

CYBER **SECURITY** **NEWS**

SECURITY OPERATIONS CENTER

**GOLPE A LA CIBERDELINCUENCIA: EE.UU.
DESMANTELA LA RED 911 S5**

30 / 05 / 2024

CONTENIDO

INTRODUCCIÓN.....	3
NOTICIA COMPLETA.....	7
CONTACTOS DE SOPORTE.....	8

INTRODUCCIÓN

En el panorama actual de la ciberseguridad, donde las amenazas evolucionan constantemente y los ataques se vuelven cada vez más sofisticados, es crucial para las empresas adoptar medidas proactivas para proteger sus activos digitales. El reciente desmantelamiento del botnet 911 S5, considerado el mayor del mundo con 19 millones de dispositivos infectados, subraya la importancia de estar preparados y conscientes de los riesgos que enfrenta cualquier organización. A continuación, presentamos diez recomendaciones esenciales para fortalecer su postura de ciberseguridad y proteger su infraestructura contra posibles amenazas.

GOLPE A LA CIBERDELINCUENCIA: EE.UU. DESMANTELA LA RED 911 S5

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2024_05_30_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	CLEAR
Fecha de publicación:	30/05/2024
Es día cero (0 day):	No

El Departamento de Justicia de EE.UU. (DoJ) anunció el desmantelamiento de lo que se considera "probablemente el botnet más grande del mundo", una red compuesta por 19 millones de dispositivos infectados utilizados por actores malintencionados para cometer una variedad de delitos. Esta red global, conocida como 911 S5, operaba como un servicio de proxy residencial y fue desmantelada gracias a un esfuerzo coordinado a nivel internacional.

Detalles del Operativo

YunHe Wang, un ciudadano chino de 35 años, fue arrestado en Singapur el 24 de mayo de 2024, acusado de ser el creador y principal administrador de la plataforma ilegal desde 2014 hasta julio de 2022. Wang enfrenta cargos por conspiración para cometer fraude informático, fraude informático sustantivo, conspiración para cometer fraude electrónico y conspiración para lavar dinero, con una pena máxima de 65 años de prisión.

El DoJ reveló que el botnet se utilizó para realizar ciberataques, fraude financiero, robo de identidad, explotación infantil, acoso, amenazas de bomba y violaciones de exportación. Los dispositivos comprometidos abarcaban más de 190 países, con 613,841 direcciones IP en Estados Unidos.

Modo de Operación

Wang y otros implicados habrían creado y diseminado malware para comprometer millones de computadoras Windows residenciales en todo el mundo. Estos dispositivos eran alquilados a ciberdelincuentes, generando millones de dólares en ingresos. Los actores maliciosos utilizaban estas IP para anonimizar sus actividades delictivas, facilitando fraudes financieros y otros delitos.

El malware se propagaba a través de programas VPN gratuitos como MaskVPN y DewVPN, además de servicios de pago por instalación que lo incluían con software pirateado. La infraestructura de Wang incluía 150 servidores en todo el mundo, de los cuales 76 estaban en EE.UU.

Impacto Económico

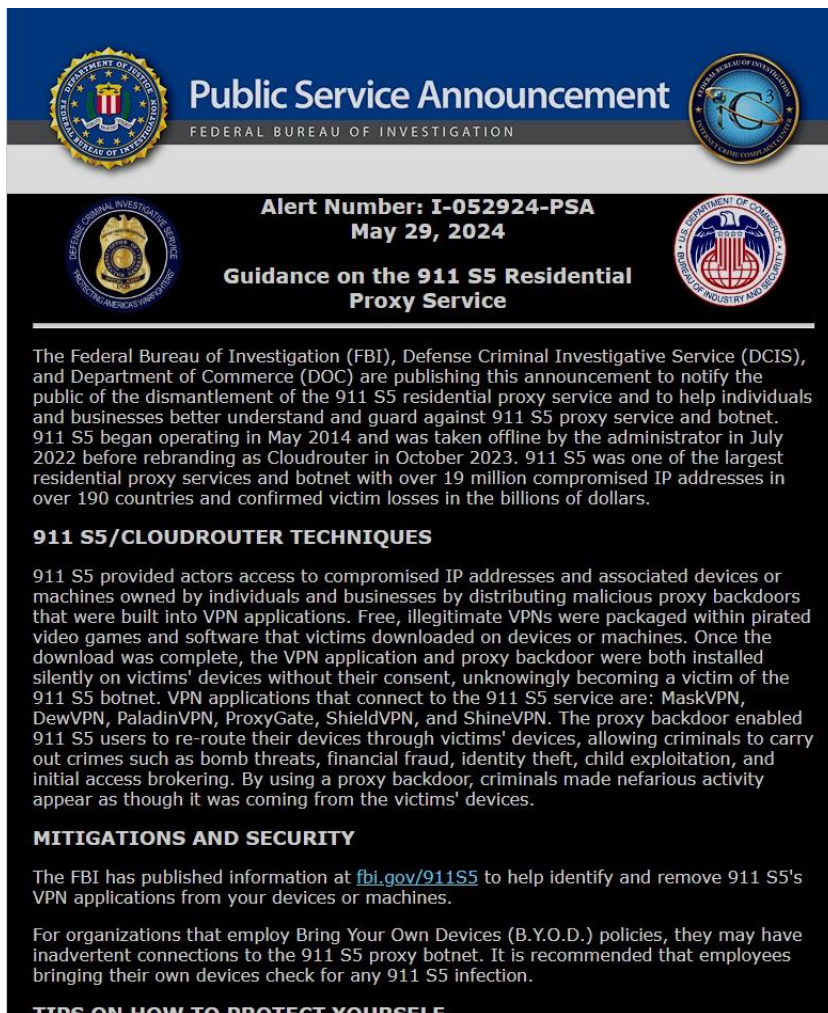
Se estima que Wang obtuvo aproximadamente \$99 millones vendiendo acceso a estas IP comprometidas, utilizando los fondos para adquirir autos de lujo, relojes costosos y propiedades en varios países. Además, Wang controlaba más de una docena de cuentas bancarias y 24 billeteras de criptomonedas, con activos valorados en \$136.4 millones en criptomonedas.

Colaboración Internacional

El desmantelamiento del 911 S5 fue resultado de una colaboración entre EE.UU., Singapur, Tailandia y Alemania, que llevó a la interrupción de 23 dominios y más de 70 servidores. Se incautaron activos valorados en aproximadamente \$30 millones.

Sanciones Adicionales

Simultáneamente, la Oficina de Control de Activos Extranjeros (OFAC) del Departamento del Tesoro de EE.UU. impuso sanciones contra Wang, su co-conspirador Jingping Liu y Yanni Zheng, apoderado, además de tres entidades en Tailandia relacionadas con Wang.



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-052924-PSA
May 29, 2024

Guidance on the 911 S5 Residential Proxy Service

The Federal Bureau of Investigation (FBI), Defense Criminal Investigative Service (DCIS), and Department of Commerce (DOC) are publishing this announcement to notify the public of the dismantlement of the 911 S5 residential proxy service and to help individuals and businesses better understand and guard against 911 S5 proxy service and botnet. 911 S5 began operating in May 2014 and was taken offline by the administrator in July 2022 before rebranding as Cloudrouter in October 2023. 911 S5 was one of the largest residential proxy services and botnet with over 19 million compromised IP addresses in over 190 countries and confirmed victim losses in the billions of dollars.

911 S5/CLOUDROUTER TECHNIQUES

911 S5 provided actors access to compromised IP addresses and associated devices or machines owned by individuals and businesses by distributing malicious proxy backdoors that were built into VPN applications. Free, illegitimate VPNs were packaged within pirated video games and software that victims downloaded on devices or machines. Once the download was complete, the VPN application and proxy backdoor were both installed silently on victims' devices without their consent, unknowingly becoming a victim of the 911 S5 botnet. VPN applications that connect to the 911 S5 service are: MaskVPN, DewVPN, PaladinVPN, ProxyGate, ShieldVPN, and ShineVPN. The proxy backdoor enabled 911 S5 users to re-route their devices through victims' devices, allowing criminals to carry out crimes such as bomb threats, financial fraud, identity theft, child exploitation, and initial access brokering. By using a proxy backdoor, criminals made nefarious activity appear as though it was coming from the victims' devices.

MITIGATIONS AND SECURITY

The FBI has published information at fbi.gov/911S5 to help identify and remove 911 S5's VPN applications from your devices or machines.

For organizations that employ Bring Your Own Devices (B.Y.O.D.) policies, they may have inadvertent connections to the 911 S5 proxy botnet. It is recommended that employees bringing their own devices check for any 911 S5 infection.

TIPS ON HOW TO PROTECT YOURSELF

Reflexión

Matthew S. Axelrod, del Buró de Industria y Seguridad (BIS) del Departamento de Comercio de EE.UU., comparó el esquema con un guion de película, destacando el arduo trabajo de las fuerzas de seguridad nacionales e internacionales y socios de la industria para lograr el arresto y desmantelamiento de una operación tan audaz.

El desmantelamiento del botnet 911 S5 es un recordatorio contundente de la importancia de la colaboración global en la lucha contra el cibercrimen y de los avances en la seguridad cibernética que protegen a usuarios y organizaciones en todo el mundo.

NOTICIA COMPLETA

<https://devel.group/blog/golpe-a-la-ciberdelincuencia-ee-uu-desmantela-la-red-911-s5/>

CONTACTOS DE SOPORTE



Correo electrónico: cert@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: <https://www.devel.group/reporta-un-incidente>