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.

Si raccomanda di non dare seguito all'apertura di file non attesi dalla dubbia provenienza o che giungono da caselle non note.

Non installate software soprattutto se a seguito di sollecitazioni via e-mail.
Non date seguito alle richieste di e-mail sospette.

Nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificate 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?

In caso di dubbio chiedete conferma ai vostri referenti.

Raccomandiamo inoltre, per quanto concerne il proprio PC di casa usato in telelavoro, di assicurarsi:

1) che il sistema operativo del proprio PC sia aggiornato

2) che il proprio PC sia dotato di antivirus e che questo sia aggiornato

3) che le proprie password siano sicure, ovvero complesse, non facilmente individuabili, diverse per servizi distinti e che afferiscono a sfera lavorativa e personale. Al momento della modifica delle password evitare di fare solo piccole modifiche come ad esempio numerazioni progressive ecc…

4) di eseguire il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa.

Grazie per la collaborazione

Ministero dell'Istruzione, dell'Università e della Ricerca

D.G. Contratti, Acquisti, Sistemi Informativi e Statistica