Grupo Smartekh

Tu Seguridad Informática es nuestra pasión

GUÍA DE CONFIGURACIÓN

Acualización de patrones para minimizar el riesgo de WannaCry con Trend Micro y Palo Alto Networks

Grupo Smartekh cree en el poder que tiene la tecnología de la información para hacer a su empresa más competitiva.

Nuestra pasión es mejorar el desempeño de nuestros clientes a través de soluciones de Seguridad y Networking.

Estamos comprometidos a acelerar su éxito en cada paso al camino.

GRUPO SMARTEKH S.A DE C.V

DF. MONTERREY.BAJIO.SURESTE

Insurgentes Sur 826 P9, Col. Del Valle 03100, México D.F.

T: 5047 1030 **E:** informacion@smartekh.com

Recomendaciones para Evitar WannaCry

Problemática

Desde la mañana del viernes 12 de Mayo, 2017 están circulando diversas noticias en relación al ataque masivo dirigido a Telefónica y a varias organizaciones a nivel mundial.

Hasta ahora se han afectado a 75 países en el mundo y se han detectado 45 mil ataques.

La amenaza explota una vulnerabilidad de varios sistemas operativos Microsoft Windows para propagarse y afectar a través de **ataques de Ransomware** identificados como **Wana cry.**

Y nos es importante hacerte saber que las tecnologías de **Palo Alto Networks** y **Trend Micro** ya son capaces de detectarlas con sus diferentes soluciones.

Recomendación: Comprobar que cuentas con las últimas actualizaciones y los patrones en las siguientes versiones o más recientes.

Procedimiento

Trend Micro lo detecta como **RANSOM_WCRY.***,esta vulnerabilidad fue descubierta el pasado 14 de Marzo de 2017 y se detalla en el **Boletín de Microsoft: ms17-010**

Trend Micro ya brinda la protección y detección necesaria para este tipo de ataques mediante varias capas de protección:

- **OSCE XGen -** Patrón 13.399.00 y 17264.014.00
- **Deep Security & Vulnerability Protection-** Patrón DSRU-ID 17-016
- 1008224 - Windows SMB RCE Vulnerabilities
- 1008228 - Windows SMB RCE Vulnerability
- 1008225 - Windows SMB RCE Vulnerability
- 1008227 - Windows SMB RCE Vulnerability
- 1008306 - Microsoft Windows SMB Remote Code Execution Vulnerability (MS17-010)
- **Deep Discovey Inspector -** Rule ID 2383: CVE-2017-0144 - RCE - SMB (Request)
- **Tipping Point -** filters: 27433, 27711, 27928
- **High-Fidelity Machine Learning** detecta SIN necesidad de patrón
- **Deep Discovery Custom Sandbox** detecta SIN necesidad de patrón

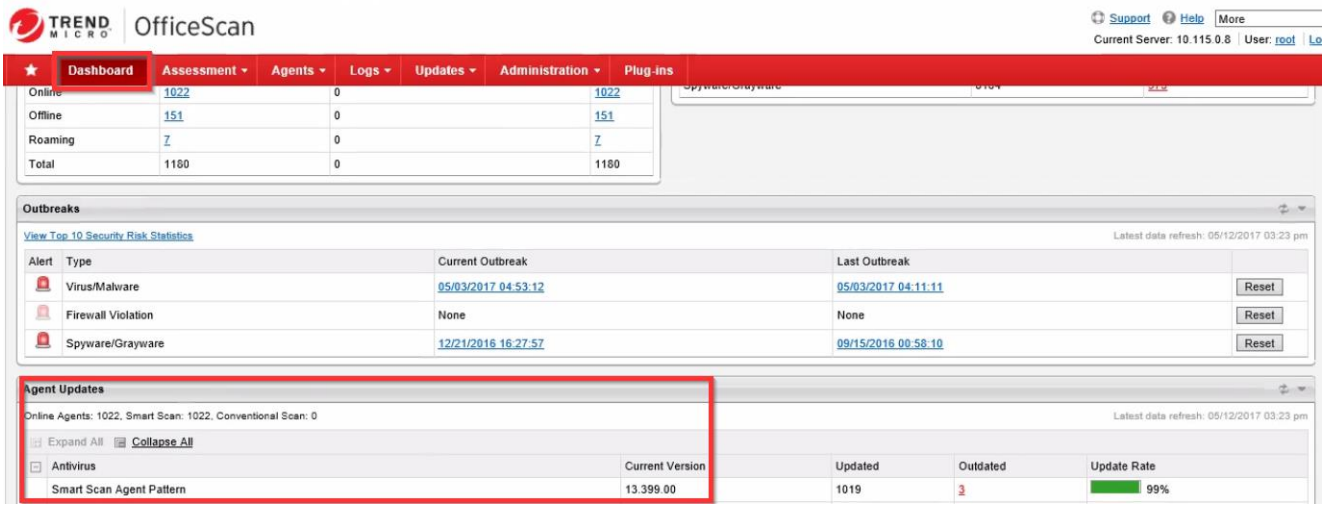
Si eres **usuario de Trend Micro** te recomendamos contar con las últimas actualizaciones, puedes comprobar que cuentas con los patrones en las siguientes versiones o más recientes:

Consumer Smart Scan Agent Pattern:13.399.00

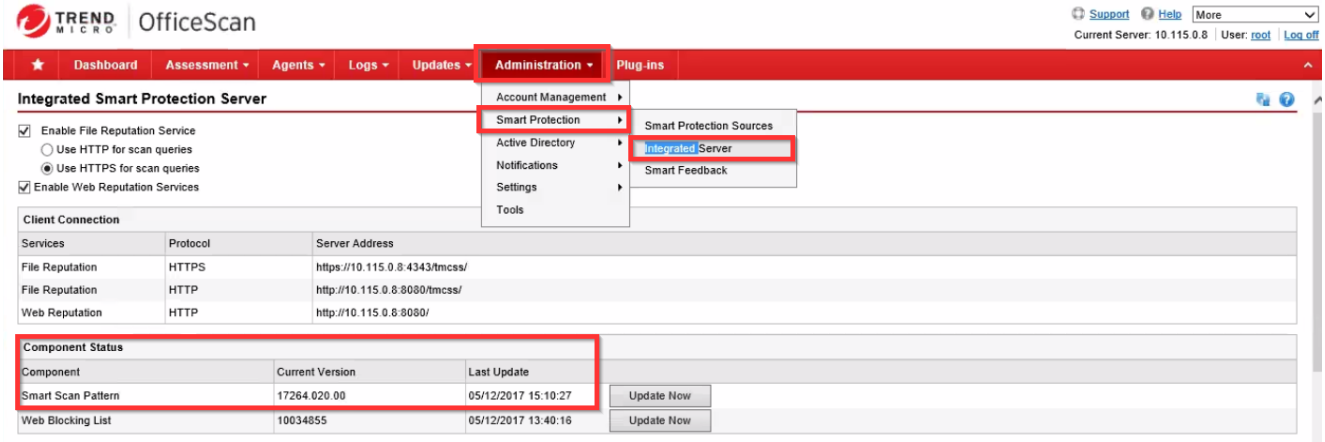
Consumer Smart Scan Pattern:17264.014.00

Lo puedes consultar en tu consola de OfficeScan:

Dashboard > Agent Updates > Antivirus > Smart Scan Agent Pattern

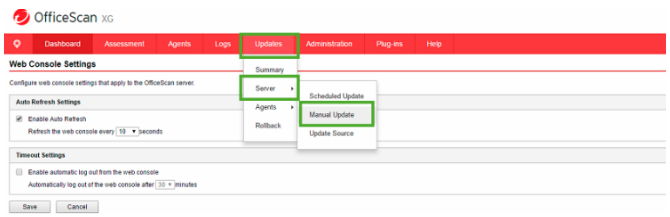


Administration > Smart Protection > Integrated Server > Component Status

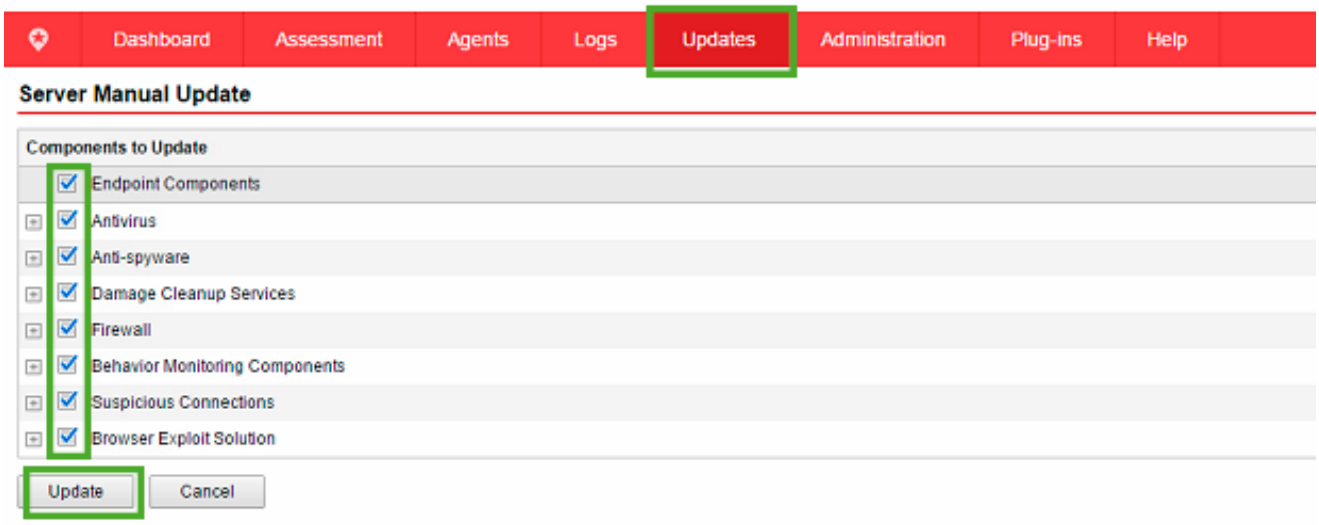


Estos patrones los puedes actualizar en la siguiente ruta:

Updates> Server> Manual Update

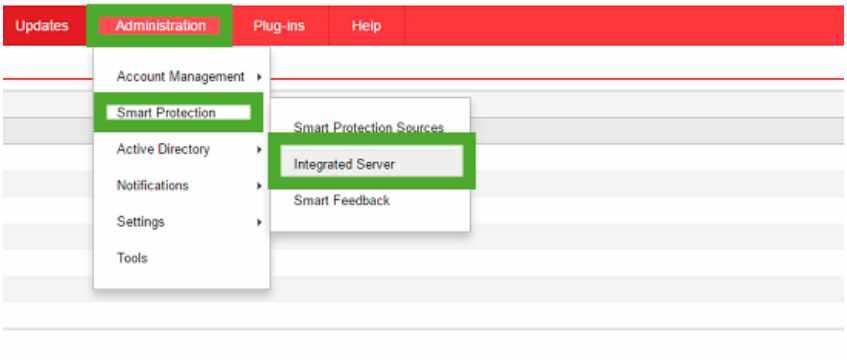


Una vez que te encuentres ahí, asegúrate de que todos los componentes se encuentren seleccionados y da clic en **Update.**



Dirígete al menú

Administration>SmartProtection>Integrated Server y da clic en ***Update.***



Para finalizar basta con dar clic en **Update Now** en el apartado **Smart Scan Pattern**

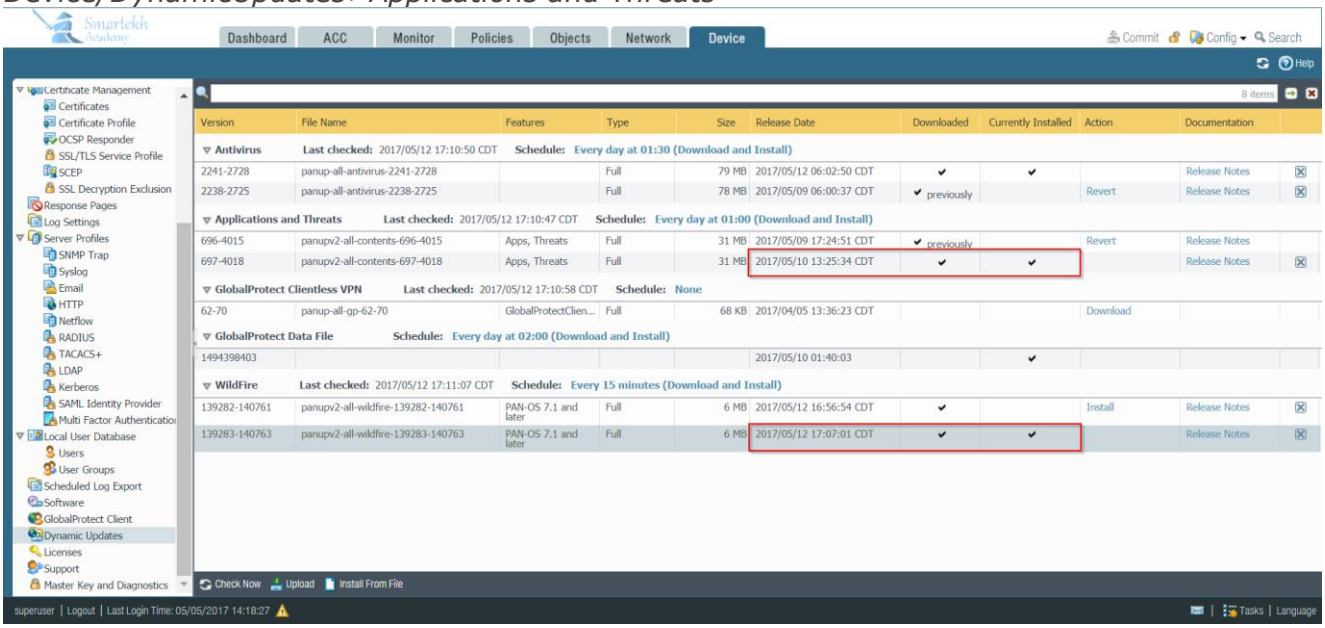
Palo Alto Networks lo detecta con la firma de vulnerabilidad **CVE-2117-0143.**

New Vulnerability Signatures (35)

Severity	ID	Attack Name	CVE ID	Vendor ID	Default Action	Minimum PAN-OS Version	Maximum PAN-OS Version
critical	30737	Dahua IPC Information Disclosure and Privilege Escalation Vulnerability	CVE-2017-7253		alert	5.0.0	
high	30854	eir D1000 Modem CWMP Code Execution Vulnerability			alert	5.0.0	
medium	31162	Artifex Ghostscript Arbitrary Command Execution Vulnerability	CVE-2017-8291		alert	5.0.0	
critical	32097	Adobe Reader Memory Corruption Vulnerability	CVE-2017-3026	APSB17-11	alert	5.0.0	
critical	32494	Microsoft Windows SMB Remote Code Execution Vulnerability	CVE-2017-0143	MS17-010	alert	5.0.0	

Si eres **usuario de Palo Alto Networks** te recomendamos contar con las últimas actualizaciones, puedes comprobar que cuentas con los patrones en las siguientes versiones o más recientes:

Device/DynamicUpdates>Applications and Threats

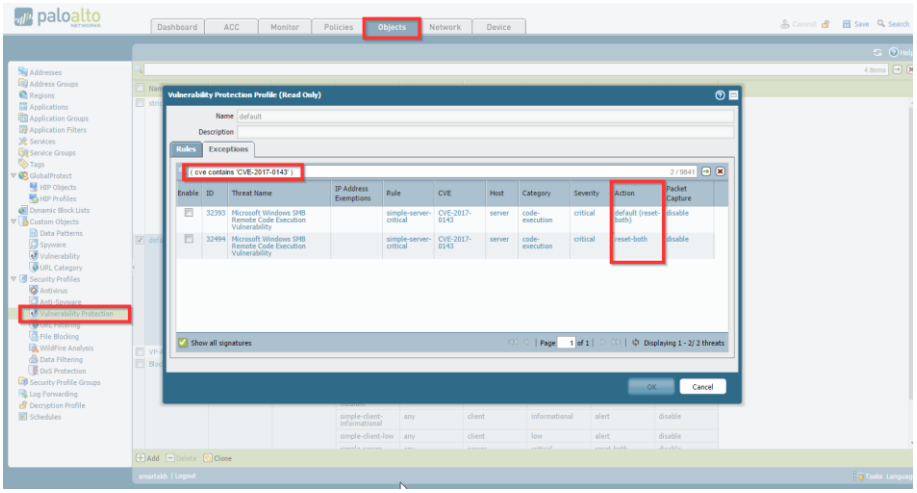


Una vez que tienes la última versión, verifica que tus políticas de seguridad tengan configurado el perfil de seguridad para protección contra vulnerabilidades.

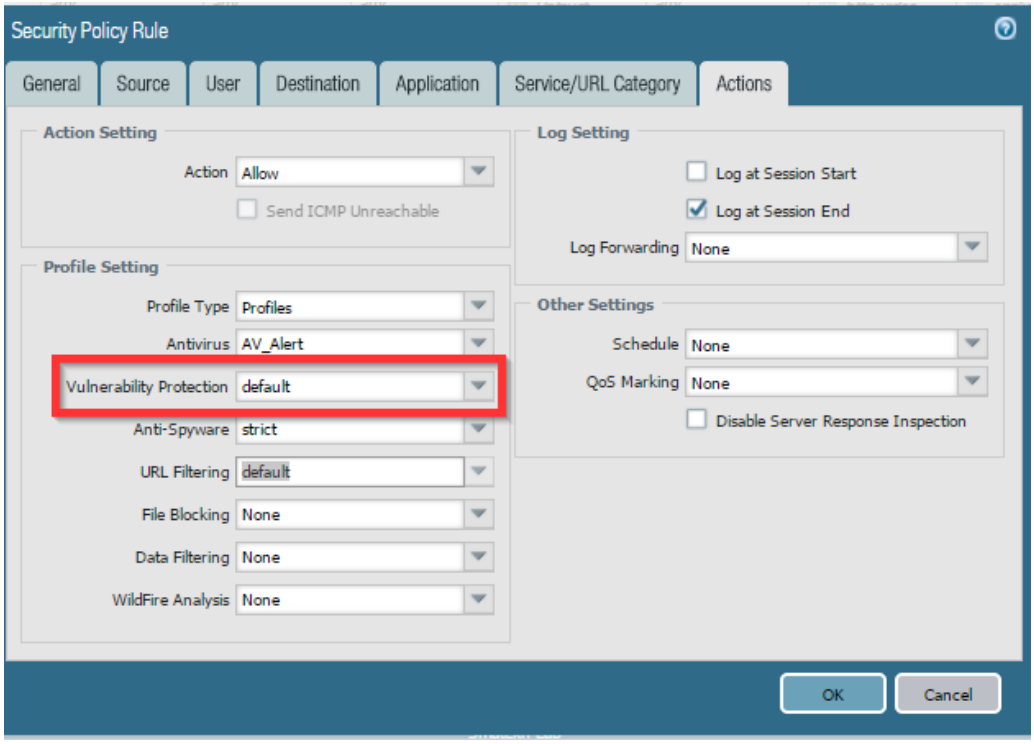
Objects >Security Profiles >Vulnerability Protection

Teclea la consulta **(cve contains 'CVE-2017-0143')**

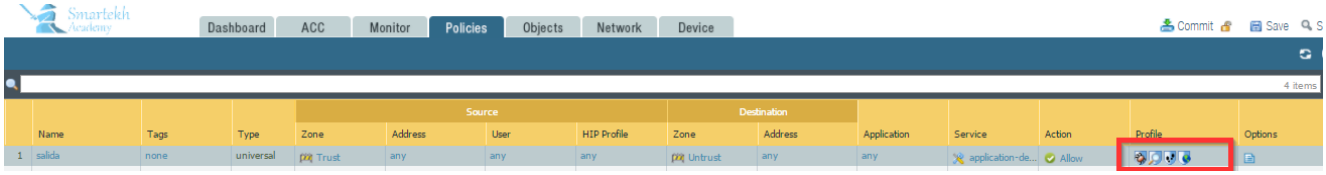
Revisar que en las dos firmas tenga las acciones en **"Reset Both"**



Seleccionas el nombre de tu perfil de Vulnerability Protection en el pestaña de excepciones da clic a **"show all signatures".**



Para revisar que tus políticas de seguridad tienen un perfil de **Vulnerability Protection** dirígete a la pestaña de *Policys* > *Security* elige alguna de tus políticas y en la pestaña de acciones verifica que tenga el perfil de vulnerabilidad.



Si cuentas con **Licencia de Wildfire,** asegúrate que la configuración de las actualizaciones sea **cada 15 min;** esto te protegerá de la descarga de este malware.

Recomendaciones

Es importante mencionar que con esta configuración mantenemos las actualizaciones y patrones al corriente y minimizamos el riesgo de ser afectados por Ransomware WannaCry.

Con esta configuración:

- **No se verán cortes a la comunicación**
- **No se necesita el reinicio del firewall**

Lo más importante para que no existan afectaciones en tu red debido a la infección o autopropagación de Ransomware WannaCry es la concientización con tus usuarios, contar con respaldos y mantener todas las actualizaciones al día. Para esto hemos creado un informativo que contiene datos y tips importantes del **porque el usuario es el eslabón más débil en un cadena de ataques.** Lee tu copia y empieza a involucrar a los usuarios en tus estrategias de seguridad.

¿No sabes cómo empezar?

El equipo de Service Desk está al tanto las nuevas problemáticas de configuración con el firewall Palo Alto Networks y las soluciones tecnológicas de Trend Micro para cualquier duda que tengas.

Si estás interesado en mejorar tus procesos de configuración y gestión de soluciones tecnológicas, solicita una asesoría personalizada con un ingeniero experto y complementa tu estrategia de seguridad en un solo paso.

¡QUIERO HABLAR CON UN CONSULTOR EXPERTO!

¡¡¡Llámanos!!!

01 800 21 25 500

¿Alguna duda o pregunta?

Nos puedes encontrar en: Insurgentes Sur 826 P9 Col. Del Valle 03100

Escríbenos: servicedesk@smartekh.com

Llámanos: +52 55 50 47 10 30 EXT 1031 – 1032 – 1033 -1034 – 01 800 21 25 500