FBI FLASH
ACTIONABLE CYBER INTELLIGENCE
12 March 2026
FLASH Number
20260312-001

AVrecon Malware-Infected Routers Exploited as Residential Proxies by SocksEscort

Summary

The Federal Bureau of Investigation (FBI) is releasing this FLASH to disseminate indicators of compromise (IOCs) and identified tactics, techniques, and procedures (TTPs) associated with AVrecon malware. This malware has been observed targeting routers and other Internet of Things (IOT) devices, located in approximately 163 countries around the world, including the United States. Threat actors have been found to compromise routers, install AVrecon Malware, and then sell access to the compromised devices as residential proxies using the SocksEscort residential proxy service. SocksEscort is believed to have compromised and sold access to approximately 369,000 devices since 2020.

The release of this FLASH follows the coordinated takedown of the SocksEscort service through a joint law enforcement operation. This operation was conducted by the FBI and partners at EUROPOL, France's Office of Anti-Cybercriminalité (OFAC), the Dutch National Police, Austria's Bundeskriminalamt (BK), the U.S. Defense Criminal Investigative Service (DCIS), and the U.S. Internal Revenue Service (IRS).

Technical Details

Overview

Routers that do not receive regular security updates can be exposed to known, but un-patched vulnerabilities. Threat actors are aware of these vulnerabilities and exploit them to install malware, gain control of the device, and sell access to them as residential proxies. Residential proxy networks are used by many types of threat actors to hide their identities online and make their activity appear as if it originates from the victim's network. By using residential proxy networks, threat actors are more likely to bypass common website filters and block lists. This allows them to more easily conduct various types of online fraud or other malicious activity such as password spraying.

SocksEscort threat actors have exploited known vulnerabilities in various routers and IOT devices to gain access to the devices and install AVrecon malware. This malware allows SocksEscort threat actors to maintain remote access to the routers and use them as part of a botnet. SocksEscort monetizes their botnet through various illicit methods, including selling access under the SocksEscort residential proxy brand.

In addition to turning the device into a SocksEscort residential proxy, AVrecon can also update its stored configuration, establish a remote shell to an attacker-controlled server, and act as a loader by downloading and executing arbitrary payloads.

SocksEscort uses AVrecon malware to target approximately 1,200 device models manufactured by Cisco, D-Link, Hikvision, MicroTik, Netgear, TP-Link, and Zyxel. The vast majority of observed devices infected with AVrecon malware are small-office/home-office (SOHO) routers infected using critical vulnerabilities such as Remote Code Execution (RCE) and command injection. AVrecon malware is written in the C language and primarily targets MIPS and ARM devices. Devices classified as End-of-Life (EOL) by their manufacturers generally do not receive security patches to address known vulnerabilities. For non-EOL devices, patches may have been released for some of the vulnerabilities used by AVrecon. However, these patches are often not applied automatically, and even if they are eventually applied, that may not remediate a device which has already been infected with AVrecon.

List of Top 20 Most Represented Device Models

- D-Link
  - DIR-818LW Wireless Router
  - DIR-850L Wireless Router
  - DIR-860L Wireless Router
- Hikvision
  - DS-2CD2020F-I IP Camera
  - DS-2CD2420F-IW IP Camera
- Netgear
  - DGN2200v4 Wireless Router
  - AC1900 R7000
- TP-Link
  - Archer C20 Wireless Router
  - TL-WR840N Wireless Router
  - TL-WR849N Wireless Router
  - WR841N Wireless Router
- Zyxel
  - EMG6726-B10A Router
  - PMG5617GA Home Gateway Unit (HGU)
  - VMG1312-B10D Wireless Router
  - VMG1312-T20B Wireless Router
  - VMG3925-B10A Wireless Router
  - VMG3925-B10C Wireless Router
  - VMG4825-B10A Wireless Router
  - VMG4927-B50A Wireless Router
  - VMG8825-T50K Wireless Route

Distribution

AVrecon malware is distributed by scanning for, identifying, and targeting Internet-connected devices with exposed vulnerable services. The SocksEscort threat actors abuse RCE, command injection vulnerabilities, flaws in exposed Simple Object Access Protocol (SOAP) interfaces, and various other exploitation techniques to compromise these devices. AVrecon's Command and Control (C2) framework is also modular in nature, allowing for the easy addition of new exploit modules when needed. This modular framework allows AVrecon to easily adapt new exploit techniques and vulnerabilities, to further expand the range of devices which can be infected.

Exploitation

Once a device has been compromised, SocksEscort threat actors initiate a series of steps which end in the execution of AVrecon malware, which enables remote access to the device. For example, on certain models, a loader is executed first to test the environment and check to see if AVrecon is already running, before downloading and deploying AVrecon.

Persistence

AVrecon persistence varies depending on the infected device type. In some cases, threat actors utilize a device's built-in update features to flash the device with a custom firmware image. This custom firmware contains a copy of AVrecon and is hardcoded to execute AVrecon on device startup. Threat actors also modify the firmware to silently disable the device's update and flashing features, making AVrecon extremely difficult to remove. These types of devices are essentially permanently infected with AVrecon.

In other cases, AVrecon is deployed without a persistence mechanism. If an infected device is power cycled, it resets to a normal state and is no longer infected by AVrecon. However, in at least one case, AVrecon C2 servers reacted to the loss of an infected device by remotely re-infecting it with the same known vulnerabilities used to initially infect the device.

Communication

Infected routers have been observed communicating with SocksEscort C2 servers over port 8080 and 8000. AVrecon malware prompts the infected device to communicate with its designated C2 server over port 8000 every 60 seconds using a custom loop in which AVrecon and the C2 server exchange the words "PING" and "PONG" until the C2 has a command for AVrecon to execute. For example, the C2 may interrupt the "PING/PONG" loop to direct the router to open a tunnel to a SocksEscort relay server. SocksEscort relay servers enable SocksEscort customers to connect and tunnel their traffic through residential routers infected with AVrecon.

The FBI and its partners have observed various indicators which suggest that SocksEscort has been used to conduct ad fraud, attempt website vulnerability exploitation, password spraying, digital marketplace fraud, banking fraud, romance fraud, and various other types of malicious activity.

Indicators

AVrecon malware primarily infects routers and IOT devices, which often lack Anti-Virus (AV), Endpoint Detection and Response (EDR), or other software which might allow a network owner to detect the infection.

The IP addresses and domain indicators included in this report have been associated with threat actor command-and-control (C2) infrastructure observed as of March 2026. The available telemetry does not contain granular timestamps for each individual indicator.

The FBI recognizes that infrastructure used for malicious activity may be hosted on cloud or virtualized platforms where IP addresses can be dynamically or temporarily assigned. As a result, an address associated with malicious activity at one point in time may later be reassigned to benign services. Accordingly, these indicators should be interpreted as historically observed infrastructure within the activity window and should be corroborated with current network telemetry or additional intelligence sources when used for defensive or investigative purposes.

AVrecon Loader MD5 Hash	
007fe05132e429ff57393163354f4c90	5f6f52fd4ece5918ee7979036a49bca3
232fdd85e07f74ea232cadafdb095d31	6e9540f68507580a3f495e9ff58dbd4e
3f83790a150a6bf71b908289fd230014	7fe57eca60841291cdd8ef1bb5c27de9
4651d6a90d24cf57c83a76ab160abf85	9f2df912212f67adcb64dbae8bfa2ca9
53f02fdf9c375c1837a31edf68694380	

AVrecon Malware MD5 Hash	
444138b1d805808a06c4b908c7b73d96	0a4e197044ad59116f0a1c2776125065
48374bfb610280c48086817cfb2bb310	006cc428088ea3766c094b421bf8e77f
48ef5c2a62d1ae95ea37d165e8a1be26	fb9d610a2b535dde194c05c099f0b307
4943e8c2a29ad616ec12cd7a507c612c	5aed40bccde5a7646c6fea17f7dd2083
4a884070ea340d89756be6575676ce85	8fc84a03b66ceccd394c6a754bb513a6
4d63235fdd3e0ace207d8fdbe19d63e0	0c5e43e51d3c2a00f4ac1b517891872d
53437d28fdf92c09821f56140c67aaca	a3e31f70b7a6abf3de15ca6646d16bfe
6501a2d2ed60b85b1080ac9edaf39b70	efb8b73d59a805e1fd9ebf0d3540b0e8
06d491b70f369b2672fce5a7b59a5c93	bf0183b2d18341c47576ba8e0d36fdff
126b1c224e8635d9571f9d769d7b55e2	22c5849855878f331d7bbf07e7ec7e41
1c8c17ef978bd4f03db672c0b2d51d00	f74c8bd1701746cce8b4bad819cdd148
1f970f5eb9cbef8dba11e2aed72373ba	f774fcbf889a8a629004f31e8b962b63
2a646682ee7f0f853605c78bb9126ed5	ffaa0890eb9a38307477157c02f63583
327c1ca93321705027e0bf47658b5f53	f81b9fceea2056ba2c3f261b56f577b1
32f1f238da09f1ebc1385317d50e94b4	8dcaf0e2a0baf54e65f46689b2a845ef

FBI FLASH
ACTIONABLE CYBER INTELLIGENCE

3bfc273e5592825443ded9c28f50cd5d	3ed1a6d57f00c1643cc85e049c82d1b4
6501a2d2ed60b85b1080ac9edaf39b70	d5d63db439bb1dba080ab27555b03a2a
667ae41f4a6201071b8cc3f88e3e02c7	de86b12800919ce8b213b51354d28ab8
6a389a89a6da7433210d9a52fc72589c	ef7f3f7cb4f3f1a90a2028d44c4fe702
6a6619b4b9a53233ca0a56606c484f9a	f0d1852065c498c3bdaec3de8e6cd626
6ec7063f03f95499b6c1821f90bda7e6	f143b44d3b8d835c09bf2c346d90ec22
70c2317f40de5b28f42d640488910140	f3cf4a369e5fb451db250c31776ba84e
74e5514cdd3ef6f703483700f04b5812	c32ac3f6cba0772de7737da60f9170c0
7d4c60c77a7d74cc3d9af4dabbecdbb8	c53397dc47ddc38a8c6daa3a02116518
8a978017496adb02eb368f3b28bc4ccd	bb5e9faa666e6d96eb95e358524213b6
8ad3f40fd8fcf2c7ee04d1219017cfe3	bd24f43084b33f13a835f661bf48b5e2
8fc84a03b66ceccd394c6a754bb513a6	bd4a12d4de4e42c4d9246aa92ddb86b8
920534d235204ced7ad2c76c1af7b3f8	9dfba3b92850a74135925e524e7b4748
963354b60552af16408cf4d82a827832	b1a32a442cdb34901f1f7ffbe47749f0
9752ac893640a027bea5a6df48ceb396	b5ad7f7e10f5d0401a2ad6b737724ff6

C2 IPs		
188.138.125.163	176.120.22.67	185.163.204.198
62.138.0.10	85.25.100.30	62.138.14.209
91.245.255.112	62.138.0.211	175.110.114.65
188.116.22.153	213.202.230.95	38.180.91.47
176.120.22.67	77.246.106.198	45.137.213.88
91.215.85.178	37.77.150.19	185.162.128.133
37.77.150.77	5.149.254.109	5.149.250.54
79.141.160.92	5.149.250.171	212.118.38.30

C2 Domains		
advstat.cc	meterstrack.cc	startsun.cc
backdump.cc	netjunk.cc	zeroback2.cc
critlan.cc	plxz.cc	zeroback3.cc
zeroback4.cc	atable.cc	cleandone.cc
evrc.space	lups.cc	dzero.cc
r0ck.online	regul.cc	fpride.cc
vdem.cc	utcp.cc	zerophone.cc
zeroback.cc	zorc.cc	

C2 URI Path	Description
lumi/config.php	lumi/test.php
lumi/ping.php	lumi/track.php

lumi/pride.php	

AVrecon C2 HTTP Header	Description
X-Proto-Cookies	X-Proto-Storage
X-Proto-UAgent	X-Proto-Core
X-Proto-Version	X-Proto-Jid
X-Proto-System	

Filename	Description
x	AVrecon Loader Filename
dnssmasq	AVrecon Malware Filename

Recommendations

- Keep all operating systems, software, and firmware up to date. Prioritize remediating known exploited vulnerabilities in internet-facing systems.
- Create and adhere to a patch schedule. Many SOHO routers and IOT devices may not automatically apply security patches and critical updates. Applying these updates often requires manual interaction with the device administration panel or manually re-flashing the device with new firmware.
  Review available device settings and enable any privacy or security-enhancing features, such as verbose logging, basic firewall rules, or automatic updates.
- Attempt to monitor, isolate, or otherwise restrict access to SOHO router and IOT devices which do not support AV or EDR software.
  - Many SOHO and IOT devices do not support commonly used AV and EDR software, which means that extra precautions must be taken to ensure that these types of devices are adequately monitored and isolated from other critical internal systems in the event of their compromise.
  - While not directly observed in the case of AVrecon, malware targeting routers and other internet-facing edge devices can be used to move laterally into a network owner's internal network. This can lead to highly damaging activity, such as the exfiltration of sensitive data or the deployment of ransomware.
- If a device is considered EOL by its manufacturer and is no longer supported, consider replacing the device with a model that is still receiving security updates.
- Change all default device passwords and comply with National Institute of Standards and Technology (NIST) standards.

- Ensure that features such as remote administration are disabled or consider using Access Control Lists (ACLs) or firewalls rules to restrict access to exposed ports and services.
- If possible, identify, detect, and investigate abnormal activity using a network monitoring tool which logs and reports all network traffic, including potential lateral movement activity on a network.
- Rebooting devices periodically can disrupt some infections. However, addressing known vulnerabilities is critical to prevent re-infection.
    - Factory resets and re-flashing with the latest firmware can also sometimes prevent infection. However, some variants of AVrecon silently disable this functionality, and for EOL devices, updating to the latest firmware will not address known vulnerabilities discovered after the device's EOL date.

Reporting Notice

The FBI encourages you to report suspicious or criminal activity to the FBI Internet Crime Complaint Center at **www.ic3.gov**. When available, each report should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact. Press inquiries should be directed to the FBI's National Press Office at npo@fbi.gov or (202) 324-3691.

Individual indicators included in this document should always be evaluated in light of your complete information security situation. Some indicators, particularly those of a nondeterministic or ephemeral nature (such as filenames or IP addresses), may not be indicative of a compromise.

Your organization has no obligation to provide information in response to this product. If, after reviewing the information provided, your organization decides to provide information to the FBI, it must do so consistent with applicable state and federal law.

Administrative Note

The information in this document is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cybersecurity professionals and system administrators guard against the persistent malicious actions of cyber actors. The FBI does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the FBI.

This FLASH was coordinated with DHS/CISA and is marked TLP:CLEAR. Subject to standard copyright rules, the information in this product may be shared without restriction.