PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4657 di Lunedì 16 marzo 2020

Le truffe informatiche legate al Coronavirus

Le segnalazioni di Phishing e Malware della Polizia di Stato e postale che sfruttano la crisi legata al Coronavirus per colpire gli utenti.

Riportiamo alcune segnalazioni circa le truffe informatiche che circolano in questi giorni e che sfruttano l'emergenza da Coronavirus per colpire le persone con attività di Phishing e Malware. Le informazioni sono tratte dai siti della Polizia di Stato e della Polizia Postale.

Phishing: le truffe informatiche legate al Coronavirus

Sfruttando le preoccupazioni che il Coronavirus sta generando tra le persone, i criminali del web stanno approfittando di questo momento di vulnerabilità per colpire le ignare vittime con attività di Phishing legate al COVID-19.

L'ultima in ordine di tempo, scoperta dalla Polizia postale e delle comunicazioni, riguarda una campagna di frodi informatiche attraverso l'inoltro di email a firma di una tale dottoressa Penelope Marchetti, presunta "esperta" dell'Organizzazione mondiale della sanità in Italia. I falsi messaggi di posta elettronica, dal linguaggio professionale ed assolutamente credibile, invitano le vittime ad aprire un allegato infetto, contenente presunte precauzioni per evitare l'infezione da Coronavirus. Il malware, della famiglia "Ostap" e nascosto in un archivio javascript, mira a carpire i nostri dati sensibili.

Il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) della Polizia postale, aveva rilevato, subito dopo il diffondersi della paura per il Coronavirus, una campagna di false email, apparentemente provenienti da un centro medico e redatte in lingua giapponese, le quali, con il pretesto di fornire aggiornamenti sulla diffusione del virus, invitavano ad aprire un allegato malevolo che mirava ad impossessarsi delle credenziali bancarie e dei dati personali della vittima.

Successivamente, veniva scoperta un'altra attività di Phishing che invitava ad aprire un file "zip" contente documenti excel, che diffondeva un virus di tipo RAT, chiamato "Pallax". A seguito dell'inconsapevole click, questo pericoloso virus (venduto per pochi dollari negli ambienti più nascosti del darkweb fin dal 2019) consentiva agli hacker di assumere il pieno controllo del dispositivo attaccato, spiando i comportamenti della vittima, rubando dati sensibili e credenziali riservate, nonché, assumendo il controllo della macchina attaccata in maniera assolutamente "invisibile".

Gli specialisti della Polizia postale individuavano anche un altro virus RAT, dal funzionamento simile, che nascosto dietro un file chiamato CoronaVirusSafetyMeasures.pdf, assumeva il controllo del dispositivo infettato, trasformandolo, all'insaputa della vittima, in un computer zombie, gestito da remoto da un computer principale per effettuare successivi attacchi informatici in tutto il mondo.

L'invito della Polizia postale è di diffidare da questi e da simili messaggi, evitando accuratamente di aprire gli allegati che essi contengono e di segnalare eventuali trntativi di Phishing al Commissariato di P.S. online.

L'avviso (pdf)

Fonte: Poliziadistato.it

Coronavirus: nuova ondata di #phishing e #malware

Il Coronavirus non ferma i criminali del web, che non si fanno scrupoli ad approfittare del rischio di epidemia in corso per architettare nuove ed insidiose frodi informatiche.
Ancora una volta il Centro Nazionale Protezione Infrastrutture Critiche #CNAIPIC della #Polizia #Postale e delle Comunicazioni, è venuto a conoscenza di una nuova campagna mirata di phishing e malware legata al tema dell'epidemia da #Coronavirus (COVID-19).

In particolare è in atto un massivo invio di messaggi email e non solo, del malware infostealer AZORult.

Nella circostanza i criminali hanno spacciato la minaccia informatica per un'applicazione che mostra la mappa della diffusione del virus nel mondo: la GUI (Graphical User Interface) che risulta particolarmente verosimile a quella ospitata sui sistemi della Johns Hopkins University (ArcGIS).

Il virus AZORult, oltre a scaricare ulteriori minacce nelle macchine colpite, è in grado di raccogliere informazioni come nome, ID/password, numero della carta di pagamento, cryptovalute e altri dati sensibili presenti nei browser; alcune varianti consentono anche connessioni di tipo Remote Desktop Protocol (RDP).

L'invito della Polizia Postale è di diffidare da questi e da simili messaggi, evitando accuratamente di aprire gli allegati che essi contengono.
Per ogni utile informazione, la Polizia mette a disposizione il proprio "commissariato virtuale", raggiungibile all'indirizzo **www.commissariatodips.it**.

Fonte: Commissariatodips.it

www.puntosicuro.it