Certamente il più conosciuto è l'applicativo Pegasus, grazie al quale è possibile inserirsi negli apparati cellulari di personaggi politici e industriali, catturando preziose informazioni, che vengono messe a disposizione del gestore dell'applicativo.

È di pochi giorni fa la notizia, pubblicata su un quotidiano israeliano, che una software house specializzata ha messo a disposizione dei clienti, esclusivamente soggetti governativi coinvolti nella sicurezza nazionale, una app, chiamata TOKA.

L'azienda è elencata sul sito web della direzione internazionale per la cooperazione nella difesa (SIBAT), il che significa che è riconosciuta come esportatrice ufficiale di sistemi di difesa.

Sempre secondo le notizie di stampa, questa app sarebbe in grado di modificare in tempo reale l'immagini video, sia in diretta, sia registrate, cambiando ad esempio il volto delle persone che vi appaiono, oppure cancellando la presenza di soggetti, ripresi dalle telecamere.

Che fosse possibile manipolare immagini video è fatto ormai ben noto, ma l'invasività di questa applicazione supera certamente il livello di conoscenze sino ad oggi disponibili. Ecco perché, nell'interesse dei lettori e mio, ho cercato di approfondire questo tema, prendendo contatto con soggetti, operanti soprattutto in Medioriente, che certamente hanno di questa situazione una conoscenza più approfondita, rispetto agli esperti occidentali.

Per potere modificare delle immagini video, è evidente che occorre dapprima catturare le immagini originali. È quindi da escludere che questa app possa essere utilizzata per operare su impianti di videosorveglianza in circuito chiuso, collegati via cavo e privi di collegamento con l'esterno. Si faccia attenzione che, se questi impianti di videosorveglianza utilizzano videoregistrazione sul cloud, non siamo più davanti ad un sistema chiuso, ma ad un sistema, cui si può accedere tramite inserimento sulla connessione cloud, che avviene perlopiù via Internet.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Su sistemi di videosorveglianza chiusi, quindi, questa app non può intervenire.

D'altro canto, bisogna prendere atto del fatto che oggi sempre più spesso impianti videosorveglianza utilizzano collegamenti Wi-Fi o Bluetooth, per collegare le telecamere alla postazione di comando e controllo; quest'ultima, a sua volta, può inviare i segnali video nel cloud, per archiviazione nel tempo.

Sia il collegamento fra la telecamera e la centrale di comando e controllo, sia il collegamento fra questa centrale ed il cloud, possono costituire un punto debole, che potrebbe consentire l'accesso da remoto ad una app sufficientemente intelligente. La conoscenza dell'indirizzo IP della telecamera rappresenta la chiave per l'accesso all'apparato, oppure al sistema.

Anche la crescente diffusione di reti Internet of Things (IoT), che si applicano alle lampade di illuminazione domestiche, agli elettrodomestici ed a molti altri apparati domestici, presenta un aspetto tecnico, che potrebbe essere, più o meno facilmente, violato.

È recente la notizia di un sistema IoT, installato in una abitazione di alto livello, che è stato violato accedendo alla password, disponibile su un lampadario domestico!

Il fatto che spesso le password di default non vengano modificate, all'atto dell'attivazione dell'impianto, oppure che gli algoritmi criptografici utilizzati non siano di adeguato livello, rappresenta un altro aspetto che può favorire l'attività di coloro che cercano di violare i dati presenti nelle reti domestiche.

Per illustrare le principio di funzionamento di questa applicazione, è bene chiarire che, già in passato, situazioni del genere avevano addirittura acquisito una posizione preminente su film di avventura.

Forse qualche lettore ricorderà il film Ocean's Eleven, in cui una banda di malviventi cercava di attaccare il caveau di un casino di Las Vegas, le immagini video provenienti dalle telecamere del caveau erano state sostituite da immagini video che provenivano da un caveau fittizio, realizzato in un capannone, a disposizione dei malviventi. Essi così poterono operare all'interno del caveau vero, mentre la sala di comando e controllo osservava immagini video che provenivano dal caveau fittizio.

Le modalità di intervento di questa applicazione sono invece piuttosto diverse, in quanto essa interviene direttamente sulle immagini originali, modificandole; nel caso illustrato nel film, per contro, le immagini originali venivano completamente sostituite da immagini provenienti dalla rete video gestita dai malviventi.

Un altro aspetto da prendere considerazione riguarda il fatto che oggi molti impianti di videosorveglianza sono dotati di sigilli di sicurezza, che vengono applicati sulle immagini, nell'istante stesso della ripresa da parte delle telecamere. L'alterazione di questi sigilli mette in evidenza una avvenuta manipolazione delle immagini.

Vi sono sigilli che lavorano su base criptografica, mentre altri sigilli lavorano condensando i codici alfanumerici dei singoli pixel in un aggregato, che rappresenta appunto il sigillo dell'immagine. L'alterazione delle immagini, anche minima, porta ad un'alterazione del calcolo del sigillo, mettendo in evidenza l'intervento.

Ricordo ai lettori che queste tecniche sono oggi sempre più diffuse, perché, diversamente, la prova esibita in giudizio potrebbe essere contestata dall'accusa o dalla difesa, in quanto l'immagine video sarebbe priva di una certificazione di autentica dell'immagine stessa.

Gli aspetti temibili della app sono quindi di due tipi:

- è una app capace di acquisire i codici di accesso e penetrare in sistemi informatici, specialmente utilizzati nel settore della videosorveglianza,
- è una app capace di acquisire in tempo reale le immagini e modificarle, in tempo altrettanto reale, in modo che l'immagine che viene inviata alla stazione di comando e controllo, e successivamente registrata, non sia quella originale, ma quella alterata.

Quale sia il livello di alterazione, come accennato in precedenza, è legato alla possibilità di sostituire dei volti, cancellare delle presenze fisiche ed altri elementi, presenti nell'immagine originariamente catturata.

Un metodo per poter verificare se queste immagini siano reali o siano state modificate potrebbe essere basato sulla installazione di una scheda di memoria, a bordo della telecamera. Confrontando la registrazione presente a bordo della telecamera con quella che viene ricevuta dalla sala operativa, o viene inviata al cloud, apparirebbe immediata la differenza. Mi rendo conto che si tratta di una soluzione piuttosto macchinosa, che però potrebbe essere utilizzate in applicazioni di altissima sicurezza.

L'altra alternativa, più economica e sempre raccomandabile, riguarda la adozione di sistemi di trasmissione video adeguatamente protetti, sia a livello di segnale video stesso, usando algoritmi crittografici di elevato livello, sia a livello di canali di trasmissione, utilizzando ad esempio le più recenti versioni del protocollo Wi-Fi, che sono decisamente più protette, rispetto a versioni precedenti.

Adalberto Biasiotti

Licenza Creative Commons