ANDORRA DIGITAL

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Informe de ciberintel·ligència

Detectada una campanya de la botnet MIRAI contra entitats a nivell global

TLP:WHITE

14/7/23

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	14/7/2023	14/07/2023

Registre de canvis			
Versió	Pàgines	Data de modificació	Motiu del canvi

Propietari del document	ANC-AD

Contingut

1. METODOLOGÍA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). Es tracta d'un esquema creat per fomentar un millor intercanvi d'informació de caràcter delicat (però no classificada) en l'àmbit de la seguretat de la informació. A través d'aquest esquema, d'una forma àgil i senzilla, s'indica fins a on pot circular la informació més enllà del receptor en qüestió, i aquest ha de consultar a l'ANC-AD (Agència Nacional de Ciberseguretat d'Andorra) [https://www.anc.ad/] quan la informació necessiti ser distribuïda a tercers.

CODI	QUAN EMPRAR-LO	COM COMPARTIR-LO
TLP:RED	S'ha d'utilitzar TLP:RED quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, reputació o operacions si és mal utilitzada.	Els receptors no han de compartir informació designada com TLP:RED amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP:AMBER	S'ha d'usar TLP:AMBER quan la informació requereix ser distribuïda de manera limitada, però suposa un risc per a la privacitat, reputació o operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com TLP:AMBER únicament amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per a protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per a compartir aquesta informació.
TLP:GREEN	S'ha d'emprar TLP:GREEN quan la informació és útil per a totes les organitzacions que participen, així com amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com TLP:GREEN amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP:WHITE	S'ha d'utilitzar TLP:WHITE quan la informació no suposa cap risc de mal ús, dins de les regles i procediments establerts per a la seva difusió pública.	La informació TLP:WHITE pot ser distribuïda sense restriccions, únicament subjecta a controls de Copyright.

2. Sobre la campanya detectada

Durant les darreres hores hem detectat una activitat inusual de la Botnet MIRAI, i les nostres anàlisis ens han permès detectar una campanya massiva i indiscriminada contra diferents organitzacions de tot el món.
Hem pogut comprovar com aquesta Botnet, que des de la seva aparició el 2016 s'ha caracteritzat per comprometre sobretot càmeres de CCTV, DVR i routers domèstics, està tractant de comprometre sistemes mitjançant peticions als ports 22/TCP, 23/TCP, 80/TCP, 2222/TCP, 2323/TCP, 5555/TCP, 7547/TCP, 8080/TCP, 8081/TCP, 52869/TCP en els quals existeixi alguna vulnerabilitat d'autenticació. El seu objectiu és executar codi remot (RCE) per, finalment, infectar l'equip mitjançant un malware amb extensió ".arm7".

3. Indicadors de compromís identificats (IoC'S)

Atenent els registres obtinguts a través dels nostres sistemes de monitoratge, així com als resultats d' una investigació complementària després de la identificació d' activitat inusual potencialment maliciosa, hem identificat els següents IoC' s:

- IP' s d' origen de l' atac:
  - 78.101.168.142 (Qatar) | Activa des de el 12/07/2023
  - 177.124.244.35 (Brasil) | Activa des de el 05/03/2022
  - 37.44.238.203 (Francia) | Activa des de el 20/10/2022
- URL Payload:
  - http[:]//127.0.0.1[/]cgi-bin[/]ViewLog[.] aspmKilledYou
- Arxiu descarregable:
  - *.arm7
- Paràmetres User-Agent empleats en les peticions web:
  - MtmKilledYou
  - Hello, world
  - r00ts3c-Owned-You
  - Mozilla/4.0 (Compatible; MSIE 6.0; Windows NT 5.1)
  - Messiah/2.0
  - Tsunami/2.0
- Paths identificatius de les peticions web:
  - /UD/Act
  - /Index.Php
  - /Cgi-Bin/ViewLog.Asp
  - /Shell
  - /UD/

- /Picdesc.Xml
- /GponForm/Diag_Form
- /Wanipcn.Xml

4. Sobre la botnet Mirai

Mirai és una Botnet que va ser detectada per primera vegada el 2016, després de realitzar un atac DDoS d'1,1 Tbps, batent tots els rècords fins a la data. Des que es té constància de la seva activitat, s'ha comprovat que els seus objectius han estat principalment dispositius d'Internet de les coses (IoT), tot i que va anar evolucionant per infectar també dispositius Windows.
El flux de dades amb què Mirai implementa els seus atacs DDoS oscil·la entre els 200 Gbps i fins a 1,2 Tbps, sent efectius contra els protocols GRE IP, GRE ETH, SYN i ACK, STOMP, DNS, UDP o HTTP.
El codi font de Mirai va ser publicat el 2016 a través del fòrum de parla anglesa Hackforums per la usuària "Anna-senpai". En aquesta publicació va participar com a coautor, Paras Jha, qui va ser condemnat a finals del 2018.
La disponibilitat pública del codi va augmentar la quantitat de dispositius IoT infectats, passant de comptabilitzar-se 213.000 fins a més de 483.000 en tan sols dues setmanes. De la mateixa manera, va augmentar dràsticament la popularitat de Mirai en l'ecosistema del cibercrim i fins ara ha tingut la capacitat d'explotar 33 CVE.

5. Històric d'atacs i campanyes més rellevants impulsades per Mirai

5.1 Any 2021

- El setembre de 2021, la botnet MIRAI va començar a explotar una vulnerabilitat crítica d'Azure OMIGOD (CVE-2021-38647) dirigits a punts de connexió OMI d'Azure Linux.

- El desembre del 2021, els investigadors de NetLab 360 van compartir que els actors d'amenaces després de la botnet MIRAI van intentar explotar la vulnerabilitat Log4Shell mitjançant atacs dirigits a dispositius Linux.

- Es va detectar una variant de MIRAI denominada Moobot que estava explotant vulnerabilitats en productes de Hikvision (CVE-2021-36260) utilitzats per empreses del Brasil i Estats Units.

5.2 Any 2022

5 L'abril del 2022, els investigadors de Fortiguard van revelar una campanya DDoS basada en Mirai, a la qual van denominar Beasmode. Es va poder observar s'explotaven vulnerabilitats de dispositius TOTOLINK.

6 Durant el tercer trimestre de 2022, el proveïdor de seguretat Cloudflare va aconseguir aturar un atac DDoS de 2,5 Tbps de Mirai, dirigit a servidors de Minecraft.

7 El novembre del 2022, els investigadors de Nozomi Networks van descriure una nova funció de desxifrat en algunes mostres de malware utilitzades per Mirai. També

es van detectar tres claus de desxifrat úniques en les noves variants de Mirai denominades pazdanoisqt, megacatnet i fakamebotnet:

7.1.1 Pazdonoisqt i Megacatnet se centren en atacs DDoS, tot i que de diferent complexitat. A més, la cadena paudanoisqt comparteix exploits amb una altra variant de Mirai anomenada Omni.

7.1.2 Fakamebotnet és més complex ja que se centra en atacs DDoS i explota una vulnerabilitat de Huawei de 2017 (CVE-2017-17215) que permet l'execució remota de codi en els dispositius.

5.3 Any 2023

El gener d'aquest mateix any, va ser revelat per la Unitat 42 que la botnet MIRAI, entre d'altres, estava apuntant a una vulnerabilitat a Realtek SDK (CVE-2021-35394) per comprometre la cadena de subministrament.

6. Recomanacions

La principal mesura de seguretat que s' ha de prendre per prevenir qualsevol intent d' atac per part de la Botnet Mirai és procedir al bloqueig de les IP' s indicades en el punt 1.1:

8 78.101.168.142 (Qatar)

9 177.124.244.35 (Brasil)

10 37.44.238.203 (França)