AVIS DE SECURITE

Objet	Services de cybercriminalité ciblant les routeurs en fin de vie pour lancer des attaques et dissimuler leurs activités
Niveau de criticité	IMPORTANT
Référence	SNCSIRT-2025-ADS-139
TLP	WHITE

Résumé

Les acteurs de la menace exploitent des vulnérabilités connues pour compromettre les routeurs en fin de vie, installer des logiciels malveillants et utiliser les routeurs dans un réseau de zombies qu'ils contrôlent pour lancer des attaques coordonnées ou vendre l'accès aux appareils.
Le Bureau fédéral des investigations (FBI) publie ce FLASH pour diffuser des indicateurs de compromission (IoC) et des tactiques, techniques et procédures (TTP) associés aux services cybercriminels 5Socks et Anyproxy qui ciblent les logiciels malveillants affectant les routeurs en fin de vie (EOL).

Risque de sécurité

- Les criminels vendent l'accès aux routeurs compromis sous forme de proxies
- Accès shell aux routeurs

Systèmes affectés

- Les routeurs EOL,
- Liste des appareils vulnérables à la compromission :
  - E1200
  - E2500
  - E1000
  - E4200
  - E1500
  - E300
  - E3200
  - WRT320N
  - E1550
  - WRT610N
  - E100
  - M10
  - WRT310N

Recommandations

- Remplacer les appareils compromis par des modèles plus récents
- Prévenir l'infection en désactivant l'administration à distance et en redémarrant le routeur
- Ci-dessous une liste de fichiers associés à la campagne d'exploitation des routeurs du logiciel malveillant :

Hash	Name
661880986a026eb74397c334596a2762	0forumdisplay-php_sh_gn-37-sh
62204e3d5de02e40e9f2c51eb991f4e8	1_banana.gif_to_elf_t
9f0f0632b8c37746e739fe61f373f795	2_multiquote_off.gif_to_elf_gn-p_forwardhw-data- to-exploit-server
22f1f4c46ac53366582e8c023dab4771	3_collapse_tcat_gif_sh_s3-sh
cffe06b0adcc58e730e74ddf7d0b4bb8	4_message_gif_to_elf_k
084802b4b893c482c94d20b55bfea47d	5_viewpost_gif_to_elf_s
e9eba0b62506645ebfd64becdd4f16fc	6_vk_gif_to_elf_b
41e8ece38086156959804becaaee8985	7_slack_gif_DATA
1f7b16992651632750e7e04edd00a45e	8_share_gif_DATA
2667a50869c816fa61d432781c731ed2	banana.gif-upx
0bc534365fa55ac055365d3c31843de7	message.gif-upx