Avviso di sicurezza del 19.12.19

Gentilissimi utenti,

Vi inviamo questa mail per informarvi sulle tre principali campagne malevoli veicolate tramite mail in atto in questi giorni contro l'Ateneo. Per le modalità con cui tali campagne sono effettuate, risulta particolarmente difficile individuarle e bloccarle in automatico; vi chiediamo quindi di prestare particolare attenzione nella consultazione delle mail in arrivo.

Campo Mittente contraffatto

Il protocollo SMTP usato per trasmettere le email purtroppo non contiene meccanismi nativi per autenticare il mittente. Questa mancanza nel protocollo originale permette di forgiare email con mittente arbitrario. Recentemente sono state segnalate email di questo tipo provenienti apparentemente dal rettore contenenti un link malevolo. Individuare tali email da parte dell'utente richiede l'analisi dell'header.

Truffa bitcoin veicolata con immagini

La seconda campagna che vogliamo segnalarviconsiste in una nuova variante del tentativo di estorsione in bitcoin per evitare la pubblicazione di improbabili filmati/foto compromettenti. Campagne di questo tipo tornano ciclicamente e sono solitamente classificate come spam dagli scanner della posta in base all'analisi del testo. La variante attuale si distingue dalle precedenti per il fatto che è costituita completamente da un immagine contenente un QRCode, rendendo estremamente complicato classificarla correttamente in maniera automatica. Qualora doveste incappare in una tale mail, non occorre segnalarla all'ufficio sicurezza; può comunque essere utile inviarla come allegato a spam@unim.it per migliorare la capacità di riconoscimento degli scanner. Qualora tale mail dovesse contenere una password e tale password corrisponde o è parte di una password in uso su un vostro account, occorre cambiare tempestivamente tali password in modo da mettere in sicurezza i vostri account.

Campo Mittente artefatto

La Seconda campagna in atto costituisce un tentativo di truffa basato sull'impersonificazione di un direttore di dipartimento o simile. La truffa inizia con una mail estremamente breve contenente una frase del tipo "sei disponibile?". Il mittente è una casella mail su un servizio gratuito esterno forgiata in modo da mimare un account istituzionale unimi, ad esempio mario.rossi.unimi.it@gmail.com. Qualora l'utente preso di mira dovesse rispondere a questa mail generica, seguirebbe una richesta economica diqualche tipo motivata dall'impossibilita da parte del sedicente direttore di effettuare tale operazione, ad esempio "potresti comprare questo buono regalo per me? Sono in riunione e non riesco adesso ma è urgente, ti rimborso quando torno". Anche in questo caso per sistemi automatici è pressoché impossibile identificare la frode in quanto si tratta di una possibile conversazione tra persone. Qualora doveste incappare in una conversazione come questa, contenenti richieste di denaro, occorre prestare la massima diffidenza.L'analisi attenta della mail del mittente in generale indica immediatamente l'eventuale tentativo di truffa. È comunque necessario verificare sempre con un canale di comunicazione differente, esempio una telefonata diretta all'interessato, la veridicità di tali richieste. Incaso di dubbio potete inviare la mail sospetta come allegato a sicurezza@unimi.it.

Raccomandiamo a tutti voi di consultare frequentemente la sezione del portale di Ateneo dedicata alla sicurezza ICT e protezione dati e in particolare:

- **gli avvisi di sicurezza delle campagne malevole (tra cui quelle odierne) in atto al link https://work.unimi.it/servizi/security_gdpr/118606.htm**

- **le linee guida e indicazioni (tra cui quelle per proteggersi dal Phishing) al link https://work.unimi.it/servizi/security_gdpr/118582.htm**

Ulteriori raccomandazioni

Si approfitta dell'occasione per ricordare altresì agli utenti quanto segue:

- utilizzare password per ciascun account univoche e robuste (lunghezza idonea, formata da lettere maiuscole e minuscole, numeri e/o caratteri speciali, senza riferimenti riconducibili all'utente);
- attivare la domanda di controllo per il recupero della password
- cambiare le password regolarmente e con frequenza almeno ogni 6 mesi;
- non riutilizzare la stessa password a breve distanza di tempo;
- mantenere sistema operativo e antivirus aggiornati.

Cordialmente

Ufficio Sicurezza ICT - Direzione Generale

Esempio di truffa con impersonificazione (le parti in rosso sono state volutamente offuscate)

Esempio di truffa bitcoin veicolata con un immagine (le parti in rosso sono state volutamente offuscate)

i am àwar[redacted]one of yoûr passphràsēs. Lets gēt right to pōint. Nō ōne has compensated me tō investigate about you. You may not knōw me and yōū'rē most likely thinking why you are getting this email?

i installed à sōftware on the adūlt vidēo clips (pornōgràphic materiàl) wēb site and you know what, you visited this web site to hàve fūn (you knōw whàt i mēàn). While you were viewing vidēōs, your browser bēgan working as à Remote control Desktop that has a kēylogger which provided mē with accēssibility to your display scrēen as wēll as web càmēra. Right after that, my software ōbtàinēd all your contàcts from yōur Messengēr, FB, and e-mailaccount. ànd then i created a doublē vidēo. 1st pàrt shows the videō yoū were watching (you hàve à fine taste :)), ànd next part shōws the view of yoûr web cam, & its you.

You hàve just two solūtiōns. Let us look àt the possibilities in particūlars:

Very first option is to disregàrd this email. in this instànce, i will send out your very own recorded material to every one of yoûr personal contàcts and thūs consider concerning the disgrace thàt yōū rēcēive. Do not fōrget if yoū happen to be in a loving rēlationship, hōw it can affect?

in the second place chōice should be to givē me $1138. Lets name it às a donation. as à result, i mōst certainly will immediately remove yoûr videotape. You will keēp yoûr daily rōūtine like this nevēr occurred and you will not hear back agàin frōm me.

You'll make the pàyment via Bitcoin (if you dō not knōw this, search 'how tō buy bitcōin' in Goōgle search engine).

BTC addrēss:

Scan the QR code with mobile to get the address.

if yōū may be making plans for going to the cōps, gōod, this message cànnot be traced back to me. i havē dēalt with my actions. i am just nōt attempting tō dēmand a hugē amoūnt, i only want to bē paid for. You now havē two days in order tō make the payment. i hàve à uniquē pixel in this email, ànd right now i know that yōu hàve rēad through this mail. if i do nōt get the BitCoins, i will, no dōūbt send out your video to àll ōf your contacts including close relatives, coworkers, and many others. However, if i receivē the payment, i will erāse thē video right awày. it is a nonnegotiable offēr, so do not wàstē mine time & yours by rēplying tō this e-mail. if you wànt proof, reply Yeah! & i definitely will send out your video rēcōrding to your 12 contacts.