AGID Agenzia per l'Italia Digitale

Computer Emergency Response Team Pubblica Amministrazione CERT-PA

Bollettino: Azioni utili per contrastare l'esecuzione e la diffusione di malware

ID: CERT-PA-B006-191119 Data: 19/11/2019

AVVERTENZE

Il documento ha lo scopo di fornire il quadro di riferimento degli scenari di minaccia rilevati dal CERT-PA, al fine di consentire tempestive valutazioni di impatto sui propri sistemi informativi e implementare le opportune misure di contrasto/contenimento dei rischi correlati.

Il CERT-PA, nell'erogare questo servizio al meglio delle proprie possibilità, si avvale di propri fornitori e di fonti pubbliche disponibili in Rete, individuati e selezionati tra i più autorevoli organismi di sicurezza, aziende specializzate e fornitori di tecnologie, al fine di garantire alla comunità di riferimento – con la massima accuratezza, affidabilità e tempestività possibile – le informazioni utili per la prevenzione e la gestione degli incidenti di sicurezza informatica.

Non è consentito far uso di queste informazioni per finalità differenti da quelle sopra indicate.

La presenza di riferimenti che vengono effettuati mediante l'utilizzo di collegamenti ipertestuali (link) non costituisce una raccomandazione del CERT-PA verso il soggetto richiamato, ma unicamente uno strumento per facilitare il rapido recupero di informazioni utili.

Indice

Sommario 2
1. Azioni utili per contrastare l'esecuzione e la diffusione di malware 2
Premessa 2
Come mitigare le minacce e gli attacchi veicolati tramite posta elettronica 3
- Disattivare l'esecuzione di VBScript 4
- Disattivare PowerShell 4
- Disattivare Windows Script Host 5
- Disattivare l'esecuzione delle Macro 7
- Disattivare JavaScript 10

Andamento sulla diffusione di nuove tipologie di malware 13
Avvertenze 14

Sommario

Il CERT-PA, a fronte della sempre maggior diffusione di campagne miranti alla diffusione di malware attraverso l'utilizzo dei canali di posta ordinaria (PEO) e posta certificata (PEC) vuole suggerire in questo documento alcune configurazioni che è possibile applicare alle postazioni di lavoro per contrastare più efficacemente questi tipi di attacco.

1. Azioni utili per contrastare l'esecuzione e la diffusione di malware

Il documento, rivolto ad un'ampia platea di utilizzatori, ha lo scopo di sensibilizzare circa i potenziali rischi e conseguenze legate alla diffusione di malware. Nel documento, il CERT-PA riporta una serie di mitigazioni - utili in termini di prevenzione - per limitare l'effetto degli attacchi cibernetici veicolati tramite i canali di posta elettronica. Le restrizioni, attuabili tramite specifiche configurazioni del software, si riferiscono agli ambienti **desktop** basati sul sistema operativo Microsoft Windows, che **per diffusione e contesto di utilizzo** sono **maggiormente esposti** a questa tipologia di attacchi informatici.

Premessa

Le caselle di posta elettronica, sia certificate (PEC) che ordinarie (PEO), sono veri e propri canali su Internet verso i quali è possibile indirizzare attacchi informatici. In questo specifico contesto, le principali e più diffuse minacce sono rappresentate da eventi di *phishing* e distribuzione di vari tipi di malware, come i *ransomware* e i *trojan,* specializzati nel **carpire dati ed altre informazioni sensibili** tra cui le credenziali d'accesso ai diversi servizi telematici.

Se nel primo caso (ransomware) il pericolo, in caso di attacco, è rappresentato dall'impossibilità di accedere ai dati personali, nel secondo (trojan), una volta compromesso il sistema operativo, possono innescarsi - in modo silente - **una serie di effetti e rischi collaterali**. Gli eventi cibernetici che ne conseguono indicano che la compromissione, ove provocata da queste tipologie di malware, possa innescare di fatto l'esposizione di informazioni e credenziali di servizi on-line **come la posta elettronica** associata o acceduta dalla postazione affetta dal malware. Ciò produce, nelle ipotesi peggiori, l'utilizzo fraudolento della postazione di lavoro, fornendo l'opportunità ai criminali di lanciare delle campagne di invio di comunicazioni, anche massive, volte alla **proliferazione di codice malevolo** a danno di altri sistemi e destinatari che vengono, a loro volta, coinvolti dal malware inviato alle caselle di posta elettronica.

A partire dal 2018, il CERT-PA ha individuato diverse campagne di diffusione di Trojan, *bancari* o *info stealer*, a danno di utenti possessori o utilizzatori di caselle PEC. Nella maggior parte delle occasioni i vettori sono caselle di posta (mittenti) compromesse ed utilizzate all'insaputa dei titolari. Da queste, gli attaccanti possono condurre **pericolose azioni** che approfittano dalla fiducia comunemente riposta in un mittente PEC, un servizio di posta generalmente ritenuto non soggetto a problematiche di sicurezza. Anche questa considerazione ha favorito il susseguirsi di eventi, creando un pericoloso effetto di amplificazione sulle caselle compromesse PEC che ha permesso di **riutilizzare le informazioni carpite per colpire destinatari specifici o casuali**. Tra questi elementi ci sono tipicamente contatti, riferimenti, documenti in uso nel contesto lavorativo o risposte a comunicazioni pregresse intercorse tra le parti. Tutte informazioni appositamente utilizzate dagli attaccanti per **aumentare i danni arrecati** ed ingannare i destinatari, per spingerli ad aprire un allegato appositamente predisposto e mettere in pericolo la sicurezza dei dati e l'integrità del sistema operativo.

Le statistiche attuali indicano che la quasi totalità degli attacchi monitorati che utilizzano i canali di posta elettronica e contenuti/allegati nocivi hanno come bersaglio primario le postazioni che utilizzano il sistema operativo Microsoft Windows, vista la sua diffusione e la possibilità di utilizzare le sue **specifiche funzionalità offerte dai programmi di produttività individuale per garantire l'esecuzione del codice malevolo**. Al fine di produrre una capillare proliferazione, le metodologie utilizzate per diffondere malware si basano principalmente sull'utilizzo fraudolento di allegati in grado di essere processati automaticamente dal sistema operativo, quando queste funzionalità sono state attivate o in fase di configurazione del sistema o quando l'utente stesso innesca l'elaborazione tramite apertura dell'allegato stesso.

Come mitigare le minacce e gli attacchi veicolati tramite posta elettronica

Esistono buone pratiche comportamentali e tecnologiche per tutelare il patrimonio informatico e, di conseguenza, mitigare la proliferazione del malware quindi impedire che i propri dati - personali o di lavoro - cadano nelle mani sbagliate e possano essere riutilizzati in modo illecito da terzi.

Le azioni di contrasto attuabili possono spaziare su più livelli e coinvolgere diversi elementi, ma principalmente si basano su:

- La **percezione del problema;**
- Le **risorse tecnologiche disponibili**.

Nel primo caso, si può aumentare la **capacità di individuare le minacce intervenendo in termini di prevenzione**, grazie ad attività indirizzate alla **formazione e sensibilizzazione del personale**. Addestrare l'utente finale rappresenta la miglior barriera per bloccare una possibile minaccia; quando ciò non accade è proprio l'interazione dell'utente stesso a dare seguito alla minaccia, permettendo l'avvio della catena di infezione del malware che consente la compromissione del sistema operativo.

Il CERT-PA, per informare la sua utenza sugli eventi cibernetici in atto, diffondere nozioni sui pericoli e indirizzare verso l'adozione di buone pratiche di utilizzo, realizza contenuti informativi come news, bollettini e pillole informative. Si tratta in generale di contributi utili **per rispondere all'esigenza di sensibilizzare l'utenza di riferimento** sul tema della sicurezza.

Sempre in termini di prevenzione, un'ulteriore azione di contrasto al malware veicolato tramite PEC e PEO riguarda **l'attivazione di configurazioni da adottare in specifici ambiti di utilizzo**. Ove non fosse possibile utilizzare tecnologie o servizi specifici lato utente per fronteggiare le minacce, è possibile adottare **principi più restrittivi di utilizzo per ridurre la superficie d'attacco** verso un sistema operativo. Questo approccio, che si realizza limitando le interazioni tra l'utente finale e il malware, si basa sulla disabilitazione preventiva di alcune funzionalità, spesso non direttamente utilizzate, ma che riducono l'esposizione alle minacce informatiche più comuni come quelle che possono nascondersi negli allegati o nei collegamenti verso risorse Internet (i cosiddetti *link*) contenuti nei messaggi di posta elettronica.

Con particolare riferimento a questo esclusivo contesto di applicazione, Il CERT-PA suggerisce di adottare, ove possibile, delle configurazioni utili ad innalzare il livello di protezione di quei PC che sono **particolarmente esposti al rischio in quanto destinati alla consultazione delle caselle di posta elettronica PEC e PEO,** in particolare quelle pubblicamente note o riferibili a caselle di servizio come quelle che hanno finalità di contatto o registrazione.

Si riportano di seguito le azioni che è possibile intraprendere sulle configurazioni del sistema per limitare l'esecuzione delle più comuni tipologie di codice malevolo diffuso via posta elettronica:

• Disattivare l'esecuzione di VBScript

VBScript è un linguaggio di scripting sviluppato da Microsoft che si è ampiamente diffuso nello sviluppo web ed è stato appositamente integrato in Internet Explorer.

Disattivare VBScript in Internet Explorer

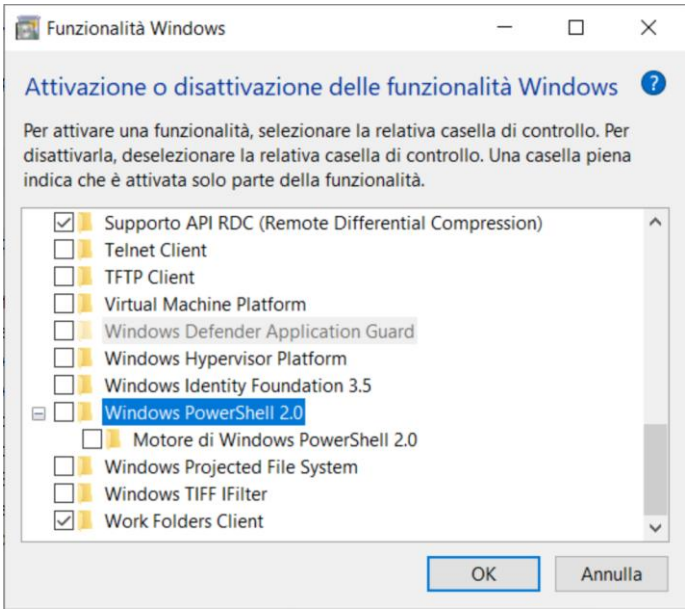
Per disabilitare VBScript in Internet Explorer 11, 10 e 9, si invita alla consultazione dell'articolo prodotto da Microsoft in lingua inglese o in italiano. La risorsa fornisce le indicazioni necessarie oltre ad un pacchetto (fix) la cui esecuzione permette di disattivare VBScript in Internet Explorer 11 per l'area Internet e per l'area dei siti con restrizioni.

Nota: Microsoft con il rilascio cumulativo di aggiornamenti, ha di recente provvedendo a disattivare VBScript limitatamente ad Internet Explorer 11, pertanto la disattivazione sulle altre versioni deve essere gestita autonomamente e in modo manuale.

• Disattivare PowerShell

Powershell è un **interprete dei comandi** utilizzabile da riga di comando (CLI) per l'esecuzione di operazioni complesse e di una serie di componenti progettate per sfruttare le caratteristiche dell'ambiente Windows. Anche il malware sfrutta script eseguiti tramite PowerShell e i suoi comandi possono essere inclusi in script malevoli. Alcuni attacchi specifici tendono ad utilizzare tecniche "*PowerShell-based*" particolarmente sofisticate anche in campagne di malware "*fileless*", dove nessun file viene memorizzato su disco e il codice dannoso va ad inserirsi, tramite la console, nella memoria RAM vanificando spesso le soluzioni di sicurezza tradizionali basate sul controllo delle firme dei file.

E' pertanto consigliabile disattivare PowerShell sui sistemi maggiormente o direttamente esposti alle consuete minacce. Questa opzione viene gestita tramite la voce "*Funzionalità Windows*", sita nel pannello di controllo, deselezionando la casella relativa a **Windows PowerShell 2.0** come mostrato nella figura seguente:



Nota: la disabilitazione del motore PowerShell non comporta impatti negativi sulle funzionalità native del sistema ma è bene sapere che alcune APP utilizzano ancora la PowerShell 2.0 nonostante sia in atto un processo di migrazione ad una versione più recente. Sebbene questa funzionalità sia già stata deprecata, rimarrà comunque attiva in Windows 10.

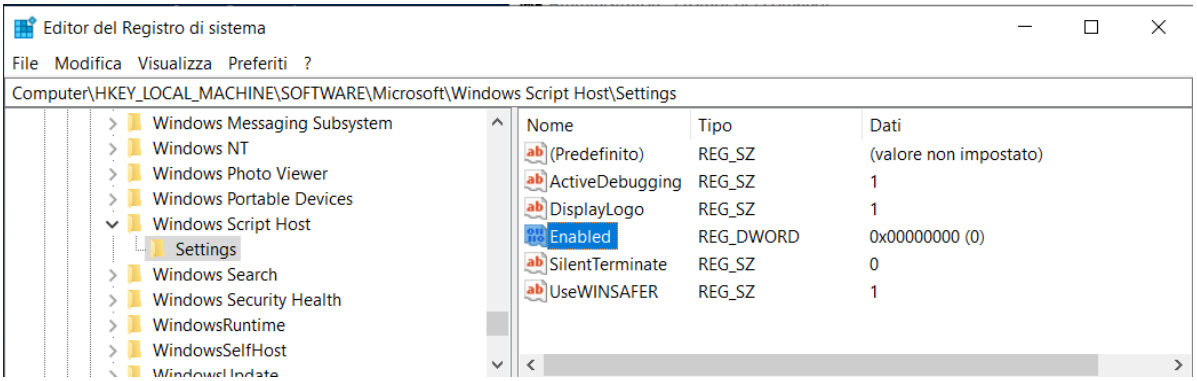
• Disattivare Windows Script Host

Windows Script Host (o WSH) è un linguaggio di scripting fornito in dotazione a tutte le principali distribuzioni di Windows e Windows Server a partire da Windows 98. La disabilitazione di questa funzionalità **impedisce l'esecuzione di file con estensione .VBS** (VBScript) che sono solitamente più potenti e versatili rispetto ai file batch (.bat) ma, per contro, la versatilità del Windows Script Host ha spinto i "malware writers" a sfruttarne i vantaggi per creare virus informatici e malware.

Su piattaforma Windows, per disattivare l'interprete di questo linguaggio, è necessario aggiungere una chiave di registro, valore DWORD dal nome "*Enabled*" settando il valore esadecimale a "*0*", al percorso seguente:

- *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings*

Il risultato, ad operazione conclusa, è rappresentato nella figura seguente:



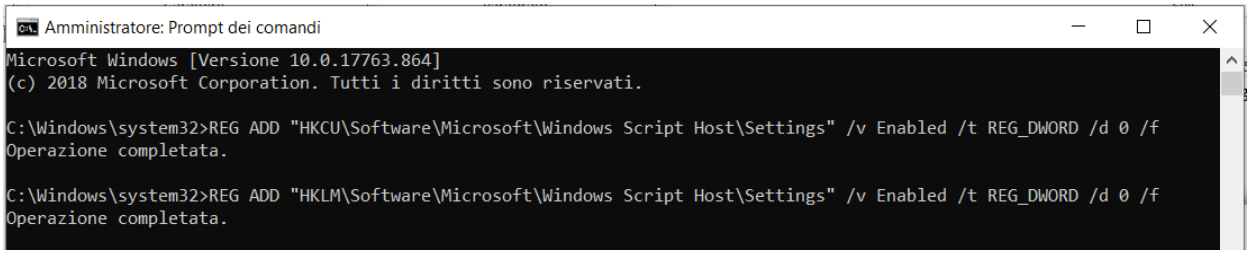
Come ulteriore alternativa, è possibile applicare la stessa chiave utilizzando il prompt dei comandi (CMD), con diritti amministrativi, lanciando il comando seguente:

- *REG ADD "HK**LM**\Software\Microsoft\Windows Script Host\Settings" /v Enabled /t REG_DWORD /d 0 /f*

Per limitare la disattivazione del componente a livello dell'utente sarà necessario agire verso il percorso:

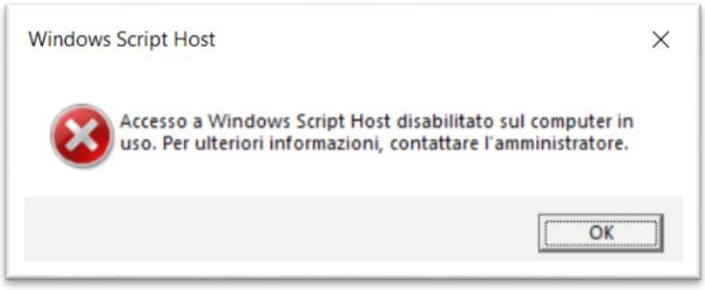
- *REG ADD "HK**CU**\Software\Microsoft\Windows Script Host\Settings" /v Enabled /t REG_DWORD /d 0 /f*

Il risultato dell'operazione è mostrato nella figura seguente:



Un articolo di riferimento della community Webroot illustra le diverse modalità per disabilitare WSH.

Verifica: Per verificare la corretta applicazione del blocco, è possibile creare un file .vbs provando ad eseguirlo. Se Windows Script Host è stato correttamente disabilitato, l'esecuzione del file viene esclusa con il seguente messaggio di errore:



Nota operativa sulle limitazioni

La disabilitazione di Windows Script Host inibisce l'esecuzione di file con estensione **.vbs, .vbe, .js, .jse, .wsf** e altre tipologie di script che sono **largamente utilizzate come allegati nelle campagne di diffusione malware**. Nel normale contesto lavorativo la disabilitazione di *Windows Script Host* non comporta reali limitazioni operative e pertanto, considerato l'elevato grado di diffusione di allegati .vbs, si consiglia la disattivazione dei tale linguaggio.

• Disattivare l'esecuzione delle Macro

Le macro sono delle mini applicazioni che si realizzano all'interno di Microsoft Office con il programma *Visual Basic for Application* che permettono di automatizzare una serie di funzionalità. Sono normalmente utilizzate soprattutto all'interno dei fogli di calcolo di Excel ma possono essere realizzate anche per altri prodotti Office. Dal momento che sono sviluppate con codice VBA è possibile utilizzarle anche per fini malevoli. Negli ultimi periodi si nota una tendenza nell'offuscare pesantemente il codice delle macro, attività che complica i controlli di sicurezza atti a verificare la natura del codice. Nonostante i vari produttori di software abbiano nativamente disattivato l'esecuzione delle macro, apponendo un avviso di sicurezza ove esse fossero presenti, un utente poco attento o che considera fidato il mittente, può superare l'avviso accettando l'esecuzione della macro che, qualora malevola, andrebbe a avviare la catena di infezione.

Di seguito le varie possibilità per disabilitare le Macro di Office:

1. **Disabilitare le macro tramite Group Policy Editor**

Eseguire "gpedit.msc" navigando fino al settaggio seguente:

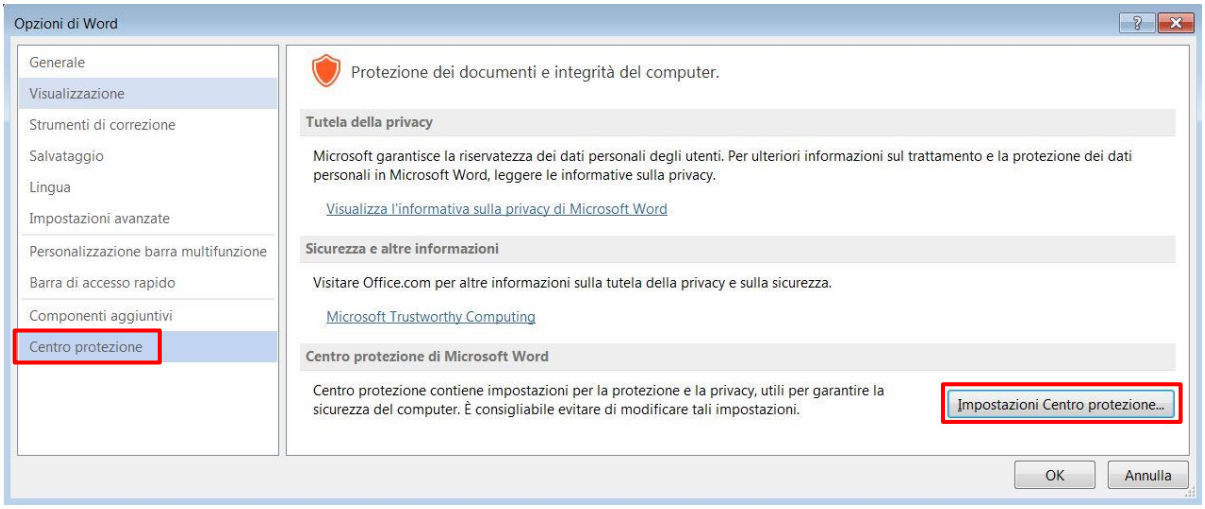
- *Configurazione utente*
- *Modelli amministrativi*
- *Microsoft Word 20xx (dove per xx si indica l'esatta versione di MS Office in uso)*
- *Opzioni Word*
- *Sicurezza*
- *Trust Center*

Fare doppio click su **blocca l'esecuzione delle macro nei file di Office da Internet**, abilitando la funzione.

2. **Cambiare le impostazioni delle macro in Centro protezione**

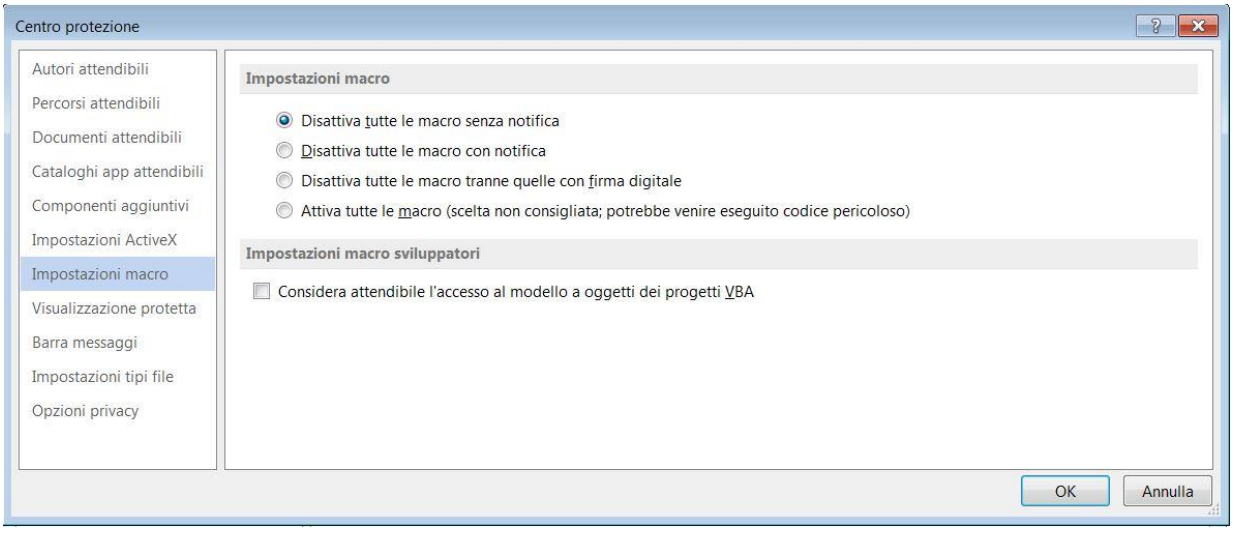
Le impostazioni delle macro sono reperibili nel Centro protezione. Se tuttavia si opera in un'organizzazione la modifica può essere gestita solo dall'amministratore di sistema.

- Fare clic sulla scheda "File".
- Fare clic su "Opzioni".
- Fare clic su "Centro protezione" e quindi su "Impostazioni Centro protezione".



- In "*Centro protezione*" fare clic su *"Impostazioni macro"*.
- Eseguire le selezioni desiderate.
- Fare clic su "*OK*".

Nella figura seguente è illustrata l'area "*Impostazioni macro*" del "*Centro protezione*" dalla quale è possibile disattivare tutte le macro senza notifica.



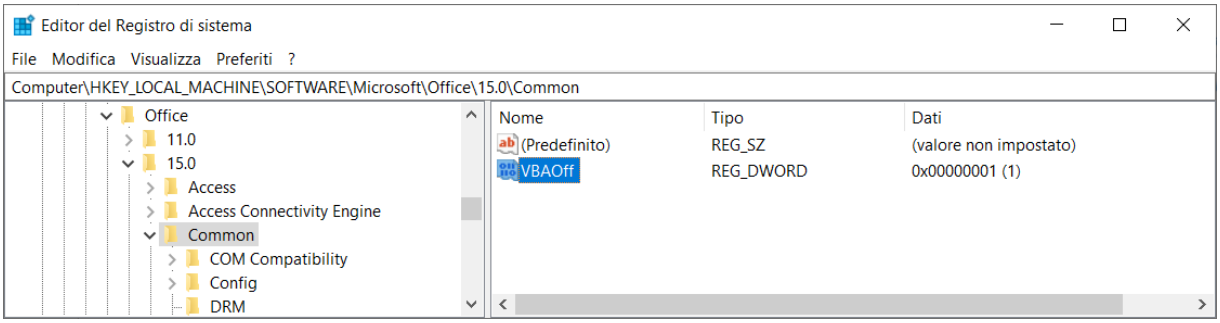
Importante: La modifica delle impostazioni delle macro in Centro protezione ha effetto solo nell'applicazione di Office corrente. Le impostazioni **non** vengono modificate per tutte le applicazioni di Office quindi occorre procedere singolarmente modificando l'autorizzazione per Excel e Word che sono le principali applicazioni della suite Office coinvolte in eventi di diffusione malware da allegati di posta elettronica.

3. Disabilitare le macro in Office tramite la modifica del registro di Windows

Per impostare il criterio di disattivare VBA (macro) per le applicazioni di Office, occorre definire la chiave DWORD denominata "**VBAOff**" applicando il valore su "***1***" nella sottochiave del registro di sistema in relazione alla versione di Microsoft Office installata:

Versione di Office	Percorso del registro di sistema
Office 2016	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\16.0\Common
Office 2013	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\15.0\Common
Office 2010	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\14.0\Common
Office 2007	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common
Office 2003	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\11.0\Common
Office XP	HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\10.0\Common

A titolo di esempio, il risultato dell'operazione di inserimento della chiave è mostrato nella figura seguente:

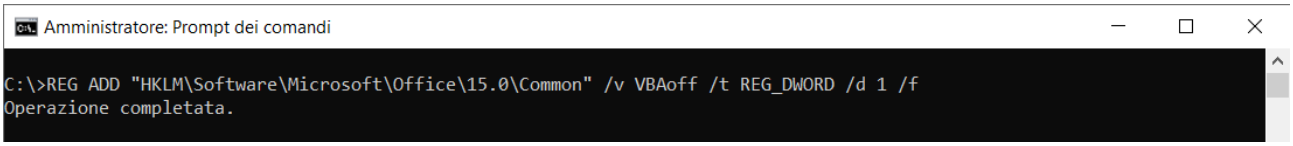


Nota: Agire tramite la chiave di registro di sistema di Windows impedisce a Microsoft Excel, FrontPage, Outlook, PowerPoint, Publisher e Word di utilizzare Visual Basic per le applicazioni.

È possibile inserire la chiave indicata anche tramite il prompt dei comandi (diritti amministrativi) nella forma:

- REG ADD "HKLM\Software\Microsoft\Office\1**X**.0\Common" /v VBAoff /t REG_DWORD /d 1 /f

Dove X è la versione di Office in uso. L'esecuzione del commando viene gestita come da immagine seguente:



Per ulteriori dettagli consultare la risorsa "Attivazione o disattivazione di macro nei file di Office" pubblicata da Microsoft in riferimento ad Office 365, Office Online, Office 2019, Office 2016, Office 2013, Office 2010, Office 2007.

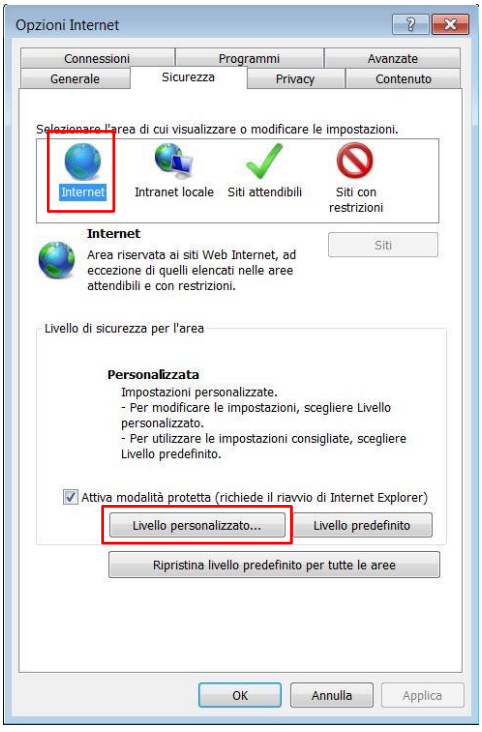
• Disattivare JavaScript

JavaScript è un linguaggio di programmazione sviluppato da Netscape Inc. e, nonostante il suo nome, non fa parte della piattaforma Java. E' uno dei componenti fondamentali per creare contenuti web insieme a HTML e CSS ed è supportato nativamente da tutti i moderni browser. JavaScript permette ai creatori di siti web di far eseguire codice agli utenti che visitano il sito, ragion per cui viene spesso abusato dai cyber criminali per il compimento dei loro attacchi. Uno dei più comuni scenari consiste nell'invitare un utente ad aprire un collegamento internet che punta verso un sito appositamente predisposto per far eseguire codice malevolo tramite il browser. Un altro contesto particolarmente insidioso è legato al salvataggio dei file JavaScript (.js), che vengono scaricati nel PC durante la navigazione. Navigando su un sito web precedentemente compromesso, tali file possono dare seguito a quello che viene definito un attacco "**drive-by**" - o "*drive-by download attack*" - che a sua volta innesca, con metodi differenti, una serie di attività malevole finalizzate alla compromissione del sistema operativo in uso. La disattivazione o la corretta gestione delle impostazioni lato browser, che consenta autorizzazioni specifiche per l'utilizzo di questo linguaggio, influisce nel mitigare un consistente numero di minacce cibernetiche anche rivolte ad attacchi di tipo zero-day.

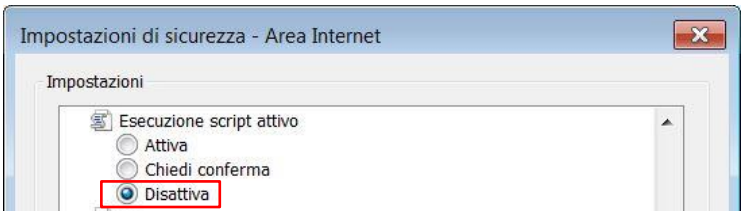
Disattivare JavaScript in Internet Explorer

Di seguito la procedura per inibire a tutti i siti Web all'interno dell'area Internet l'esecuzione di script in Internet Explorer:

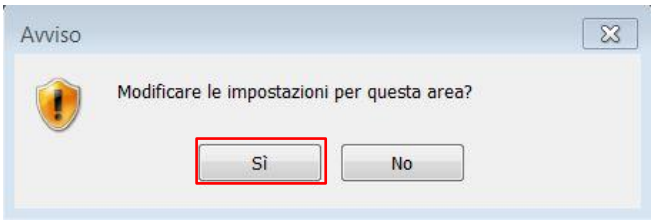
Nel menu del browser web, fare clic sull'icona "*Strumenti*" (simile a un ingranaggio) quindi selezionare "*Opzioni Internet*". Una volta aperta la finestra "*Opzioni Internet*", selezionare la scheda "*Sicurezza*" verificando che sia selezionata l'area "*Internet*" quindi fare clic sul pulsante "*Livello personalizzato...*".



Nella finestra di dialogo "*Impostazioni di sicurezza - Area Internet*", individuare "*Esecuzione script attivo*" facendo clic su "*Disattiva*" per impedire l'esecuzione degli script attivi:



Confermando la modifica tramite il pulsante "*Ok*" verrà mostrato un *messaggio di Avviso* nel quale viene richiesta un'ulteriore conferma per "*Modificare le impostazioni per questa area*".

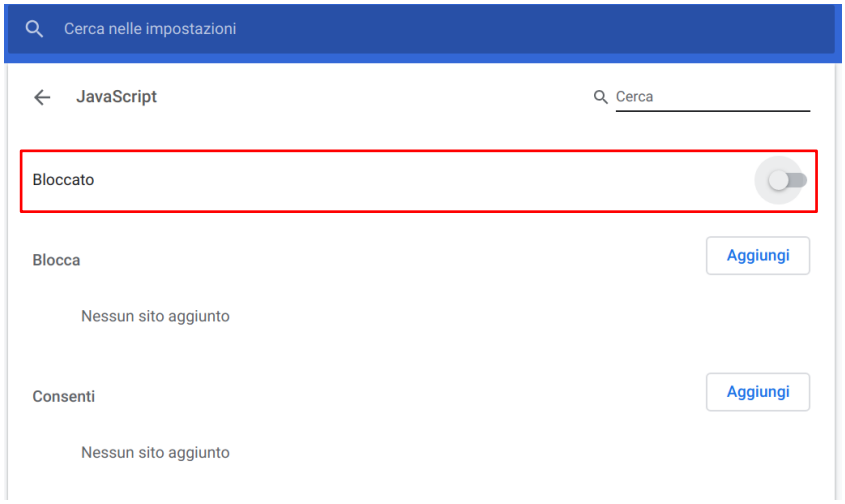


Fare clic su "*OK*" nella parte inferiore della finestra "*Opzioni Internet"* per chiudere la finestra di dialogo.

NOTA: Per consentire l'esecuzione di script per uno o più siti Web specifici è necessario lasciare disabilitata l'impostazione relativa allo scripting nell'area Internet quindi aggiungere i siti Web ritenuti sicuri all'area siti attendibili:

Disattivare JavaScript in Google Chrome

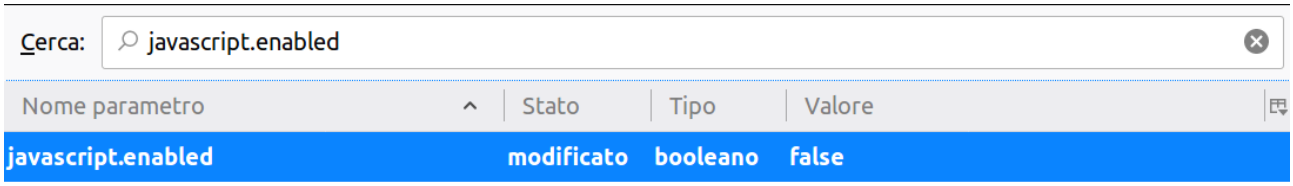
Per disabilitare JavaScript in Google Chrome, occorre accedere alle "*Impostazioni*", quindi alla funzionalità "*Avanzate*". Successivamente da "*Impostazioni contenuti*", individuare "*JavaScript*" quindi disabilitare la voce "*Consentita*" ottenendo una schermata simile a quella di seguito mostrata:



In alternativa è possibile digitare sulla barra degli indirizzi "*chrome://settings/content/javascript*" dando invio per accedere al medesimo pannello, quindi impostare l'opzione da "*Consentita*" a "*Bloccato*".

Disattivare JavaScript in Firefox

A partire da Firefox versione 23, per disabilitare JavaScript occorre digitare "*about:config*" nella barra degli indirizzi del browser e premere "*Invio*", quindi individuare nella lista la voce "*javascript.enabled*" e cliccare due volte per cambiare il valore in "*False*". Per rendere effettiva la modifica occorre riavviare Firefox.



Per riattivare JavaScript, sarà necessario impostare il valore di "*javascript.enabled*" sul valore "*True*".

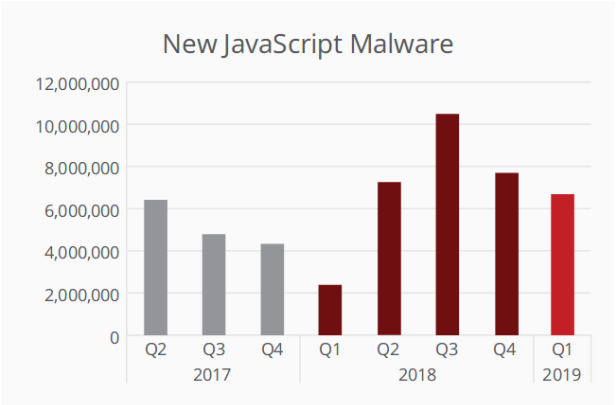
Nota sulle limitazioni derivate dalla disabilitazione di JavaScript:

Disabilitare JavaScript dal browser in uso **interferisce con le funzionalità erogate da quei servizi web** che utilizzano questo linguaggio di scripting. É pertanto possibile compensare l'eventuale limitazione:

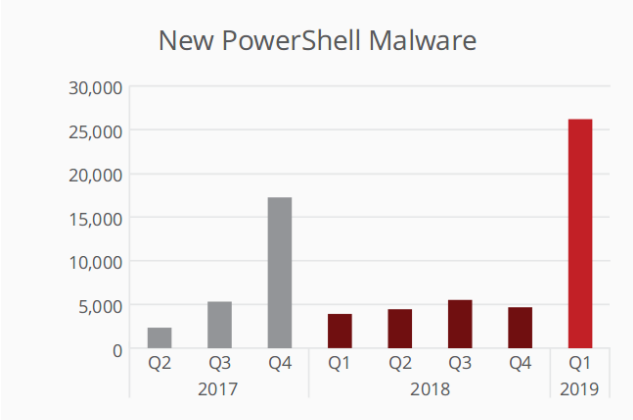
- Definendo una **lista dei siti consentiti** - quindi non soggetti alle limitazioni – dichiarando tutti i domini internet attinenti l'attività lavorativa o quelli fidati consultati per finalità personali;
- Dotando la postazione di lavoro di due distinti browser, impostando **come predefinito** quello con le **restrizioni** JavaScript ed utilizzando quello secondario - con JavaScript abilitato - per navigare sui siti internet consentiti in quanto legati all'attività lavorativa;
- Valutando l'utilizzo di specifici componenti aggiuntivi per Chrome o Firefox, prelevati dai rispettivi store, utili nel facilitare la gestione in tempo reale e puntuale dei JavaScript.

Andamento sulla diffusione di nuove tipologie di malware

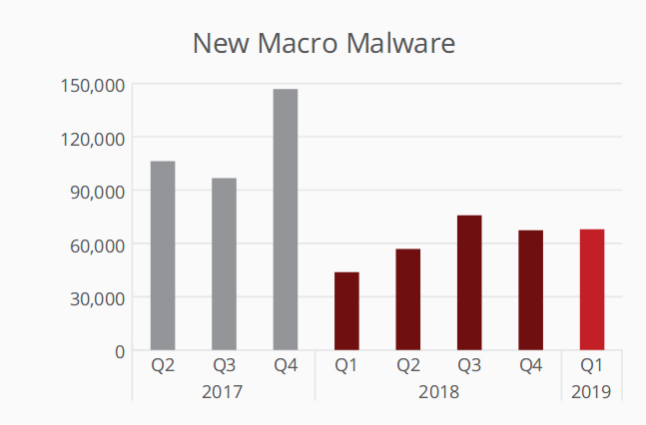
A titolo informativo, si riportano alcuni grafici estratti dal Report 2019 di **McAfee Labs Threats** nei quali di evince l'andamento, in termini di nuovi elementi rilevati, per le tipologie di malware che sfruttano le funzionalità oggetto del bollettino:



Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.



Source: McAfee Labs, 2019.

Avvertenze

Il presente bollettino contiene informazioni volte a sensibilizzare la percezione dei possibili pericoli che si celano nelle campagne di diffusione malware veicolati tramite i servizi di posta elettronica.

Pur trattandosi di informazioni di generico interesse, le configurazioni qui indicate si rivolgono in particolare a quei sistemi che hanno dirette interazioni con la posta elettronica istituzionale.

La valutazione sull'adozione degli accorgimenti suggeriti compete alle singole strutture mentre l'applicazione delle configurazioni è demandata al personale tecnico, qualificato ed autorizzato, di riferimento per ogni struttura.

Le azioni qui indicate non esulano dall'adozione delle pratiche volte al contrasto delle comuni minacce cibernetiche. Gli utilizzatori o titolari delle caselle PEC/PEO sono comunque tenuti, direttamente o indirettamente, ad adottare tutte le norme di sicurezza di solito raccomandate per mitigare i rischi associati all'uso della posta elettronica.

In tal senso, le indicazioni sono:

1. Modificare le credenziali delle caselle, con cadenza trimestrale, adottando requisiti di complessità;
2. Non ignorare eventuali attività sospette rilevate, in ingresso o in uscita, dalle caselle;
3. Al manifestarsi di una sospetta anomalia o attività legata ad accessi non autorizzati in una casella, provvedere subito a cambiare la password del servizio, quindi allertare il supporto tecnico di riferimento;
4. Utilizzare la protezione di un antivirus accertandosi che sia sempre attivo ed aggiornato e non ignorando la presenza di avvisi di sicurezza;
5. Eseguire periodicamente una scansione antivirus della propria postazione/dispositivo ed in particolare degli allegati che si desidera aprire;
6. Se si ritiene di aver aperto un allegato non sicuro, eseguire una scansione AV completa quindi utilizzare, per ulteriore accertamento, un antivirus esterno come i "rescue disk" che permettono di sfruttare un'unita CD, DVD, USB per esaminare il sistema dall'esterno;
7. Accertarsi che il sistema operativo abbia tutti gli aggiornamenti di sicurezza rilasciati e che siano attivi gli "Aggiornamenti Automatici", in modo da garantire l'applicazione delle correzioni di sicurezza non appena disponibili;
8. Evitare di cliccare su un link quando punta su destinazioni non note (posizionando il puntatore del mouse sul link **senza cliccare** dà in genere la possibilità di vedere l'indirizzo contenuto nel link stesso);
9. Non aprire allegati e file provenienti da mittenti sconosciuti senza gli opportuni controlli del caso;
10. In genere, diffidare da comunicazioni che richiedono l'esecuzione di azioni non richieste o che invitano ad inserire credenziali di accesso, o altre informazioni sensibili, all'interno di *form* online in quanto, con altissima probabilità, si tratta di pagine fasulle appositamente predisposte per catturare le informazioni.
11. Verificare regolarmente sul sito del CERT-PA l'emergere di campagne o attacchi attivando, ove rilevato un caso analogo, le contromisure suggerite.