BOLETIN DE SEGURIDAD #OPICARUS2018

28 de Junio del 2018
CONFIDENCIAL

OPERACIÓN #opIcarus2018

DESCRIPCIÓN

La Operación #OpIcarus2018 ha sido anunciada y abarca varias campañas en curso, incluidas #OpPayBack, #OpIcarus, #DeleteTheElite y #SosNicaragua. Los ataques cibernéticos están siendo impulsados por el grupo hacktivista Anonymous con motivos en su mayoría políticos y estos han manifestado su intención de atacar entidades bancarias e incluso individuos en especifico entre el **21** y el **28** de junio de 2018.

Actualmente, no existe una organización central para este grupo hacktivista, por tanto, es difícil determinar si los ataques son generados por parte de un individuo o un grupo; adicional se ha evidencia que grupos de crimen organizado, aprovechan esto para ocultar sus propias actividades ilícitas.

COMPORTAMIENTO

Estos grupos operan bajo diferentes alias y alianzas para coordinar un ataque usando varios métodos y técnicas. Estos atacantes se pueden encontrar en línea por su operación o nombre **"op"**. La causa de los grupos hacktivistas, como Anonymous, a menudo es estimulada por un evento al que se oponen. El alcance de soporte a menudo se comunica a través de los canales de Twitter, Facebook o IRC.

Estos grupos a menudo comparten herramientas de su elección para atacar el sitio objetivo. Si hay más de un objetivo identificado asociado con una operación con nombre, como en este caso, también comparten la lista de objetivos. Estas listas a menudo se publican en sitios de pegado (pastebin.com, piratepaste.com, entre otros).

Aunque las instituciones financieras tienden a ser el objetivo principal desde una perspectiva histórica, los atacantes continúan ampliando su alcance y participando en diversas operaciones. Las principales observaciones y tendencias hasta la fecha son que los ataques "exitosos" son algo arbitrarios. Tienden a centrarse en objetivos "más suaves" y menos defendidos para lograr su objetivo y obtener publicidad para su causa. Los informes iniciales revelan que muchos sistemas se vieron comprometidos como resultado de la explotación de sitios web sin parches y con una configuración insegura, en lugar de técnicas sofisticadas que un atacante más habilidoso podría

En las operaciones del presente año, Anonymous recomiendan que los usuarios de Linux que lancen ataques DDoS utilicen herramientas como Loic, xerxes, Slowloris, Ufonet o la botnet Mirai, advirtiendo a los seguidores que el uso de otras botnets como ZEUS corre un mayor riesgo de estar vinculado al atacante. Adicional, les indica que utilicen una VPN frente a 4nomiziner, ya que registrará la actividad.

TÁCTICAS Y TÉCNICAS

Anonymous, tiene como ataque predilecto la denegación de servicios (DoS) y desfiguración de sitios web. Se sabe que utilizan varios otros métodos, como inyección SQL e inclusión de archivos locales (LFI), ataques de aplicaciones web, crossScripts (XSS), robo de identidad, phishing e ingeniería social, para obtener datos confidenciales que avergüenzan públicamente a sus usuarios objetivo.

Como se dijo anteriormente, utilizan un conjunto de herramientas relativamente estándar en sus ataques. Estos están disponibles y son fáciles de usar; la intención es minimizar los obstáculos para permitir la entrada de cualquier persona que pueda estar interesada en participar en la campaña. Afortunadamente, las herramientas más utilizadas también son fáciles de defender.

OBJETIVOS

A partir de la consulta de diferentes fuentes de información, se han identificado los siguientes objetivos del grupo hacktivista:

https://www.el19digital.com/
http://canal2tv.com
http://canal6.com.ni/
https://www.tn8.tv/
https://www.vivanicaragua.com.ni/
https://nuevaya.com.ni/
www.nicaraguacompra.gob.ni
https://www.inss.gob.ni/
http://www.cse.gob.ni/
http://www.migob.gob.ni/
http://www.bcn.gob.ni/
http://www.pgr.gob.ni/
https://www.bancorp.com.ni/
http://www.bfp.com.ni/
https://www.banprogrupopromerica.com.ni/
https://secure.bancolafise.com.ni/
https://www.bdfnet.com/
https://www1.sucursalelectronica.com/redir/showLogin.go

RECOMENDACIONES Y CONCLUSIONES

Desde el CSVD, se recomienda estar alerta frente a cualquier comportamiento anómalo que se presente en su organización y mas si esta se encuentra nombrada en una operación o tiene asociación con una organización objetivo de ataque. Adicional nuestro equipo de trabajo estará alerta frente a los eventos de seguridad que puedan ocurrir con nuestros clientes y se realizará constante investigación frente a actualización de listas de objetivos del grupo hacktivista para su comunicación y prevención.

Adicional le invitamos a tener en cuenta las siguientes recomendaciones:

- ✓ Revisar la configuración de Routers y Firewalls para detener IPs inválidas, así como también el filtrado de protocolos que no sean necesarios. Algunos firewalls y routers proveen la opción de prevenir inundaciones (floods) en los protocolos TCP/UDP.

- ✓ Configuración de políticas en su Firewall que le permitan detectar y contener posibles ataques de DoS y DDoS (por ejemplo: cp_syn_flood, tcp_port_scan, tcp_src_session, udp_scan, sctp_flood, icmp_flood, entre otros).

- ✓ Implementar plataformas anti-DoS como lo son Arbor, CloudFire y Radware.

- ✓ En la configuración de su Firewall:
  - Limitar la tasa de tráfico proveniente de un único host.
  - Limitar el número de conexiones concurrentes al servidor.
  - Restringir el uso del ancho de banda por aquellos hosts que cometan violaciones.

- ✓ Usar plataformas de monitoreo que le permita supervisar y medir de manera proactiva sus aplicaciones web, con el fin de determinar si un sitio web se encuentra caído.

- ✓ Trabaje con su equipo de IT para garantizar que todas las reglas nuevas estén activadas y que todas las configuraciones asociadas a su cuenta estén actualizadas y configuradas correctamente.

- ✓ Cuando se materialice un evento de ataque por parte de los grupos hacktivista y la organización decide responder públicamente, tenga cuidado con su respuesta. Cualquier declaración pública podría desafiar al actor directamente y poner a su organización en mayor riesgo, fomentando más ataques.

- ✓ Realice una auditoría proactiva y supervise su entorno en busca de cualquier actividad anormal, como un aumento de las alertas, una latencia creciente o la degradación de la cuenta.

REFERENCIAS

https://www.radware.com/products/defensepro/

https://blogs.akamai.com/sitr/2018/06/anonymous-opicarus2018.html

https://ghostbin.com/paste/ppkrk

http://ghostsecurity.bitballoon.com/

http://ghostsecurity.bitballoon.com/

https://pastebin.com/dVyqyJi5

http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-firewall-52/Firewall%20Policies/IPv4%20DoS%20Policy.htm

A3SEC. ESPAÑA C/ Aravaca, 6 2º Piso 28040 Madrid, España T.+34 915330978	**A3SEC S.A.S** Carrera 49A # 94-76 Oficina 304 Edificio Empresarial Castellana Bogotá, COLOMBIA **T.**+57 1 3099533	**A3SEC USA** 1401 Brickell Ave #320 Miami, FL 33131, USA T. +1 786 556 90 32	**A3SEC. México** Shakespeare 95, Piso 2. Anzures 11590. Ciudad de Mexico +5255 6725 7748