

# Grupo Smartekh

**Tu Seguridad Informática  
es nuestra pasión**

## GUÍA DE CONFIGURACIÓN

Actualización de reglas y patrones  
para minimizar el riesgo de  
Ransomware BadRabbit 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 Pg, Col. Del Valle 03100, México D.F.

**T: 5047 1030 E: [informacion@smartekh.com](mailto:informacion@smartekh.com)**

# Recomendaciones para Evitar BadRabbit

## Problemática

Desde el día de ayer, martes 24 de octubre, 2017 están circulando diversas noticias en relación al nuevo ransomware BadRabbit identificado como **RANSOM\_BADRABBIT.A** que está afectando a Europa del Este y se propaga para atacar a varias organizaciones a nivel mundial.

Los primeros análisis indican que este ataque usa técnicas de propagación similares a la familia de Ransomware Petya, la amenaza **se propaga a través de actualizaciones falsas de Flash**.

Incorporando el uso de Mimikatz para extraer credenciales (una herramienta de código abierto que se ha usado en ataques anteriores), y aparentemente intenta usar una lista de credenciales codificadas comunes como Administrador, Invitado, Usuario, Root, etc. También hay evidencia de que utiliza una herramienta legítima, DiskCryptor, para el cifrado de los sistemas de la víctima.

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

Los usuarios de los productos Trend Micro con **XGen Security** detectan este ransomware como **TROJ.Win32.TRX.XXPE002FF019**.

Si eres **usuario de Trend Micro** te recomendamos contar con las últimas actualizaciones y aplicar las siguientes reglas de configuración:

### PARCHEO VIRTUAL

#### Deep Security

- **Rules** 1008224, 1008225, 1008228, 1008285, y 1008306 - MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities.
- **Rules** 1003222, 1006906, 1008327, 1008328, 1008422, and 1008423 may help to prevent potential lateral movement of the ransomware using PsExec.

Estas reglas se aplican en el siguiente menú:

**POLICY > INTRUSION PREVENTION > GENERAL > ASSIGNED INTRUSION PREVENTION RULES > ASSING/UNASSIGN**

The screenshot shows the 'IPS Rules' management interface. At the top, there are filters for 'All', 'All', and 'By Type'. A search bar contains the text '1008224'. Below the search bar are buttons for 'New', 'Delete...', 'Properties...', 'Duplicate', 'Export', 'Application Types...', and 'Columns...'. A table with columns 'NAME', 'APPLICATION TYPE', and 'PRIOR' is displayed. Under the 'Vulnerability (1)' section, a single rule is listed: '1008224 - Microsoft Windows SMB Remote Code Execution Vulnerabilities (CVE-2017-0144 a... DCERPC Services' with a priority of '2 - No'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Busca y habilita las reglas:

The screenshot shows the 'Assigned Intrusion Prevention Rules' interface. On the left is a sidebar menu with options: Overview, Anti-Malware, Web Reputation, Firewall, Intrusion Prevention (highlighted), Integrity Monitoring, Log Inspection, Application Control, Interface Types, Settings, and Overrides. The main panel has tabs for 'General', 'Advanced', and 'Intrusion Prevention Events'. Under the 'Assigned Intrusion Prevention Rules' section, there is a filter set to 'All' and buttons for 'Assign/Unassign...', 'Properties...', 'Export', 'Application Types...', and 'Columns...'. A table with columns 'NAME' and 'APPLICATION TYPE' is shown, but it contains the message '(There are no items in the list)'. At the bottom, there is a 'Recommendations' section with 'Current Status: N/A'.

Una vez habilitadas las reglas, están se reflejarán de la siguiente manera.

**Intrusion Prevention**

Intrusion Prevention State:  ● Prevent, 12 rules

Intrusion Prevention Behavior

☒ Prevent  
☐ Detect

**Assigned Intrusion Prevention Rules**

All

Assign/Unassign... Properties... Export Application Types... Columns...

| NAME                                                                                | APPLICATION TYPE  |
|-------------------------------------------------------------------------------------|-------------------|
| 1008327 - Identified Server Suspicious SMB Session                                  | DCERPC Services   |
| 1008306 - Microsoft Windows SMB Remote Code Execution Vulnerability (MS17-010)      | DCERPC Services   |
| 1008285 - Microsoft Word Remote Code Execution Vulnerability (CVE-2017-0199)        | Web Client Common |
| 1008228 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0148) | DCERPC Services   |
| 1008225 - Microsoft Windows SMB Remote Code Execution Vulnerability (CVE-2017-0145) | DCERPC Services   |

Recommendations

Save Close

## DETECCIÓN Y PROTECCIÓN DE LA RED

### Deep Discovery Inspector

- Rule **2383**: CVE-2017-0144 - Remote Code Execution - SMB (Request)
- Rule **2441**: PsExec PETYA - Ransomware - SMB
- Rules **35** and **1307** help monitor potential lateral movement of PsExec

Estas reglas se aplican en el siguiente menú:

**ADMINISTRATION > MONITORING/SCANNING > DETECTION RULES**

Busca las reglas mencionadas y asegúrate que se encuentran habilitadas.

You are here: Administration > Monitoring / Scanning > Detection Rules

Monitoring / Scanning

Hosts / Ports
Threat Detections
Web Reputation
Application Filters
Deny List / Allow List
Detection Rules
Exceptions

### Detection Rules

Save Changes
Cancel

--- Change all rules to ---

Enable
Disable
Default Status

| Current | ID | Risk Type | Confidence | Reason                                            |
|---------|----|-----------|------------|---------------------------------------------------|
| ✓       | 1  | MALWARE   | High       | Suspicious executable file extension              |
| ⊗       | 2  | MALWARE   | High       | Suspicious script file extension                  |
| ⊗       | 3  | MALWARE   | High       | Suspicious executable file extension - Variant 2  |
| ⊗       | 4  | MALWARE   | High       | Script file name with multiple consecutive spaces |

2383
1 de 1

|   |      |         |        |                                                                |
|---|------|---------|--------|----------------------------------------------------------------|
| ✓ | 2377 | OTHERS  | High   | Remote Code Execution Vulnerability - RDP                      |
| ✓ | 2378 | OTHERS  | High   | EXAMINE Buffer Overflow - IMAP4 (Request)                      |
| ✓ | 2379 | OTHERS  | High   | CRAM-MD5 Authentication Buffer Overflow - IMAP4 (Request)      |
| ✓ | 2380 | OTHERS  | Medium | CVE-2017-0147 - Information Disclosure Exploit - SMB (Request) |
| ✓ | 2382 | OTHERS  | Medium | CVE-2017-0145 - Remote Code Execution - SMB (Request)          |
| ✓ | 2383 | OTHERS  | High   | CVE-2017-0144 - Remote Code Execution - SMB (Request)          |
| ✓ | 2384 | OTHERS  | Low    | Possible EQUATED - Remote Code Execution - SMB (Request)       |
| ✓ | 2385 | MALWARE | High   | MIRAI - HTTP (Request)                                         |

2441
1 de 1

|   |      |         |        |                                                                     |
|---|------|---------|--------|---------------------------------------------------------------------|
| ✓ | 2440 | OTHERS  | Medium | CVE-2015-5374 - SIEMENS SIPROTECT DENIAL OF SERVICE - UDP (Request) |
| ✓ | 2441 | OTHERS  | High   | PsExec PETYA - Ransomware - SMB                                     |
| ✓ | 2442 | OTHERS  | Medium | Possible PsExec PETYA - Ransomware - SMB                            |
| ✓ | 2443 | MALWARE | High   | SPORA - Ransomware - HTTP (Response)                                |
| ✓ | 2444 | MALWARE | High   | INDUSTROYER - HTTP (Request)                                        |

35
1 de 47

|   |    |         |        |                                                                                       |
|---|----|---------|--------|---------------------------------------------------------------------------------------|
| ✓ | 34 | MALWARE | Medium | Transmitted executable or script file - IRC (Request)                                 |
| ✓ | 35 | MALWARE | Medium | Executable file dropped in administrative share - SMB                                 |
| ✓ | 36 | MALWARE | High   | Archive file containing executable file with suspicious extension - Email - Variant 2 |
| ✓ | 37 | MALWARE | Medium | Packed executable file - IM                                                           |

1307
1 de 1

|   |      |         |        |                                                                        |
|---|------|---------|--------|------------------------------------------------------------------------|
| ✓ | 1306 | OTHERS  | Medium | SMB or SMB2 PE file Upload to non-administrative share folder detected |
| ⊗ | 1307 | OTHERS  | Medium | SMB or SMB2 PE file Upload detected                                    |
| ✓ | 1309 | MALWARE | High   | PSYRAT - HTTP (Request)                                                |
| ⊗ | 1310 | OTHERS  | Low    | SMB CreateService request detected                                     |
| ⊗ | 1311 | OTHERS  | Low    | SMB DeleteService request detected                                     |

## Tipping Point

- Rule **27931 y 27928** SMB: coverage for MS17-010 and some specific protection against Windows SMB remote code execution vulnerabilities and attacks.
- Digital Vaccine (DV) Filter 28471 - May be configured to enforce generic policy at the network perimeter by blocking SMB v1 traffic (this is disabled by default).

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: 2017/10/25 09:41:39 CDT Schedule: Every day at 01:30 (Download and Install)                |                               |               |         |       |                         |              |                     |          |               |
| 2410-2904                                                                                                                 | panup-all-antivirus-2410-2904 |               | Unknown | 80 MB | 2017/10/25 06:00:06 CDT | ✓            | ✓                   |          | Release Notes |
| 2407-2901                                                                                                                 | panup-all-antivirus-2407-2901 |               | Unknown | 80 MB | 2017/10/22 06:02:37 CDT |              |                     | Download | Release Notes |
| 2409-2903                                                                                                                 | panup-all-antivirus-2409-2903 |               | Unknown | 79 MB | 2017/10/24 06:03:44 CDT | ✓ previously |                     | Revert   | Release Notes |
| 2406-2900                                                                                                                 | panup-all-antivirus-2406-2900 |               | Unknown | 80 MB | 2017/10/21 06:04:30 CDT |              |                     | Download | Release Notes |
| 2408-2902                                                                                                                 | panup-all-antivirus-2408-2902 |               | Unknown | 80 MB | 2017/10/23 06:01:14 CDT |              |                     | Download | Release Notes |
| <b>Applications and Threats</b> Last checked: 2017/10/25 09:12:06 CDT Schedule: Every day at 01:00 (Download and Install) |                               |               |         |       |                         |              |                     |          |               |
| 738-4236                                                                                                                  | panupv2-all-contents-738-4236 | Apps, Threats | Unknown | 32 MB | 2017/09/26 19:13:45 CDT |              |                     | Download | Release Notes |
| 740-4262                                                                                                                  | panupv2-all-contents-740-4262 | Apps, Threats | Unknown | 32 MB | 2017/10/10 14:09:12 CDT |              |                     | Download | Release Notes |
| 742-4268                                                                                                                  | panupv2-all-contents-742-4268 | Apps, Threats | Unknown | 32 MB | 2017/10/13 13:01:03 CDT |              |                     | Download | Release Notes |
| 739-4252                                                                                                                  | panupv2-all-contents-739-4252 | Apps, Threats | Unknown | 32 MB | 2017/10/05 18:13:22 CDT |              |                     | Download | Release Notes |
| 743-4236                                                                                                                  | panupv2-all-contents-743-4236 | Apps, Threats | Unknown | 32 MB | 2017/10/12 13:01:03 CDT |              |                     | Download | Release Notes |
| 745-4296                                                                                                                  | panupv2-all-contents-745-4296 | Apps, Threats | Unknown | 32 MB | 2017/10/24 17:59:08 CDT | ✓            | ✓                   |          | Release Notes |
| 741-4265                                                                                                                  | panupv2-all-contents-741-4265 | Apps, Threats | Unknown | 32 MB | 2017/10/11 19:31:20 CDT |              |                     | Download | Release Notes |
| 744-4278                                                                                                                  | panupv2-all-contents-744-4278 | Apps, Threats | Unknown | 32 MB | 2017/10/18 00:13:09 CDT | ✓ previously |                     | Revert   | 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.

Si cuentas con licencia de **URL filtering**. Asegúrate que las siguientes categorías se encuentren bloqueadas en tus perfiles: **malware y command and control**.

URL Filtering Profile (Read Only)

Name default

Description

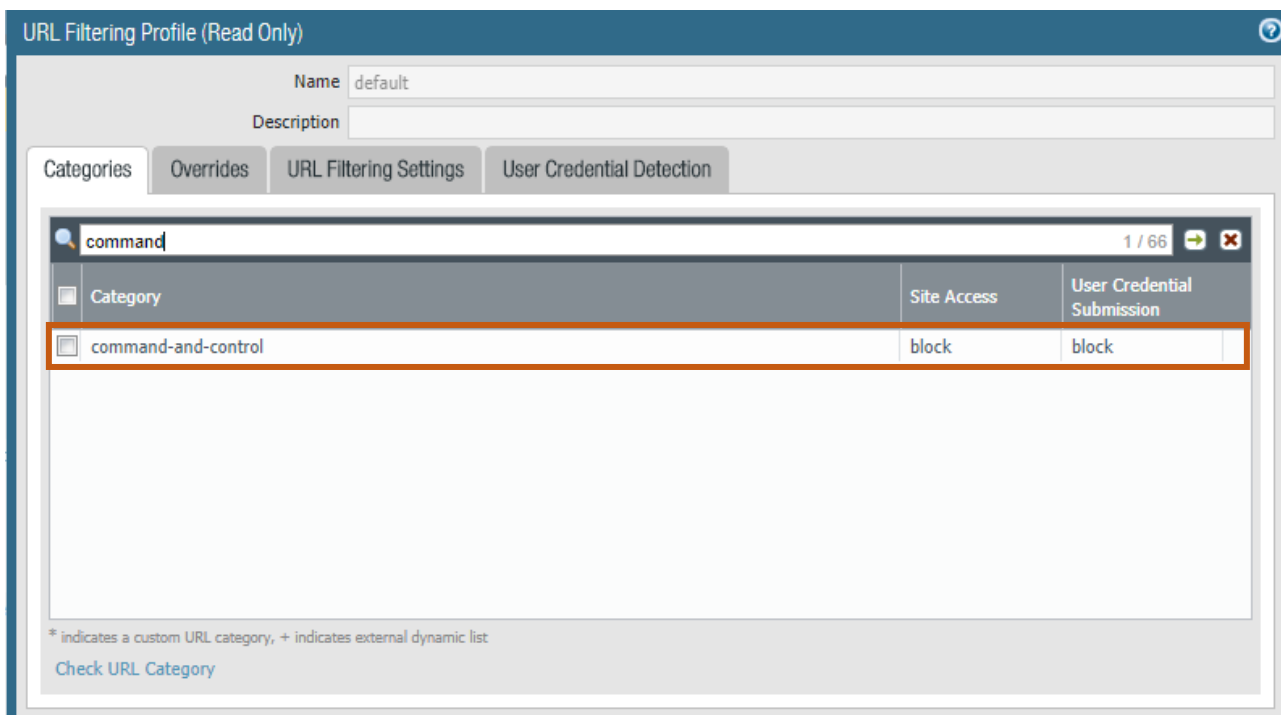
Categories Overrides URL Filtering Settings User Credential Detection

malware 1 / 66

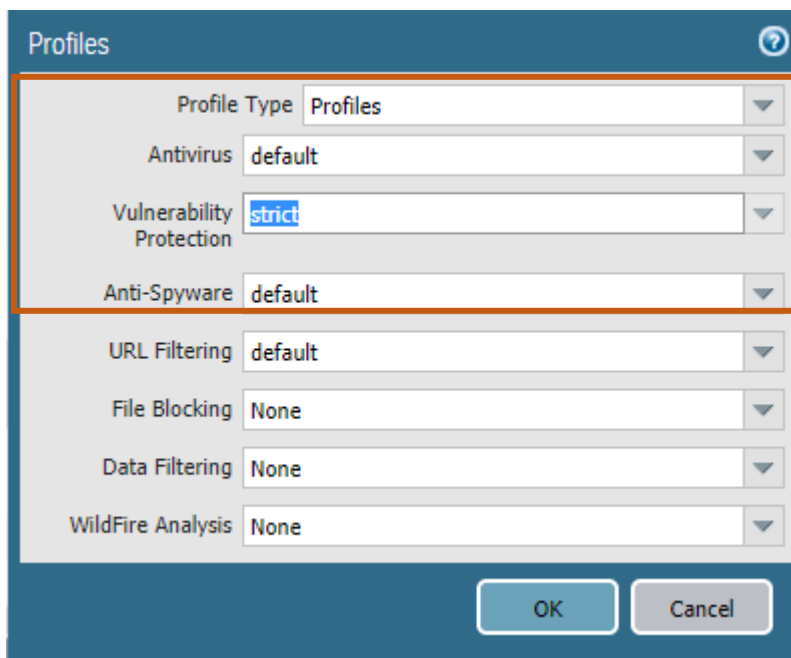
| Category | Site Access | User Credential Submission |
|----------|-------------|----------------------------|
| malware  | block       | block                      |

\* indicates a custom URL category, + indicates external dynamic list

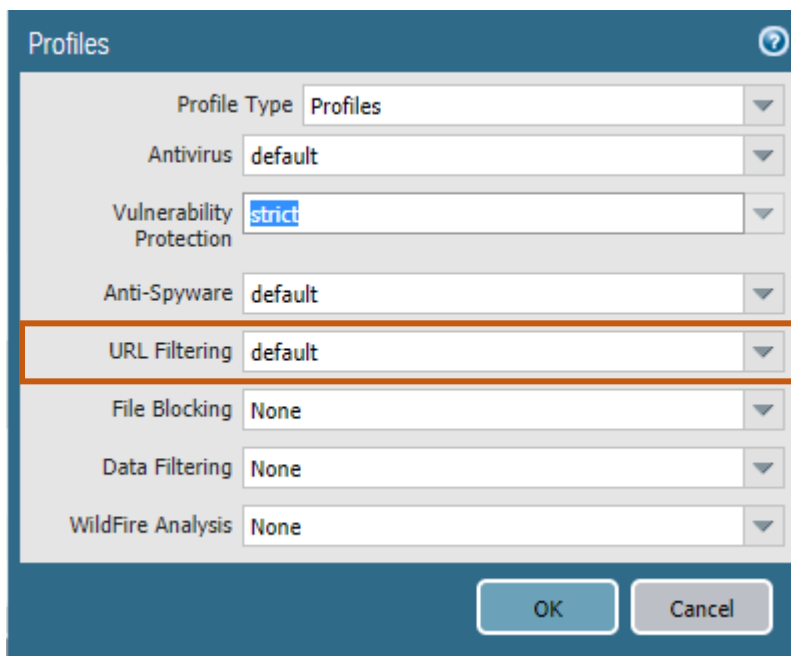
Check URL Category



Para revisar que tus políticas de seguridad tienen un **Perfil de Antivirus, Vulnerability Protection y Anti-Spyware**. Dirígete a la pestaña de **Policies > Security**, elige alguna de tus políticas y en la pestaña de acciones verifica que tenga los perfiles, en este ejemplo el nombre de los perfiles se llaman **antivirus > default**, **vulnerability protection > strict** y **Anti-Spyware > default**. El nombre de los perfiles diferirá en cada configuración.



Asegúrate que en las políticas que dan acceso a internet se encuentre el perfil de **URL Filtering** por default.



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. También asegúrate que se encuentre aplicado al perfil a las políticas como se mostró anteriormente.

---

## Recomendaciones Generales.

---

El equipo de Trend Micro y Grupo Smartekh te recomienda las siguientes acciones como estrategia de prevención proactiva:

- **Asegúrate de que se apliquen todos los parches más recientes** (si es posible usando la solución de Parcheo Virtual ) a los sistemas operativos afectados, especialmente los relacionados con MS17-010 y cualquier boletín de seguridad reciente
- **Habilita tu firewall, así como los sistemas de prevención y detección de intrusiones.**
- **Monitorea y valida de forma proactiva el tráfico** entrante y saliente de la red.
- **Implementa mecanismos de seguridad para tus sitios web y servidores de correo.**
- Implementa **control de aplicaciones para evitar la ejecución de archivos sospechosos** para identificar modificaciones no deseadas en el sistema.

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



- **Segmenta la red y haz una categorización de datos** para mitigar la exposición y daño de los datos.
- **Deshabilita SMB (v1) en máquinas vulnerables**, utilizando GPO o siguiendo las instrucciones proporcionadas por Microsoft.

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

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 propagación de Ransomware BadRabbit, 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

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

Escríbenos: [servicedesk@smartekh.com](mailto:servicedesk@smartekh.com)

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