Botnets: Estado del arte y taxonomía de una amenaza sigilosa

Valentín Torassa Colombero, Santiago Roatta, Pedro Lopez

Facultad de Tecnología Informática, Universidad Abierta Interamericana (UAI), Rosario, Argentina
{Torassa Colombero}valentintorassa@hotmail.com
{Roatta}santiago.Roatta@uai.edu.ar
{Lopez}Pedro.Lopez@uai.edu.ar

Resumen. Las botnets se han convertido en una de las amenazas más prominentes y, a su vez, sigilosas en el panorama de la ciberseguridad. Estas redes de dispositivos comprometidos por malware, controladas de forma remota por ciberdelincuentes, representan una preocupación real tanto para individuos como para grandes organizaciones, empresas e incluso gobiernos. Estos dispositivos abarcan desde computadoras personales y servidores hasta dispositivos IoT y móviles, combinando la potencia de todos los equipos infectados de la red para lanzar ataques coordinados y masivos que pueden comprometer la infraestructura digital y la seguridad en línea en general. Para comprender estas redes en profundidad, se explorará la anatomía de las mismas y sus etapas de desarrollo y sus posibles estructuras de comando y control. Se examinan los diversos tipos de ataques más frecuentes perpetrados a través de botnets, incluidos ataques DDoS, distribución de malware y ransomware, así como la minería de criptomonedas y las campañas de spam masivo y phishing. Se incluyen casos de estudio de ataques modernos, como la botnet Mirai y Meris. Finalmente, se analizan estrategias de defensa, detección y mitigación.

Palabras clave: Botnet, Ataques DDoS, Malware, Ciberseguridad, Cibercrimen

1 Introducción

En el contexto de la ciberseguridad la amenaza latente de las botnets se plantea como uno de los más persistentes, pero a su vez uno de los que más de ser percibido. Estas redes de dispositivos comprometidos, controladas de manera remota por un operador, han demostrado ser la columna vertebral de una amplia gama de actividades delictivas en línea, desde ataques de denegación de servicio distribuido (DDoS) hasta robo de información personal y corporativa, y una variedad de otros ciberdelitos. A medida que la tecnología avanza y con la globalización de la interconexión y el internet, el impacto y la proliferación de las botnets solo parecen crecer, presentando desafíos cada vez mayores para individuos, empresas y gobiernos en todo el mundo [1].

El término "botnet" es un acrónimo de "robot" y "red", que describe la naturaleza distribuida de estas infraestructuras maliciosas. En su forma más básica, una botnet consta de una serie de dispositivos comprometidos, conocidos como bots o zombis, que han sido infectados con malware y pueden ser controlados remotamente por un operador, el “pastor de robots” o atacante. Estos dispositivos infectados pueden incluir computadoras, servidores, dispositivos IoT e incluso dispositivos móviles [1].

Una de las funciones principales de las botnets es facilitar los ataques de denegación de servicio distribuido (DDoS), una táctica que ha sido utilizada para interrumpir servicios en línea, sitios web y redes empresariales. Los ataques DDoS funcionan abrumando un objetivo con un flujo abrumador de tráfico de red, lo que resulta en la saturación de sus recursos y la incapacidad de responder a solicitudes legítimas [3]. Las botnets son instrumentales en la ejecución de estos ataques, ya que permiten a los operadores coordinar y dirigir grandes volúmenes de tráfico malicioso desde una variedad de dispositivos comprometidos, lo que dificulta su mitigación.

Sin embargo, la utilidad de las botnets no se limita a los ataques DDoS. Estas redes también se han utilizado para una variedad de otros fines delictivos en línea, incluido el robo de información confidencial, el lanzamiento de campañas de phishing, la distribución de malware y ransomware, y la participación en actividades ilegales como la minería de criptomonedas [2]. La flexibilidad y escalabilidad de las botnets las convierten en una herramienta poderosa para los actores malintencionados, que pueden adaptar su funcionalidad para adaptarse a una amplia gama de objetivos y escenarios de ataque.

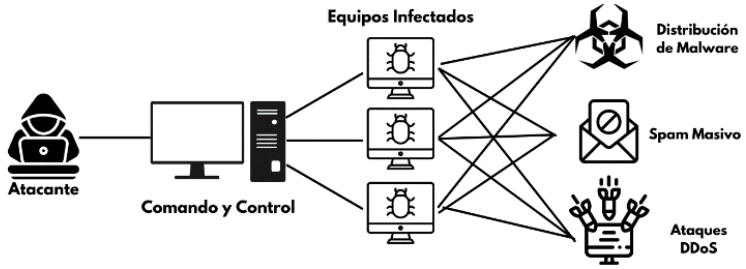

Fig. 1. Cadena de control y ataque de una botnet con comando centralizado.

La evolución de las botnets ha sido un proceso constante, impulsado en gran medida por avances en tecnología y tácticas de defensa cibernética. A medida que los sistemas de seguridad se han vuelto más sofisticados, los operadores de botnets han respondido con técnicas de evasión más elaboradas y métodos de ocultamiento, como el uso de técnicas de encriptación y comunicaciones encubiertas y P2P [1]. La creciente popularidad de dispositivos IoT ha ampliado aún más el conjunto de posibles objetivos para las botnets, ya que muchos de estos dispositivos carecen de las protecciones de seguridad adecuadas y son vulnerables a la explotación.

2 Anatomía de una botnet

2.1 Componentes de una botnet

El primer componente clave de una botnet son los dispositivos comprometidos, también conocidos como bots o zombis. Estos dispositivos, que abarcan una amplia gama de tecnologías y plataformas, constituyen la infraestructura básica sobre la cual se construye y opera la botnet. Desde computadoras personales hasta servidores, dispositivos IoT (Internet de las cosas) e incluso dispositivos móviles como smartphones y tabletas, todos son susceptibles de ser comprometidos y utilizados como nodos en una botnet [1]. La infección de estos dispositivos se produce a menudo a través de técnicas de ingeniería social, como correos electrónicos de phishing, descargas de archivos maliciosos o aprovechamiento de vulnerabilidades de software [2]. Una vez infectados, estos dispositivos se convierten en nodos dentro de la botnet, listos para recibir y ejecutar comandos del operador.

El siguiente componente es el sistema de comando y control (C&C). Este sistema actúa como el cerebro de la botnet, permitiendo al operador comunicarse y controlar de manera remota los dispositivos infectados. Los sistemas de comando y control pueden ser servidores centralizados, redes descentralizadas con sistemas P2P (peer-to-peer). El operador utiliza el sistema de comando y control para enviar instrucciones a los dispositivos infectados, como lanzar ataques DDoS, robar información o propagar malware adicional [5].

Otro elemento de la botnet es el operador, también conocido como botmaster o "pastor de robots". Este individuo, o grupo de individuos, es responsable de establecer y mantener la botnet, reclutar nuevos dispositivos infectados, enviar comandos a través del sistema de comando y control y beneficiarse de las actividades delictivas llevadas a cabo por la botnet [1]. Los operadores de botnets suelen ser hackers experimentados o criminales cibernéticos que buscan obtener ganancias financieras o causar daño a sus objetivos.

2.2 Etapas de una botnet

Las botnets pasan por varias etapas en su ciclo de vida, desde la infección inicial de dispositivos hasta su activación para actividades maliciosas. Estas etapas son cruciales para entender su funcionamiento y diferencias con otros tipos de malware.

1. **Infección inicial**: Los dispositivos objetivo son comprometidos y se convierten en parte de la botnet mediante la explotación de vulnerabilidades

de software, ingeniería social o engaño de usuarios para descargar malware. Una vez comprometido, el malware se instala y se comunica con el sistema de comando y control (C&C) [4].

2. **Ampliación:** La botnet se expande reclutando nuevos dispositivos comprometidos para aumentar su tamaño y capacidad, propagando el malware a través de redes locales o Internet [4]. Algunas botnets utilizan técnicas automatizadas para escanear dispositivos vulnerables y propagar el malware eficientemente [6].
3. **Estado latente:** Los dispositivos comprometidos permanecen inactivos, sin actividad maliciosa visible, esperando instrucciones del operador. Durante esta fase, los dispositivos pueden realizar actividades encubiertas como la minería de criptomonedas o espionaje mediante keyloggers [7].
4. **Activación:** Los dispositivos reciben instrucciones del operador a través del sistema de C&C y se activan para llevar a cabo actividades maliciosas como ataques DDoS, robo de información o propagación de malware adicional [4]. La activación puede ser desencadenada por eventos específicos, instrucciones programadas o comandos del operador [6].

2.3 C&C: Centralizado vs. Descentralizado

El sistema de comando y control (C&C) actúa como el cerebro central que permite al operador comunicarse y controlar remotamente los dispositivos infectados. A continuación, se describen los dos modelos de administración más frecuentes de C&C en botnets: los servidores centralizados y descentralizados [5].

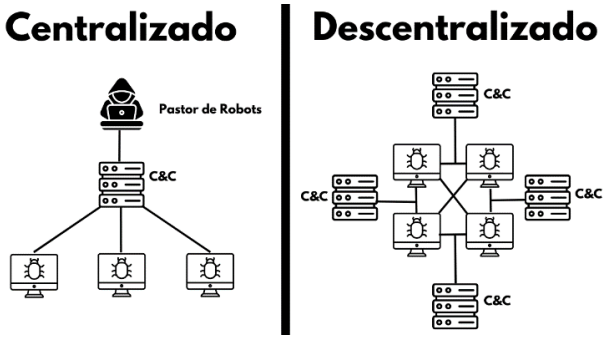

Fig. 2. Comando y control centralizado y descentralizado

En un modelo de administración de C&C centralizado, todos los dispositivos comprometidos se comunican directamente con un servidor central que actúa como punto de control único. Este servidor central, controlado por el operador de la botnet, coordina todas las actividades maliciosas y envía instrucciones a los nodos infectados. El uso de un servidor centralizado simplifica la gestión y el control de la botnet, ya que todas las comunicaciones pasan a través de un punto central. No obstante, este modelo centralizado presenta ciertas vulnerabilidades. Si el servidor central es identificado y desactivado por las autoridades o los equipos de seguridad, la botnet puede quedar inactiva y perder su capacidad de coordinación y control y, sobre todo, las comunicaciones directas con un servidor central son más fáciles de detectar,

bloquear y trackear por parte de los sistemas de seguridad, lo que es una preocupación no menor para los ciberdelincuentes que buscan la mayor seguridad y privacidad posible [5].

En contraste con el modelo centralizado, el modelo de administración de C&C descentralizado distribuye la comunicación y el control entre múltiples nodos dentro de la botnet. En este modelo, no hay un servidor central único; en su lugar, los dispositivos comprometidos se comunican entre sí de forma peer-to-peer (P2P) o a través de una red descentralizada. Cada nodo infectado actúa como un punto de comando y control, lo que permite una mayor resiliencia ante fallas o desconexiones de nodos. Esto a su vez, ayuda a dificultar la detección y la desactivación. Dado que no hay un punto centralizado de control, no existe un único punto de falla que pueda ser identificado y deshabilitado para neutralizar la botnet; Siendo más difíciles de detectar y bloquear, ya que no siguen patrones de tráfico predecibles [5].

3 Ataques a través de botnets

Las botnets se han consolidado como herramientas preferidas por delincuentes cibernéticos para llevar a cabo una cierta gama de ataques en los que se desenvuelven especialmente bien.

3.1 Ataques DDoS

Un ataque de denegación de servicio distribuido (DDoS) se caracteriza por abrumar un objetivo con un flujo masivo de tráfico de red, saturando sus recursos e impidiendo que responda a solicitudes legítimas [3]. A diferencia de un ataque de denegación de servicio (DoS) convencional, que involucra uno o pocos dispositivos, un ataque DDoS utiliza numerosos dispositivos comprometidos distribuidos geográficamente, coordinados a través de una botnet [8].

La ejecución de un ataque DDoS implica tres pasos: reclutamiento de dispositivos comprometidos, coordinación a través de la botnet y lanzamiento del ataque [3]. El operador envía instrucciones a los dispositivos, que inundan el objetivo con tráfico malicioso, saturando sus recursos y derribando el servicio.

El objetivo principal de un ataque DDoS es interrumpir servicios en línea como sitios web, servidores y aplicaciones web. Al abrumar estos servicios, los atacantes causan interrupciones en las operaciones comerciales, generan pérdidas financieras y dañan la reputación de las organizaciones afectadas.

Una técnica común en los ataques DDoS es obtener la dirección IP pública del servidor objetivo, permitiendo a los atacantes dirigir el tráfico malicioso directamente al servidor [8]. Esto se logra mediante escaneo de red, análisis de tráfico o ingeniería social. Con la dirección IP pública, los atacantes pueden lanzar ataques DDoS de manera más efectiva.

Los ataques DDoS pueden clasificarse en varios tipos según su ejecución y el objetivo específico del ataque. A continuación, se analizarán los tres tipos de ataques DDoS más comunes, centrándose en sus técnicas y el impacto en los servicios en línea.

3.1.1 Ataques volumétricos

Los ataques volumétricos son una de las formas más destructivas de ataques DDoS y se caracterizan por su capacidad para inundar la infraestructura de red del objetivo con un volumen masivo de tráfico malicioso. Estos ataques se centran en abrumar los recursos de ancho de banda del servidor objetivo, lo que resulta en la saturación de la conexión de red y la inaccesibilidad del servicio para los usuarios legítimos [9].

La técnica principal utilizada en los ataques volumétricos es la amplificación de tráfico, donde los atacantes aprovechan protocolos de red vulnerables para amplificar el tráfico malicioso dirigido al servidor objetivo [10].

Los ataques volumétricos son una de las formas más destructivas de ataques DDoS y se caracterizan por su capacidad para inundar la infraestructura de red del objetivo con un volumen masivo de tráfico malicioso. Estos ataques se centran en abrumar los recursos de ancho de banda del servidor objetivo, lo que resulta en la saturación de la conexión de red y la inaccesibilidad del servicio para los usuarios legítimos [9]. Uno de los métodos más comunes para lograr esto es a través de ataques de amplificación de DNS.

En un ataque de amplificación de DNS, los atacantes envían solicitudes falsificadas a servidores DNS abiertos que están configurados para responder a consultas de manera indiscriminada. Cuando el servidor DNS recibe estas solicitudes falsificadas, responde enviando una respuesta mucho más grande de lo que fue la solicitud inicial, lo que amplifica el tráfico dirigido al objetivo [10].

La amplificación de DNS es especialmente efectiva porque los servidores DNS abiertos pueden responder con respuestas amplificadas que son muchas veces más grandes que las solicitudes originales. Esto significa que los atacantes pueden utilizar un pequeño volumen de solicitudes falsificadas para generar un gran volumen de tráfico dirigido al objetivo; Lanzando ataques de gran escala con relativa facilidad [10].

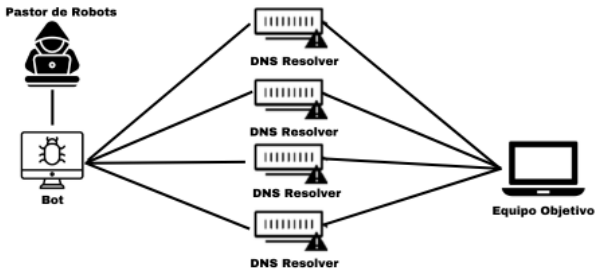

Fig. 3. Ataque volumétrico de ampliación de tráfico por DNS

Los ataques de amplificación de DNS son solo uno de los muchos métodos utilizados en los ataques volumétricos. Otros métodos, como los ataques de inundación UDP, SYN flood y ICMP flood [9].

3.1.2 Ataques de protocolo

Los ataques de protocolo se centran en explotar vulnerabilidades en los protocolos de

comunicación utilizados por el servidor objetivo, lo que resulta en la interrupción o la degradación del servicio. Estos ataques pueden dirigirse a protocolos de red o incluso protocolos de aplicación. En un ataque de inundación SYN, por ejemplo, los atacantes explotan la forma en que el protocolo TCP maneja las conexiones de red, enviando una gran cantidad de solicitudes SYN falsificadas al objetivo y haciendo que el servidor agote sus recursos al intentar establecer conexiones que nunca se completan [9]. Estos ataques pueden ser muy difíciles de defender, ya que a menudo no se pueden distinguir del tráfico legítimo.

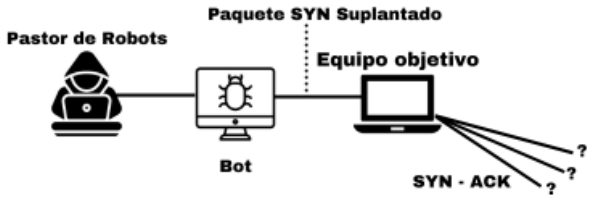

Fig. 4. Ataque de protocolo de inundación de SYN

3.1.3 Ataques a la capa de aplicación

Los ataques a la capa de aplicación se centran en explotar vulnerabilidades en las aplicaciones y servicios alojados en el servidor objetivo. Estos ataques apuntan a agotar los recursos de la aplicación, como la CPU, la memoria y el ancho de banda, mediante el envío de solicitudes maliciosas diseñadas para consumir recursos de manera ineficiente [9].

Los ataques de solicitud de HTTP es un ejemplo común de ataque a la capa de aplicación. En este los atacantes envían un gran número de solicitudes HTTP al servidor objetivo sobrecargando sus recursos y haciendo que la aplicación sea inaccesible para los usuarios legítimos.

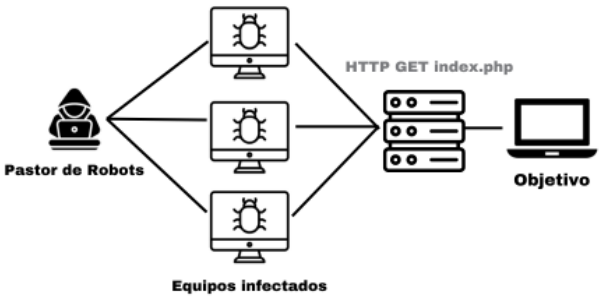

Fig. 5. Ataque de capa de aplicación

3.2 Distribución de Malware y Ransomware

La distribución de malware y ransomware a través de botnets representa una de las mayores amenazas que este tipo de redes pueden desencadenar, ya que no solo comprometen la integridad de los sistemas informáticos, sino que también pueden tener impactos significativos en la privacidad, la seguridad financiera y la estabilidad

de las organizaciones.

El ransomware, por otro lado, es una forma específica de malware que cifra los archivos o bloquea el acceso a un sistema informático y luego exige un rescate a cambio de restaurar el acceso [11]. Los ataques de ransomware han proliferado en los últimos años, y las empresas se han visto enfrentadas hacia este nuevo desafío donde muchas veces los ciberdelincuentes piden sumas millonarias para rescatar datos sensibles tanto de la empresa como de los clientes y con la amenaza de hacerlos públicos en caso de que el pago no se vea efectuado.

Los dispositivos comprometidos por malware a través de botnets pueden ser utilizados como herramientas para distribuir malware adicional sin la intervención o conocimiento del usuario. Los operadores de botnets pueden enviar comandos a los dispositivos infectados a través del sistema de comando y control para iniciar la descarga y ejecución de malware adicional [2]. Los tipos de malware comúnmente distribuidos mediante botnets incluyen spyware y keyloggers [12].

La distribución de spyware y la minería de criptomonedas encubierta suelen llevarse a cabo en la etapa de latencia de la botnet, ya que son malwares discretos y los ciberdelincuentes buscan mantenerse en el anonimato y evitar la detección. Los ataques más evidentes, como los de ransomware o adware, pueden ocurrir en las etapas finales del ciclo de vida de la botnet, alertando a las víctimas sobre la presencia de malware en sus dispositivos [2-11].

Aunque los gusanos informáticos pueden propagarse y comprometer más equipos en una red, el principal método de infección sigue siendo a través de troyanos distribuidos mediante phishing, ingeniería social y vulneraciones de seguridad masivas [6].

3.3 Campañas de Phishing y Spam Masivo

En las etapas iniciales de infección y ampliación de una botnet, los ciberdelincuentes emplean una variedad de técnicas, como el phishing, la ingeniería social y el spam, para distribuir malware y comprometer una amplia gama de dispositivos [4]. Estas estrategias se utilizan como medio para establecer y ampliar el control sobre la botnet, aprovechando la confianza de los usuarios y su susceptibilidad a las tácticas de manipulación psicológica. El phishing, la ingeniería social y el spam se convierten así en herramientas fundamentales para los atacantes en la creación y expansión de redes de dispositivos comprometidos que constituyen una botnet [13].

Una vez que el troyano o malware utilizado para establecer el control y comando de la botnet ha sido distribuido con éxito en los dispositivos comprometidos, los ciberdelincuentes inician campañas de phishing y spam masivo como parte de la siguiente fase de su estrategia. Estas campañas se centran en el uso de correos electrónicos fraudulentos, mensajes de texto engañosos y otras formas de comunicación digital para engañar a los usuarios y persuadirlos para que revelen información confidencial o realicen acciones que beneficien a los atacantes [1].

Con la infraestructura de la botnet, los ciberdelincuentes pueden alcanzar a un gran número de víctimas potenciales rápidamente, multiplicando así el alcance y el impacto de sus ataques [2].

A través de estas campañas, los ciberdelincuentes pueden expandir su red de dispositivos comprometidos, reclutando nuevos nodos para la botnet y fortaleciendo su control sobre los sistemas infectados. Estas tácticas pueden utilizarse para robar información confidencial o personal, difundir propaganda, desinformación o contenidos maliciosos, o influir en la opinión pública, socavar la confianza en las instituciones o promover agendas políticas o ideológicas [13].

3.4 Criptominería encubierta

Una forma relativamente nueva pero creciente de explotación a través de botnets es el malware de criptominería. Este tipo de malware aprovecha los recursos de los dispositivos comprometidos para llevar a cabo operaciones de minería de criptomonedas sin el conocimiento ni el consentimiento del usuario [7]. La criptominería involucra la resolución de complejos algoritmos matemáticos para verificar y agregar transacciones a una cadena de bloques, lo que resulta en la generación de nuevas unidades de criptomoneda como Bitcoin, Ethereum y otras.

Los ciberdelincuentes utilizan la potencia de procesamiento de los dispositivos infectados dentro de la botnet para llevar a cabo estas operaciones de minería de manera masiva y rentable. A medida que la criptominería requiere una gran cantidad de recursos computacionales, como potencia de CPU y GPU, así como una cantidad considerable de energía eléctrica, los dispositivos comprometidos pueden experimentar un rendimiento degradado, un aumento en el consumo de energía y un mayor desgaste del hardware [7].

Fig. 6. Criptominería en segundo plano encubierta

Uno de los principales desafíos de la criptominería a través de botnets es su capacidad para pasar desapercibida. A diferencia de otros tipos de malware que pueden causar interrupciones obvias en el funcionamiento de un dispositivo, la criptominería suele operar en segundo plano de manera silenciosa y sin ser detectada [7]. Los usuarios pueden no ser conscientes de que sus dispositivos están siendo utilizados para la minería de criptomonedas.

4 Ataques de botnets modernas

4.1 Nuevas estrategias de infección

Tradicionalmente, las botnets dependían de métodos como el phishing y la

explotación de vulnerabilidades conocidas en software desactualizado. Sin embargo, recientes estudios han identificado el uso creciente de técnicas avanzadas como la explotación de vulnerabilidades de día cero, la utilización de la red Tor y la manipulación de dispositivos IoT (Internet of Things) [17].

4.2 Casos de estudio

Caso de estudio: Botnet Meris

La botnet Meris es una de las amenazas cibernéticas más recientes y sofisticadas, emergiendo a mediados de 2021. Esta botnet se destacó rápidamente por su capacidad para generar una cantidad sin precedentes de tráfico malicioso, alcanzando picos de hasta 21.8 millones de solicitudes por segundo (RPS) durante los ataques DDoS. La botnet Meris utiliza principalmente dispositivos Mikrotik, routers que han sido vulnerados debido a configuraciones incorrectas y software desactualizado [18].

Meris se propaga aprovechando múltiples vulnerabilidades en los routers Mikrotik, principalmente aquellas relacionadas con la interfaz de administración del dispositivo. Una vez que el dispositivo es comprometido, Meris instala un conjunto de scripts que permiten al atacante tomar control total del dispositivo a través de exploits y vulnerabilidades en el RouterOS, el sistema operativo que MikroTik implementa en sus enrutadores. Estos scripts convierten al router en un nodo de la botnet, listo para recibir comandos y participar en ataques coordinados. Si bien la compañía parcheo rápidamente esta brecha de seguridad, a día de hoy puede ser explotada en aquellos routers que no tienen una versión actualizada del OS [18].

Uno de los ataques más significativos de Meris ocurrió en septiembre de 2021, cuando se lanzó un ataque DDoS masivo contra Yandex, una de las empresas tecnológicas más grandes de Rusia. Este ataque generó un tráfico extremo que saturó los servidores de Yandex, demostrando la capacidad devastadora de Meris para interrumpir servicios en línea. Este ataque con HTTP pipelining involucro a más de 56 mil equipos de MikroTik comprometidos [19].

Caso de estudio: Botnet Mirai

La botnet Mirai surgió en 2016, centrada inicialmente en dispositivos IoT como cámaras IP y routers y cualquier dispositivo que funcione en base a un procesador ARC, aprovechando credenciales por defecto y configuraciones de seguridad débiles [20].

En su ataque más notable, la botnet Mirai fue responsable de un ataque DDoS masivo contra la empresa de DNS Dyn en octubre de 2016. Este ataque causó interrupciones significativas en numerosos servicios en línea, incluyendo Twitter, Netflix, y Reddit, debido a la saturación de tráfico dirigida a los servidores de Dyn. El ataque logró generar un tráfico superior a 1 Tbps, utilizando una red masiva de dispositivos IoT comprometidos controlados de manera remota por el botmaster [21].

Técnicamente, Mirai se distribuía a través de un escáner incorporado que buscaba dispositivos IoT vulnerables en Internet, accediendo a ellos mediante credenciales predeterminadas Una vez que un dispositivo era comprometido, se convertía en parte de la botnet, esperando instrucciones del sistema de comando y control (C&C). El malware se mantenía residente en la memoria de los dispositivos infectados, evitando

la detección al no escribir en el sistema de archivos [20].

Desde su aparición, Mirai ha sido modificada por varios actores maliciosos para explotar nuevas vulnerabilidades como por ejemplo la NoaBot de la que se ha estado escribiendo ultimamente. Las variantes de Mirai han sido adaptadas para usar técnicas avanzadas de comunicación C&C y su peligro actual sigue vigente debido a su constante mutación [22].

5 Detección, mitigación y defensa

5.1 Detección

Detectar la presencia y actividad de botnets es fundamental para protegerse contra sus ataques y mitigar su impacto en la infraestructura de red. La detección temprana permite a los administradores de sistemas y a los profesionales de seguridad cibernética tomar medidas proactivas para prevenir daños y limitar la propagación. No obstante, debido a su naturaleza compleja, la detección puede ser un desafío. Por eso a continuación se comparten ciertos métodos de detección comunes que han demostrado efectividad a la hora de detectar una propagación:

- Anomalías de Tráfico: Uno de los enfoques principales para detectar botnets es monitorear el tráfico de red en busca de patrones anómalos. Las botnets a menudo generan un alto volumen de tráfico de red no deseado, como paquetes de datos maliciosos o solicitudes de conexión inusuales, que pueden ser indicativos de una actividad de botnet. Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) son herramientas comunes utilizadas para monitorear y analizar el tráfico de red en busca de estas anomalías [14].
- Comportamiento de Hosts: Otra estrategia de detección implica el monitoreo del comportamiento de los dispositivos individuales en una red. Esto implica el análisis de los procesos en ejecución, los archivos modificados y otros indicadores de compromiso en los dispositivos finales. Los sistemas de detección de endpoint (EDR) y las herramientas de análisis de comportamiento de malware pueden identificar actividades sospechosas que podrían indicar la presencia de una botnet [14].
- Firmas de Malware: Las firmas de malware son patrones únicos asociados con software malicioso específico. Los motores antivirus y las soluciones de seguridad pueden utilizar firmas conocidas para identificar y bloquear malware asociado con botnets [14]. No obstante, cabe agregar que, dado que las botnets a menudo utilizan variantes de malware y técnicas de evasión, este enfoque puede no ser completamente efectivo por sí solo.

A pesar de que las tácticas mencionadas anteriormente son efectivas para detectar y mitigar las botnets, verdaderamente se encuentran ciertas dificultades implícitas que pueden obstaculizar esta tarea; Las botnets están diseñadas para evadir la detección y pueden utilizar técnicas de ocultamiento, como el cifrado de comunicaciones, el uso de direcciones IP dinámicas y la segmentación de actividades; Otro problema puede

ser el volumen, el gran volumen de datos generado por las redes modernas puede dificultar la identificación de actividades de botnets entre el tráfico legítimo; Finalmente, la detección de botnets puede estar acompañada de falsos positivos, donde las actividades legítimas se identifican incorrectamente como maliciosas [15].

5.2 Mitigación

Una vez detectada la presencia de una botnet en la red, es crucial implementar estrategias efectivas de mitigación para reducir su impacto y proteger la infraestructura digital de una organización. A continuación, se presentan algunas estrategias clave de mitigación:

1) Implementar firewalls y sistemas de prevención de intrusiones (IPS) para bloquear el tráfico sospechoso es una medida fundamental de mitigación [14], evitando así que los dispositivos infectados se comuniquen con el sistema de comando y control (C&C) y limitando la propagación y el ataque.
2) Mantener los sistemas y dispositivos actualizados con los últimos parches de seguridad es esencial para mitigar las vulnerabilidades conocidas que las botnets pueden aprovechar para infiltrarse en la red. La implementación oportuna de parches de seguridad puede cerrar las brechas de seguridad y reducir la superficie de ataque, dificultando que las botnets infecten nuevos dispositivos y sistemas [16].
3) Establecer políticas de seguridad claras y procedimientos de respuesta a incidentes ayuda a fortalecer las defensas. Estas políticas deben abordar aspectos como la gestión de contraseñas, el acceso a recursos de red, la monitorización del tráfico y las prácticas de seguridad de los empleados y sobre todo un protocolo o plan para mitigar los daños.

5.3 Defensa

La defensa contra botnets implica la implementación de medidas de seguridad sólidas y la adopción de prácticas que ayuden a prevenir la infección, detectar la actividad maliciosa y responder de manera efectiva a las amenazas. A continuación, se presentan algunas estrategias clave para defenderse contra las botnets:

- Utilizar soluciones de seguridad avanzadas, como sistemas de prevención de intrusiones (IPS), sistemas de detección y respuesta de endpoints (EDR) y soluciones de gestión unificada de amenazas (UTM), puede ayudar a detectar y bloquear actividades maliciosas asociadas con botnets. Estas herramientas utilizan técnicas de inteligencia artificial y análisis de comportamiento para identificar patrones de tráfico sospechosos y responder de manera proactiva a las amenazas [14-16].
- Mantener todos los sistemas y software actualizados con los últimos parches de seguridad es crucial para cerrar las vulnerabilidades que las botnets pueden explotar. Establecer políticas y procedimientos para aplicar parches de seguridad de manera oportuna y regular puede ayudar a reducir la exposición a las amenazas de botnets y otros tipos de malware [16].
- Realizar un monitoreo activo del tráfico de red y del comportamiento del

sistema puede ayudar a identificar signos de actividad maliciosa asociada con botnets. Las organizaciones deben implementar herramientas de monitoreo de seguridad que les permitan detectar anomalías, como patrones de tráfico inusuales, comunicaciones con dominios maliciosos y actividad sospechosa de los dispositivos en la red [16].

- Brindar capacitación sobre seguridad cibernética a los empleados.

6 Conclusiones

La investigación sobre botnets revela la complejidad y peligro que estas redes representan para los sistemas. Desde su anatomía hasta sus métodos de distribución de malware y los ataques que pueden lanzar, las botnets representan una amenaza significativa para individuos, empresas y organizaciones a lo largo y ancho del ecosistema digital.

botnets abarcan una amplia gama de actividades maliciosas, desde ataques DDoS hasta distribución de malware, pasando por campañas de phishing y spam masivo. Estos ataques pueden causar daños significativos, incluida la pérdida de datos, interrupción de servicios y robo de información confidencial.

Para defenderse contra botnets, es decisivo implementar medidas de detección, mitigación y defensa efectivas; tales como protección activa de endpoints, filtrado de tráfico de red, actualización y parcheo de sistemas, autenticación y control de acceso, monitoreo de actividad anómala y educación para los usuarios.

La lucha contra las botnets es una responsabilidad compartida que requiere la participación de usuarios, empresas, gobiernos y la comunidad de ciberseguridad en su conjunto. Al trabajar juntos para identificar, prevenir y mitigar las amenazas de botnets, podemos fortalecer la seguridad cibernética y proteger nuestra infraestructura digital contribuyendo y colaborando.

Referencias

1. C. C. Elisan, Malware, Rootkits & Botnets: A Beginner's Guide. McGraw Hill, 2012.
2. C. Schiller, J. R. Binkley, A. Bradley, M. Cross MD, G. Evron, D. Harley, C. Ries, C. Willems, Botnets: The Killer Web Applications. Syngress, 2007.
3. N. Hoque, D. K. Bhattacharyya, y J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," en IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2242-2270, Fourth quarter 2015.
4. R. A. Rodríguez-Gómez, G. Maciá-Fernández & P. García-Teodoro, "Survey and taxonomy of botnet research through life-cycle," ACM Computing Surveys (CSUR), 2013, vol. 45, no. 4, p. 1-33.
5. D. Dagon, G. Gu, C. P. Lee, y W. Lee, "A Taxonomy of Botnet Structures," en Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), Florida, USA, 2007, pp. 325-339.
6. S. Yu, G. Gu, A. Barnawi, S. Guo and I. Stojmenovic, "Malware Propagation in Large-Scale Networks," in IEEE Transactions on Knowledge and Data Engineering, vol. 27, no. 1, pp. 170-179, 2015.

7. D. Plohmann and E. Gerhards-Padilla, "Case study of the Miner Botnet," 2012 4th International Conference on Cyber Conflict (CYCON 2012), Tallinn, Estonia, 2012, pp. 1-16.

8. L. F. Eliyan & R. Di Pietro, DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems, 2021, vol. 122, p. 149-171.

9. B. B. Gupta y A. Dahiya, Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC Press, 2023.

10. M. Nawrocki, M. Jonker, T. C. Schmidt, y M. Wählisch, "The far side of DNS amplification: tracing the DDoS attack ecosystem from the internet core," en Proceedings of the 21st ACM Internet Measurement Conference (IMC '21). Association for Computing Machinery, New York, USA, 2021, pp. 419–434.

11. N. Dutta, N. Jadav, S. Tanwar, H. K. D. Sarma, y E. Pricop, "Introduction to Malware Analysis," en Cyber Security: Issues and Current Trends, Studies in Computational Intelligence, vol. 995. Springer, Singapore, 2022.

12. Bhardwaj y S. Goundar, "Keyloggers: silent cyber security weapons," Network Security, 2020, vol. 2020, no. 2, p. 14-19.

13. S. D. Shivanna y M. R. Pooja, "An Empirical Assessment of Botnets and Detection Methods," Grenze International Journal of Engineering & Technology (GIJET), 2024, vol. 10, p. 2828. ISSN: 2395-5287.

14. V. Matta, M. Di Mauro and M. Longo, "DDoS Attacks With Randomized Traffic Innovation: Botnet Identification Challenges and Strategies," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1844-1859, Aug. 2017.

15. Y. Xing, et al., "Survey on botnet detection techniques: Classification, methods, and evaluation," Mathematical Problems in Engineering, 2021, vol. 2021, p. 1-24.

16. M. Albanese, et al., "Adaptive cyber defenses for botnet detection and mitigation," en Adversarial and Uncertain Reasoning for Adaptive Cyber Defense: Control-and Game-Theoretic Approaches to Cyber Security, 2019, p. 156-205.

17. Lohachab, A., y Karambir, B., "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," en Journal of Communications and Information Networks, vol. 3, pp. 57–78, 2018

18. Singh, N. J., Hoque, N., Singh, K. R., y Bhattacharyya, D. K., "Botnet-based IoT network traffic analysis using deep learning," en Security and Privacy, vol. 7, no. 2, p. e355, 2024.

19. Spring, T. "Yandex Pummeled by Potent Meris DDoS Botnet", Threatpost, 2021.

20. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J. & Zhou, Y. "Understanding the Mirai Botnet," in 26th USENIX Security Symposium, 2017.

21. Jerkins, J. A., "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," en 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1-5, 2017.

22. Kupchik, S., "You Had Me at Hi — Mirai-Based NoaBot Makes an Appearance," Akamai, 2024.