

# Grupo Smartekh

**Tu Seguridad Informática  
es nuestra pasión**

## GUÍA DE CONFIGURACIÓN

Actualización 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](mailto: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 Discovery 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**

Síguenos [smartekh.com](http://smartekh.com) también en Facebook [Twitter](#) [Linked In](#)

## Consumer Smart Scan Pattern:17264.014.00

Lo puedes consultar en tu consola de OfficeScan:

*Dashboard > Agent Updates > Antivirus > Smart Scan Agent Pattern*

**OfficeScan** | Support | Help | More  
Current Server: 10.115.0.8 | User: root | Log off

Dashboard | Assessment | Agents | Logs | Updates | Administration | Plug-ins

Online	1022	0	1022
Offline	151	0	151
Roaming	7	0	7
<b>Total</b>	<b>1180</b>	<b>0</b>	<b>1180</b>

**Outbreaks**

Alert	Type	Current Outbreak	Last Outbreak
Virus/Malware		05/03/2017 04:53:12	05/03/2017 04:11:11
Firewall Violation		None	None
Spyware/Grayware		12/21/2016 16:27:57	09/15/2016 00:58:10

**Agent Updates**

Online Agents: 1022, Smart Scan: 1022, Conventional Scan: 0

Antivirus	Current Version	Updated	Outdated	Update Rate
Smart Scan Agent Pattern	13.399.00	1019	3	99%

*Administration > Smart Protection > Integrated Server > Component Status*

**OfficeScan** | Support | Help | More  
Current Server: 10.115.0.8 | User: root | Log off

Dashboard | Assessment | Agents | Logs | Updates | Administration | Plug-ins

**Integrated Smart Protection Server**

- Account Management
  - Smart Protection
    - Smart Protection Sources
    - Integrated Server
    - Smart Feedback
  - Active Directory
  - Notifications
  - Settings
  - Tools

**Client Connection**

Services	Protocol	Server Address
File Reputation	HTTPS	https://10.115.0.8:4343/mcscs/
File Reputation	HTTP	http://10.115.0.8:8080/mcscs/
Web Reputation	HTTP	http://10.115.0.8:8080/

**Component Status**

Component	Current Version	Last Update
Smart Scan Pattern	17264.020.00	05/12/2017 15:10:27
Web Blocking List	10034855	05/12/2017 13:40:16

Estos patrones los puedes actualizar en la siguiente ruta:

*Updates > Server > Manual Update*

**OfficeScan XG**

Dashboard | Assessment | Agents | Logs | Updates | Administration | Plug-ins | Help

**Web Console Settings**

Configure web console settings that apply to the OfficeScan server:

**Auto Refresh Settings**

Enable Auto Refresh  
Refresh the web console every: 10 seconds

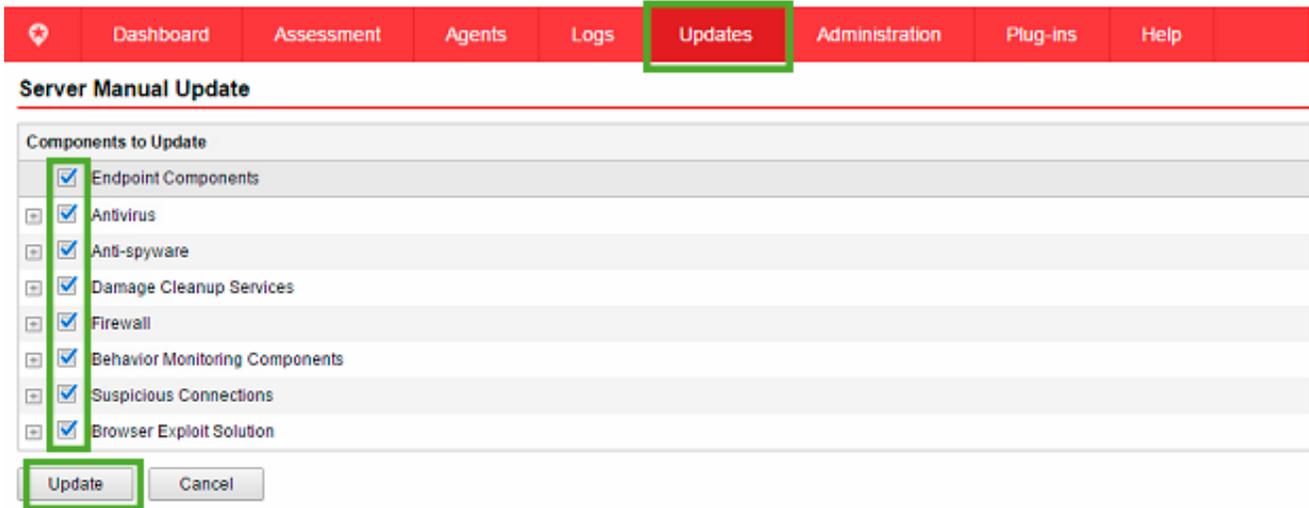
**Timeout Settings**

Enable automatic log out from the web console  
Automatically log out of the web console after: 30 minutes

Save | Cancel

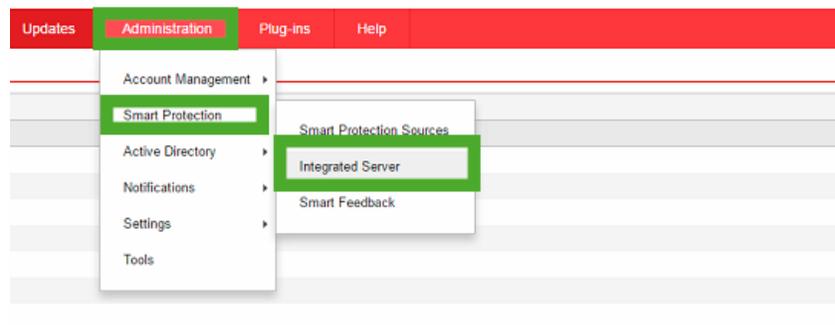
Síguenos [smartekh.com](http://smartekh.com) también en Facebook Twitter Linked In

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**

Web Reputation HTTP http://130.60.1.11:8080/

Component Status			
Component	Current Version	Last Update	
Smart Scan Pattern	17264.021.00	05/12/2017 17:11:03	<input checked="" type="button" value="Update Now"/>
Web Blocking List	10034858	05/12/2017 17:10:17	<input type="button" value="Update Now"/>

Web Reputation Service Approved/Blocked List

## 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	<b>MS17-010</b>	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

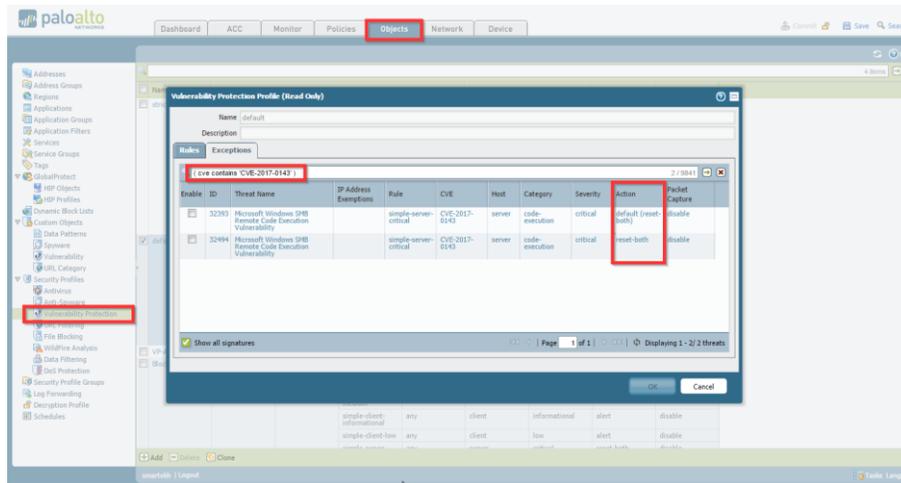
Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation
<b>Antivirus</b> Last checked: 2017/05/12 17:10:50 CDT Schedule: Every day at 01:30 (Download and Install)									
2241-2728	panup-all-antivirus-2241-2728		Full	79 MB	2017/05/12 06:02:50 CDT				Release Notes
2238-2725	panup-all-antivirus-2238-2725		Full	78 MB	2017/05/09 06:00:37 CDT	✓ previously	✓	Revert	Release Notes
<b>Applications and Threats</b> Last checked: 2017/05/12 17:10:47 CDT Schedule: Every day at 01:00 (Download and Install)									
696-4015	panupv2-all-contents-696-4015	Apps, Threats	Full	31 MB	2017/05/09 17:24:51 CDT	✓ previously		Revert	Release Notes
697-4018	panupv2-all-contents-697-4018	Apps, Threats	Full	31 MB	2017/05/10 13:25:34 CDT	✓	✓		Release Notes
<b>GlobalProtect Clientless VPN</b> Last checked: 2017/05/12 17:10:58 CDT Schedule: None									
62-70	panup-all-gp-62-70	GlobalProtectClien...	Full	68 KB	2017/04/05 13:36:23 CDT			Download	
<b>GlobalProtect Data File</b> Schedule: Every day at 02:00 (Download and Install)									
1494398403					2017/05/10 01:40:03		✓		
<b>WildFire</b> Last checked: 2017/05/12 17:11:07 CDT Schedule: Every 15 minutes (Download and Install)									
139282-140761	panupv2-all-wildfire-139282-140761	PAN-OS 7.1 and later	Full	6 MB	2017/05/12 16:56:54 CDT	✓		Install	Release Notes
139283-140763	panupv2-all-wildfire-139283-140763	PAN-OS 7.1 and later	Full	6 MB	2017/05/12 17:07:01 CDT	✓	✓		Release Notes

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

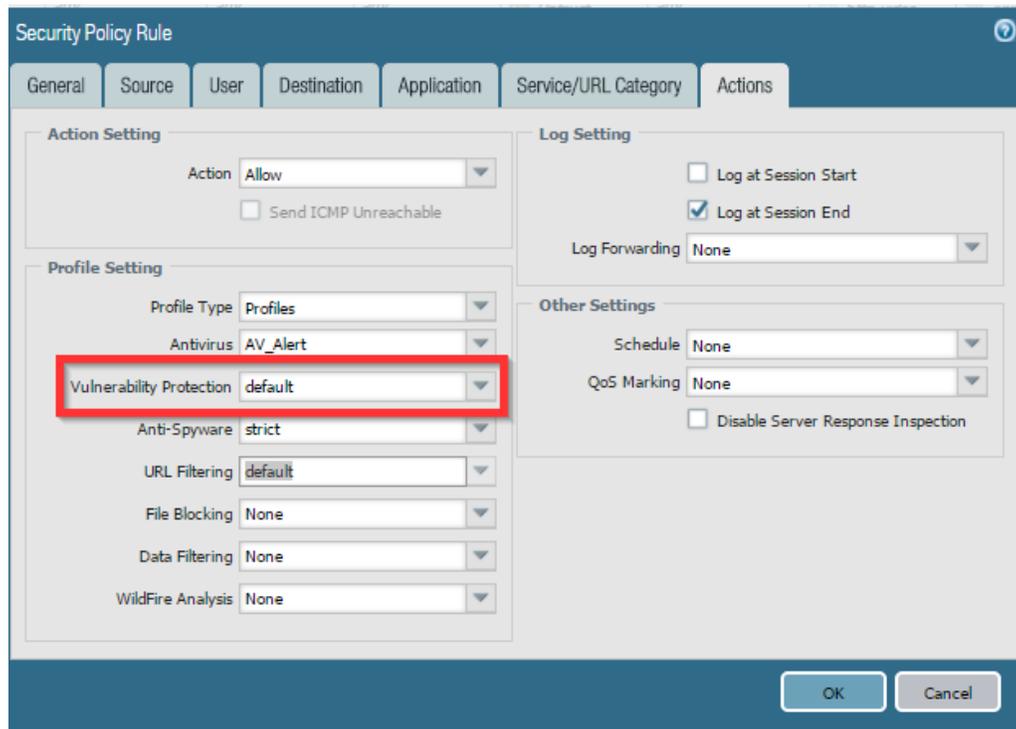
### Objects >Security Profiles >Vulnerability Protection

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 *Polícy*s > *Security* elige alguna de tus políticas y en la pestaña de acciones verifica que tenga el perfil de vulnerabilidad.



Síguenos [smartekh.com](http://smartekh.com) también en Facebook Twitter Linked In

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!!!

Síguenos [smartekh.com](http://smartekh.com) también en Facebook [Twitter](#) [Linked In](#)

# 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](mailto:servicedesk@smartekh.com)

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

Síguenos [smartekh.com](http://smartekh.com) también en Facebook [Twitter](#) [Linked In](#)

