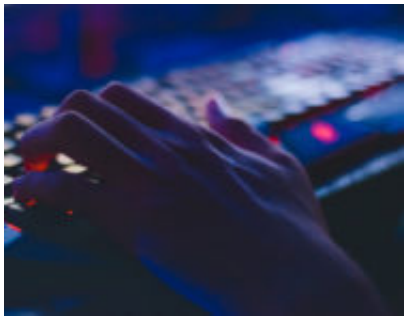
Sextortion: Analisi di una mail del ricatto

Author : Salvatore Lombardo

Date : 20 novembre 2018



Nel mese di Settembre il CNAIPIC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) ha diramato una comunicazione riguardante una massiva attività di spamming a scopo estorsivo. Un'email informa che il proprio account di posta elettronica è stato violato e che attraverso un malware installato mentre si visitavano siti web per adulti sono state fatte delle registrazioni video compromettenti. Pertanto per non condividere il materiale con i contatti personali viene fatta una richiesta di denaro in criptovaluta.

Ovviamente trattatasi di una mail allestita ad hoc per indurre la vittima a pagare il riscatto. Ecco di seguito alcune considerazioni al riguardo che ritengo possano essere utili per capire di cosa si tratta.

Cercherò attraverso una trattazione più semplice possibile e senza richiedere al lettore particolari conoscenze tecniche, di fornire degli spunti per valutare l'attendibilità delle mail che si ricevono. Tenendo sempre bene in mente che, in caso di reati telematici, bisogna rivolgersi alle autorità competenti. A tale scopo la Polizia di Stato, per avviare l'iter investigativo, ha reso disponibile un servizio di denuncia via web.

Come funziona la posta elettronica

Quando si spedisce una mail da un PC ad un altro attraverso la rete, nella trasmissione vengono coinvolti anche altri computer, i cosiddetti server di posta. Il mittente e il destinatario, dispongono di un client di posta elettronica, ossia un programma in grado di gestire, scaricare e spedire le email.

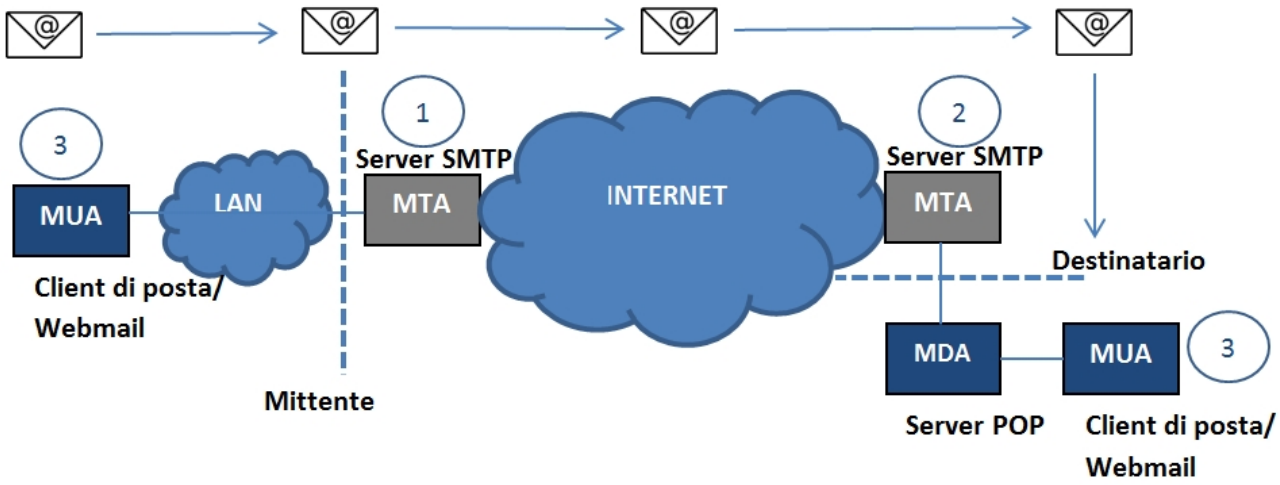
È opportuno che il client sia opportunamente configurato per dialogare con predeterminati server, demandando a questi il compito di contattare il server destinatario oppure di immagazzinare la posta in attesa di lettura.

Detto questo, vediamo di capire quali siano i passaggi seguiti da un messaggio di posta elettronica dal momento in cui il client del mittente lo spedisce a quello in cui viene consegnato

definitivamente al client del destinatario.

1. Quando si invia una email, il messaggio viene consegnato al server di posta elettronica mittente deputato al suo trasporto, il cosiddetto **MTA** (*Mail Transport Agent*) e inoltrato fino al raggiungimento dell'MTA del destinatario. Gli MTA comunicano tra loro attraverso il protocollo *SMTP (Simple Mail Transfer Protocol)* e vengono per questo chiamati server SMTP.
2. Il server MTA del destinatario consegna quindi la posta al server di posta elettronica in entrata l'MDA (*Mail Delivery Agent*), il cui compito è quello di conservare il messaggio in attesa che venga scaricato dal client di posta del proprio utente (ricevente). I protocolli di comunicazione degli MDA sono il POP3 (*Post Office Protocol*) e l'IMAP (*Internet Message Access Protocol*).
3. L'invio ed il ritiro della posta avviene tramite un software detto **MUA** (*Mail User Agent*):

- Se si utilizza un software installato sul proprio sistema, si parla di **client di posta** (esempio *Microsoft Outlook*, Eudora Mail, etc.).
- Se si tratta di un'interfaccia web, si parla di **servizio Webmail.**



Gli header di una email

Ogni messaggio email è composto da un intestazione e da un corpo:

- Il corpo comprende il contenuto del messaggio (body).
- L'intestazione (header) comprende delle indicazioni standard visibili, come il nome mittente, l'oggetto e la data d'invio, e delle altre informazioni nascoste, riguardanti soprattutto il mittente e il percorso fatto dal messaggio, che possono essere visualizzate su richiesta. Per visualizzare le intestazioni complete, sia nel caso si utilizzi un client di posta che un servizio Webmail, occorre cercare tra le proprietà e le opzioni del messaggio una voce di menu del tipo "visualizza intestazioni", "mostra dettagli" o "leggi header".

Gli header visibili standard sono:

1. **From/Da**: indica l'indirizzo mail del mittente, cioè autore del messaggio.
   Da: nomeMittente
2. **To/A:** indica gli indirizzi mail dei destinatari, separati da una virgola.
   A: nomeDestinatario , nomeDestinatario2 , etc.
3. **Cc**: indica gli indirizzi mail di uno o più destinatari, separati da una virgola, che devono ricevere una copia dell'email (opzionale).
   NomeDestinatarioInCopia , nomeDestinatarioInCopia2
4. **Subject/oggetto:** indica una spiegazione sintetica sul contenuto della mail.
   Oggetto: spiegazione del contenuto mail

Gli header nascosti possono essere:

1. **Return-Path**: se presente, indica l'opzione di rinvio per il mail server.
   Return-Path:
2. **Received:** indica il percorso del messaggio di posta, la data e gli indirizzi dei mail server coinvolti. Generalmente sono presenti almeno due di queste righe, rispettivamente per server mittente e destinatario.
   Received: from mta.slv.esempio (mail@mta.slv.esempio [indirzzo IP x.y.z.k])
   by mailserver.dest.it with SMTP
   for ; Thu, gg m anno ore:min:sec
3. **Message-ID**: indica un codice alfanumerico identificativo del messaggio.
   Message-ID:
4. **Content-Type**: indica il tipo e il codice del corpo del testo.
   Content-Type: text/plain; charset=UTF-8

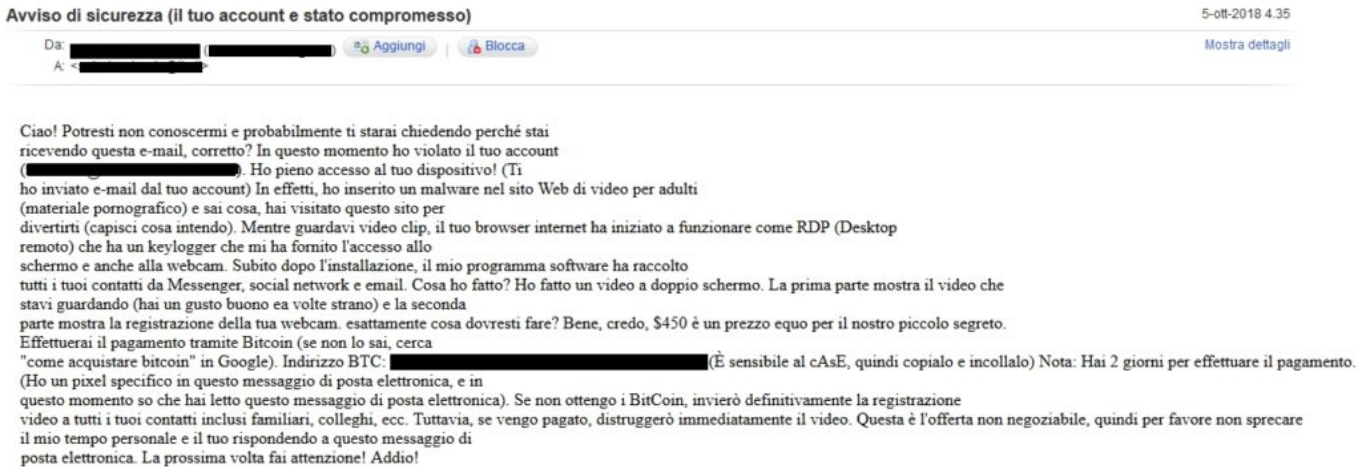
Come risulta evidente gli header più importanti e utili per la ricostruzione del percorso fatto da una email sono le righe *Received*, le quali aggiunte di volta in volta alla busta da ciascun server coinvolto nella trasmissione, individuano a ritroso il mittente e il destinatario.

Le righe Received, almeno in parte, possono essere ritenute affidabili, anche se eventuali righe di Received possono essere falsificate ed inserite all'inizio dell'header (solitamente le righe Received più in basso). Nel dettaglio "from mta.slv.esempio (mail@mta.slv.esempio [indirzzo IP x.y.z.k])" il campo mta.slv.esempio è il nome con cui il mittente si identifica al destinatario e può essere camuffato, mentre il campo [indirizzo IP x.y.k.z] può verosimilmente indicare il reale indirizzo del mittente.

Analisi di una mail del ricatto

Analizziamo il corpo e il relativo header completo di una mail della campagna estorsiva.

Negli screenshot che seguono alcune parti sono state oscurate.



Avviso di sicurezza (il tuo account e stato compromesso) 5-ott-2018 4.35

Da: [redacted] Aggiungi | Blocca Mostra dettagli

A: [redacted]

Ciao! Potresti non conoscermi e probabilmente ti starai chiedendo perché stai ricevendo questa e-mail, corretto? In questo momento ho violato il tuo account ([redacted]). Ho pieno accesso al tuo dispositivo! (Ti ho inviato e-mail dal tuo account) In effetti, ho inserito un malware nel sito Web di video per adulti (materiale pornografico) e sai cosa, hai visitato questo sito per divertirti (capisci cosa intendo). Mentre guardavi video clip, il tuo browser internet ha iniziato a funzionare come RDP (Desktop remoto) che ha un keylogger che mi ha fornito l'accesso allo schermo e anche alla webcam. Subito dopo l'installazione, il mio programma software ha raccolto tutti i tuoi contatti da Messenger, social network e email. Cosa ho fatto? Ho fatto un video a doppio schermo. La prima parte mostra il video che stavi guardando (hai un gusto buono ea volte strano) e la seconda parte mostra la registrazione della tua webcam. esattamente cosa dovresti fare? Bene, credo, $450 è un prezzo equo per il nostro piccolo segreto. Effettuerai il pagamento tramite Bitcoin (se non lo sai, cerca "come acquistare bitcoin" in Google). Indirizzo BTC: [redacted] (È sensibile al cAsE, quindi copialo e incollalo) Nota: Hai 2 giorni per effettuare il pagamento. (Ho un pixel specifico in questo messaggio di posta elettronica, e in questo momento so che hai letto questo messaggio di posta elettronica). Se non ottengo i BitCoin, invierò definitivamente la registrazione video a tutti i tuoi contatti inclusi familiari, colleghi, ecc. Tuttavia, se vengo pagato, distruggerò immediatamente il video. Questa è l'offerta non negoziabile, quindi per favore non sprecare il mio tempo personale e il tuo rispondendo a questo messaggio di posta elettronica. La prossima volta fai attenzione! Addio!

Dopo un saluto confidenziale e diretto, il ricattatore informa il destinatario di aver violato il suo account di posta elettronica “*Ti ho inviato una mail dal tuo account*” – scrive.

Prosegue affermando che tramite un keylogger installato sul dispositivo, ha proceduto alla registrazione, attraverso la webcam frontale, di ogni azione fatta durante la visione di un video clip a luci rosse, minacciando di inviare tutto il materiale ai suoi contatti. Per mantenere il segreto viene chiesto il versamento di una somma in un conto bitcoin.

L’email si conclude con un monito e un secco saluto: “*La prossima volta fai attenzione. Addio*”.

Purtroppo l’indirizzo di posta elettronica del destinatario di tale messaggio è finito nella rete di indirizzi di uno spambot. Non ci resta che esaminare le righe dell’header mail.

Dettagli:
1 Return-Path: <[redacted]>
Original-Recipient: rfc822;[redacted]
2 2.3 Received: from [redacted] by [redacted] (unknown [redacted])
id 5BB5D8F60009D1B8 for [redacted]; Fri, 5 Oct 2018 04:45:30 +0200
2 2.2 Received: from [redacted] by [redacted] (unknown [redacted])
id 5AF5979B3C629355 for [redacted]; Fri, 5 Oct 2018 04:45:30 +0200
2 2.1 Received: from [redacted] (unknown [redacted])
by [redacted] (Postfix) with ESMTPA id 7690DEEA04
for <[redacted]>; Fri, 5 Oct 2018 05:35:40 +0300 (MSK)
Date: Fri, 05 Oct 2018 05:35:41 +0300
Mime-Version: 1.0
3 From: [redacted] <[redacted]>
4 X-Auto-Response-Suppress: All
base: NS4xODcuNC4yOSwyNSxpbmZvQHByYXZvcG9zdC5ydSwxMjM0NTY=
To: [redacted] <[redacted]>
Subject: Avviso di sicurezza (il tuo account e stato compromesso)
X-Priority: 3
Message-Id: <2e69235c-8def-413c-a26a-2b2a11341419[redacted]>
Content-Transfer-Encoding: base64
Reply-To: [redacted]
Content-Type: text/plain;; charset=UTF-8
Content-Transfer-Encoding: base64

1. La riga return-path indica un indirizzo email, che non è quello della vittima. Da una semplice ricerca su internet, risulta essere il contatto di uno studio legale (*l’autore del*

messaggio si prende gioco di noi!)
Return-Path:

2. Le tre righe *Received* tracciano, a ritroso, il percorso della mail dal mittente al destinatario:
   (*Received 2.1)* il messaggio originale è partito da un MTA, con nome identificativo falsificato (spoofing del server SMTP: non c'è corrispondenza tra l'indirizzo IP e l'MTA dichiarato);
   (Received 2.2) il messaggio è stato successivamente inoltrato ad un MTA intermedio e recapitato all'MTA del destinatario;
   (*Received 2.3*) il messaggio infine è stato consegnato all'MDA della vittima.
3. Con questa riga, per rendere più verosimile il messaggio, il truffatore fa credere che la mail sia stata inviata dallo stesso account della vittima (spoofing del mittente). L'affermazione "*ti ho inviato una e-mail dal tuo account*" è falsa.
   From: indirizzoVeroMail@vittima
4. Questa riga, per la quale non esiste una standard ed è stata inserita dal client di posta mittente, indica che tutte le tipologie di notifiche e delivery reports sono state disattivate. Pertanto anche l'affermazione della presenza di un pixel specifico per la notifica di lettura e per il conseguente scatto del countdown è falsa.

Senza scendere troppo nei particolari, tramite una geo localizzazione degli indirizzi IP, è stato possibile individuare la posizione geografica dell'MTA che ha preso in carico il messaggio di posta. Dall'IP del mittente si è potuto constatare che l'autore del messaggio ha inviato la mail da un computer collegato ad una rete appartenente ad un provider estero.

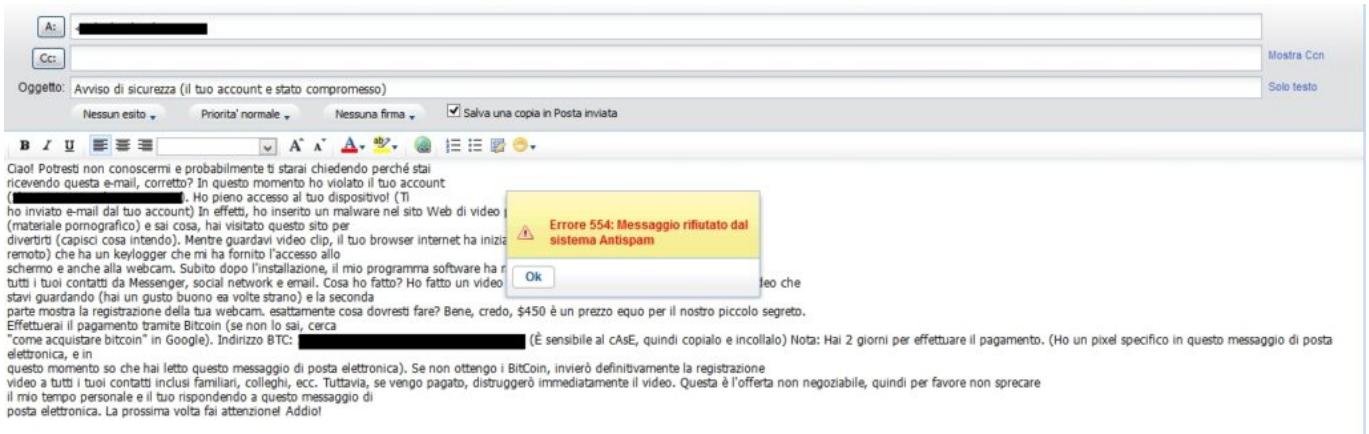
Di seguito riporto l'header completo e reinterpretato con i dettagli più significativi evidenziati.

```
HEADER
(1)Return-Path: <indirizzoMail@studiolegale.xx>
Original-Recipient: indirizzoVeroMail@vittima
(2.3) Received: from nomeMTAMailVittima (*.*.*.*) by nomeMDAVittima (*.*.*.*)
        id 5BB5D8F60009D1B8 for indirizzoVeroMail@vittima; Fri, 5 Oct 2018
04:45:30 +0200
(2.2) Received: from nomeMTAintermedio (*.*.*.*) by nomeMTAMailVittima (*.*.*.*)
        id 5AF5979B3C629355 for indirizzoVeroMail@vittima; Fri, 5 Oct 2018
04:45:30 +0200
(2.1) Received: from nomeMTAcontraffatto=nomeMTAintermedio (unknown [*.*.*.*])
      by MTAintermedio (*.*.*.*) (Postfix) with ESMTPA id 7690DEEA04
      for < indirizzoMail@vittima>; Fri, 5 Oct 2018 05:35:40 +0300 (MSK)
Date: Fri, 05 Oct 2018 05:35:41 +0300
Mime-Version: 1.0
(3)From: indirizzoMail@vittima <indirizzoMail@uso.criminale>
(4)X-Auto-Response-Suppress: All
base: NS4xODcuNC4yOSwyNSxpbmZvQHByYXZvcG9zdC5ydSwxMjM0NTY=
To: indirizzoMail@vittima <indirizzoMail@vittima>
Subject: Avviso di sicurezza (il tuo account e stato compromesso)
X-Priority: 3
Message-Id: <2e69235c-8def-413c-a26a-2b2a11341419@dominio.it>
Content-Transfer-Encoding: base64
Reply-To: indirizzoMail@vittima
Content-Type: text/plain;; charset=UTF-8
```

Ulteriore verifica

Se si prova a fare ciò che il criminale dice di aver fatto, inviandoci una copia fedele della mail del ricatto dal nostro stesso account, ecco cosa dovrebbe apparire:

Il server di posta dovrebbe impedire l'invio con un codice blocco errore *554*.



Qualora, invece, il filtro antispam dovesse incorrere in un errore di valutazione, generando un falso negativo, consiglio di segnalare l'anomalia al proprio gestore di posta.

Considerazioni finali

Non bisogna assolutamente pagare alcun riscatto, perché il criminale, in questo caso, non dispone di alcun filmato compromettente e di nessuna lista dei nostri contatti. Ciò che invece è necessario ed indispensabile fare è proteggere i nostri account, cambiare periodicamente la propria password, utilizzare quando possibile l'autenticazione multi fattore e non abbassare mai la guardia nei confronti di possibili episodi di phishing. A tal proposito, per verificare se l'account della nostra mail è stato violato, come ulteriore accertamento possiamo consultare il servizio web HIBP.

Ad oggi, sul conto bitcoin riportato nel messaggio, il cui saldo risulta ancora attivo e destinato verosimilmente a crescere, sono stati effettuati versamenti per un totale di circa 3.000$ (0,505 BTC). Se si tiene conto dell'entità di tale fenomeno, risulta facile stimare l'indebito guadagno percepito dai truffatori attraverso le diverse campagne in atto.

Ancora una volta, gli attaccanti non sfruttano una vulnerabilità software ma fanno leva sull'elemento umano. L'unico fix possibile, in questi casi, è l'aggiornamento e il miglioramento della CONSAPEVOLEZZA.

Riferimenti Sitografici

https://www.cybersecitalia.it/cybercrime-in-italia-arriva-una-nuova-ondata-di-estorsioni-di-tipo-sextortion/6860/
https://www.punto-informatico.it/truffe-email-sextortion-bitcoin/
https://it.ccm.net/contents/659-funzionamento-della-posta-elettronica-mta-mda-mua
https://www.ionos.it/digitalguide/e-mail/tecnica-e-mail/lheader-delle-e-mail-e-il-loro-ruolo-nelle-e-mail-spam/
https://www.techeconomy.it/2016/11/30/osint-cosa-dice-header-di-una-email/

Articolo a cura di: **Salvatore Lombardo**