Da: noreply@istruzione.it
Oggetto: MIUR - Sicurezza Informatica - ATTENZIONE A NUOVE MINACCE
Data: 01/04/2020 09:41:54

Gentile utente,

il CERT-PA ci segnala diverse tipologie di nuove minacce in essere in questi giorni.

1) Nuova campagna di malspam volta a veicolare il malware Ursnif.

La email veicolo della minaccia ha come oggetto "Invio fattura" e invita le vittime a scaricare il file allegato con le "procedure di sicurezza da attuare in fase di consegna della merce".

NON APRITE GLI ALLEGATI DI QUESTA TIPOLOGIA DI EMAIL

2) Nuove campagne di diffusione di malware sfruttano il crescente uso delle piattaforme come ZOOM e TEAMS.

Approfittando dell'uso più frequente delle suddette piattaforme di videoconferenza, utenti malintenzionati inviano file dannosi che utilizzano nomi come "zoom-us-zoom_##########" e "microsoft-teams_V#mu#D_##########" . L'utente che scarica questi file avvia InstallCore, un programma che tenta di installare applicazioni di terze parti potenzialmente indesiderate o dannose.

NON APRITE GLI ALLEGATI DI QUESTA TIPOLOGIA DI EMAIL

3) Falsi aggiornamenti di Google Chrome.

Molti siti WordPress sono stati presi di mira da criminali per veicolare malware. I siti web WordPress compromessi reindirizzano i visitatori verso un sito web creato ad hoc che invita gli utenti ad installare un importante aggiornamento di sicurezza per il browser Chrome. Se l'utente procede con il download scarica ed eventualmente installa un malware invece dell'aggiornamento di Chrome.

CHROME SI AGGIORNA AUTOMATICAMENTE, NON DATE SEGUITO AD AGGIORNAMENTI PROPOSTI TRAMITE ALTRI SITI WEB

4) Campagne di phishing.

E' stato osservato un importante incremento di attività di phishing che fanno leva su fantomatiche comunicazioni di vincite, apparentemente provenienti da grandi catene di supermercati (COOP, PENNY, BILLA, JUMBO, etc.), o su problemi di consegna da parte dei corrieri per la spedizione di prodotti tecnologici: un notebook o l'ultimo modello di smartphone. Fine ultimo del processo di phishing è quello di carpire i dati degli utenti ed in particolare gli estremi delle carte di credito.

NON DATE SEGUITO A COMUNICAZIONI DI QUESTO TIPO

E' possibile trovare ulteriori informazioni ai seguenti indirizzi:

https://www.cert-pa.it/notizie/campanga-malspam-ursnif-veicolata-in-italia-sfrutta-emergenza-coronavirus/

https://www.cert-pa.it/notizie/la-piattaforma-zoom-sfruttata-per-veicolare-malware/

https://www.cert-pa.it/notizie/campagna-malware-utilizza-falso-aggiornamento-google-chrome/

https://www.cert-pa.it/notizie/campagne-di-phishing-ai-danni-di-utenti-di-supermercati-e-corrieri/

Ribadiamo le seguenti raccomandazioni.