PROCEDIMIENTO PARA LA INSTALACIÓN DEL MÓDULO DE SOPHOS XPLOIT PREVENTION

Si se tiene instalado el Antivirus SOPHOS en los Programas y Características de Windows, se mostrarán de esta manera:

Sophos Anti-Virus	Sophos Limited	17/05/2017	98.1 MB	10.7.2.49
Sophos AutoUpdate	Sophos Limited	17/05/2017	30.0 MB	5.7.220
Sophos Endpoint Defense	Sophos Limited	01/04/2017	1.89 MB	1.0.0.265
Sophos Network Threat Protection	Sophos Limited	01/04/2017	12.6 MB	1.2.2.50
Sophos Remote Management System	Sophos Limited	01/04/2017	22.9 MB	4.1.0
Sophos System Protection	Sophos Limited	01/04/2017	4.78 MB	1.3.1

Esta instalación funciona tanto para si contamos con el SOPHOS ya instalado, como para una instalación nueva del Antivirus junto con el Parche; se ejecutará como Administrador el archivo de instalación "SophosEndpoint - Remotos_EXPLOIT.exe"

Si se conoce el proceso de ingreso y descarga de archivos del FTP, pasar al **PASO 3.**

El Archivo de Instalación se encuentra en el FTP; a continuación se explicarán los procesos de descarga tanto por el FTP Público como por el de la Red Privada.

<u>PASO 1.</u>

DESCARGA POR FTP PÚBLICO

Ingresamos por medio de un Navegador de Internet a la dirección:

ftp://148.223.57.35



Identificación requerida X					
() ftp://148.223.57.35 está solicitando tu usuario y contraseña.					
Nombre de usuario:	batta.net\usuario				
Contraseña:	•••••				
	Aceptar Cancelar				

Seguimos la Ruta "Software/Antivirus/Sophos"

Itp://148.223.57.35		C ^e Q Buscar	Q Buscar	
	Normatividad Corporativa	09/11/16 10:	1:00	
	ofertazo	14/03/17 13:	3:00	
	Prueba	18/05/17 18:3	5:00	
	Software	17/05/17 18::	4:00	
	TELCEL	10/02/17 22:	2:00	
	TELCEL DLL	09/02/17 14:0	1:00	
	Tor_CeltorTriana.txt	1 KB 18/05/17 16:0	7:00	
	Usuarios	17/05/17 11:4	9:00	
	UISAA 🔡	15/05/17 13:2	9:00	
	VISAA_MOVIL	22/08/16 12:	9:00	
		15/04/17 11:	8:00	

i ftp://148.2	223.57.35/Software/	C	Q Buscar	
	Índice de ftp://148.223.57.35/Software/			
	🖺 Subir al directorio superior.			
	Nombre	Tamaño	Última mo	dificación
	_Drivers		12/05/16	08:34:00
	TeamViewer		06/02/16	11:22:00
			07/03/17	17:52:00
	Utilerias		17/05/17	11:07:00
	UPN Client		06/03/17	10:35:00
			05/02/16	11:39:00
	06 OPEN OFFICE 4.1.1		01/05/17	16:02:00
	🔒 20 Tarjetas Drivers LPT		24/04/17	18:32:00
	ABC_Requisitos		20/08/16	14:42:00
	ABC_Requisitos - copia		17/05/17	18:34:00
	Adobe		06/05/16	12:00:00
	Antivirus 🔒		18/05/17	10:35:00
	BattaNetTiendas_Setup		19/12/16	13:30:00

i) ftp://148.22	23.57.35/Software/Antivirus/	ď	Q Buscar
	Índice de ftp://148.223.57.35/Software/Antivirus/		
	Le Subir al directorio superior		
	Unit al directorio superior.		
	Nombre	Tamaño	Última modificación
	 Subir al directorio superior. Nombre Desinstalar_Kaspersky 	Tamaño	Última modificación 10/02/16 09:45:00
	Subir al directorio superior. Nombre Desinstalar_Kaspersky FSecure	Tamaño	Última modificación 10/02/16 09:45:00 03/03/15 12:25:00
	 Subir al directorio superior. Nombre Desinstalar_Kaspersky FSecure Kaspersky 	Tamaño	Última modificación 10/02/16 09:45:00 03/03/15 12:25:00 04/02/16 20:43:00
	Sophos	Tamaño	Última modificación 10/02/16 09:45:00 03/03/15 12:25:00 04/02/16 20:43:00 18/05/17 14:04:00

Descargamos el archivo "SophosEndpoint - Remotos_EXPLOIT.exe"

Índice de ftp://148.223.57.35 × +			
(ftp://148.223.57.35/Software/Antivirus/Sophos/	C	Q Buscar	
Índice de ftp://148.223.57.35/Software/Antivirus/Sophos/			
Nombre	Tamaño	Última modifica	ción
No Usar		18/05/17 14:04	200
SophosEndpoint - Remotos_EXPLOIT.exe	15073 KB	17/05/17 12:26	200 A

<u>PASO 2.</u>

DESCARGA SOLO USUARIOS EN CORPORATIVO

Ingresamos por medio de FileSystem la dirección:

\\172.16.1.8 o bien \\desseo

Aquí seguimos la Ruta "Software/Antivirus/Sophos"





	🔜 🔻 Software			
Archivo	Inicio Compartir Vista			
$\leftarrow \ \rightarrow$	✓ ↑ → Red > 172.16.1.8 > FtpRoot > S	oftware		
	Nombre	Fecha de modifica	Тіро	Tamaño
📌 Ac	Antivirus	18/05/2017 10:35 a	Carpeta de archivos	
💽 Oı	BattaNetTiendas_Setup	19/12/2016 12:30	Carpeta de archivos	
Archivo ← →	Inicio Compartir Vista ~ ^ I + Red > 172.16.1.8 > FtpRoot >	Software > Antivirus		
← →	 	Sottware > Antivirus	Time	T ~ ~ -
📌 Ac	Nombre	Fecha de modifica	npo	Tamano
	Desinstalar_Kaspersky	10/02/2016 08:45 a	Carpeta de archivos	
💽 Oı	FSecure	03/03/2015 11:25 a	Carpeta de archivos	
Es Es	📙 Kaspersky	04/02/2016 07:43	Carpeta de archivos	
Es	📙 Kaspersky 📙 Sophos	04/02/2016 07:43 18/05/2017 02:04	Carpeta de archivos Carpeta de archivos	

Copiamos el archivo "SophosEndpoint - Remotos_EXPLOIT.exe" y lo pegamos de manera local a nuestro equipo.

🗸	- - -	Herramientas de aplicación	Sophos				
Archivo	Inicio Compartir Vista	Administrar					
$\leftarrow \ \ \rightarrow$	← → → ↑ 🔄 > Red > 172.16.1.8 > FtpRoot > Software > Antivirus > Sophos						
<u>م</u>	Nombre	Fecha de mo	odifica Tipo	Tamaño			
A A	No Usar	18/05/2017 0	2:04 Carpeta de archivos				
📧 Oı	🚭 SophosEndpoint - Remotos_	EXPLOIT 17/05/2017 1	2:26 Aplicación	15,073 KB			

PASO 3.

Una vez descargado o copiado; lo ejecutaremos como administrador para comenzar la instalación.



Una vez ejecutado automáticamente el proceso comenzará a cerrar la aplicación del Sophos si es que se encuentra en ejecución y comenzará a instalarse la característica de xploit prevention.

Como se mencionaba anteriormente si el equipo no contaba con una instalación previa del SOHOS, se comenzarán a descargar e instalar las librerías necesarias para la instalación de la aplicación junto con la característica de XPLOIT.

<u>PASO 4.</u>

Para poder visualizar el avance de la instalación nos dirigimos al panel de tareas activas en la parte Inferior Derecha y sobre el icono del SOPHOS damos click derecho y seleccionamos "Ver estado de actualización"



Se nos mostrará un cuadro de avance de ocho partes como este (Cuando no se cuenta la característica de Shopos y se está instalando por primera vez, mostrara menor cantidad de paquetes, esto es normal ya que al terminar de instalar los paquete base de 1 al 6 continuara con los paquetes 7 y 8 que son los módulos del XPLOIT):



<u>PASO 5.</u>

Al finalizar la instalación, se reinicia el equipo para asegurarnos que el servicio del XPLOIT se corra correctamente, en administrador de programas debe estar el proceso HitmanPro.exe



Procesos Rendimiento Historial de anlic	aciones	Inicio	Usuarios	Detalles	Servic	ios	
Renamiento Tristonal de apric	aciones	micro	03ddillo3	Detunes	Jerrie		
^		0%	32%	0	1%	0%	
Nombre	22	CPU	Memoria	Dis	co	Red	_
		076	0.0 100	0 101		o Mibps	
Bonjour Service		0%	0.9 MB	0 MI	B/s	0 Mbps	
🔎 Búsqueda		0%	37.6 MB	0 MI	B/s	0 Mbps	
COM Surrogate		0%	1.1 MB	0 MI	B/s	0 Mbps	
📧 CyberLink MediaLibrary Service		0%	1.2 MB	0 MI	B/s	0 Mbps	
🌍 Google Chrome	(0.1%	47.3 MB	0 MI	B/s	0 Mbps	
🌍 Google Chrome		0%	27.5 MB	0 MI	B/s	0 Mbps	
🌀 Google Chrome		0%	0.7 MB	0 MI	B/s	0 Mbps	
🌍 Google Chrome		0%	0.7 MB	0 MI	B/s	0 Mbps	
🏟) HD Audio Background Process		0%	1.4 MB	0 MI	B/s	0 Mbps	
🦁 HitmanPro.Alert (32 bits)		0%	2.2 MB	0 MI	B/s	0 Mbps	
🥘 HitmanPro.Alert (32 bits)		0%	6.2 MB	0.1 MI	B/s	0 Mbps	
📧 Host de intercambio de datos		0%	4.9 MB	0 MI	B/s	0 Mbps	
IAStorDataSvc (32 bits)		0%	16.5 MB	0 MI	B/s	0 Mbps	
igfxCUIService Module		0%	1.0 MB	0 MI	B/s	0 Mbps	
📧 igfxEM Module		0%	1.9 MB	0 MI	B/s	0 Mbps	
📧 igfxHK Module		0%	1.6 MB	0 MI	B/s	0 Mbps	
🔲 🔳 Instalador de módulos de Wind		0%	1.3 MB	0 MI	B/s	0 Mbps	
Intel(R) Dynamic Application Lo		0%	0.6 MB	0 M	R/s	0 Mbns	

Se agregará un servicio llamado "Hitmanpro.exe"

También comprobamos que está instalado el modulo en Panel de Control -> Programas y características.



Sophos Anti-Virus	Sophos Limited	17/05/2017	98.1 MB	10.7.2.49
5 Sophos AutoUpdate	Sophos Limited	17/05/2017	30.0 MB	5.7.220
Sophos Endpoint Defense	Sophos Limited	17/05/2017	1.89 MB	1.0.0.265
Sophos Exploit Prevention	Sophos Limited	17/05/2017	3.89 MB	1.0.3.258
Sophos Network Threat Protection	Sophos Limited	17/05/2017	12.6 MB	1.2.2.50
Sophos Remote Management System	Sophos Limited	17/05/2017	22.9 MB	4.1.0
Sophos System Protection	Sophos Limited	17/05/2017	4.78 MB	1.3.1