Avviso di sicurezza del 26/02/2024

Segnalazione di campagna malevola veicolata tramite allegato zippato

Gent.Utenti,

pubblichiamo questo avviso per segnalare una campagna malevola veicolata tramite un allegato zip e contenente frammenti di conversazioni per aumentarne la verosimiglianza. La campagna mira a convincere l'utente ad aprire ed eseguire un allegato malevolo.

La campagna può essere riconosciuta come malevola dalle seguenti caratteristiche:

- La mail non proviene da un dominio riferibile all'Ateneo;
- l'oggetto della mail contiene inserimenti/sostituzioni di caratteri con lo scopo di non aggregare la mail malevola ad eventuali altre conversazioni esistenti, es: *_Sp3dizi0ne* al posto di *Spedizione;*
- L'allegato ha un nome non riconoscibile.

Vi chiediamo di non aprire l'allegato e cancellare la mail. Di seguito potete trovare il dettaglio della campagna malevola.

Ricordiamo di mantenere alta la diffidenza rispetto a richieste inusuali soprattutto se di tipo economico e/o allarmistico.

Grazie per l'attenzione.

I più cordiali saluti.

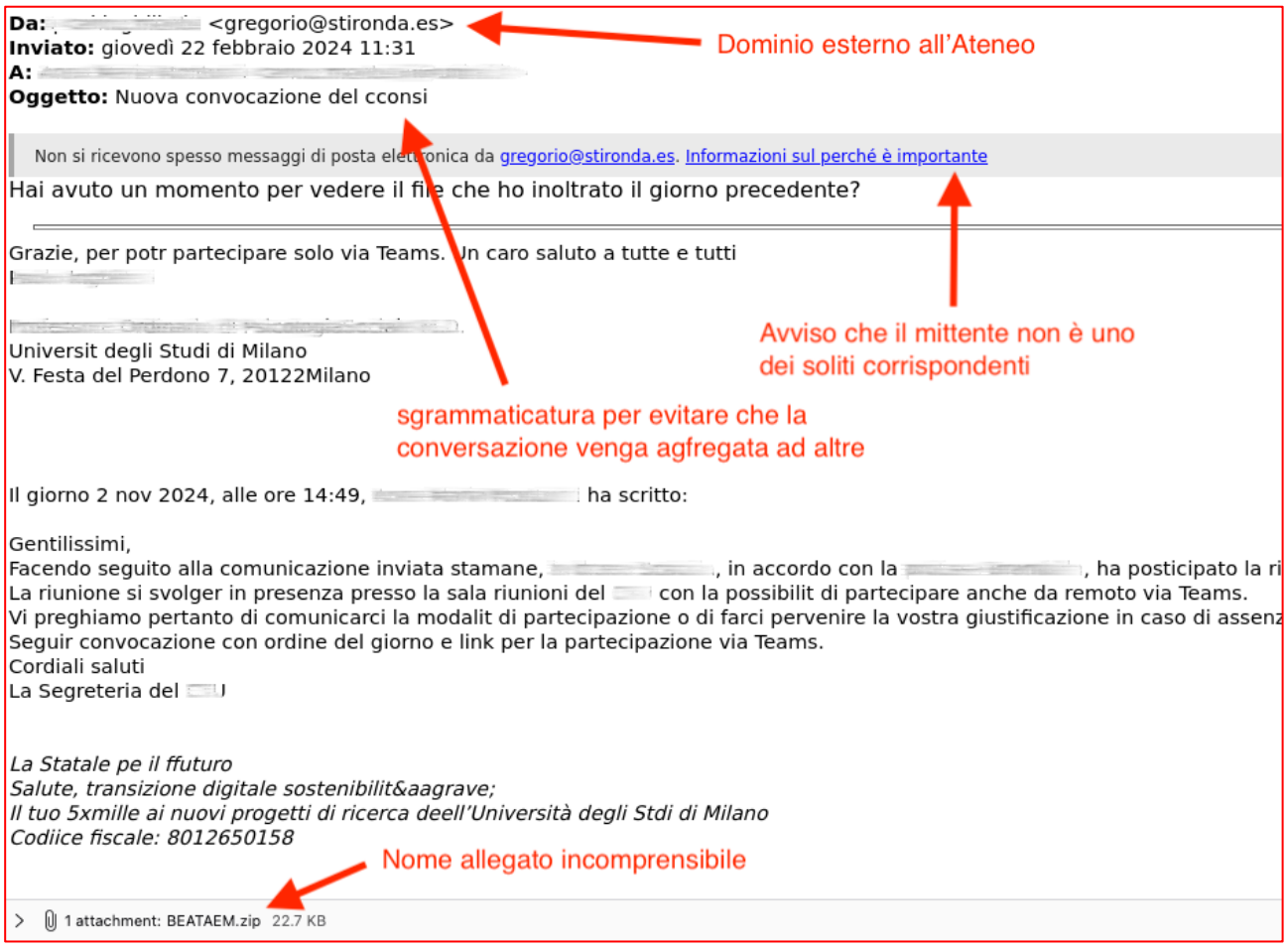
Massimo Marchi

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

UNIMI-SOC-202402260000000001 Per favore, non cancellate questa riga
e usate questa mail per ulteriori comunicazioni su questa segnalazione

Dettaglio della campagna malevola

La campagna malevola è veicolata attraverso una mail che riporta un frammento di conversazione creato ad hoc o rubato in precedenti compromissioni. La mail chiede di visionare un allegato di tipo zip:



Dall'esame visuale della mail e del link proposto si possono individuare delle caratteristiche anomale:

- La mail non proviene da un dominio riferibile all'Ateneo:

  <gregorio@stironda.es>

- Il mittente e/o l'oggetto della mail contiene inserimenti/sostituzioni di caratteri con lo scopo di non fare aggregare la mail malevola con altre conversazioni presenti nel client di posta usato:

  Oggetto: Nuova convocazione del cconsi

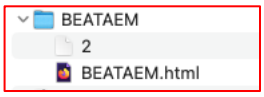
- L'allegato ha un nome poco chiaro:

E' possibile ottenere informazioni analoghe anche analizzando l'header nascosto della mail seguendo le indicazioni della guida scaricabile al link:

https://work.unimi.it/filepub/sicurezza_ict/DICT_IO_GuidaPraticaAnalisiMail_rev.3del16062021.pdf

Se per errore si scarica l'allegato e si spacchetta il file zip, si ottiene una struttura simile a questa:



Il primo file, in questo caso di "2" ma potrebbe essere differente, è inserito al solo scopo di sviare gli algoritmi degli antivirus e offuscare il vero file malevolo.
Il secondo file è il file effettivamente malevolo. In questo caso si tratta di un file di tipo HTML contenente un codice malevolo con l'obbiettivo di sottrarre le password dell'utente. In altri casi il file malevolo consiste in un segmento eseguibile di tipo javascript (.js) che ha lo scopo di scaricare da remoto ed eseguire un file malware.

Nel caso abbiate per errore aperto l'allegato ed eseguito il file malevolo, occorre:

- Eseguire una scansione completa del dispositivo con un antivirus aggiornato
- Darne pronta comunicazione a questo ufficio scrivendo a sicurezza@unimi.it

Contromisure

La migliore contromisura contro le mail malevole è la prudenza nell'apertura delle stesse.
Occorre controllare con attenzione il reale mittente delle mail e prestare particolare diffidenza alle mail non attese, di contenuto poco chiaro e tono allarmistico, contenenti link e/o allegati sospetti.

In caso di dubbio è possibile inoltrare la mail sospetta come allegato a sicurezza@unimi.it per un ulteriore controllo.

Grazie per la collaborazione

Massimo Marchi

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

UNIMI-SOC-202402260000000001 Per favore, non cancellate questa riga
e usate questa mail per ulteriori comunicazioni su questa segnalazione