Risposte degli esperti alle domande dei partecipanti durante l'evento on line del 25 novembre - La sicurezza informatica nella pubblica amministrazione

Webinar 3. Social Engineering – Phishing e modelli

Esperti
Michele Petito (AGID)
Massimiliano Rossi (AGID)

Domande dei partecipanti durante l'evento on line

V.C.: ieri nel portale inPA c era un collegamento strano a telegram..

Risposta fornita in diretta da Michele Petito

A.C.: Come tinyurl, da evitare suppongo.

Risposta fornita in diretta da Michele Petito

M.C.: come individuare link malevoli presenti in servizi di URL shortest (p.e., bit.ly) rispetto a url corretti?

Risposta fornita in diretta da Michele Petito

E.B.: url che iniziano con protocollo https come si distinguono da quelli clonati malevolmente?

Risposta fornita in diretta da Michele Petito

P.M.: Un modo abbastanza sicuro di verificare una URL di cui non si è sicuri è di aprirla in una macchina virtuale (isolata dal sistema principale) e con un sistema operativo Linux, meglio ancora se "hardened". Non è perfetto ma è ragionevolmente sicuro per gran parte degli utilizzi.

Risposta fornita in diretta da Michele Petito

M.M.: Come ci si comporta quando le url nelle mail sono riscritte dal software del firewall?

Risposta fornita in diretta da Michele Petito

A.C.: Eventualmente, avete in Cert-Agid personale di supporto per un test con Gophish?

Risposta fornita in diretta da Michele Petito

B.M.: potrebbe spiegare se usando telegram (usata con bot per segnalazione al comune da parte dei cittadini) ci sono modalità sicure da attivare? Grazie

Risposta fornita in diretta da Michele Petito

R.C.: una banca spagnola BHDLEON mi ha mandato diverse email. come se io avessi un conto e facessi prelievi poi l'ho travata su FB e ho mandato un messaggio privato in cui ho informato che sbagliavano persona. non ero certa fosse fishing. la domanda è: ho compromesso qualcosa mandando un messaggio privato contattandoli su fb ? loro hanno risposto dicendo che mi avrebbero cancellato dall'archivio

Risposta fornita in diretta da Michele Petito

A.C.: Ritengo molto utile effettuare dei test di conoscenza degli utenti (es. Gophish). Ricordo bene l'attacco alla Regione Lazio dello scorso luglio.

Risposta fornita in diretta da Michele Petito

L.D.R.: le tecniche di phishing sono sempre più sofisticate, non conviene mai cliccare su link che arrivano su messaggi o posta e poi valutare se è giusto o falso, meglio andare direttamente sulla home del sito che sembra aver indirizzato il messaggio, digitando l'URL originale

Risposta fornita in diretta da Michele Petito

L.R.: Gli URL a volte vengono riscritti dalle sandbox di antispam (come nel caso di LibraESVA)

Risposta fornita in diretta da Michele Petito

L.R.: Comunque LibraESVA non riscrive completamente gli URL, ma lo integra

Risposta fornita in diretta da Michele Petito

L.R.: LibraESVA: antispam e sandbox per posta elettronica

Risposta fornita in diretta da Michele Petito

G.R.: salve M. ho letto il file sulle criptovalute del link cert-agid.gov.it volevo sapere cosa ne pensa di esse e del bitcoin, ha mai investito o investirebbe mai?

Risposta fornita in diretta da Michele Petito

M.S.: dietro il pulsante accetta cookie è possibile che si nasconda un link malevolo?

Risposta fornita in diretta da Massimiliano Rossi

P.S.: Negli IOC di cert-agid c'è qualche link 'benevolo' da usare per test delle policy firewall senza creare danni?

Risposta fornita in diretta da Massimiliano Rossi

M.C.: x segmentazione rete LAn, intende creazione di Vlan?

Risposta fornita in diretta da Massimiliano Rossi

B.M.: Ma ci sono mail che possono essere pericolose anche se solo aperte su un pc?

Risposta fornita in diretta da Massimiliano Rossi

P.C.: Power shell riesce ad essere sfruttato anche se l'utente ha solo permessi user?

Risposta fornita in diretta da Massimiliano Rossi

M.C.: questo indirizzo http://6y8.me/9VdsKP potrebbe essere un falso indirizzo ?! come si verifica?! GRAZIE

Risposta fornita in diretta da Massimiliano Rossi

R.S.P.: una suite antispam come Barracuda può essere una buona difesa?

Risposta fornita in diretta da Massimiliano Rossi

B.M.: la posta elettronica certificata ha dei margini maggiori di sicurezza?

Risposta fornita in diretta da Massimiliano Rossi

C.C.: ma anche un allegato pdf potrebbe essere pericoloso?

Risposta fornita in diretta da Massimiliano Rossi

F.P: Ma comunque devo cliccare sul link nel pdf?

Risposta fornita in diretta da Massimiliano Rossi

E**.P.**: sussiste ancora la vulnerabilità SIMjacker?

Risposta fornita in diretta da Massimiliano Rossi

Domande che hanno avuto risposta in chat

F.V.G.: Esistono app sicure per smartphone/tablet, per verificare l'indirizzo reale a cui punta uno short url prima di cliccarci sopra? E servizi simili per pc?

D.B.: http://checkshorturl.com/

F.V.G.: grazie con il pc va bene. Conosci anche uno strumento più efficiente per smartphone?

D.B.: di app specifiche non so se esistono non ho mai approfondito. Cmq http://checkshorturl.com/ è utilizzabile anche da smartphone via browser

M.M.F.: Il sito http://checkshorturl.com/ è valido per testare le short url?

D.B.: è valido per capire la reale landing page di una short url

D.B.: come se cercate in rete ci sono molti servizi che fanno ciò

Risposte degli esperti alle domande dei partecipanti rimaste inevase durante l'evento on line

M.C.: prima mi estato scritto: salve M. il suo pacco e stato trattenuto presso il nostro centro spedizione …si prega di seguire le istruzioni qui http://6y8.me/9VdsKP

Per essere sicuri della bontà o meno del link occorre analizzare l'sms/mail ricevuta. A tal proposito invitiamo a mandarla a malware@cert-agid.gov.it