Bollettino di Sicurezza del 16 Settembre 2020
Campagna malevola in atto a tema Agenzia delle Entrate

Gentilissimi Utenti,
pubblichiamo questo bollettino di sicurezza per informarvi di una campagna malevola che in questi giorni è diretta a colpire le caselle di posta elettronica dell'Ateneo. La mail in questione contiene, infatti, in allegato un virus che ha l'obiettivo di compromettere la sicurezza informatica del PC del ricevente. Di seguito trovate un esempio di come potrebbe presentarsi la mail malevola.
Vi invitiamo quindi a prestare la massima diffidenza nei confronti di mail non sollecitate specie se contenenti allegati di tipo office (ad esempio con formato *.xlsx), protetti da password o con nomi di file generici e a seguire le indicazioni contenute nella sezione del portale LaStatale@Work:

Servizi per Tutti / Sicurezza informatica e protezione dei dati personali / Regolamenti, istruzioni e linee guida

ed in particolare alla guida:
https://work.unimi.it/filepub/sicurezza_ict/Indicazioni%20utili%20a%20proteggersi%20dal%20Phishing.pdf

Il settore Cybersecurity, Protezione Dati e Conformità, venuto a conoscenza delle campagne di phishing in esame, ha attuato tutte le misure tecnologiche utili a proteggere gli utenti collegati alla rete di Ateneo e quelli collegati alla VPN. Tuttavia, non è possibile escludere che, tra gli utenti a cui è stata consegnata la mail fraudolenta nella casella INBOX, ve ne sia qualcuno che abbia cliccato sul collegamento malevolo da una rete esterna ad Unimi (ad es. reti cellulari/domestiche o reti di altri enti o fornitori di connettività a Internet).

Qualora aveste aperto uno di questi allegati occorre:

- Procedere ad una scansione completa del vostro PC con un antivirus di Ateneo Sophos aggiornato
- Procedere ad un cambio password delle credenziali di Ateneo usando il sito di Ateneo: https://auth.unimi.it/password
- Darcene rapido riscontro a: sicurezza@unimi.it

Con l'occasione vi informiamo che abbiamo ricevuto notizia di un'intensificazione degli attacchi informatici diretti alle comunità accedamiche europee. Vi invitiamo quindi a prestare la massima attenzione nella gestione delle e-mail.
Di seguito trovate una guida con alcune istruzioni pratiche utili a consentirvi di valutare in autonomia la bontà delle e-mail e che è disponibile al link:

https://work.unimi.it/filepub/sicurezza_ict/20191210_GuidaPraticaAnalisiMail_v2.pdf

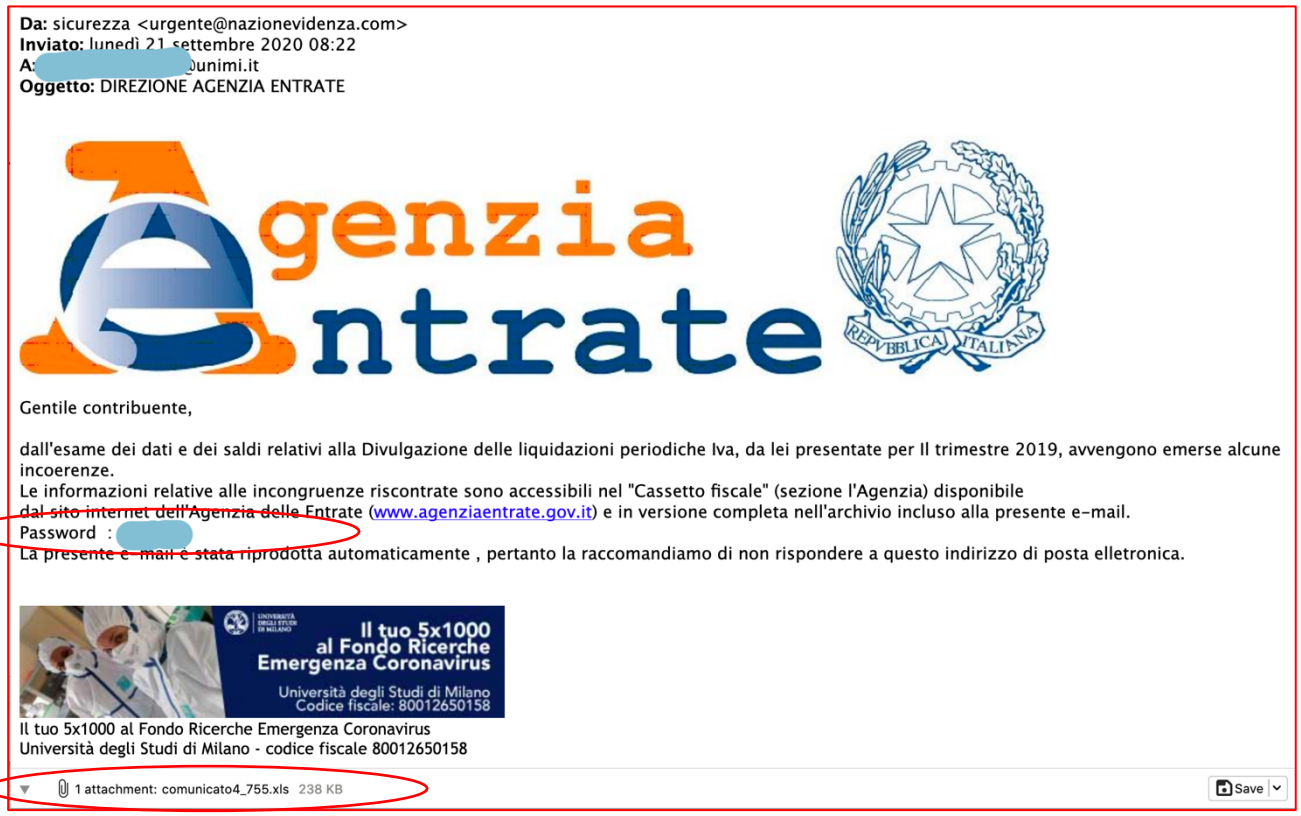
Grazie per la collaborazione e buon proseguimento di lettura.

Cordialmente.

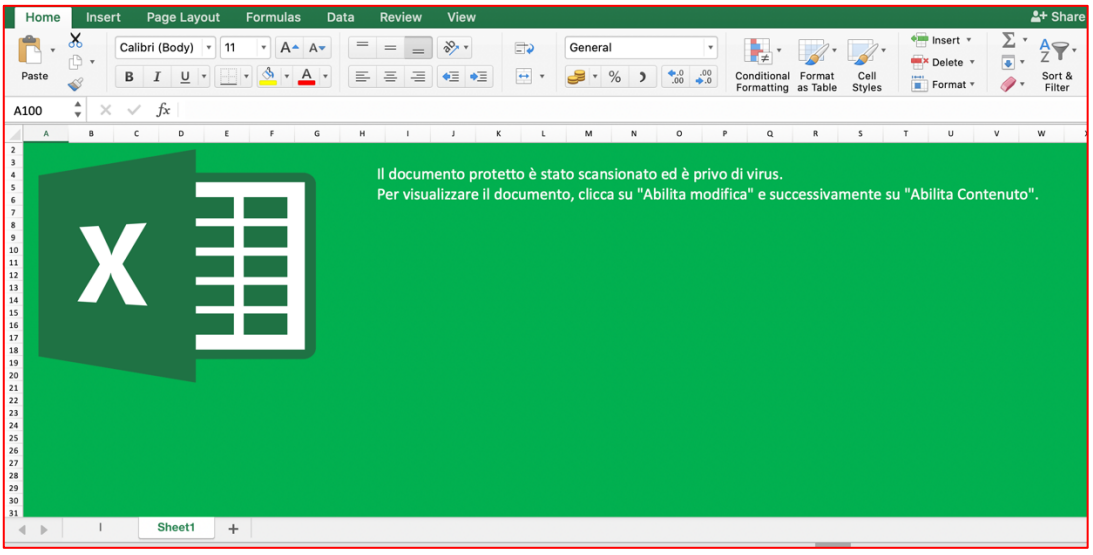
Nicla Diomede
Settore Cybersecurity, Protezione Dati e Conformita' - Direzione ICT
Universita' degli Studi di Milano
Via Giuseppe Colombo n. 46 - 20133 Milano
Info: https://work.unimi.it/servizi/security_gdpr/118546.htm

Campagna malevola veicolata tramite file Excel protetto da password

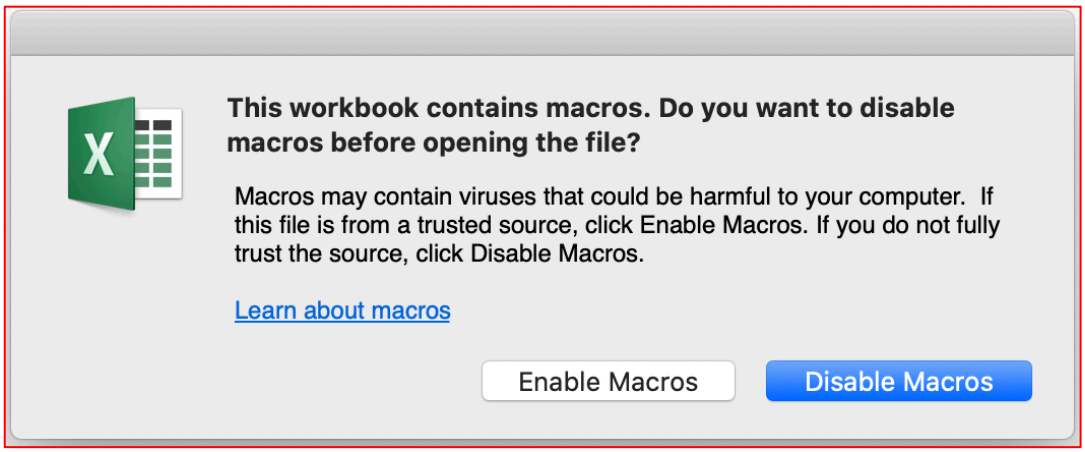
Di seguito trovate l'esempio di una mail malevola veicolata attraverso il servizio di posta elettronica di Ateneo contenente un allegato di tipo Office Excel Macro. L'allegato è stato protetto con password in modo da sfuggire alla scansione anti-virus e richiede per essere aperto dell'inserimento da parte della vittima di una password specificata nel testo.



Per aprire il documento malevolo contenente occorre inserire la password indicata nella mail. L'allegato contiene un codice malevolo sotto forma di macro Excel che ha lo scopo di scaricare da Internet il virus vero e proprio. Una volta aperto il file si presenta come segue:



A seconda di come è settato Excel durante l'apertura potrebbe essere richiesto di attivare le macro:



Nel caso abbiate ricevuto una mail simile occorre non aprire l'allegato e cancellare la mail immediatamente. In caso di dubbi potete inoltrare la mail come allegato a:

sicurezza@unimi.it

Qualora abbiate aperto il documento ed attivato le macro occorre:

- Procedere ad una scansione completa del vostro PC con un antivirus aggiornato
- Procedere ad un cambio password delle credenziali di Ateneo usando il sito di Ateneo:
  https://auth.unimi.it/password
- Darcene rapido riscontro a:
  sicurezza@unimi.it