

## TAD (Detección de ataques a objetivos)

En la versión del 7 de junio, el TAD pasó de ser una detección de base de campaña a una detección de ataques a objetivos (TAD). Puede proporcionar el nivel de riesgo por fase de ataque objetivo dentro de toda la organización, por lo que el cliente puede predecir el impacto en el negocio y luego priorizar las acciones.

Este documento presentará el TAD en varias secciones.

1. Qué es el TAD.
2. Nivel de riesgo alto, medio y bajo, y tendencia del TAD en cada fase del Análisis de Progresión de Ataques
3. Total de puntos finales en riesgo
4. Elementos de seguridad recomendados
5. Campaña de ataque

### 1. Qué es el TAD

Objetivo:

- Analizar el riesgo de las amenazas en la vista de toda la organización basándose en el ciclo de vida de los ataques
- Proporcionar una advertencia de detección de ataques al cliente en cada fase de ataque
- Sugerir cómo arreglar, dónde arreglar primero para reforzar la seguridad de forma adaptativa

El motor de TAD escaneará **el registro de Smart Feedback de SPN y el registro de consulta en la nube de SPN** en busca de indicadores dignos de mención, e identificará todos los indicadores como cuatro fases de ataque. Las cuatro fases de ataque son: Acceso inicial, Persistente, Acceso de credenciales, Movimiento lateral. El acceso a las credenciales y el movimiento lateral están más cerca de ser atacados.

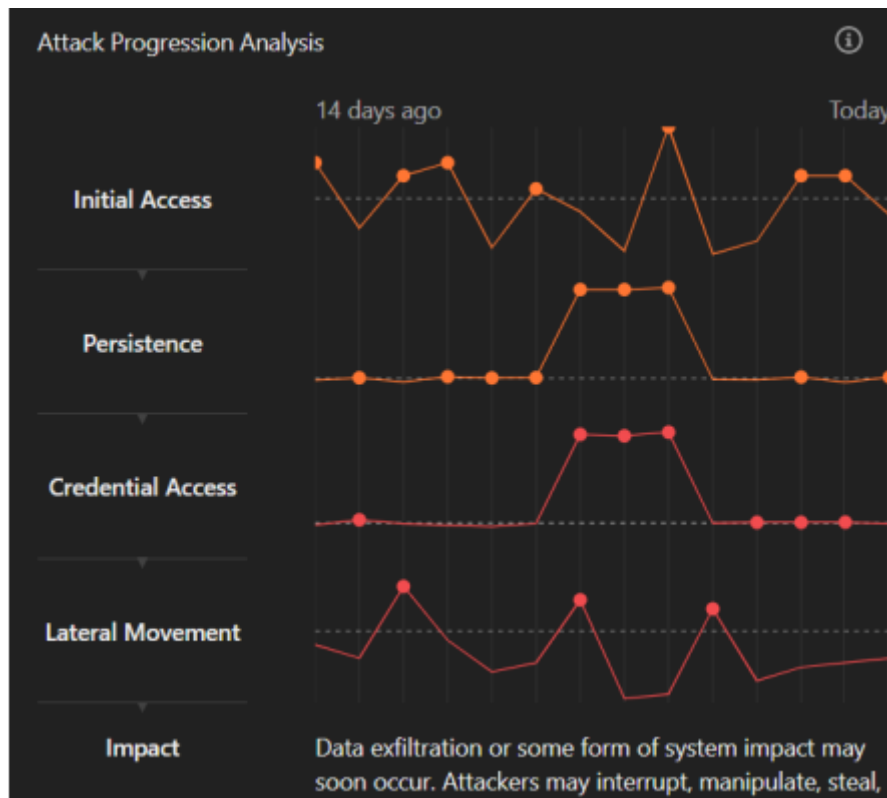


En términos generales, TAD es una visión de la empresa y a través de la agrupación de productos para proporcionar la fase de progreso del ataque, y también proporcionar la priorización del punto final para que el cliente pueda mitigar el problema.

Como se puede ver en la captura de pantalla de abajo, en TAD proporciona el progreso de cuatro fases de ataque por el resultado de TAD, para que el cliente pueda saber la fase de progreso del ataque en su organización. El evento más importante y peligroso del punto final según el resultado del TAD.

Hay cuatro fases de ataque, que son Acceso Inicial, Persistente, Acceso a Credenciales y Movimiento Lateral. Cada una de las fases tiene una línea de base. La línea base se calcula a partir de la media móvil de tad\_score de 30 días.

Si cualquier puntuación diaria en los últimos 14 días es superior a la línea base en cada fase, entonces se destacará como evento notable en TAD en el Análisis de Progreso de Ataque.



## 2. Tendencia del TAD en el análisis del progreso del ataque y el nivel de riesgo

Basado en las cuatro fases de ataque, hay un nivel de riesgo resumido que se muestra en la esquina superior izquierda como abajo:

ATTACK EXPOSURE

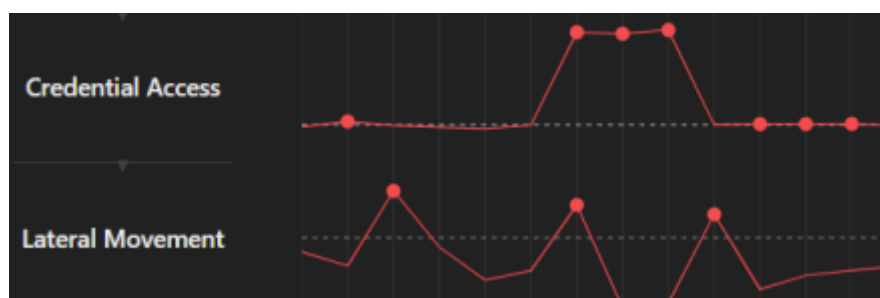
# High Risk

Action Required

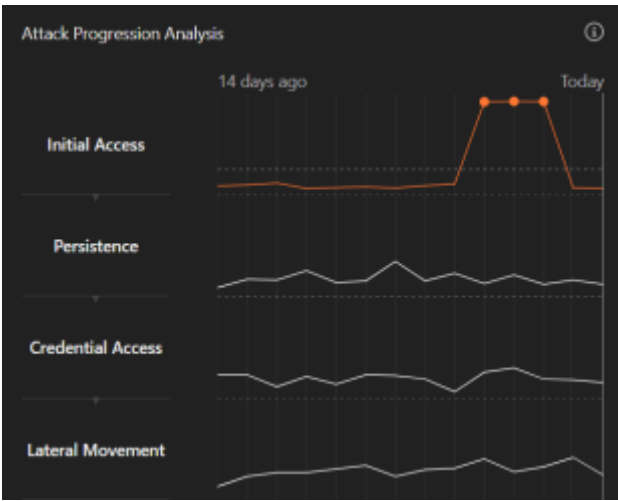
Attack indicators were found in your environment! Active campaigns (**Ryuk**, **Conti**) are targeting your organization. Immediate action is required.

Request help from Trend Micro Threat Experts

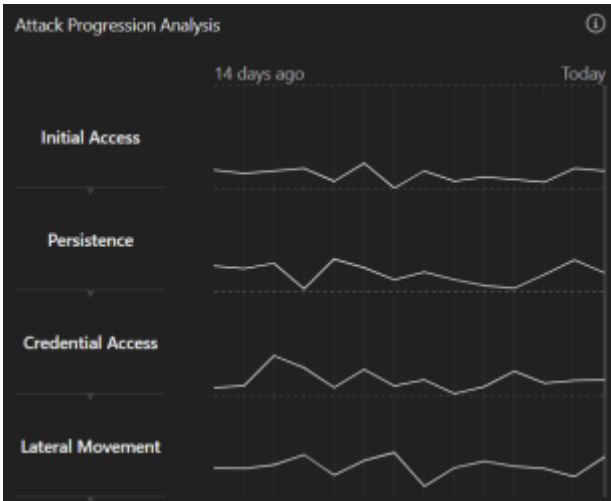
Si se produce algún evento notable en el acceso a credenciales o en el movimiento lateral, como se indica a continuación, el riesgo será alto. Esto significa que el entorno ha sido comprometido. El ataque ha sido progresado cerca de la etapa final y el ataque de alta severidad puede ocurrir en cualquier momento.



En caso contrario, si se produce algún evento digno de mención en el Acceso Inicial o en el Persistente, como se indica a continuación, será el riesgo medio. Esto significa que el entorno está bajo ataque.

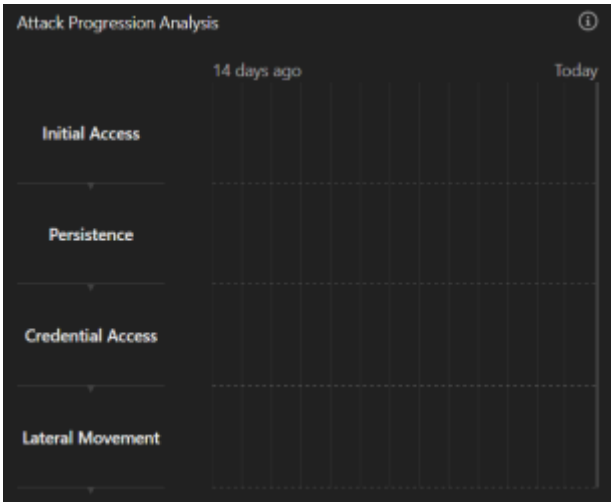


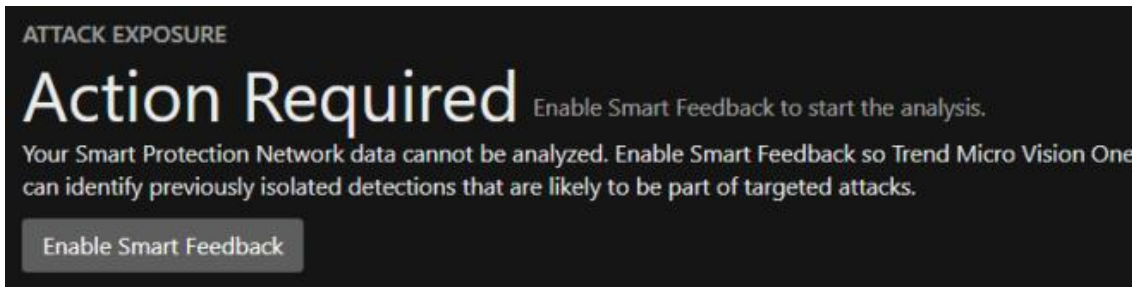
Si no hay ningún acontecimiento digno de mención en ninguna de las cuatro fases, se definirá como de bajo riesgo.



**No se puede analizar**

Si Trend Micro no puede recibir datos de retroalimentación en los últimos 14 días, se mostrará incapaz de analizar. Podría deberse a que el Smart Feedback no está habilitado, o en el entorno, un firewall impidió la retroalimentación.





Si el cliente es de **bajo riesgo**, y tiene un estado de **Smart Feedback inferior al 50%**. También se tratará como “No se puede analizar”.

### 3. Total at-risk Endpoints

El cliente puede obtener información más detallada sobre el evento digno de mención haciendo clic en el número de riesgo total junto al nivel de riesgo. El TAD proporciona la priorización, la razón y la acción recomendada para los puntos finales dignos de mención. Para que el riesgo pueda ser mitigado.



El cliente puede agrupar por punto final, gravedad o acción recomendada.

Total At-Risk Endpoints (10)					Contact Experts
Endpoint	Severity	Reason	Recommended action	First observed	
61d7592e-a41d-4d17-a0f9-99904e52ba9d	High	Attachment in phishing email opened by user (Path: C:\Downloads\vcsl\Error4.zip via EVX...	Enable Behavior Monitoring (Malware Behavior Blocking) and configure Predictive Machine Learning (Process detections L...	2021-05-20T15:27:00Z	
56f53c4d-6998-4384-baa7-dc22c5151352	Medium	Highly active malware found through user activity (Detection name: PUJWin32\MediaGet...	Configure the following settings: Web Reputation (Block pages containing malicious script), Behavior Monitoring (Malwar...	2021-05-20T15:27:00Z	
d7f8622a-4530-47f6-90b5-98d309121e6	Low	CBC website accessed (URL: https://www.google.com/Process: EVM\Specio Activator\VM...	Check account activity logs and use strong passwords.	2021-05-20T15:27:00Z	
Server GUID: 00000000-1013-0000-0000-000000000000					
Endpoint	Severity	Reason	Recommended action	First observed	
9c78332e-48b2-4255-85c1-e8bbaf3e9b63	High	Highly active malware found through user activity (Detection name: PUJWin32\MediaGet...	Configure the following settings: Web Reputation (Block pages containing malicious script), Behavior Monitoring (Malwar...	2021-05-20T15:27:00Z	
78200511-7804-4b79-ad9d-39dc98dc3ef	Medium	Attachment in phishing email opened by user (Path: C:\Downloads\vcsl\Error4.zip via EVX...	Configure the following settings: Web Reputation (Block pages containing malicious script), Behavior Monitoring (Malwar...	2021-05-20T15:27:00Z	
afbaa8c2-9081-43c3-9404-6222a2d3d54	Low	Attachment in phishing email opened by user (Path: C:\Downloads\vcsl\Error4.zip via EVX...	Contact Trend Micro Incident Response or Technical Support.	2021-05-20T15:27:00Z	
Server GUID: 00000000-1012-0000-0000-000000000000					
Endpoint	Severity	Reason	Recommended action	First observed	
b6f88955-0b66-4d97-a7d6-d661558264	High	Suspicious web shell running (Detection name: PUJWin32\MediaGet\AP) (Path: C:\Downloa...	Enable Behavior Monitoring (Malware Behavior Blocking) and configure Predictive Machine Learning (Process detections L...	2021-05-20T15:27:00Z	
5a29f8ae-4d75-4d88-a26a-d1601780a027	High	Attachment in phishing email opened by user (Path: C:\Downloads\vcsl\Error4.zip via EVX...	Enable Behavior Monitoring (Malware Behavior Blocking) and configure Predictive Machine Learning (Process detections L...	2021-05-20T15:27:00Z	
e8e0d83c-ec55-4832-b4a3-c0ef8aa10ad	Medium	CBC website accessed (URL: https://www.google.com/Process: EVM\Specio Activator\VM...	Enable Behavior Monitoring (Malware Behavior Blocking) on this endpoint.	2021-05-20T15:27:00Z	
930ec38d-df8b-4727-9d61-daff07db438	Low	CBC website accessed (URL: https://www.google.com/Process: EVM\Specio Activator\VM...	Enable Behavior Monitoring (Malware Behavior Blocking) on this endpoint.	2021-05-20T15:27:00Z	

### 4. Recommended Security Features

Además de la detección, TAD también muestra el estado de comprobación de la salud en el entorno del cliente. Es una función de seguridad recomendada.

#### Productos compatibles

No todos los productos de Trend Micro son soportados. A continuación, se enumeran los productos compatibles con TAD:

- Apex One OnPrem
- Apex One SaaS
- Deep Security Software
- Cloud One Workload Security

- Deep Discovery Inspector

A continuación, se definen el Smart Feedback, Predictive Machine Learning y Behavior Monitoring.

Antes de 2021/11/22

- Estado de la retroalimentación inteligente: recuento de servidores habilitados para la retroalimentación inteligente / recuento total de servidores
- Aprendizaje automático predictivo Estado: recuento de servidores habilitados para trendx / recuento total de servidores
- Monitorización del comportamiento Estado: recuento de puntos finales habilitados para la monitorización del comportamiento / recuento total de puntos finales

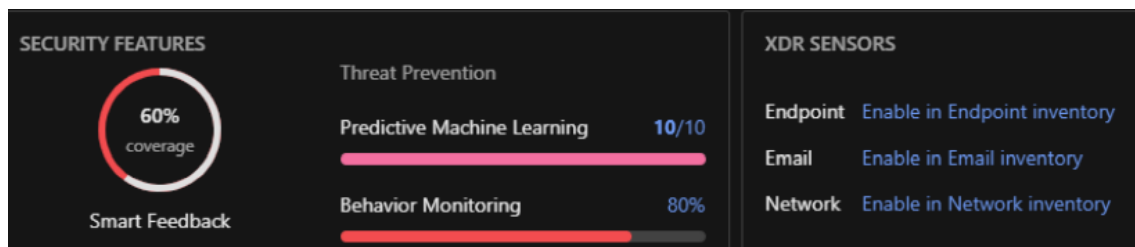
Después de 2021/11/22

- Smart Feedback: retroalimentación inteligente habilitada recuento de puntos finales / recuento total de puntos finales
- PML: trendx\_enabled\_server\_count / total\_server\_count
- BM: behavior\_monitoring\_enabled\_endpoint\_count / total\_endpoint\_count

Si todos los índices de retroalimentación pueden ser tan altos como sea posible, TAD puede tener más visibilidad para la evaluación del cliente. Sin embargo, *el estado se actualiza diariamente, por lo que habrá un retraso como máximo para el estado.*

En cuanto a los sensores del punto final, la red y el correo electrónico, están habilitados o deshabilitados para cada sensor. Sin embargo, si el cliente no es elegible para el sensor de punto final o de correo electrónico, sólo se mostrará el sensor de red a continuación.

(La siguiente es la nueva interfaz de usuario después de 2021/11/22)



El cliente puede habilitar la retroalimentación o el sensor haciendo clic en los enlaces "Habilitar".

Para indicar claramente al usuario el estado de Smart Feedback, PML y BM mediante los siguientes cajones.

- Smart Feedback: Calcula por conteo de servidores
- PML: Calcula por recuento de servidores
- BM: Calcular por el recuento de puntos finales

Smart Feedback Status		Behavior Monitoring Status	
Trend Micro Apex One (On-premises)		Trend Micro Apex One (On-premises)	
Management server +	Status	Management server +	Agent status
US-mng (%ipaddress%)	Disabled	US-mng (%ipaddress%)	23/125 (18.4%)
%hostname% (%ipaddress%)	Disabled	%hostname% (%ipaddress%)	n/N (nn.n%)
%hostname% (%ipaddress%)	Disabled	%hostname% (%ipaddress%)	n/N (nn.n%)
%GUID%	Enabled	%GUID%	n/N (nn.n%)
%GUID%	Enabled	%GUID%	n/N (nn.n%)
%GUID%	Disabled	%GUID%	n/N (nn.n%)
Deep Security Software		Predictive Machine Learning Status	
Trend Micro Apex One (On-premises)		Trend Micro Apex One (On-premises)	
Management server +	Status	Management server +	Status
%hostname% (%ipaddress%)	Enabled	US-mng (%ipaddress%)	Disabled
%hostname% (%ipaddress%)	Enabled	%hostname% (%ipaddress%)	Enabled
%Product name%		%hostname% (%ipaddress%)	Disabled
Management server +	Status	%GUID%	Enabled
%hostname% (%ipaddress%)	Disabled	%GUID%	Enabled
%hostname% (%ipaddress%)	Enabled	%GUID%	Disabled

## 5. Attack Campaign

Hay 6 campañas que Trend Micro está monitoreando y rastreando. TAD puede ayudar al cliente a detectar tempranamente una campaña potencial.

Sin embargo, cuanto antes identifiquemos el riesgo potencial, más difícil será concluir de qué campaña se trata, ya que el atacante puede utilizar herramienta genérica para realizar el ataque al principio.

Name	Description
<div> <div></div> <div>Ryuk</div> <div>New</div> </div>	<p>The number of targeted ransomware attacks, such as Ryuk, is rising. Attackers typically use BazarBackdoor to drop malware and the next step is to deploy the ransomware Ryuk to critical assets.</p> <p>North America Western Europe Windows Manufacturing Telecommunications Healthcare</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>
<div> <div></div> <div>Conti</div> </div>	<p>Malicious actors that use the Conti ransomware have operated continuously since May 2020. They send phishing emails to deliver delivery. In some cases, Cobalt Strike beacons linger quietly in the infected system for hours before deploying the Conti payload.</p> <p>North America South Asia Ethiopia Thailand Windows Hospitality and Leisure Healthcare Manufacturing</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>
<div> <div></div> <div>LockBit</div> </div>	<p>LockBit, which was first observed in 2019, recently resurfaced with version 2.0. Its updated features include automatic encryption for disabling processes and services in the affected system. LockBit 2.0 employs the double extortion scheme where operators threaten to leak data if the ransom is not paid.</p> <p>Europe North America East Asia Windows Manufacturing Education Government - Local</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>
<div> <div></div> <div>REvil / Sodinokibi</div> </div>	<p>Cybersecurity &amp; Infrastructure Security Agency (CISA) is taking action to understand and address the recent supply chain ransomware attacks. CISA encourages organizations to review the Kaseya advisory and immediately follow their recommendation to shut down the Kaseya VSA service.</p> <p>North America Southeast Asia Western Europe Windows Energy Manufacturing Telecommunications</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>
<div> <div></div> <div>Darkside</div> </div>	<p>In August 2020, the threat actor group Carbon Spider, associated with the REvil group, introduced a new ransomware called Darkside. Once it gains a foothold, it moves to the Domain Controller (DC), where it proceeds to steal credentials as well as other sensitive data.</p> <p>North America South America India Windows Manufacturing Financial Services</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>
<div> <div></div> <div>Nefilim</div> </div>	<p>First seen in March 2020, Nefilim employed a wide arsenal of tools and malware. It has also been analyzed as one of the first few ransomware groups to use double extortion, threatening to publish stolen information if the ransom is not paid.</p> <p>Windows Technology Manufacturing</p> <p><a href="#">Recommended actions</a> <a href="#">Learn more</a></p>