

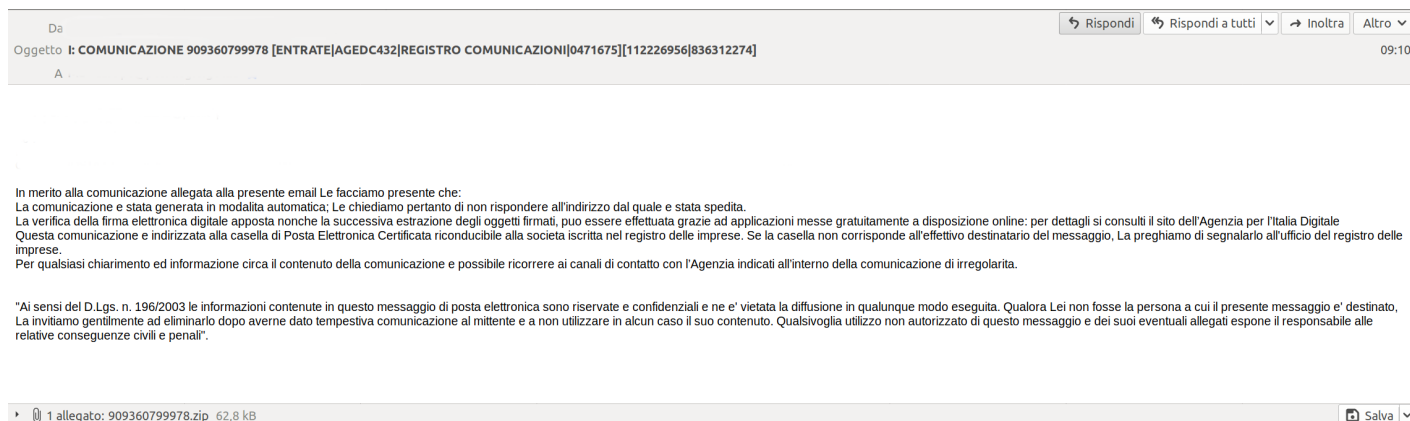
Diffusione sLoad via PEC rivolta a Privati e Professionisti

12/09/2019

pec sLoad

A partire dalla giornata di ieri è stata individuata una vasta campagna di malspam, indirizzata principalmente ad aziende private e professionisti, che utilizza il canale PEC per veicolare il malware all'interno di un archivio ZIP.

La campagna in atto è del tutto simile a quella riportata in data 19/07/2019 relativa alla diffusione via PEC del malware sLoad e rivolta a Privati e Professionisti. Un esempio è di seguito rappresentato:



Da

Oggetto: I: COMUNICAZIONE 909360799978 [ENTRATE]AGEDC432[REGISTRO COMUNICAZIONI][0471675][112226956][836312274]

A.



In merito alla comunicazione allegata alla presente email Le facciamo presente che:
La comunicazione è stata generata in modalità automatica; Le chiediamo pertanto di non rispondere all'indirizzo dal quale è stata spedita.
La verifica della firma elettronica digitale apposta nonché la successiva estrazione degli oggetti firmati, può essere effettuata grazie ad applicazioni messe gratuitamente a disposizione online; per dettagli si consulti il sito dell'Agenzia per l'Italia Digitale.
Questa comunicazione è indirizzata alla casella di Posta Elettronica Certificata riconducibile alla società iscritta nel registro delle imprese. Se la casella non corrisponde all'effettivo destinatario del messaggio, La preghiamo di segnalarlo all'ufficio del registro delle imprese.
Per qualsiasi chiarimento ed informazione circa il contenuto della comunicazione e possibile ricorrere ai canali di contatto con l'Agenzia indicati all'interno della comunicazione di irregolarità.

Ai sensi del D.Lgs. n. 196/2003 le informazioni contenute in questo messaggio di posta elettronica sono riservate e confidenziali e ne è vietata la diffusione in qualunque modo eseguita. Qualora Lei non fosse la persona a cui il presente messaggio è destinato, La invitiamo gentilmente ad eliminarlo dopo averne dato tempestiva comunicazione al mittente e a non utilizzare in alcun caso il suo contenuto. Qualsivoglia utilizzo non autorizzato di questo messaggio e dei suoi eventuali allegati espone il responsabile alle relative conseguenze civili e penali.

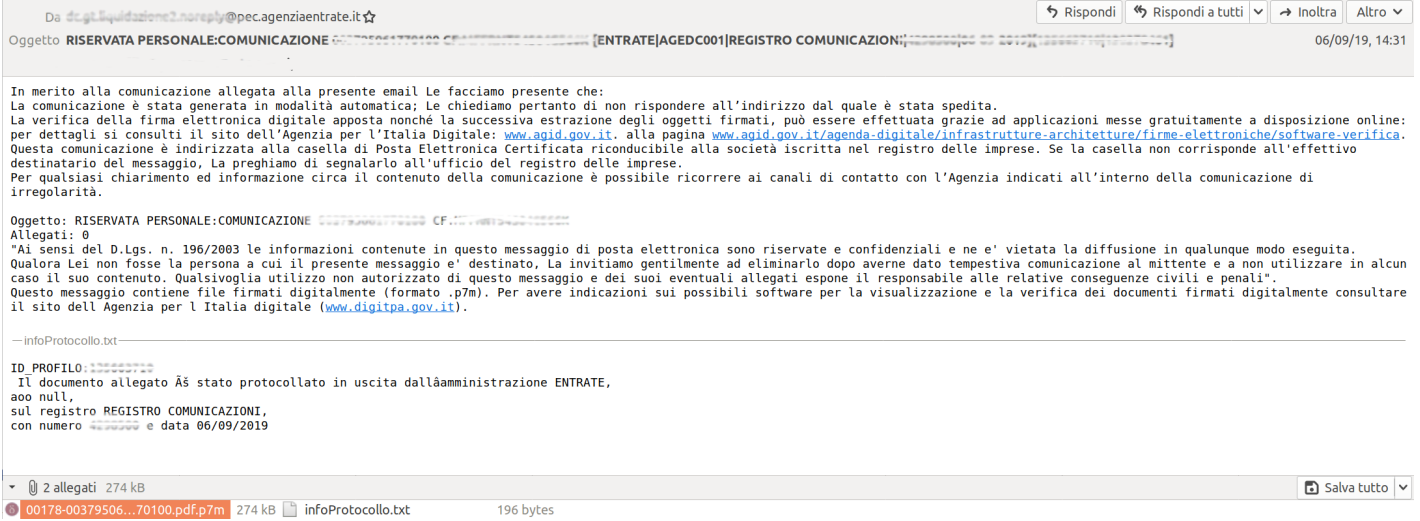
1 allegato: 909360799978.zip 62,8 kB

L'allegato è definito da un archivio .zip contenente due file con lo stesso nome, uno è un .pdf malformato la cui apertura provoca volontariamente un errore di visualizzazione **inducendo così l'utente ad aprire l'altro che è un file .vbs malevolo**.

In tutti i casi fin ora rilevati i due file (pdf e vbs) hanno lo stesso nome, variabile da caso a caso, similmente a quanto sotto rappresentato:

Nome	Dimensione
 IT95812451822.pdf	80,4 kB
 IT95812451822.vbs	7,9 kB

La campagna di diffusione malware utilizza un modello di comunicazione **molto simile a quello in uso da Agenzia delle Entrate** come di seguito mostrato:



Naturalmente la comunicazione ufficiale differisce dalla campagna in oggetto sia per il mittente PEC che per il tipo di allegato presente. Nel caso reale si tratta di un file pdf firmato digitalmente (.p7m) come visibile nell'immagine sopra.

Catena di infezione

L'esecuzione del file .vbs determina l'accesso ad un file .jpg posto su un server remoto, tale file viene scaricato e salvato nel percorso locale in `c:\Users\Public\Downloads*.ps1` quindi eseguito dando seguito all'infezione.

Il malware è una variante di **sLoad noto per essere capace di eseguire comandi arbitrari sul sistema tra cui catturare le informazioni salvate nei browser.**

Il CERT-PA sta analizzando il malware per verificare eventuali nuove funzionalità rispetto alla versione precedentemente utilizzata.

Raccomandazioni

Prestare attenzione a non aprire allegati presenti in messaggi di posta elettronica che provengono da caselle PEC di utenti, professionisti o società a vario titolo, riportanti come oggetto:

- **COMUNICAZIONE XXXXXXXXXXXX**
[ENTRATE|AGEDCXXX|REGISTRO COMUNICAZIONI|XXXXXXXXX]
[XXXXXXXXXXXX|XXXXXXXXXXXX]

Un ulteriore campagna in atto in queste ore è stata osservata da un ricercatore che ne ha dato visione tramite il proprio account Twitter.

Indicatori di compromissione

⚠ Dichiarazione di esclusione di responsabilità

DROP URL

- hXXps://fanaaru[.]com/
- hXXps://dreamacinc[.]com/
- hXXps://kd5ndz[.]com/
- hXXps://interloc-tp[.]com/
- hXXps://memoriesmadelb[.]com/
- hXXps://clutchmagazine[.]com/
- hXXps://rdtber[.]eu/

C&C

- hXXps://rdtber.eu/
- hXXps://uilomiku.eu/

Sono in corso ulteriori analisi di cui il CERT-PA darà riscontro non appena possibile.

Aggiornamento 12 settembre 2019

Si informa che specifiche azioni di contrasto sono state indirizzate alla sospensione delle caselle PEC utilizzate come veicolo di infezione della campagna in oggetto.

Dalle analisi svolte nel corso della giornata odierna sono inoltre stati raccolti aggiuntivi indicatori di compromissione. A tal proposito si provvede a fornire, in formato testuale scaricabile, l'insieme degli stessi per le necessarie azioni di contrasto e verifica.

- **IoC (.txt)** – IP, Hash
- **IoC (HASHr.txt)** – Lista dei soli hash file da utilizzare in combinazione con il tool HASHr

Aggiornamento 13 settembre 2019

Nuovi indicatori di compromissione:

- **IoC (.txt)** – IP, Hash
- **IoC (HASHr.txt)** – Lista dei soli hash file da utilizzare in combinazione con il tool HASHr

