LOGICALIS

Threat Trends Lab Report

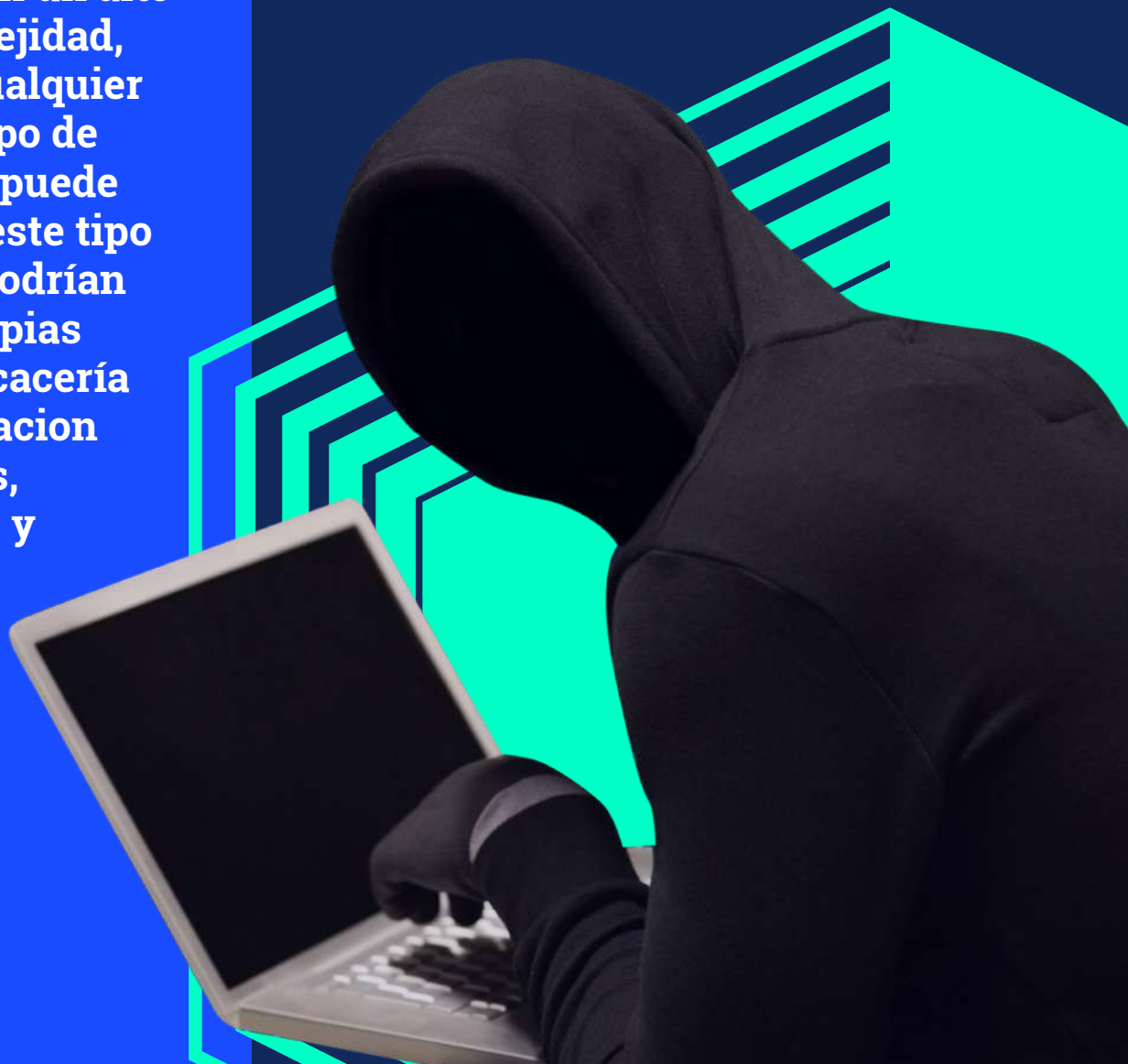
El Arte del Threat Hunting, Ventajas y Desafíos

Junio 2022

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.

La cacería de amenazas o “Threat Hunting” es un término muy utilizado en la actualidad, que probablemente hemos escuchado debido al crecimiento de ciberataques y ciberamenazas. Este término suena como algo sofisticado y con un alto grado de complejidad, sin embargo, cualquier empresa y equipo de ciberseguridad puede tener acceso a este tipo de servicios o podrían realizar sus propias actividades de cacería con una preparacion previa, recursos, procedimientos y herramientas.

El equipo del centro de operaciones de seguridad (SOC) de Logicalis se encarga de realizar actividades continuas y periódicas para cacería de amenazas sobre los ecosistemas e infraestructura de sus clientes, para propender en detectar y analizar comportamientos y patrones maliciosos, que no son detectados de forma automática por las herramientas de seguridad y podrían estar relacionados con una ciber amenaza. De igual manera en obtener la mayor cantidad de información posible, para comprender las características, comportamientos, indicadores, técnicas y tácticas utilizadas; con el objetivo de detectar oportunamente y responder a tiempo ante las ciberamenazas.



¿Qué es Threat Hunting?

Son actividades proactivas y periódicas, ejecutadas por personas (humanos), para realizar la búsqueda de comportamientos sospechosos, malicosos o patrones no seguros en los entornos tecnológicos e infraestructuras de las empresas, como podría ser en comunicaciones y conexiones de red, correo electrónico, navegación web, recursos en la nube, a nivel de dispositivos y usuarios finales, etc.

No podemos confiar 100% y basarnos únicamente con la detección de las herramientas y soluciones de ciberseguridad que están implementadas en nuestra organización; ya que muchas actividades, malware y amenazas de día cero y comportamientos maliciosos pueden pasar desapercibidos (activación de cuentas, escalamiento de privilegios, conexiones de gestión remota a través de RDP/SSH). Con la experiencia y conocimiento de los equipos de ciberseguridad, más el entendimiento de los objetivos del negocio, modo de operación y otros factores, se pueden realizar actividades de cacería de amenazas, para ir en búsqueda de patrones maliciosos presentes en el ecosistema, que no han sido detectados.

Este ha sido un foco importante en los centros de operaciones de seguridad modernos, que trabajan para mejorar la detección a toda costa, debido al gran crecimiento de nuevas amenazas con mayores niveles de complejidad. Nos encontramos con amenazas y actores de amenaza más sofisticados, que hacen lo posible por evadir los controles de seguridad y no ser detectados. Esto hace más compleja la detección de amenzas y protección de las organizaciones.

Según la reciente encuesta “Threat Hunting in uncertain times” realizada por SANS [3], se menciona que el 91% de las organizaciones reportan mejoras en la velocidad y la precisión de la respuesta ante ciberamenazas, realizando actividades de Threat Hunting. También a la pregunta ¿cuál es su nivel de madurez en Threat Hunting?, el 39,6% respondió que están aún en proceso de maduración, 24,8% se consideran maduros, 20,8 limitados e inmaduros y el 14,4% muy maduros.

Algunos otros datos relevantes de esta encuesta son:

- **75%** de las empresas encuestadas prefieren herramientas de detección tradicional como antimalware, SIEM, IPS; para la detección en actividades de Threat Hunting
- **51%** de los encuestados realizan el seguimiento de las actividades de Threat Hunting de forma manual
- **51%** de las organizaciones identifican o reconocen la falta de habilidades y entrenamiento de las personas, como la barrera principal para realizar actividades de Threat Hunting de forma exitosa

Hay algunos mitos alrededor de la cacería de amenazas:

Se puede hacer de forma automatizada

El principal aporte humano en una cacería es remediar el resultado de algo que una herramienta no encontró automáticamente o que pudo haber ignorado. Debe ser proactivo y no reactivo. Requiere el aporte de un analista humano, basado en una hipótesis. El propósito es encontrar lo que su sistema automatizado o una herramienta de seguridad no detecta. Una alerta de una herramienta ciertamente puede brindar un punto de partida para una investigación o informar una hipótesis, pero un analista debe trabajar en una investigación para comprender y ampliar el contexto de lo que se encontró y obtener realmente el valor total de la cacería.

La cacería solo se puede llevar a cabo con una gran cantidad de datos y herramientas avanzadas

Aunque puede parecer un término nuevo, los analistas y equipos de seguridad han realizado actividades de “cacería” durante años. Un analista que quiera iniciar la cacería de amenazas debe sacar provecho de todos los recursos que tenga disponibles dentro de su equipo y organizacion. Entender cómo funcionan las herramientas de seguridad para hacer búsquedas avanzadas, entender en dónde buscar, qué buscar, cómo buscar, etc. Investigar y definir algunos procesos o técnicas de cacería, además pensar cómo poder identificar algunas técnicas y tácticas comunes de ataque conocidas.

Threat Hunting es una actividad que preferiblemente deben ejecutar los analistas de élite con muchos años de experiencia y conocimiento

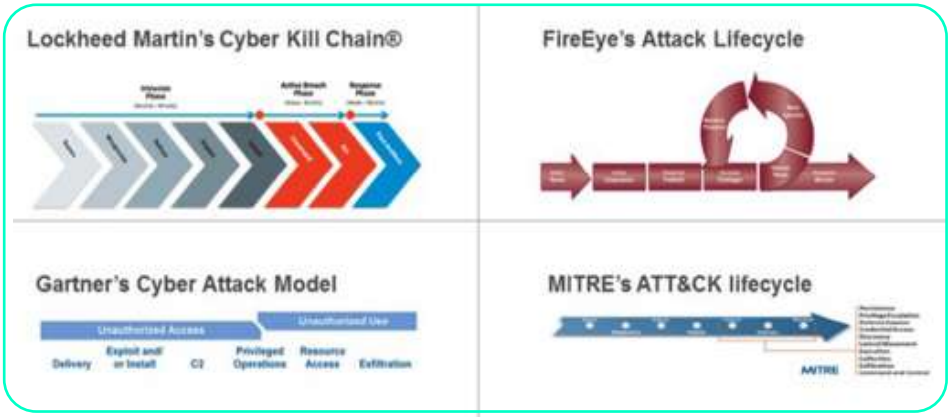
Hay muchas técnicas de cacería con diferentes niveles de complejidad. Sin embargo, no todas requieren años en dominarse. El analista y los equipos deben prepararse para saber qué hacer, definir procedimientos, tener algunas búsquedas base para identificar eventos interesantes, qué hacer con la información o pistas obtenidas, cómo reconocer la presencia o sospecha de una ciberamaneza y cómo poder definir una estrategia para neutralizarla. Aunque tenga que aprender sobre el camino, no deben tener temor de sumergirse en este mundo e ir mejorando las habilidades, experiencia y capacidades del equipo progresivamente.

Elegir un modelo de ataque

Existen diferentes modelos de ataque que pueden servir de referencia, se debe elegir el más adecuado, como Cyber kill chain, Mitre ATT&CK, entre otros. Estos ayudarán a identificar TTPs, actividades y comportamientos de los atacantes, que queremos buscar a través de las actividades de cacería a realizar. Después de seleccionar un modelo, el siguiente paso es entender cada una de sus fases e identificar las actividades de los atacantes que más le preocupan, como: explotación, elevación de privilegios, exfiltración de datos, etc. Definir cuáles de estas actividades son críticas, altas, medias o bajas. Cada fase de un modelo puede incluir múltiples categorías de tácticas de alto nivel que un adversario podría emplear. Aquí una lista de ejemplo de algunas posibles actividades de atacantes que podría identificar:

Reconocimiento, escaneo
Entrega, armamento
Explotación, persistencia
Inyección DLL
Comando y control
Pass the hash
Tunelización de DNS

A continuación, compartimos algunos modelos de ataque que podrían ser utilizados en las actividades de Threat Hunting:



¿Cada cuánto hacer estas actividades?

Luego de definir el modelo de ataque, entender sus fases y nivel de criticidad, es de gran utilidad contar con un calendario que incluya la periodicidad de las actividades de hunting a realizar.

Es importante priorizar la cacería de acuerdo con la criticidad de las actividades o eventos encontrados. Entre más adelante o avanzada la cadena de ataque dentro del modelo seleccionado, mayor criticidad y relevancia tendrán. No se puede tratar de la misma manera un evento identificado en la fase de reconocimiento a uno que esté en la fase de escalación de privilegios o movimiento lateral, ya que podría significar un compromiso en algunos recursos de la organización.

Se podría dedicar una semana a la búsqueda de actividades que se pueden ubicar en el fin de la cadena de ataque, que podríamos considerar como altos y críticos (Acción en objetivos, instalación, ejecución, exfiltración, mantener acceso). Otra semana para los eventos que se pueden catalogar como de criticidad media (Entrega, explotación, evasión de defensas, acceso a credenciales) y otra para los eventos bajos (Reconocimiento, escaneo, armamento, desarrollo de herramientas, acceso inicial). También se pueden realizar estas actividades, por ejemplo, la misma semana, en diferentes días y horarios. Esta programación estará a discreción del equipo, las necesidades de la empresa, los clientes y el entorno.

Vamos a definir un proceso de ejemplo Threat Hunting con 4 fases, sugerido por Sqrrl [1]

1. Crear hipótesis: Una cacería comienza con la creación de una hipótesis, sobre algún tipo de actividad que podría estar ocurriendo en el ecosistema o la infraestructura. Estas hipótesis suelen ser formuladas por los analistas de seguridad, basados en su conocimiento, experiencia, factores externos, inteligencia de amenazas, alertas o eventos anómalos, además de experiencias pasadas.

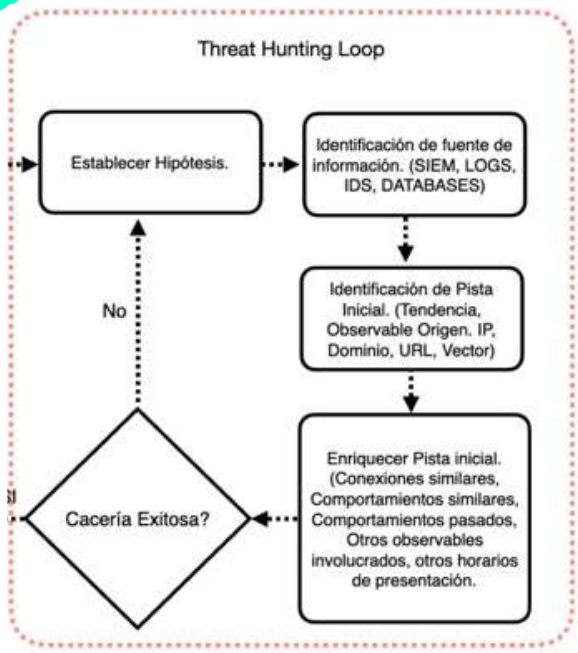
2. Investigar: Un cazador sigue las hipótesis investigando a través de varias herramientas y técnicas para descubrir nuevos patrones maliciosos, reconstruir rutas de ataque y técnicas utilizadas.

3. Enriquecer y descubrir: Usando técnicas manuales, procedimientos, herramientas y flujos de trabajo, el cazador podrá trabajar en descubrir técnicas, tácticas y procedimientos (TTPs). En este paso se puede comprobar o refutar la hipótesis inicial y determinar si hay la presencia de alguna anomalía o ciberamenaza, obtener las evidencias y realizar las investigaciones necesarias.

4. Análisis: Las cacerías exitosas forman la base para realizar actividades que permitan mejorar la detección de amenazas, reconocimiento de comportamientos, patrones y TTPs. Además, enriquecer la información de inteligencia, procedimientos y herramientas automatizadas. Estas cacerías deben ser documentadas, con los detalles obtenidos, que sirva como una buena base de conocimiento para el equipo, para definir flujos de trabajo, buenas prácticas, tipos, herramientas, no repetir la investigación y detalle de patrones ya identificados previamente.

De igual manera, la información de las cacerías se puede utilizar para mejorar mecanismos de detección existentes, como la actualización de reglas de SIEM, firmas de IPS/IDS, detección en herramientas antimalware, EDR, etc. Cuanto más conozcas el entorno y tu propia red, mejor podrás defenderla, por lo que tiene sentido registrar y aprovechar nuevos hallazgos en las cacerías realizadas.

En la siguiente ilustración un loop de Threat Hunting, que también puede ser utilizado como referencia.



¿Cuáles son algunas herramientas recomendadas para realizar Threat Hunting?

El resultado de la cacería puede depender de 3 factores importantes: habilidades, visibilidad e inteligencia de amenazas. Visibilidad podría ser la más importante, ya que, sin una buena visibilidad de fuentes de datos, eventos, alertas y logs, es complejo detectar amenazas. Se debe tener el panorama completo de lo que pasa en la organización para poder hacer un seguimiento y trazabilidad de un ataque, para poder aplicar inteligencia y utilizar las herramientas indicadas, junto con las habilidades del equipo.

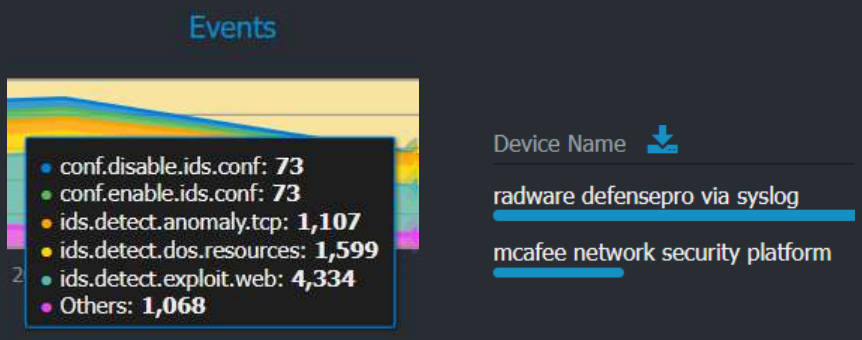
SANS [3] menciona en su reporte que el 75% de las organizaciones utilizan en primer lugar herramientas como EDR, SIEM, IPS/IDS, para la detección y respuesta. En segundo lugar, herramientas de búsqueda configurables y personalizables como Powershell, scripts, WMI. En tercer lugar, se destacan las plataformas de threat intelligence. Dentro de otras herramientas, se menciona el uso de inteligencia artificial (AI) y machine learning (ML). Además del uso de herramientas comerciales y licenciadas, como el de herramientas open source como: SIFT, SOF-ELK, Rekall, Plaso.

Ejemplo:

Desarrollo actividades de Threat Hunting equipo Logicalis

Iniciamos realizando una búsqueda sobre nuestras herramientas más utilizadas para la detección e investigación, como el SIEM/correlacionador. En query vamos a buscar eventos medios, altos o críticos que fueron permitidos (no se descartaron/denegaron), en herramientas de seguridad IPS y AntiDDoS.

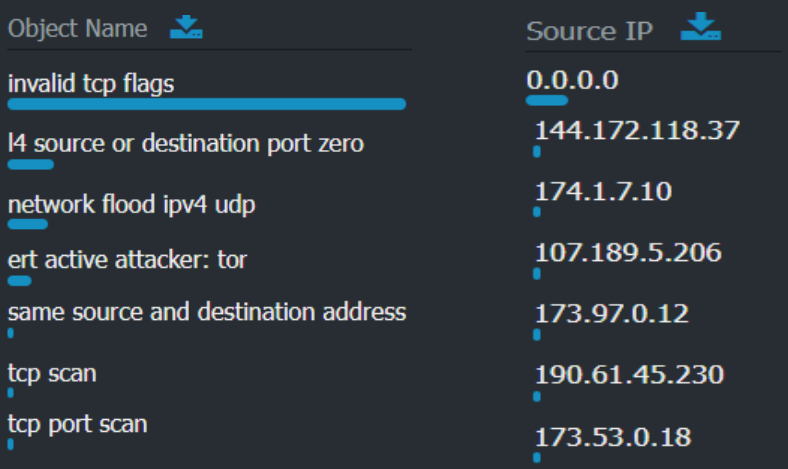
Query: ('Device Name' = 'radware defensepro via syslog' OR 'Device Name' = 'mcafee network security platform') AND 'Event Type' NOT LIKE *deny* AND 'Vendor Priority' != low



Podemos apreciar una importante cantidad de eventos con estas características, en la búsqueda realizada para las últimas 24 horas, 3 a 7 días y 15 a 30 días. Vamos a enfocarnos en los eventos más destacados, con mayor número de repeticiones, los tipos de ataque más comunes, direcciones IP origen/destino con más eventos, puertos origen/destino más utilizados, etc.

Por el conocimiento del equipo, hemos identificado que las peticiones de red que se hacen desde el puerto de origen 0, están relacionadas a actividades de escaneos de red y reconocimiento.

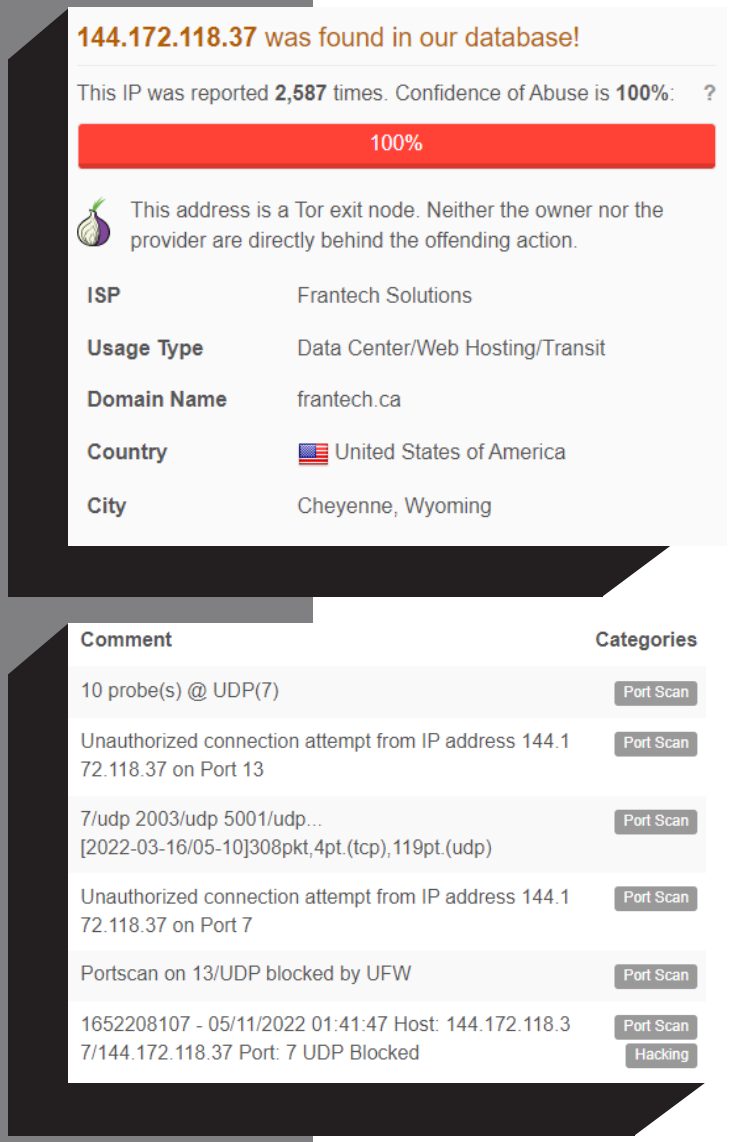
Esta podría ser una hipótesis, si agregamos a la búsqueda este parámetro, podríamos encontraremos peticiones con comportamientos de escaneo de red. 'Source Port' = 0



En los resultados nos encontramos con eventos relacionados a escaneo/reconocimiento de red, como pueden ser “invalid tcp flags”, banderas TCP inválidas en las conexiones, muy utilizadas por herramientas de escaneo como “nmap”, en donde por el tipo de escaneo se pueden enviar peticiones con las banderas SYN, ACK, RST, para saber si un puerto/servicio está abierto y en escucha o está filtrado por algún dispositivo de seguridad red. También “l4 source or destination port zero”, el puerto de origen o destino utilizado en la conexión de red es el cero, relacionado con escaneos de red. “same source and destiantion address” utiliza la misma dirección de origen y destino, no se hace referencia a una dirección IP en detallada, sino que se utiliza una dirección no especificada como 0.0.0.0. “tcp por scan”. Es evidente que allí se están haciendo escaneos de puertos TCP disponibles en la red.

Esto es un comportamiento habitual para recursos expuestos o que le dan la cara a internet. “internet facing” son eventos que se pueden generar todos los días en un SOC, ya que hay miles de aplicaciones y robots haciendo escaneos y reconocimientos de redes y segmentos de red en internet.

Si buscamos mayor información de las direcciones IP con más eventos generados, probablemente vamos a encontrar comportamientos relacionados con escaneo de red y otras actividades maliciosas reportadas en diferentes centrales de inteligencia de amenazas. Por ejemplo, la dirección IP 144.172.118.37, tiene reportes de actividades maliciosas, dentro de las categorías reportadas, se destaca principalmente Port Scan. Además, esta IP es un nodo de Tor, que permite la salida de comunicaciones entre las diferentes zonas de la web, como la web superficial, web profunda y web oscura (deep-dark web); en donde se mueve un mercado negro de ciberamenazas y actividades ilícitas, con grupos de crimen organizado.



144.172.118.37 was found in our database!

This IP was reported **2,587** times. Confidence of Abuse is **100%**: ?

100%

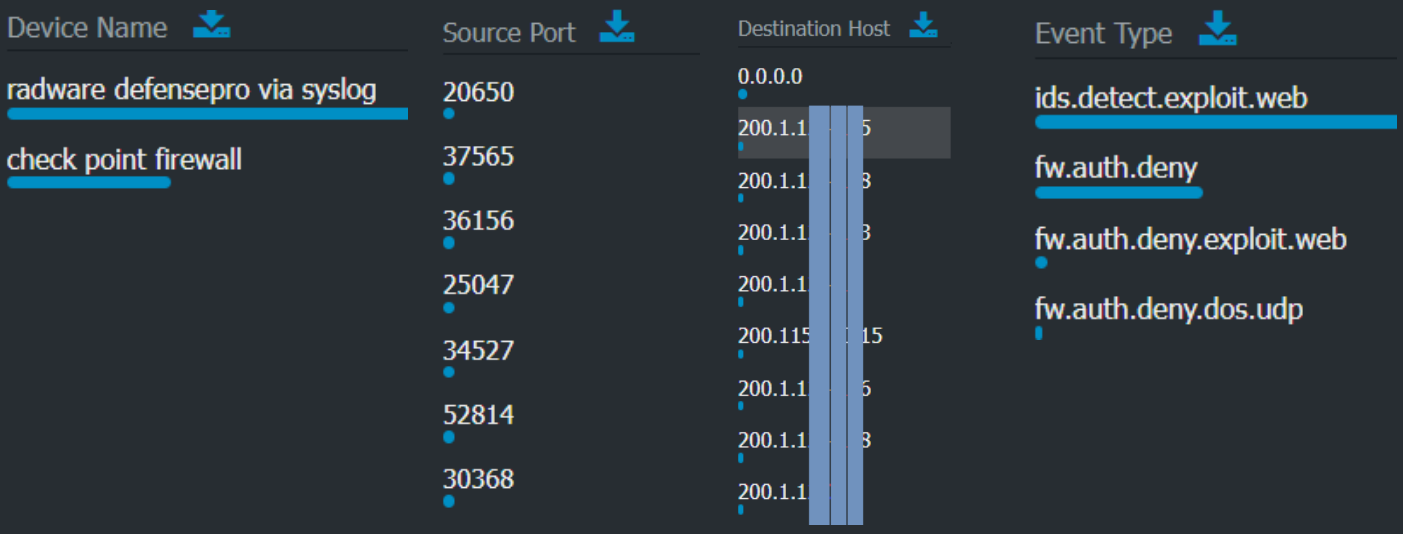
This address is a Tor exit node. Neither the owner nor the provider are directly behind the offending action.

ISP	Frantech Solutions
Usage Type	Data Center/Web Hosting/Transit
Domain Name	frantech.ca
Country	United States of America
City	Cheyenne, Wyoming

Comment	Categories
10 probe(s) @ UDP(7)	Port Scan
Unauthorized connection attempt from IP address 144.172.118.37 on Port 13	Port Scan
7/udp 2003/udp 5001/udp... [2022-03-16/05-10]308pkt,4pt.(tcp),119pt.(udp)	Port Scan
Unauthorized connection attempt from IP address 144.172.118.37 on Port 7	Port Scan
Portscan on 13/UDP blocked by UFW	Port Scan
1652208107 - 05/11/2022 01:41:47 Host: 144.172.118.37/144.172.118.37 Port: 7 UDP Blocked	Port Scan Hacking

Podríamos hacer más búsquedas con esta IP identificada, como verificar que otros eventos se han generado en las herramientas de seguridad disponibles, buscando comunicaciones entrantes y salientes en la infraestructura en las últimas 24 horas, 7 días, un mes, para identificar otros comportamientos.
'Source IP' = 144.172.118.37

En la gráfica podemos ver tendencias en las comunicaciones y eventos generados por esta dirección IP. Ha realizado constantemente peticiones sobre la infraestructura, muchos de estos eventos han sido denegados en dispositivos de seguridad de red como firewalls y otros alertados por AntiDDoS.



En las imágenes anteriores podemos identificar que esta IP utiliza múltiples puertos de origen y destino en sus comunicaciones, como patrón de escaneos. También se identifican peticiones sobre múltiples direcciones IP de destino, IPs públicas de la infraestructura de la empresa, como reconocimiento de segmentos de red públicos, estas peticiones se hicieron sobre más de 100 direcciones IP. Otras actividades reconocidas son intentos de explotación web y peticiones de denegación de servicio.

Con estas búsquedas estaríamos haciendo actividades de hunting, enfocadas a la fase de reconocimiento de los modelos de ataque, asimismo podríamos buscar eventos para las siguientes fases.

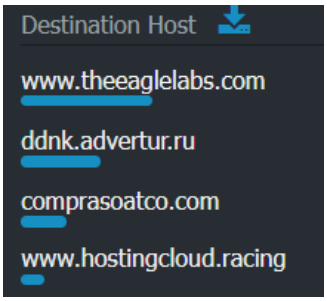
Si nos movemos hacia otra fase de la cadena de ataque y buscamos eventos relacionados con intrusión o explotación, realizamos otra búsqueda 'Object Type' = intrusions. Estas búsquedas se pueden realizar sobre tipos de ataque, técnicas, tácticas o comportamientos conocidos.

Encontramos eventos de **“memchached-server-reflect”** y “**http-misc-zmeu-scanner”**. Si buscamos más información de ZmEu scanner, encontramos lo siguiente: “escáner de vulnerabilidades que busca servidores web que estén abiertos a ataques a través de phpMyAdmin. También intenta adivinar contraseñas SSH a través de métodos de fuerza bruta y deja una puerta trasera persistente. Es un bot que intenta encontrar vulnerabilidades en phpMyAdmin (generalmente busca el archivo phpmyadmin/scripts/setup.php) y otras aplicaciones web.

Con esta información, conocemos que el objetivo de este tipo de robot son los servidores de bases de datos con phpMyAdmin y con el servicio SSH disponible. Podríamos hacer búsquedas para verificar si algún servidor de base de datos o con SSH ha establecido conexiones hacia esta dirección IP, si las peticiones han sido permitidas o han sido denegadas.

En el resultado, también encontramos otros observables con más eventos generados, direcciones IP haciendo escaneo de aplicaciones (como ZmEu), en búsqueda de vulnerabilidades, para un posterior intento de explotación. Para la dirección IP 72.5.34.114 encontramos reportes de actividades maliciosas relacionadas con el Port Scan, Web App Attack y Hacking.

Vamos un poco más adelante, sobre otra fase de ataque y realizamos búsquedas sobre eventos relacionados con malware, presencia, infección o compromiso por malware 'Event Type' = av.detect.virus.



Encontramos varios sitios web alertados por malware. Si consultamos la reputación de los sitios web, podemos encontrar que algunos están reportados en centrales de inteligencia de amenazas, como sitios usados por malware. Hacemos un nslookup, para consultar la dirección IP que tiene este dominio en registros DNS.

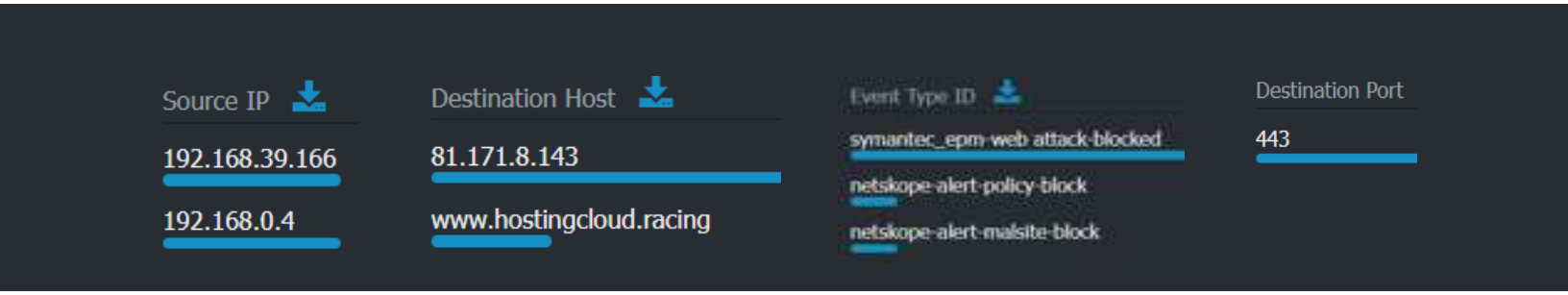
C:\Users\despinosa>nslookup hostingcloud.racing
Respuesta no autoritativa:
Nombre: hostingcloud.racing
Address: 81.171.8.143

Ahora, podemos investigar si esta dirección IP tiene más dominios maliciosos registrados, para ello utilizamos un servicio que verifica los registros DNS pasivos y efectivamente encontramos que tiene más dominios configurados y apuntando hacia esta IP. Estos sitios web pueden ser utilizados en campañas maliciosas de phishing, sitios web falsos o como servidores de comando y control, para descargar partes de código malicioso dentro la cadena de ataque.

81.171.8.143 reverse IP lookup

Domain	Hosting Provider
hostingcloud.racing	Netherlands
freecontent.date	Netherlands
webassembly.stream	Netherlands
freecontent.stream	Netherlands
www.wasm.stream	Netherlands
wasm.stream	Netherlands
www.hostingcloud.racing	Netherlands
hashing.win	Netherlands

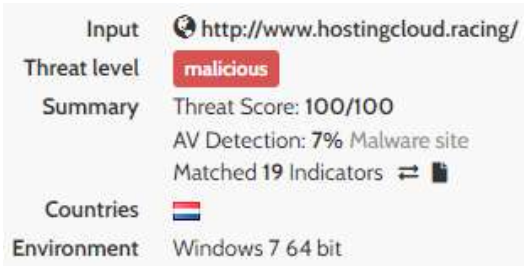
Buscamos que peticiones o conexiones se realizaron dentro de la red interna hacia esta IP maliciosa 'Destination IP' = 81.171.8.143.
Obtuvimos algunos resultados y esto se puede traducir en que alguna máquina podría estar comprometida, hay algún código malicioso presente tratando de establecer conexión hacia internet, para realizar otras acciones de comando y control.



Hay que verificar en estas máquinas porque se están realizando estas peticiones hacia el sitio web malicioso, si hay la presencia de un código malicioso, si son hábitos de navegación no seguros del usuario final, que programas o aplicaciones están instaladas o ejecutándose, que conexiones de red se han establecido, porque puertos, que servicios y procesos están corriendo en la máquina, que extensiones están instaladas en los navegadores web, que usuarios han iniciado sesión en el sistema, entre otros.

Estas peticiones fueron bloqueadas por las herramientas de seguridad antimalware, sin embargo, en ciberseguridad es importante tener en cuenta no solamente si la acción final, si la petición/conexión fue permitida, sino la intencionalidad. Una máquina interna puede realizar 2.000 peticiones que son denegadas hacia un destino no seguro, así se contengan las peticiones, es necesario investigar que está generando las peticiones, pensar qué, cómo, cuándo, dónde, por qué, para qué. Esto permite identificar comportamientos maliciosos y generar alertas tempranas, para responder oportunamente a los incidentes de seguridad.

Si vamos más allá, podemos buscar en algunos servicios de sandboxing, muestras de malware relacionadas con los indicadores de compromiso (IOCs), que hemos identificado, como la dirección IP 81.171.8.143 y el sitio web hostingcloud.racing. En estos servicios de sandboxing permiten subir y analizar muestras de software sospechoso que pueden ser malware, para identificar sus comportamientos y características. Podemos identificar si hay malware que establezca conexiones esta IP y dominio; así tendremos más detalles de la amenaza.
Efectivamente encontramos en hybrid-analysis [4] muestras de malware que establecen conexiones con esta misma IP y dominio malicioso:



El resultado del análisis de una de estas muestras, nos muestran peticiones y conexiones sobre la IP y el dominio, por lo tanto, podríamos mejorar nuestra detección a través de reglas y casos de uso en las herramientas de seguridad, agregando estos indicadores, para que se genere una alerta temprana si algún recurso de la red intenta hacer una resolución DNS o intenta establecer una conexión.

Network Analysis

DNS Requests

Download DNS Requests (CSV)

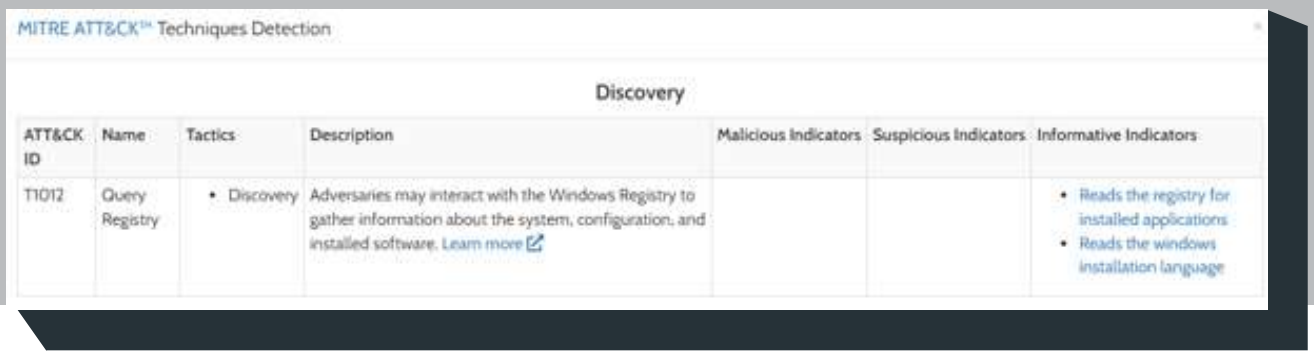
Domain	Address
www.hostingcloud.racing OSINT	81.171.8.143 TTL: 471

Contacted Hosts

Download Contacted Hosts (CSV)

IP Address	Port/Protocol
81.171.8.143 OSINT	80 TCP

Allí también podemos encontrar técnicas utilizadas por el malware, con relación al MITRE ATT&CK y conocer más de la amenaza



MITRE ATT&CK™ Techniques Detection

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more			• Reads the registry for installed applications • Reads the windows installation language

A continuación, algunos otros indicadores maliciosos:

Malicious Indicators

External Systems

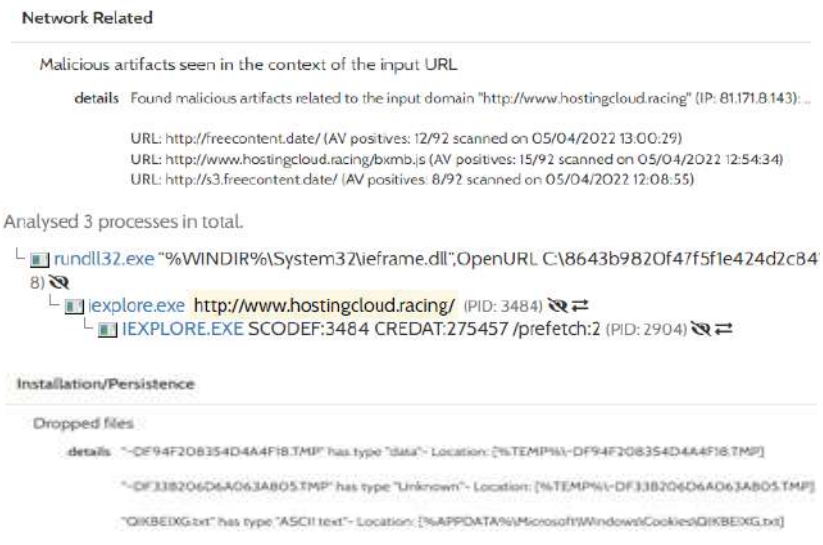
Sample was identified as malicious by a large number of Antivirus engines

details 13/92 Antivirus vendors marked sample as malicious (14% detection rate)
source External System
relevance 10/10
research Show me all reports matching the same indicator

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.



Network Related

Malicious artifacts seen in the context of the input URL

details Found malicious artifacts related to the input domain "http://www.hostingcloud.racing" (IP: 81.171.8.143): ..

URL: http://freecontent.date/ (AV positives: 12/92 scanned on 05/04/2022 13:00:29)
URL: http://www.hostingcloud.racing/bxmb.js (AV positives: 15/92 scanned on 05/04/2022 12:54:34)
URL: http://s3.freecontent.date/ (AV positives: 8/92 scanned on 05/04/2022 12:08:55)

Analysed 3 processes in total.

rundll32.exe "%WINDIR%\System32\ieframe.dll",OpenURL C:\8643b9820f47f5f1e424d2c84
8)
iexplore.exe http://www.hostingcloud.racing/ (PID: 3484)
IEXPLORE.EXE SCODEF:3484 CREDAT:275457 /prefetch:2 (PID: 2904)

Installation/Persistence

Dropped files

details "~DF94F2083S4D4A4F18.TMP" has type "data" - Location: [%TEMP%\~DF94F2083S4D4A4F18.TMP]

"~DF338206D6A063AB05.TMP" has type "Unknown" - Location: [%TEMP%\~DF338206D6A063AB05.TMP]

"QIKBEIXG.txt" has type "ASCII text" - Location: [%APPDATA%\Microsoft\Windows\Cookies\QIKBEIXG.txt]

Estas peticiones del código malicioso afortunadamente fueron detectadas y bloqueadas por el antimalware de endpoint, estaba relacionado a actividades de minado de criptomonedas “JSCoinminer”. Sin embargo, para tomar una acción oportuna y pensar en neutralizar la amenaza, debemos tomar los detalles de indicadores de compromiso y comportamiento, para que las herramientas de seguridad los puedan reconocer y neutralizar.

Object Name	Field 4
jscoinminer download 55 attack	c:\program files\google\chrome\applicati...
jscoinminer website attack	c:\users\jcifuentes\appdata\local\google\...

c:\program files\google\chrome\application\chrome.exe (10)

(6)

Un resumen de los indicadores y observable obtenidos:

IOCs
www[.]hostingcloud[.]racing
www[.]hostingcloud[.]racing/wyzw.js
http://freecontent.date/
http://s3.freecontent.date/
freecontent.date
webassembly.stream
hashing.win
81.171.8.143
File SHA256: 3c58a8b5dfc41d7d6145ebee8a520e6a4dfcb6a7f8f8dec2c5cd6c67556b0d24 (AV positives: 8/74)
File SHA256: d107b5ade99a35bd7fbada7cbebd566ff8b6bb0889d3112fffa5b424ced2a4e4 (AV positives: 18/74)
File SHA256: 2b129a812d5db300084ea598fb6f7baff734128b7bbf78cc60b1b59753850527 (AV positives: 8/74)
File SHA256: 48fadb4da982b77fcc8cc59c60174ebb20309d3e6fb30ebe714a5d8a2898d13c (AV positives: 8/74)
File SHA256: 8ebd8f8ef196af479c9996861d446d4a594b897e09acbae9dd08e7b4609d9589 (AV positives: 9/74)
File SHA256: de76ad183eb5854faeef3e79c09c58393a94d475341f4d0bef6def5610b597fe
urlblockindex_1_.bin
e4f30e49120657d37267c0162fd4a08934800c69
05NIEQ7W.txt
af39ea1015ad4bf5098d3c1cae3476f8cf5690d4
OBUV2R2W.htm
7dd71afcfb14e105e80b0c0d7fce370a28a41f0a
DF33B206D6A063A805.TMP
3ea9aa188ee5eab175b616826f4cc8e9bf545a87
D0E654D9-CBA4-11EC-A9D8-080027C1C7D3.dat
217825b92ca4abc4553634ae912686041415441e
search_1_.json
08afdc36927b6c4e03c3088e5c9c812cc4215ede

Recomendaciones

Trabajar en la capacitación, desarrollo de conocimiento y habilidades del equipo de ciberseguridad para realizar actividades de Threat Hunting, gestión de incidentes e investigaciones.

Tener una buena visibilidad de los eventos de seguridad del ecosistema desde múltiples frentes, a nivel de red, correo, navegación, control de acceso, gestión de identidades, endpoint aplicaciones y bases de datos, etc.

Contar con las herramientas adecuadas para las actividades de Threat Hunting, en la búsqueda de eventos, comportamientos y patrones sospechosos (SIEM, IPS, IDS, EDR, Antimalwrae, Gateway de correo, web proxy, etc).

Definir un procedimiento de Threat Hunting, una periodicidad y documentar estas actividades de cacería, para mejorar la base de conocimiento y buenas prácticas del equipo.

Mejorar las capacidades de detección de amenazas a través de los resultados exitosos de la cacería de amenazas.

Implementar y mejorar las capacidades de detección y respuesta dentro del centro de operaciones de seguridad (SOC).

Mejorar las capacidades del equipo en cacería de amenazas a través de análisis de malware, investigaciones a nivel de red, endpoint, correo y aplicaciones.

Utilizar servicios de terceros que cuenten con la experiencia y capacidades para realizar actividades de Threat Hunting.

Referencias

1 https://www.threathunting.net/files/hunt-evil-practical-guide-threat-hunting.pdf

2 https://www.betaalvereniging.nl/wp-content/uploads/DEF-TaHiTI-Threat-Hunting-Methodology.pdf

3 https://www.sans.org/white-papers/sans-2021-survey-threat-hunting-uncertain-times/

4 https://www.hybrid-analysis.com/sample/8643b9820f47f5f1e424d2c8413850d2e271d3f30bf455e39912d0957037a4cc/62728b87fc4d480b077e4862

¡Comencemos!

LOGICALIS