Avviso di sicurezza del 05/03/2021

Segnalazione di campagne malevole in atto

Gent.Utenti,
pubblichiamo il presente avviso per informarvi delle campagne malevole che in questi giorni stanno colpendo l'Ateneo. In fondo a questo documento potete trovare alcune schermate di esempio.
Il primo esempio che vogliamo mostrarvi è un tentativo di estorsione che ha come obbiettivo convincere l'utente a pagare una somma in moneta elettronica **bitcoin** (potete trovare un esempio in Figura 1). A volte le email sono personalizzate con dati personali facilmente recuperabili dal web o con vecchie password compromesse. Tali mail arrivano in Ateneo a migliaia ogni giorno, non costituiscono un effettivo problema di sicurezza e vengono generalmente marcate come SPAM dal sistema di antispam di Ateneo. Qualora dovessero sfuggire al filtro anti-spam ed essere consegnate nella INBOX della vostra casella di posta vi preghiamo di inoltrarle come allegato a spam@unimi.it per migliorare la risposta dell'antispam. Per supporto sul servizio antispam potete aprire un ticket presso l'Ufficio Servizi di Posta Elettronica al seguente indirizzo:
https://auth.unimi.it/servicedesktlc
Il secondo esempio è una mail malevola contenente un virus protetto da password per sfuggire all'antivirus della posta elettronica. La mail si presenta come un avviso di una giacenza, un documento postale o legale che per essere visionato deve essere aperto inserendo una password che viene data all'interno della mail stessa. Un esempio di questo tipo di mail lo trovate in Figura 2.
Allegati protetti da password non concordati preventivamente con il mittente vanno sempre considerati malevoli e cancellati. In generale occorre prestare la massima diffidenza nell'aprire allegati specie se di tipo Microsoft Office **doc, xls, ppt** ma anche **exe, scn, bat, iso**; prima dell'apertura è necessario scannerizzare preventivamente l'allegato con l'antivirus. La presenza all'apertura di messaggi che richiedono l'attivazione di macro o l'inserimento di password indica con elevata probabilità che il file che si tenta di aprire sia un virus.
Il terzo esempio che vi illustriamo è un tentativo di phishing che periodicamente ritorna a colpire l'Ateneo in varie forme. La mail si presenta come una segnalazione relativa ad un problema sulla posta elettronica e richiede di cliccare su un link malevolo che porta ad un sito esterno all'Ateneo che costituisce l'effettiva pagina malevola di phishing.
La mail dell'esempio di Figura 3 può essere riconosciuta come phishing da queste caratteristiche:

- La mail è di tono allarmistico: "se non si procede la posta non funzionerà più".
- **Rimanda ad un sito al di fuori del dominio unimi.it**: in questo caso il link rimanda ad un sito del dominio **. mipropia*. in***. (vedi Figura 4) Il link può solitamente essere visto in anteprima prima del click sostando con il puntatore del mouse sopra il bottone per alcuni secondi.
- Una volta cliccato sul bottone si raggiunge la pagina di phishing vero e proprio (vedi figura 5) **all'esterno del dominio unimi.it.**

Il sito di phishing di Figura 5 può essere riconosciuto come tale da queste caratteristiche:

- **Il dominio che ospita il sito è chiaramente fuori dal dominio unimi.it**.
- Il tema generale del sito non ha nessun riferimento a unimi.it: probabilmente viene usato per tentativi di phishing verso più organizzazioni.
- E' servito con protocollo insicuro HTTP.
- Il titolo della finestra è anomalo: la parola Outlook è stata spezzata con un trattino.

Ricordiamo che, **per qualunque problema relativo al servizio di posta elettronica di Ateneo, l'unico servizio che può darvi supporto è accessibile attraverso la piattaforma di ticketing dell'Ufficio di Posta Elettronica di Ateneo**:

https://auth.unimi.it/servicedesktlc

Ricordiamo che il protocollo email non ha nessun meccanismo di sicurezza che possa proteggere le informazioni in esse contenute. Per tale motivo nessuna mail che richiede l'invio in chiaro di password o altri dati sensibili può essere considerata benigna.

Vi chiediamo, **se foste incappati in una di queste campagne ed aveste inserito le vostre credenziali,** di:

- Cambiare immediatamente la password attraverso il sito istituzionale: https://auth.unimi.it/password/
- Effettuare una scansione completa del proprio PC con un antivirus aggiornato
- Darne rapida comunicazione, sicurezza@unimi.it avendo cura di specificare l'orario indicativo in cui si è cliccato sul link malevolo e l'orario in cui è stato effettuato il cambio della password.

In caso contrario, non occorre fare nulla oltre che cancellare la mail.

Si raccomanda sempre di prestare la massima prudenza su email contenenti link o allegati soprattutto se non sollecitate.

Qui trovate delle istruzioni pratiche per proteggersi dal phishing ed evitare la sottrazione di dati riservati e personali:

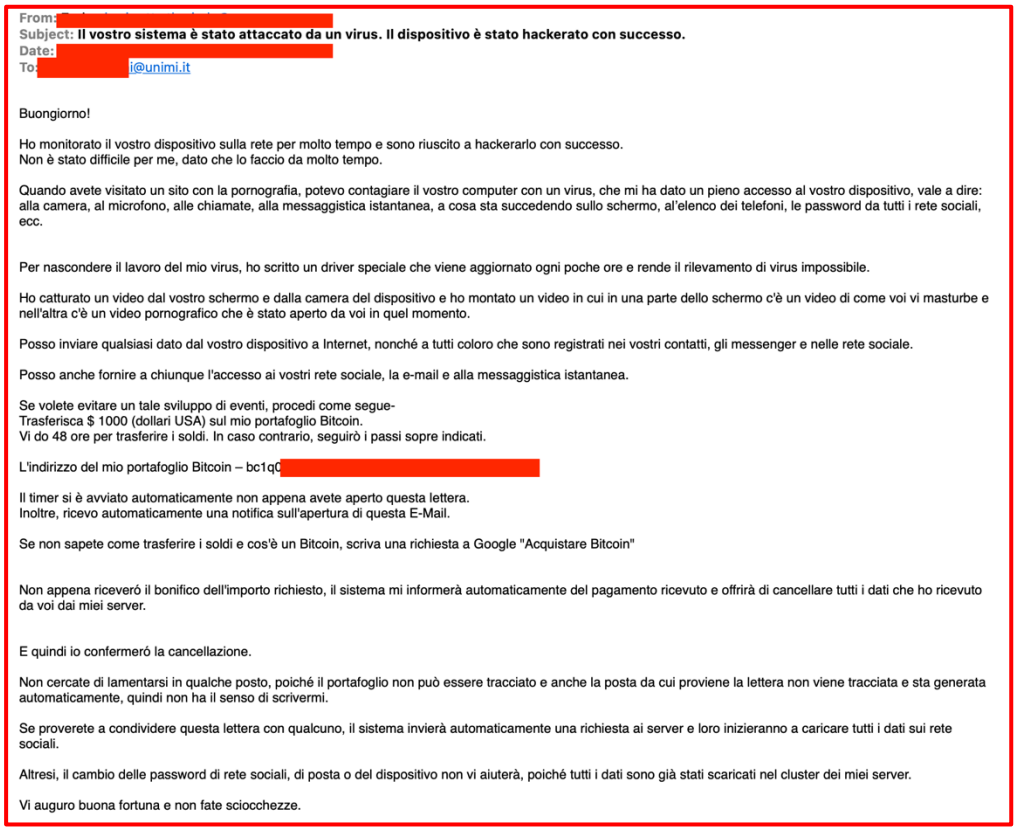
https://work.unimi.it/filepub/sicurezza_ict/Indicazioni%20utili%20a%20proteggersi%20dal%20Phishing.pdf

Altre informazioni su come migliorare la sicurezza dell'Ateneo possono essere trovate sul portale istituzionale al link: https://work.unimi.it/servizi/security_gdpr/118546.htm

I più cordiali saluti.

Nicla Diomede
Settore Cybersecurity, Protezione Dati e Conformità - Direzione ICT
Università degli Studi di Milano - Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Figura 1: Email malevola a tema bitcoin



From: [redacted]
Subject: **Il vostro sistema è stato attaccato da un virus. Il dispositivo è stato hackerato con successo.**
Date: [redacted]
To: [redacted]i@unimi.it

Buongiorno!

Ho monitorato il vostro dispositivo sulla rete per molto tempo e sono riuscito a hackerarlo con successo.
Non è stato difficile per me, dato che lo faccio da molto tempo.

Quando avete visitato un sito con la pornografia, potevo contagiare il vostro computer con un virus, che mi ha dato un pieno accesso al vostro dispositivo, vale a dire: alla camera, al microfono, alle chiamate, alla messaggistica istantanea, a cosa sta succedendo sullo schermo, al'elenco dei telefoni, le password da tutti i rete sociali, ecc.

Per nascondere il lavoro del mio virus, ho scritto un driver speciale che viene aggiornato ogni poche ore e rende il rilevamento di virus impossibile.

Ho catturato un video dal vostro schermo e dalla camera del dispositivo e ho montato un video in cui in una parte dello schermo c'è un video di come voi vi masturbe e nell'altra c'è un video pornografico che è stato aperto da voi in quel momento.

Posso inviare qualsiasi dato dal vostro dispositivo a Internet, nonché a tutti coloro che sono registrati nei vostri contatti, gli messenger e nelle rete sociale.

Posso anche fornire a chiunque l'accesso ai vostri rete sociale, la e-mail e alla messaggistica istantanea.

Se volete evitare un tale sviluppo di eventi, procedi come segue-
Trasferisca $ 1000 (dollari USA) sul mio portafoglio Bitcoin.
Vi do 48 ore per trasferire i soldi. In caso contrario, seguirò i passi sopre indicati.

L'indirizzo del mio portafoglio Bitcoin – bc1q[redacted]

Il timer si è avviato automaticamente non appena avete aperto questa lettera.
Inoltre, ricevo automaticamente una notifica sull'apertura di questa E-Mail.

Se non sapete come trasferire i soldi e cos'è un Bitcoin, scriva una richiesta a Google "Acquistare Bitcoin"

Non appena riceverò il bonifico dell'importo richiesto, il sistema mi informerà automaticamente del pagamento ricevuto e offrirà di cancellare tutti i dati che ho ricevuto da voi dai miei server.

E quindi io confermerò la cancellazione.

Non cercate di lamentarsi in qualche posto, poiché il portafoglio non può essere tracciato e anche la posta da cui proviene la lettera non viene tracciata e sta generata automaticamente, quindi non ha il senso di scrivermi.

Se proverete a condividere questa lettera con qualcuno, il sistema invierà automaticamente una richiesta ai server e loro inizieranno a caricare tutti i dati sui rete sociali.

Altresi, il cambio delle password di rete sociali, di posta o del dispositivo non vi aiuterà, poiché tutti i dati sono già stati scaricati nel cluster dei miei server.

Vi auguro buona fortuna e non fate sciocchezze.

Figura 2: Email malevola contenente un virus

Da: **customerservice** <admin@[redacted]uisson.com>
Data: 05/mar/2021 12.56.45
Oggetto: POSTA CERTIFICATA: 589989671
A: [redacted]@unimi.it

Buongiorno,
inoltro allegati aggiornati come da accordi.
Rimango a disposizione.

password : Marzo2021

Cordiali saluti.

ZIP

condiz_03.05.2
021.do...876.zip

Figura 3: Email malevola di phishing

From: Helpdesk@unimi.it
Subject: **Aggiornamento dell'account**
Date: 5 March 2021 at 14:52:48 CET
To: Recipients@unimi.it

Caro utente,

Il tuo account e-mail non può essere aggiornato automaticamente alla versione 2021 di Outlook più recente con 10 GB aggiuntivi gratuiti a causa dei recenti aggiornamenti del server.

Fai clic qui e accedi per eseguire l'aggiornamento gratuitamente.

È obbligatorio attenersi per evitare l'interruzione del servizio,
Il mancato rispetto porterebbe alla chiusura temporanea dell'Account.

Ci scusiamo per l'inconveniente.

Saluti,
Helpdesk

Figura 4: url malevolo

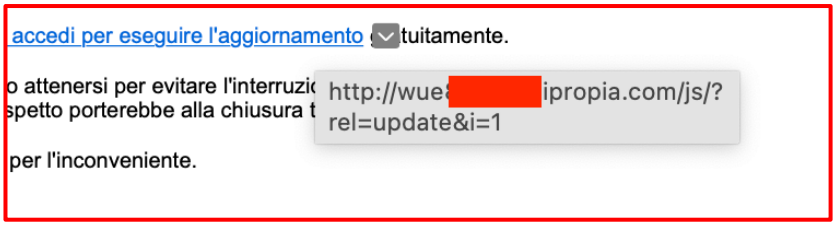


Figura 5: sito malevolo di phishing