Risposte degli esperti alle domande dei partecipanti rimaste inevase durante l'evento on line del 18 novembre - La sicurezza informatica nella pubblica amministrazione

Webinar 2. Malware rivolti alla PA e Cyber Threat Actor

Esperti

Luca Lusini (AGID)

Vito Lucatorto (AGID)

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

A. C: Office365 nella console amministrativa online (Exchange), consiglia di non fare mai scadere le password e reclamizza questa pratica come sicura. Cosa c'è di concreto?

Probabilmente l'idea di Office365 è di avere un cambio di password molto frequente senza attendere la scadenza definitiva. Cambiare password frequentemente è un attività più sicura ma più onerosa.

L. R.: Al di là del vendor, da ciò che leggo il classico antivirus basato solo sulle firme virali non basta più, serve un prodotto che con tecniche di machine learning sia in grado di analizzare i comportamenti sospetti e sia in grado di reagire velocemente, oltre ad avere sistemi che consentano di capire ciò che sta avvenendo sulla propria rete

Le firme antivirus rimangono ancora un meccanismo molto valido per il riconoscimento dei malware. Riguardo i sistemi di machine learning è una tecnologia molto promettente.

A. C.: Le macro servono ancora, soprattutto nelle piccole strutture con pochi mezzi a disposizione.

Ogni realtà si assume i rischi che è disposta a sostenere. Sicuramente uno dei principali vettori di malware è utilizzare macro malevole.

R. A.: Diciamo che è l'ottimo è una difesa stratificata e distribuita, non una semplice difesa perimetrale come il firewall o gli ids. Servono strumenti evoluti per difendersi da tecniche di attacco evolute

Il concetto di difesa on depth è un nuovo paradigma sicuramente più efficace che si possa utilizzare. Per poterlo applicare è necessario avere competenze tecniche e risorse economiche più ampie. Il ritorno di investimento dipende dal fattore di rischio legato all'amministrazione.

L. D.: serve soprattutto un comportamento attento e vigile nella navigazione e nell'accesso ai contenuti (web, mail, doc allegati), in quanto l'innalzamento esagerato di difese può ingessare la macchina fino a rallentarla talmente nei controlli che non ci si può più lavorare

È necessario un equilibrio tra difesa e facilità di utilizzo. La sicurezza a scapito dell'usabilità non è sicurezza.

R.A.: E la prima di queste difese è certamente l'attenzione e la competenza delle persone

La consapevolezza e attenzione delle persone è la prima delle difese più efficaci.

M.C.: Come mi accorgo se nel mio pc e entrato un Banking Trojan ?

Se hai sms/notifiche push relativi ad addebiti non previsti o accessi non autorizzati sulla tua banca, può essere sintomo di infezione. Controllare regolarmente i movimenti bancari sana ogni dubbio.

E. Z.: Qualche caso di violazione per le credenziali di SPID o CIE ?

A livello di phishing non vi è evidenza che ci sono compromissioni del servizio CIE o SPID. Tuttavia macchine compromesse possono portare alla violazione di SPID o CIE.

F. V.: Qualche esempio di validi password manager? Keepass quindi non va bene? Ci si può fidare dei servizi cloud?

Keepass è un password manager valido cosi come Bitwarden. Alcune funzionalità come quella di Auto-type sono da usare con cautela perché potrebbero essere non immuti a Keylogger.

F. M.: le violazioni sono possibili anche su PC connessi ad un dominio?

Si. La federazione a domino non è garanzia di maggiore sicurezza.

G. P.: Quando si utilizzano le cartelle condivise, viaggiano lo stesso i malware?

Si. Ad esempio Trickbot o Ransomware odierni utilizzano le cartelle condivise per muoversi tra un PC e l'altro modificando i file presenti.

W. C: quale software si può utilizzare per scansionare la rete ed i computer a titolo gratuito e decifrabile

Esistono molteplici strumenti gratuiti e open-source (cfr. github). Chiaramente sono strumenti che richiedono un minimo di conoscenza oppure affidarsi a servizi a pagamento.

D. G.: Quanto è sicuro il psw manager di google?

Se si intende il Password Manager di Chrome, questo non offre nessuna protezione contro malware che si occupano di rubare password.

M. D. C.: buongiorno per quanto riguarda i ransomware ed il dato compromesso, vorrei capire quanto è sicuro il backup su One drive e se risultano casi di dati cifrati su One drive.

OneDrive è un servizio di sincronizzazione di file e cartelle. In caso di cifratura dei dati locali, questi verrebbero sovrascritti. È sempre bene consultare il supporto ufficiale per configurazioni specifiche o approfondimenti tecnici.

D. D. forse la nostra amministrazione dovrebbe fornircene uno di password manager certificato per lo smartworking e anche per quando stiamo in ufficio

Potrebbe essere una buona pratica, tuttavia l'utilizzo di un password manager è consigliato anche fuori dall'ambito lavorativo.

S. B.: Ma a loro volta, i password manager, non possono essere dei raccoglitori maligni di password?

È possibile. È necessario affidarsi a quelli più conosciuti e possibilmente open-source.

R. A.: Mi permetto un suggerimento ai colleghi: la sicurezza informatica non è solo un software o una buona pratica. Richiede preparazione e aggiornamento, non improvvisatevi o non limitatevi ai consigli, è preferibile rivolgersi a professionisti della materia.

M. C. : In effetti come dicevi te A., ho abilitato nella barra arancione sopra il file world....grazie rischio che ora mi prendano i dati delle carte?!

In questo caso ti consigliamo una scansione antivirus aggiornato e cambiare le password da un altro dispositivo per maggiore sicurezza.

C. R.: Forse la domanda sull'account per salvare password era per l'account di Google. Meglio non usarlo?

Il Single-Sign-On è di fatto un meccanismo sicuro grazie ai meccanismi di Google. Il Password Manager di Chrome, questo non offre nessuna protezione contro malware che si occupano di rubare password.

M. C.: come verificare se ho subito un attacco bancking trojan con Ursnif?!Grazie

Se hai sms/notifiche push relativi ad addebiti non previsti o accessi non autorizzati sulla tua banca, può essere sintomo di infezione. Controllare regolarmente i movimenti bancari sana ogni dubbio.

L. B.: DOMANDA: meglio avere policy di password lunghe minimo 10 caratteri oppure di almeno 8 caratteri con complessità (almeno 1 lettera minuscola, 1 maiuscola, 1 carattere speciale, 1 numero) D'accordo poi che meglio ancora minimo 10 caratteri e complessità, ma per impostare a step successivi

Meglio una password da 10 caratteri. Da un rapido calcolo approssimativo, 62^10 + maggiore di 72^8. Però è sempre meglio seguire delle linee guida che tengono conto dell'usabilità.

M. C.: come mi accorgo se nel mio pc e entrato un banking trojan, come posso fare

Se hai sms/notifiche push relativi ad addebiti non previsti o accessi non autorizzati sulla tua banca, può essere sintomo di infezione. Controllare regolarmente i movimenti bancari sana ogni dubbio.

M. C.: ? se l'url è ridotta usando il servizio bit.ly , come si fa

Visitare una pagina quasi mai comporta conseguenze. Occorre non interagire con la pagina stessa o aprire allegati o inserire dati personali. Se aggiunge il carattere "+" alla fine della URL, bit.ly le farà vedere la URL estesa.

A. P.: Defender mi sembra non possa essere utilizzato nelle aziende ma solo ad uso personale

Si consiglia di fare riferimento ai termini e condizioni del prodotto.

L. R.: @A. P.: Microsoft rilascia una versione di Defender (chiamata se non erro Windows Defender APT) pensata proprio per la aziende, e a quanto leggo pare un buon prodotto, concordo che il normale Windows Defender è adatto solo per uso personale.

A. A.: Vorrei chiedere se la casistica dei virus noti include anche l'attivazione non voluta della webcam

Abbiamo rilevato malware in grado di utilizzare la webcam sia su PC sia su Mobile.

Domande che hanno avuto risposta in chat

G. R: https://docs.italia.it/AgID/documenti-in-consultazione/lg-cert-regionali/it/bozza/processo-di-gestione-degli-incidenti-di-sicurezza.html chi aggiorna docs.italia.it ?

Il link da lei indicato riguarda la messa in consultazione pubblica delle LG sui cert regionali. Il sito viene utilizzato per la messa in consultazione pubblica di tutte le LG di AgID.

G. R.: Certo, intendevo che rispetto a quanto ci stiamo dicendo quel documento andrebbe aggiornato :-D

Lo stato del documento (bozza) è alla data di pubblicazione. Il contenuto sarà poi aggiornato quando le LG verranno pubblicate in gazzetta ufficiale terminato iter art.71 del CAD

F. G.: quale password manager consiglieresti?

Keepass è un password manager valido cosi come Bitwarden. Alcune funzionalità come quella di Auto-type sono da usare con cautela perché potrebbero essere non immuti a keylogger.

G. R.: Se può interessare, utilizziamo https://monitor.shodan.io/ per essere avvisati tempestivamente in caso vengano rilevate vulnerabilità

È sicuramente una buona soluzione. Sarebbe consigliato adottare un processo di patch managment / early warning.

D. G. : Ma infatti proprio perché siamo noi esseri umani il vero problema sarebbe interessante una puntata con esempi pratici di gestione e conservazione sicura delle password e dei dati al di là di ogni firewall o antivirus

Grazie del feedback. Ci pensiamo.