Comunicazione Alert di Sicurezza

PHISHING 'GOZI'

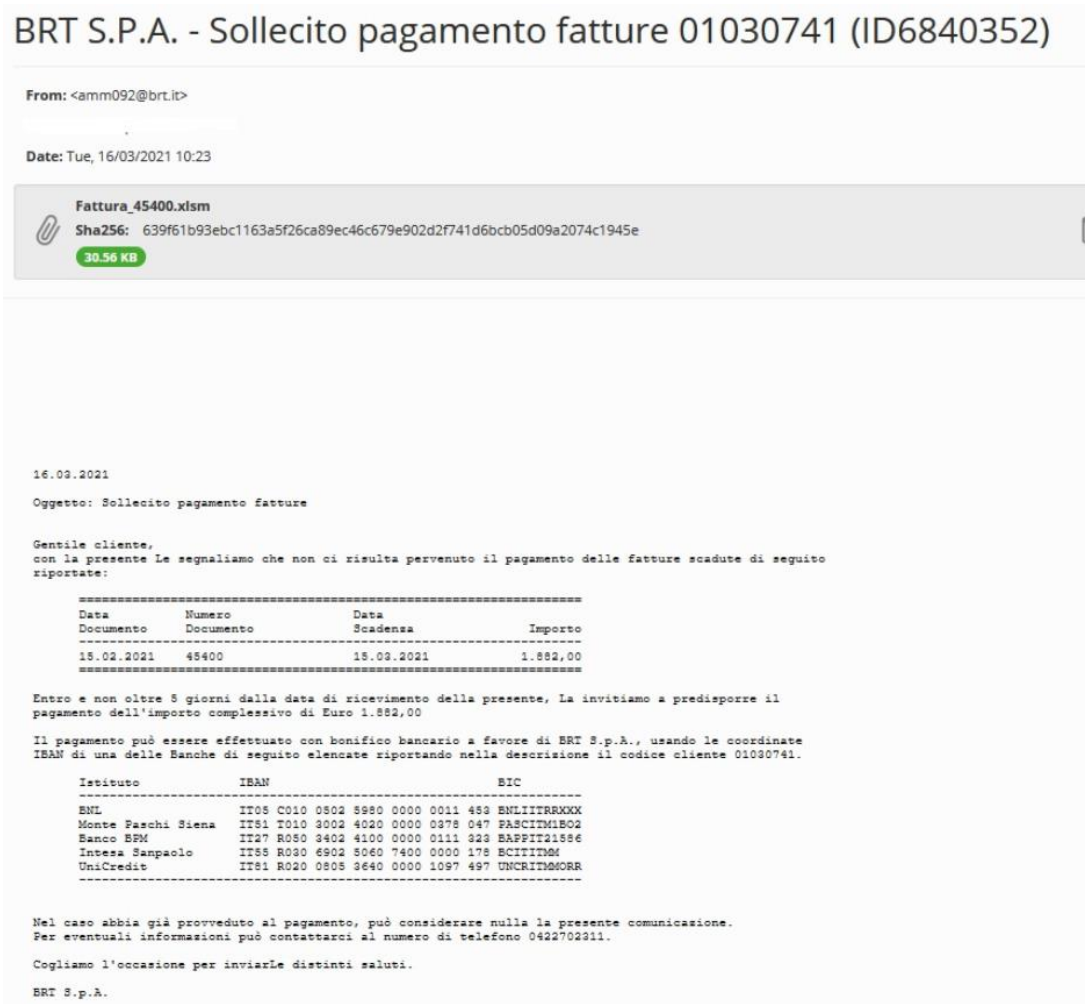
19 Marzo, 2021

Gentile Utente,

si segnala in queste ore un'intensa azione di tentativi di phishing ai danni del Ministero dell'Istruzione.

Tali messaggi sono indirizzati a caselle di posta elettronica istituzionali, provenendo da mittenti verosimili quali **brt.it** e **Agenzia delle Entrate**, per cui per quanto il mittente possa essere noto il messaggio può essere malevolo.

Di seguito esempi di come si possono presentare le mail in oggetto:



BRT S.P.A. - Sollecito pagamento fatture 01030741 (ID6840352)

From: <amm092@brt.it>

Date: Tue, 16/03/2021 10:23

Fattura_45400.xlsm
Sha256: 639f61b93ebc1163a5f26ca89ec46c679e902d2f741d6bcb05d09a2074c1945e
30.56 KB

16.03.2021

Oggetto: Sollecito pagamento fatture

Gentile cliente,
con la presente Le segnaliamo che non ci risulta pervenuto il pagamento delle fatture scadute di seguito riportate:

Data Documento	Numero Documento	Data Scadenza	Importo
15.02.2021	45400	15.03.2021	1.882,00

Entro e non oltre 5 giorni dalla data di ricevimento della presente, La invitiamo a predisporre il pagamento dell'importo complessivo di Euro 1.882,00

Il pagamento può essere effettuato con bonifico bancario a favore di BRT S.p.A., usando le coordinate IBAN di una delle Banche di seguito elencate riportando nella descrizione il codice cliente 01030741.

Istituto	IBAN	BIC
BNL	IT05 C010 0502 5980 0000 0011 459	BNLIITRRXXX
Monte Paschi Siena	IT51 T010 3002 4020 0000 0378 047	PASCITM1BO2
Banco BPM	IT27 R050 3402 4100 0000 0111 323	BAPPIT21586
Intesa Sanpaolo	IT55 R030 6902 5060 7400 0000 178	BCITITMM
UniCredit	IT81 R020 0805 3640 0000 1097 497	UNCRITMMORR

Nel caso abbia già provveduto al pagamento, può considerare nulla la presente comunicazione.
Per eventuali informazioni può contattarci al numero di telefono 0422702311.

Cogliamo l'occasione per inviarLe distinti saluti.

BRT S.p.A.

Informativa del 3/15/2021

From: conferma <admin@mikailozdemir.com>
To:
Date: Mon, 15/03/2021 03:21

attiv_2800.zip
Sha256: f2aa25390d7f704d1a22f48ac888baf4f6fca058c2dbcc9b3334decfc7b76da4
66.62 KB

Agenzia Entrate
Direzione Centrale Gestione Tributi

Gentile contribuente,
dall'esame dei dati e dei versamenti inerenti alla Comunicazione delle liquidazioni periodiche Iva, da lei mostrata per l'ultimo trimestre 2020, sono emerse alcune incongruenze.
Le informazioni inerenti alle incongruenze sono disponibili nel file in allegato o nel "Cassetto fiscale" (sezione L'Agenzia scrive) e nel servizio "Fatture e Corrispettivi (sezione Consultazione - L'Agenzia scrive),
entrambi accessibili dal area internet dell'Agenzia delle entrate (www.agenziaentrate.gov.it).

Password: gov2021

La presente email è stata generata automaticamente, pertanto la preghiamo di non rispondere a questo indirizzo di posta elettronica.

I sistemi di sicurezza stanno operando per la protezione da tale attacco, la presente comunicazione è pertanto a fini di ulteriore precauzione.

E' possibile riscontrare evidenza di un'azione malevola sulle mail passando il puntatore del mouse sul nome dello stesso mittente e verificando eventuali anomalie nell'indirizzo mail visualizzato (disallineamento con il nome visualizzato, stringhe alfanumeriche complesse o non interpretabili nel nome utente, dominio estero, ecc.).

Qualora giungessero nella posta in arrivo, tali mail non devono essere assolutamente considerate e devono essere cancellate.

Non si devono assolutamente aprire i file eventualmente presenti in allegato a tali mail, di nessun formato (excel, word, zip, ecc.).

Qualora ciò fosse stato fatto, occorre procedere immediatamente alla **scansione della postazione di lavoro utilizzata** e, subito dopo, provvedere al **cambio delle credenziali** di tutti gli account utilizzati a fini lavorativi (la stessa posta elettronica, accesso al sistema informativo dell'istruzione, ecc.).

Non solo nella situazione della segnalazione in oggetto, bensì sempre, qualora doveste incorrere in messaggi mail del suddetto tipo, allo scopo di limitare l'occorrenza di incidenti di sicurezza, si devono seguire le seguenti raccomandazioni.

- **non dare seguito all'apertura di file non attesi**, dalla dubbia provenienza o che giungano da caselle di posta non note;

- **non installare software sulle proprie postazioni di lavoro**, soprattutto se a seguito di sollecitazioni via e-mail;
- **non dare seguito alle richieste di e-mail sospette**;
- nel caso in cui la richiesta provenga da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: *l'e-mail era attesa? Le frasi sono scritte con grammatica corretta? Il software da installare ha un fine specifico? Eventuali link nell'e-mail puntano a siti conosciuti? Il mittente è corretto?*
- disporre di supporti removibili quali chiavette usb e/o hard disk esterni ecc. con molta cautela; al momento della connessione di un supporto removibile, si consiglia di avviare una scansione completa dello stesso attraverso il software antivirus.

Inoltre si ricorda di:

- **scansionare periodicamente per la ricerca malware le postazioni di lavoro** ed i dispositivi utilizzati per lavoro;
- nel caso di utilizzo del PC personale (telelavoro/smart working) assicurarsi periodicamente:

  - **che il sistema operativo della propria postazione di lavoro sia aggiornato**;

  - **che la propria postazione di lavoro sia dotata di antivirus aggiornato** per la periodica scansione;

  - che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano apportate solo piccole modifiche (come ad esempio numerazioni progressive ...)

Si ricorda inoltre che nell'area riservata intranet allo CSIRT MI (dopo il login, sezione: *Area Riservata > Computer Security Incident Response Team > Security Awareness*) sono presenti i contenuti relativi a campagne malevole di phishing in corso ed aggiornamenti su nuovi virus che potrebbero infettare le postazioni di lavoro del personale della Pubblica Amministrazione.

E' fortemente consigliata la lettura dei suddetti contenuti, allo scopo di tenersi aggiornati sui rischi informatici incombenti sull'Amministrazione e proteggere sia la propria operatività sia il patrimonio informativo del Ministero da possibili attacchi.

Inoltre, ai fini tutela delle informazioni riservate di lavoro, ivi inclusi i dati personali propri e di terzi, si raccomanda fortemente di non lasciare mai il personal computer di lavoro incustodito o comunque non sotto il proprio diretto controllo (e.g. computer lasciato in bagagliaio auto in propria assenza).

Grazie della collaborazione

CSIRT MI