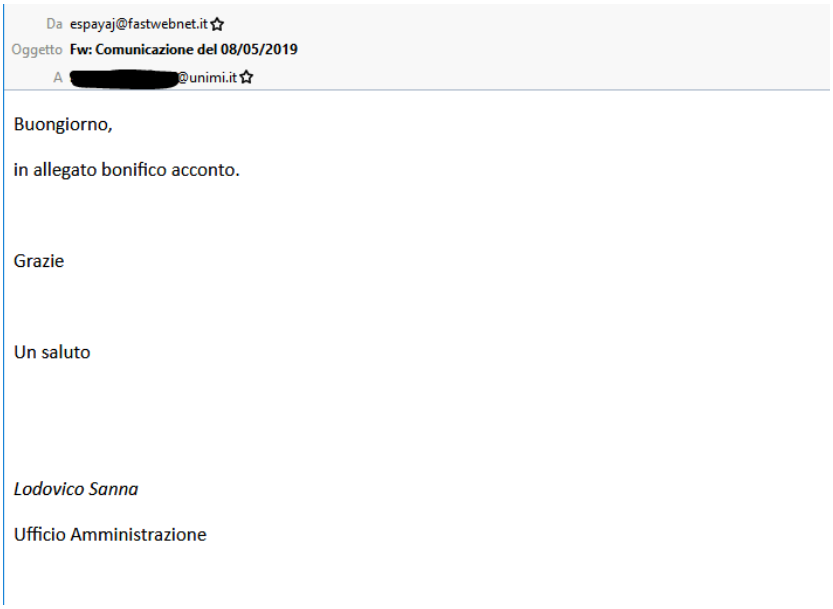
Campagna di phishing "Comunicazione con allegato XXX-2019 Segnatura_xml_.xls"

E' attualmente in corso una nuova campagna di malspam, veicolata tramite la posta elettronica, il cui obiettivo è quello di **infettare con un malware il dispositivo dei destinatari.**

Le mail in esame hanno il testo scritto in italiano, e fanno riferimento ad un bonifico. L'allegato è un file in formato .xls**.**

Ecco un esempio di email:


Da espayaj@fastwebnet.it
Oggetto **Fw: Comunicazione del 08/05/2019**
A [redacted]@unimi.it

Buongiorno,

in allegato bonifico acconto.

Grazie

Un saluto

Lodovico Sanna

Ufficio Amministrazione

Si fa presente che la mail, nel mittente, oggetto e testo, potrebbe presentare alcune modifiche.

L'Ufficio di Staff Sicurezza ICT invita gli utenti a:

- **non rispondere all'email ricevuta;**
- **non aprire l'allegato.**

Per coloro i quali abbiano riconosciuto la mail fraudolenta come sospetta, dunque abbiano ignorato l'email e non abbiano aperto l'allegato, **non è richiesta alcuna azione**.

Chiunque avesse erroneamente cliccato e aperto l'allegato è invitato a:

- effettuare una scansione antivirus, e salvare lo screen del risultato
- inviare una email all'Ufficio di Staff Sicurezza ICT all'indirizzo sicurezza@unimi.it, precisando nell'oggetto la campagna malevola, ed indicando le seguenti informazioni:

    1. IP del dispositivo
    2. sistema operativo del dispositivo

3. tipo di antivirus in possesso

4. screenshot del risultato della scansione antivirus

Ricordiamo infine che l'Ufficio Sicurezza ICT nella sezione dedicata del portale di Ateneo pubblica:

- **gli avvisi di sicurezza della campagne malevoli 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**

Vi ringraziamo per la collaborazione.

Cordialmente,
Ufficio di Staff Sicurezza ICT