SCHEDA TECNICA *SEXTORSION*

La sextorsion in generale

La sextorsion è un metodo utilizzato per ricattare una persona usando foto o video che la ritraggono nuda o mentre compie atti sessuali (masturbazione). La stragrande maggioranza delle vittime di ricatto mediante video sexy sono uomini, adolescenti o adulti. Spesso la conversazione si svolge in una lingua italiana, francese, tedesca o inglese approssimativa. I criminali operano spesso dall'estero e anche i pagamenti devono essere effettuati su conti che si trovano all'estero. Succede regolarmente che il materiale compromettente sia pubblicato, anche se la vittima ha pagato il riscatto, o che venga richiesto un secondo pagamento.

Tre diversi tipi di sextorsion

Variante classica: le persone prese di mira sono contattate sulle reti sociali da un'avvenente sconosciuta che desidera essere aggiunta alla loro lista di amici. Se la persona presa di mira accetta, la sua nuova amica virtuale le dà appuntamento in una chat. Durante la conversazione, l'amica propone di continuare in modalità video. Poi la vittima è invitata a spogliarsi, masturbarsi, ballare nuda o assumere posizioni lascive. La seducente sconosciuta fa credere alla sua vittima che la trova attraente, che la eccita sessualmente e che lei stessa non ha inibizioni nei confronti della nudità e della masturbazione. Prende d'altronde l'iniziativa mostrando i suoi seni o accarezzandosi. Gli atti compiuti dalla vittima davanti alla webcam sono registrati a sua insaputa. Poco dopo sarà contattata da ricattatori che le chiederanno del denaro, altrimenti diffonderanno le immagini in questione.

Nel video della prima parte della campagna nazionale di prevenzione del 16 aprile 2020, che racconta la storia di Leo e delle sue disavventure con il personaggio fittizio di Anna, Leo è vittima della variante classica di sextortion.

Variante malware: in questo caso di sextortion, i computer, i tablet e gli smartphone delle persone che navigano su siti con contenuti pornografici appositamente preparati sono infettati da un software dannoso o malware. Quest'ultimo attiva la webcam della persona presa di mira mentre guarda immagini o video pornografici senza che sospetti nulla. Questi video spesso compromettenti sono trasmessi ai criminali che poi ricattano la vittima minacciandola di pubblicare il video o di inviarlo alla lista di amici che ne frattempo sono anche riusciti a rubarle.

Variante spam: succede anche che questi tentativi di ricatto siano inviati a molte persone sotto forma di "minacce poco credibili" nei messaggi di spam. I criminali sperano infatti che tra i destinatari vi siano persone che hanno guardato recentemente immagini o video pornografici e che, intimidite dalla minaccia, paghino quanto viene loro richiesto. In questi casi, il computer

della persona presa di mira non è infettato e i criminali non possiedono alcun materiale compromettente.

Alcuni dati

In generale, non esiste una statistica ufficiale sulla sextortion a livello svizzero. Tuttavia, per la sola variante spam della sextortion si è osservata una moltiplicazione dei casi tra luglio 2018 e dicembre 2018. Dall'analisi degli indirizzi bitcoin indicati nelle e-mail inviate alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI risulta che nel secondo semestre del 2018 sono stati pagati quasi 100 bitcoin, che all'epoca corrispondevano a circa CHF 360'000.-. Questo guadagno è stato ancora più importante in quanto l'invio di e-mail di massa non costa praticamente nulla.

All'inizio del 2019, inoltre, bitcoin per più di CHF 40'000.- sono stati versati in meno di cinque giorni su un unico conto utilizzato per un'importante campagna sulla sextortion in tedesco. In seguito a questa campagna, MELANI ha ricevuto centinaia di segnalazioni. Data la lingua utilizzata, l'attacco era diretto contro i paesi germanofoni. Inoltre, le similitudini tra i diversi indirizzi bitcoin suggeriscono che si è trattato della stessa campagna per almeno cinque ondate di spam, iniziate il 7 gennaio 2019, anche se la lingua e il tipo di e-mail erano diversi.

Come proteggersi?

Variante classica di sextorsion

Ecco come potete evitare di cadere in questa trappola.

- Non accettate mai richieste di amicizia o di incontri online da parte di persone che non siete in grado di identificare chiaramente o che non avete mai incontrato nella vita reale.
- Tenete sempre presente che qualsiasi conversazione tramite webcam può essere registrata. Di conseguenza, evitate di compiere qualsiasi atto che potrebbe mettervi in imbarazzo.
- Disattivate sempre la vostra webcam quando non state chattando tramite video e incollate un foglio di carta sull'obiettivo.
- Aggiornate regolarmente il sistema operativo, il browser e il software antivirus dei vostri dispositivi elettronici per proteggerli dai malware.
- Informate la vostra cerchia di familiari, parenti, amici e conoscenti su questo metodo di ricatto.

Siete vittime di un tale ricatto? Ecco come potete agire.

- Non date seguito alle richieste dei ricattatori. Non pagate!
- Interrompete subito ogni contatto con la donna usata come esca e con i ricattatori. Cancellateli dalla vostra lista di amici e non reagite ad alcun messaggio.
- Se i ricattatori hanno pubblicato del materiale fotografico o video, segnalatelo immediatamente alla piattaforma in questione e chiedete di cancellare tutto.
- Attivate un "Google Alert" personalizzato. Sarete così avvisati non appena una foto o un video con il vostro nome saranno pubblicati in Internet.
- Conservate tutte le prove e avvisate la polizia.

- Parlatene con una persona di cui vi fidate e cercate un sostegno psicologico se questa situazione vi pesa.

Variante malware della sextorsion

- Non pagate nulla, anche se i ricattatori vi sollecitano insistentemente!
- Controllate il vostro computer o fatelo controllare da un professionista per individuare eventuali malware e, se necessario, reinstallate o fate reinstallare il sistema operativo.
- Modificate tutte le vostre password e sceglietele tutte diverse e difficili da indovinare.

Testimonianze di vittime[1]

"È riuscita abbastanza rapidamente a conquistare la mia fiducia, e io mi sono veramente fatto del tutto abbindolare."

"Quello che voleva erano i soldi. Sono una persona che si stressa molto, quindi mi sono molto stressato, ma mi sono tenuto tutto dentro. Mi sono rinchiuso in me stesso e poi, beh, non ho fatto altro che obbedire."

"Mi ha fatto sapere che aveva ricevuto [i soldi] *(N.d.R)* ma che ne voleva di più."

"Ho pensato al suicidio. Ero completamente disperato."

"Certo, ho fatto una brutta esperienza. Tanto vale utilizzarla a scopi educativi e per fare prevenzione, invece di non dire nulla. Così qualcuno eviterà di farsi fregare."

[1] Testimonianze di vittime pubblicate su YouTube dalla Polizia cantonale neocastellana il 20 maggio 2015.