LOGICALIS
Architects of Change

Threat Trends Lab Report

Cyber Threat Intelligence:
Una Postura Proactiva de Ciberseguridad

SEPTIEMBRE 2021

'Threat Trends Lab Report', es un informe de investigaciones de seguridad, creado por el equipo de análisis e inteligencia de amenazas de Logicalis en Latinoamérica.

Ordinario

Extraordinario

Crítico

En la actualidad, la industria de la ciberseguridad se enfrenta a múltiples desafíos, actores de amenazas cada vez más persistentes, ciberataques materializados a nivel global, ciberamenazas más complejas y especializadas, además de una avalancha diaria de alertas de múltiples sistemas de seguridad no relacionadas y escasez de profesionales capacitados.

Por su parte, **Logicalis cuenta con una central de inteligencia de amenazas** que integra múltiples fuentes de información relacionada con IoCs, técnicas, tácticas, malware, actores y ciberamenazas. Además, realiza actividades de monitoreo, detección e investigación, para identificar patrones que ayudan a las empresas a prepararse mejor y anticiparse a las amenazas.

CTI, Inteligencia de Amenazas Cibernéticas ('**Cyber Threat Intelligence**' por sus siglas en inglés), es el conocimiento que permite **anticiparnos, prevenir y mitigar ciberamenazas**. Esta metodología está fundamentada en datos de valor que proporcionan un contexto acerca de quién está atacando, motivaciones, capacidades e indicadores de compromiso identificados, que permiten decisiones con un mayor grado de certeza.

Según Gartner, la inteligencia de amenazas es conocimiento basado en evidencia que incluye contexto, mecanismos, indicadores, implicaciones y asesoramiento orientado a la acción sobre una amenaza existente o emergente para los activos de información; agrega valor en todas las funciones, estrategia y operaciones de seguridad para todo tipo de empresas.

Imagina poder obtener información y detalles de un ciberataque ocurrido al otro lado del mundo, que te permita identificar sus características, el vector de ataque utilizado, las **técnicas, tácticas y procedimientos** (**TTP**s), el actor de amenaza detrás de los eventos, vulnerabilidades asociadas, tecnologías y herramientas involucradas, así como información de indicadores de compromiso maliciosos como direcciones IP, dominios y artefactos. Además, recomendaciones para tomar **medidas y aplicar controles de seguridad** que se anticipen a la ciberamenaza, que ayuden a neutralizarla o contener algún punto de su cadena de ataque, si esta llega a tu infraestructura.

De acuerdo con **Recorded Future** [1], compañía de seguridad cibernética, el **ciclo de vida de la inteligencia de amenazas** se compone de las siguientes **6 fases**:

1. Planificación y Dirección

Se inicia por hacer las **preguntas correctas para enfocar y priorizar la inteligencia**, de acuerdo con los objetivos y los factores que influyen en la organización. También es importante identificar **quién consumirá el resultado de las actividades de inteligencia**, como un equipo técnico de analistas o si va dirigido hacia un equipo gerencial o directivo encargado de tomar decisiones para la proyección de inversión en ciberseguridad.

2. Colección

Se **recolectan datos sin procesar**, de acuerdo con lo establecido en el punto 1, desde diferentes fuentes que pueden ser internas y externas, herramientas de seguridad, registros de gestión de incidentes, datos de la web abierta-profunda-oscura, etc. Esto puede contemplar información de **indicadores de compromiso (IoC), direcciones IP, hashes y dominios maliciosos**. Así mismo, puede incluir datos de vulnerabilidades, información relacionada a las empresas, noticias, tendencias, entre otros. Existen diferentes soluciones que utilizan aprendizaje autónomo para procesar y recopilar los datos; además, pueden integrarse con las herramientas de seguridad de las empresas (soluciones existentes) y luego conectar todos los puntos para proporcionar contexto sobre los eventos e indicadores de compromiso (IoC) y las tácticas, técnicas y procedimientos de los actores de amenazas.

3. Procesamiento

En esta fase se **organizan, clasifican y filtran los datos**. Se reconocen los datos de valor, la información redundante, los falsos positivos y negativos. Las organizaciones de todos los tamaños generan cientos, miles o incluso millones de eventos por día; demasiado para que un equipo de personas pueda procesarlas generando una tarea humanamente imposible. El objetivo ideal es **automatizar las tareas** por medio de herramientas y soluciones que tengan la capacidad de procesar los eventos, correlacionarlos, identificar eventos anómalos e inseguros y hacer una **primer clasificación (triage) de acuerdo con su nivel de criticidad**.

4. Análisis

Esta fase tiene como objetivo encontrar el **origen de los datos procesados**, identificar ciberamenazas, posibles incidentes de seguridad y notificar a los equipos encargados el detalle y los requisitos definidos en fases anteriores.

5. Difusión

El **producto obtenido se distribuye a los interesados**, esto debe llegar a las personas adecuadas en el **momento indicado**. Es recomendable hacer seguimiento al ciclo, utilizar herramientas de gestión de tickets, para tener trazabilidad de las solicitudes y que varios frentes puedan trabajar en conjunto para atender y documentar las solicitudes.

6. Comentarios

Se completa el ciclo después de recibir el resultado de inteligencia. Quien haya realizado la solicitud analiza si fue cubierta y respondidas las preguntas iniciales. Esto impulsa una **retroalimentación y mejora continua**.

La inteligencia de amenazas permite tener mejor conocimiento preparación y prevención con el objetivo de responder de forma anticipada a las ciberamenazas

Existen, regularmente referenciadas, **3 subcategorías para la inteligencia de amenazas**:

Estratégica

Proporciona una vista del panorama de ciberamenazas, con el objetivo de tener una **visión más amplia que permita tomar decisiones** acertadas relacionadas con la seguridad de la información y la ciberseguridad **a nivel ejecutivo y directivo**.

La información es presentada a través de reportes, dashboards y resúmenes, abarcando, desde una perspectiva estratégica, el contexto integral del sector y las características de la organización.

Táctica

Provee información relacionada con **TTPs** (**Técnicas-Tácticas-Procedimientos**), utilizados por actores de amenaza para realizar ciberataques.

Esta información está enfocada a **profesionales de TI y ciberseguridad**, para desarrollar estrategias de **detección y mitigación** contra estas amenazas.

Operacional

Brinda información relacionada con ciberataques, eventos y campañas de actores de amenaza para que los **equipos de gestión y respuesta a incidentes**, entiendan la **naturaleza, características, metodologías y tiempos de los ataques, como vulnerabilidades presentes, tecnologías o activos afectados y vectores de ataque**.

De esta forma, se pueden identificar los puntos vulnerables, el impacto y el riesgo de un ataque exitoso.

Muchas personas, equipos de trabajo y empresas que se beneficiarían de la inteligencia de amenazas, **no tienen acceso a este tipo de información**, lo que les genera una **visión limitada**, procesando los eventos que pasan al interior de sus ambientes tecnológicos, pero sin el contexto de lo que pasa a nivel global, nuevas tecnologías, técnicas de ataque, vulnerabilidades, amenazas de día cero e indicadores de compromiso, entre otros.

Así mismo, se abre la puerta a **ataques sobre la cadena de suministro** que podrían causar que cualquier software, aplicación o sistema al interior de la empresa (aún confiable para todos), sea comprometido y se convierta en malicioso (por ejemplo, los **casos SolarWinds y Kaseya**), poniendo en riesgo a toda la organización. Esto implica que, si no se toman acciones rápidamente para contener la amenaza, recursos internos como estaciones y servidores serán comprometidos, ya que se trata de una aplicación "legítima" que las soluciones de seguridad **no detectan como maliciosas, sino hasta después de 24, 48 o más horas**, tiempo durante el cual el daño puede ser catastrófico.

La inteligencia de amenazas se integra con las soluciones de ciberseguridad utilizadas por las organizaciones, ayudando a identificar lo que no es evidente, -como una dirección IP, dominio o artefacto sospechoso o malicioso-, sumando inteligencia y nuevas capas de seguridad. Estos son algunos de los beneficios de la CTI:

22%
más amenazas de seguridad identificadas antes del impacto

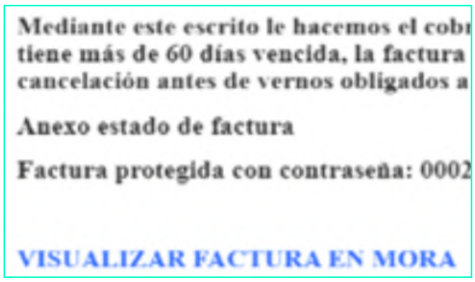
63%
resolución más rápida de amenazas de seguridad

10x
identificación temprana de amenazas

El SOC (Security Operations Center) de Logicalis aplicando Cyber Threat Intelligence

A continuación, veremos un ejemplo de actividades de **Cyber Threat Intelligence desarrolladas por el equipo del SOC** (Security Operations Center) **de Logicalis**, respecto a los eventos relacionados con una amenaza de **phishing-malware**.

Mensaje original:


Mediante este escrito le hacemos el cobr
tiene más de 60 días vencida, la factura
cancelación antes de vernos obligados a

Anexo estado de factura

Factura protegida con contraseña: 0002

VISUALIZAR FACTURA EN MORA

El mensaje informa acerca de un **supuesto cobro** de una factura vencida que deberá pagarse de forma inmediata para no incurrir en otras consecuencias. Se observa cómo **invita a abrir/descargar** la supuesta factura en mora con el objetivo oculto de instalar **malware**.

Artefactos:
Archivo adjunto "SUCEPDFINFO4633460001.rar" (protegido con contraseña)

Asunto:
"GACETA INFORMATIVO N°003, PERCEPCIÓN DE IMPORTE VENCIDA N°014, RATIFICAR EL RECIBIDO"

Remitente:
"smxxza@coxxnzasbxa.com.co"

Verificación de header (IoC)

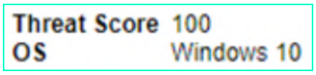
Una de las primeras opciones para obtener IoCs rápidamente es analizar la cabecera o header del correo electrónico. Allí, se pueden identificar detalles, como el remitente original del mensaje (puede estar enmascarado), la dirección IP original que envió el mensaje, entre otros.

Análisis dinámico (sandboxing)

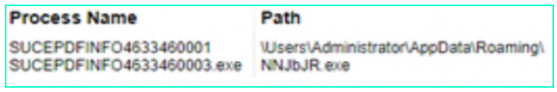
Análisis sobre los archivos o artefactos identificados en el correo electrónico que permite conocer el comportamiento y características de un artefacto (como un malware).

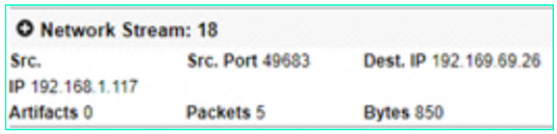
Esta muestra se ejecutó en una sandbox privada, sin embargo, existen servicios disponibles para uso público como Hybrid Analysis y Joe Sandbox.

Se identifica un score de 100, el artefacto es malicioso:



Se destacan algunos **comportamientos maliciosos** como la creación de un archivo ejecutable por parte de un proceso, inyección excesiva de código a través de un proceso remoto, peticiones DNS hacia un dominio malicioso y conexiones hacia una dirección IP pública:





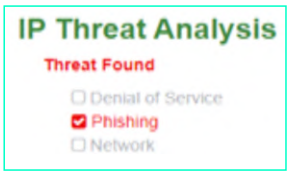
En este análisis se identificaron IoCs adicionales:

- **Peticiones IP pública:** 192.169.69.26
- **Peticiones DNS:** osiris8612.duckdns.org
- **SHA256:** be29ba1886febe73c7f7a4b1b663d14a9a0270ab8aec354a334266d0ffa51ff8

Profundizar información de IoCs

Ahora, podemos investigar y obtener mayor información de estos IoCs a través de fuentes de inteligencia abiertas (OSINT) o a través de fuentes privadas comerciales, como centrales de CTI:

- **192.169.69.26 (phishing-malware) [6] [7]**

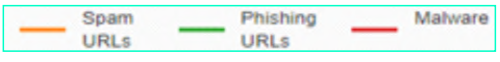


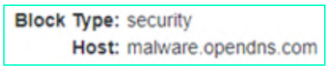
El **análisis permite detectar más de 200 dominios** relacionados, identificados con un look-up reverso, los cuales pueden ser utilizados como **aplicaciones supuestamente válidas en mensajes de phishing y sitios web falsos** como:

- hypercube-softwares.duckdns.org
- banquepopulaire.duckdns.org
- cpanel.bokepviral18-whasappgrup.duckdns.org

Al utilizar un servicio de DNS gratuito como 'duckdns', se busca “anonimizar” las operaciones. Esta IP también tiene más de 200 puertos TCP abiertos para establecer conexiones HTTP, HTTPS, SMTP, SSH, LDAP, entre otras.

- **osiris8612.duckdns.org (phishing-malware) [8] [9]**





Con estos IoCs se pueden buscar reportes públicos de otros artefactos que tengan relación.

Este es un ejemplo de otros artefactos o muestras de malware, con comunicaciones hacia esta misma IP y dominio. De estos, podemos identificar características, técnicas, comportamientos y tácticas:

Adicionalmente, podemos investigar la familia de malware a la que pertenecen estos artefactos y qué actor de amenaza o grupo de APT esta detrás. APT36 y APT41 se relacionan con esta amenaza y familias de malware como njRAT, AsyncRAT, XtremeRAT y Azorult.

Adicionar IoCs en plataformas de seguridad

Finalmente, podemos **tomar acciones para contener la amenaza** a través de actividades como remover los correos electrónicos sospechosos de los buzones de los usuarios, bloquear el buzón y dirección IP del remitente, bloquear las firmas digitales (hash) de los artefactos (archivos) y bloquear direcciones IP y dominios de comunicaciones de C&C (comando y control) identificados. Esto se puede aplicar en múltiples herramientas a nivel de perímetro, endpoint, correo electrónico, navegación, entre otros. Además, se pueden agregar alertamientos en herramientas como un SIEM, para identificar la presencia de estos IoCs.

El **equipo de contraofensiva de Logicalis**, utiliza las características e indicadores de compromiso identificados dentro de las actividades de inteligencia de amenazas, para emitir reportes, boletines y recomendaciones hacia las empresas y sus equipos de ciberseguridad. También, dentro de los servicios gestionados, junto con su equipo de MSSP (managed security service providers), se realizan actividades de **preparación, detección, análisis y contención** de indicadores observables y amenazas.

Recomendaciones

- Contar con un **equipo encargado de la ciberseguridad** al interior de la organización.
- Contar con un **equipo de gestión y respuesta a incidentes**.
- Desarrollar **habilidades y capacidades** en inteligencia de amenazas.
- **Integrar soluciones** de inteligencia de amenazas con las plataformas y herramientas de seguridad al interior de la organización.
- Integrar la **inteligencia de amenazas a procesos, procedimientos y prácticas** de ciberseguridad en la organización.
- **Entrenar y capacitar** a los equipos de seguridad de la información, ciberseguridad y equipos de TI, en inteligencia de amenazas y respuesta a incidentes.
- Tener una **respuesta rápida, oportuna y efectiva** contra las amenazas
- **Identificación y detección** temprana de amenazas.
- Implementar medidas y soluciones que permitan **automatizar y tomar acciones rápidas** durante un incidente de seguridad, como bloquear IoCs en múltiples plataformas.
- **Automatizar** procesos y procedimientos de ciberseguridad.
- **Aumentar** las habilidades y capacidades de los equipos de ciberseguridad.

Indicadores de Compromiso

Algunos **IoC**s relacionados son:

- 192.169.69.26
- .duckdns.org
- be29ba1886febe73c7f7a4b1b663d14a9a0270ab8aec354a334266d0ffa51ff8
- f081ae101d95d4555bb6e068e7e3d3b3b0b8688030bf156b8c642ad0d293a59c
- 8e04c5a167e27303f532e6cf3f6196e27b641690
- 7097dd1811f4ac95699d05f4acdbef0d

Referencias

- [1] https://www.recordedfuture.com/threat-intelligence/
- [2] https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
- [3] https://labs.k7computing.com/index.php/malspam-campaigns-download-njrat-from-paste-sites/
- [4] https://unaaldia.hispasec.com/2017/05/continuos-ataques-a-usuarios-colombianos-por-xtremerat.html
- [5] https://lab52.io/blog/apt-c-36-recent-activity-analysis/
- [6] https://exchange.xforce.ibmcloud.com/ip/192.169.69.26
- [7] https://www.virustotal.com/gui/ip-address/192.169.69.26
- [8] https://www.virustotal.com/gui/domain/osiris8612.duckdns.org
- [9] https://exchange.xforce.ibmcloud.com/url/osiris8612.duckdns.org

---

La **ciberseguridad** es uno de los **desafíos más importantes** que las organizaciones enfrentan hoy en día. El enfoque manejable, adaptable, resistente y receptivo del esquema de seguridad de Logicalis, permite a empresas de todo tamaño e industria, **impulsar los negocios digitales de manera segura**. **Contáctanos** a continuación y conoce nuestras soluciones:

¡Comencemos!

LOGICALIS
Architects of Change