A Broken System Fueling Botnets

By Synthient Research

Published: 2026-01-02 · Archived: 2026-04-06 00:30:40 UTC

Warning: To maintain the historical and technical accuracy of the systems discussed, some of the original code and documentation included below contain offensive terminology. This language is preserved only to provide a comprehensive report on the subject matter.

Executive Summary

Synthient continues to track the Kimwolf DDoS and proxy botnet with this report, delivering significant findings on the inner workings, infection chain, and reliance on the residential proxy ecosystem. Kimwolf has been highly active since early August of 2025, with substantial growth over the past four months. The Synthient's research team assesses with high confidence that the total number of infected devices has surpassed 2 million, primarily targeting Android devices running an exposed Android Debug Bridge (ADB) service via residential proxies. These findings further reveal an expansive network of compromised TV streaming devices used by providers to obtain large pools of IP addresses.

Given Kimwolf's reliance on residential proxies for infections, we advise all proxy providers to block high-risk ports and restrict access to the local network. Users should check whether they are affected by visiting synthient.com/check. Infected TV boxes should be wiped or destroyed. Organizations should block connections to the referenced C2 servers and domains, and monitor network traffic for suspicious activity.

Synthient expects to observe a growing interest among threat actors in gaining unrestricted access to proxy networks to infect devices, obtain network access, or access sensitive information. Kimwolf highlights the risks posed by unsecured proxy networks and their viability as an attack vector.

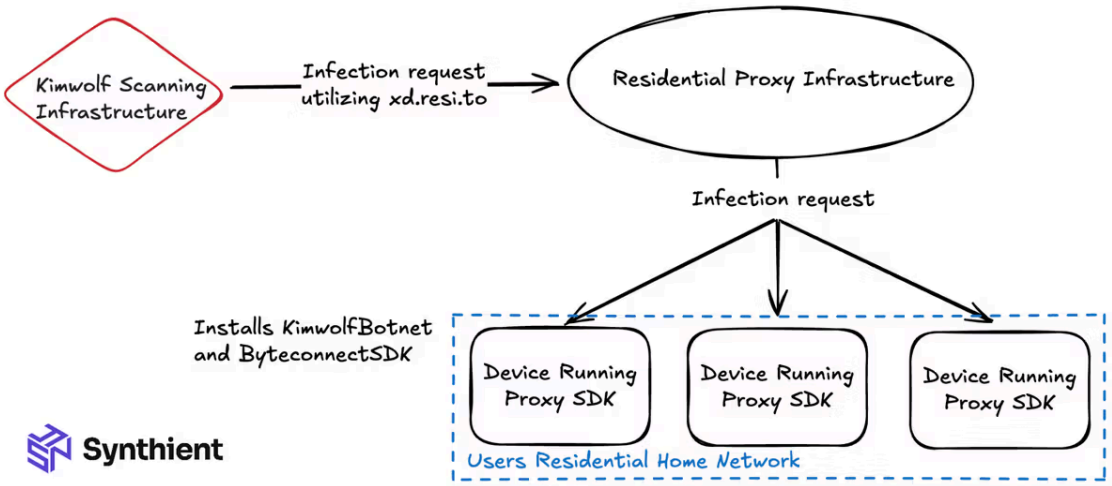
Background

Kimwolf, the android variant of the Aisuru DDoS Botnet, has grown to at least 2 million compromised devices over several months through its novel exploitation of residential proxy networks. Kimwolf remains a significant threat to organizations, as it continues to launch Distributed Denial-of-Service (DDoS) attacks, with Cloudflare reporting peak attack rates of 29.7 Tbps or 14.1 Bpps. Key actors involved in the Kimwolf botnet are observed monetizing the botnet through app installs, selling residential proxy bandwidth, and selling its DDoS functionality.

Over the last 3 months, Synthient's Research Team has conducted a comprehensive investigation of Kimwolf, revealing key insights into the group's operations.

Infection through Residential Proxies

Kimwolf's rapid growth can be attributed to its targeting of vulnerable devices through its novel exploitation of residential proxy networks. Our honeypot network saw an increase in targeting of the domain `xd[.]resi[.]to` on November 12th from IPIDEAs proxy network. This domain notably resolves to `0[.]0[.]0[.]0,` which points to the device running the proxy SDK.



> Fig 1 Kimwolf Scanning Infrastructure

Synthient's Research Team captured the following payload on December 1st, confirming the active exploitation of residential proxy networks.

This payload expands to the following bash script.

Synthient would capture four additional payloads, each making slight adjustments to the Kimwolf botnet, either to its protocol, C2 servers, or binaries.

December 11th

December 14th

December 25th

December 27th

December 28th [EDIT]

At the time of publishing our report we received one more sample. We've decided to include this in the report to further disrupt their operations.

During this period, the Kimwolf actors used a variety of domains and methods to circumvent restrictions and compromise devices. The following is an exhaustive list of domains and IPs observed targeting the residential proxy providers. (EDIT: Do not import this as a list of IOCs unless you are a proxy provider, please refer to the iOCs section of this report if you are an organization.)

Domains:

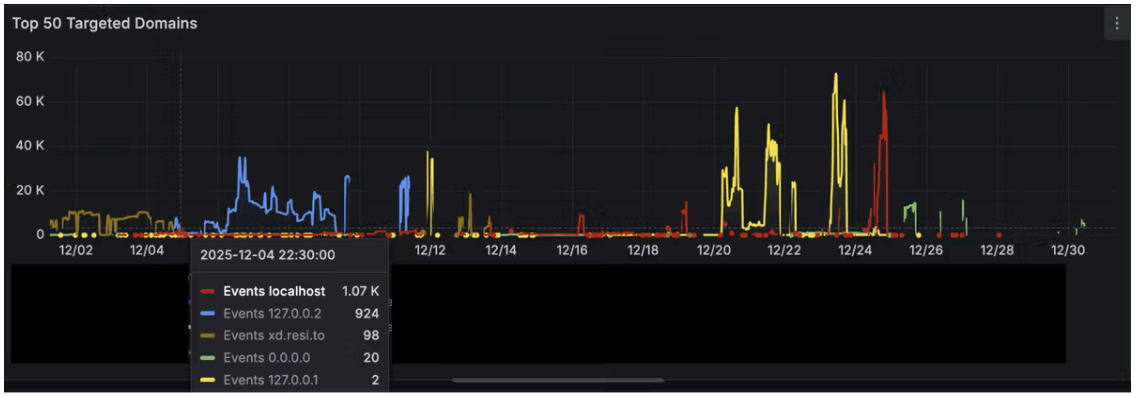
- localhost

- 127[.]0[.]0[.]0
- 127[.]0[.]0[.]1
- 127[.]0[.]0[.]2
- 0[.]0[.]0[.]0
- xd[.]resi[.]to
- xd[.]mob[.]to
- onetwoseven[.]14emeliaterracewestroxburyma02132[.]su
- lolxd[.]713mtauburnctcolumbusoh43085[.]st

Targeted Ports:

- 3222
- 5555
- 5858
- 12108

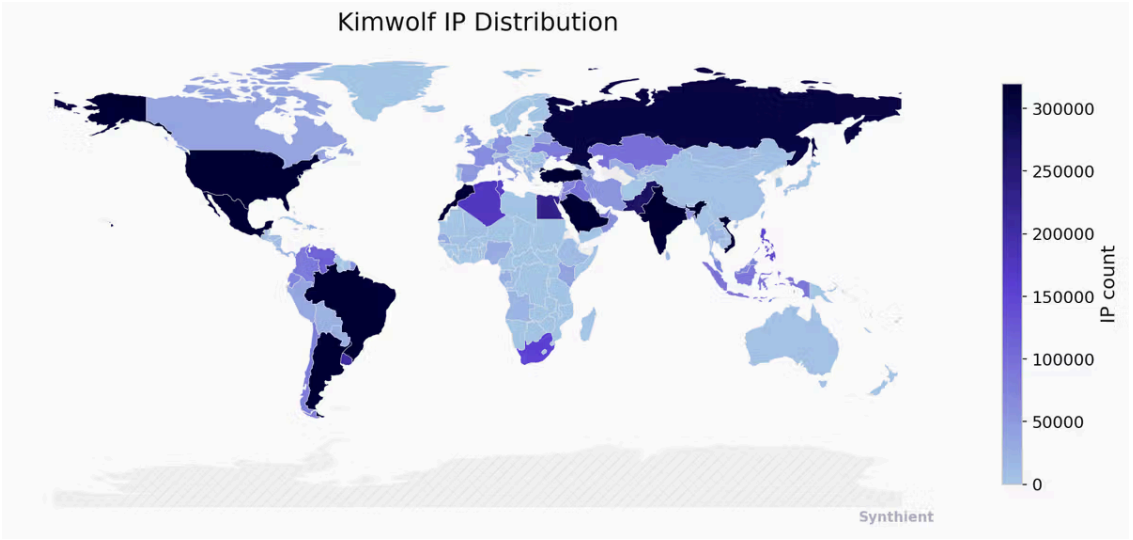
Kimwolf's scanning of proxy networks was at an unprecedented scale, with them holding the number one position many times for the most-targeted domain. Their scanning was often 24/7, with downtime limited to null routing or infrastructure changes.



> Fig 2. Synthient capturing the various Kimwolf scanning and exploitation attempts.

Infection Demographic

Synthient's Research Team believes Kimwolfs' infected device count to be well above 2 million, with significant numbers in Vietnam, Brazil, India, and Saudi Arabia. Even with their device count hovering around 2 million, Synthient's Research Team observes around 12 million unique IP addresses per week for Kimwolf.

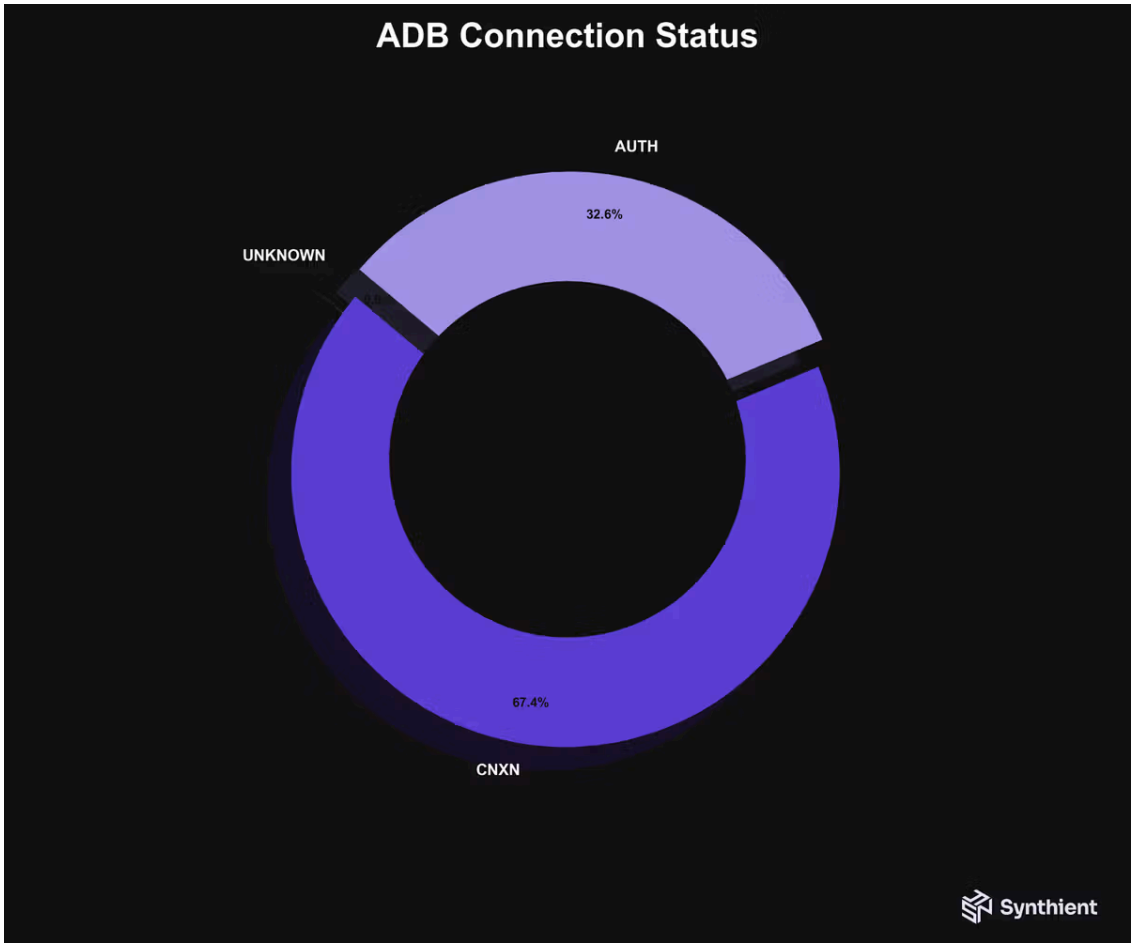


> Fig 3. Kimwolf geographic distribution of compromised devices.

Synthient's Research Team also received a screenshot from the backend Grafana instance in early November that matches this distribution. Please note the massive growth in the past 2 months.

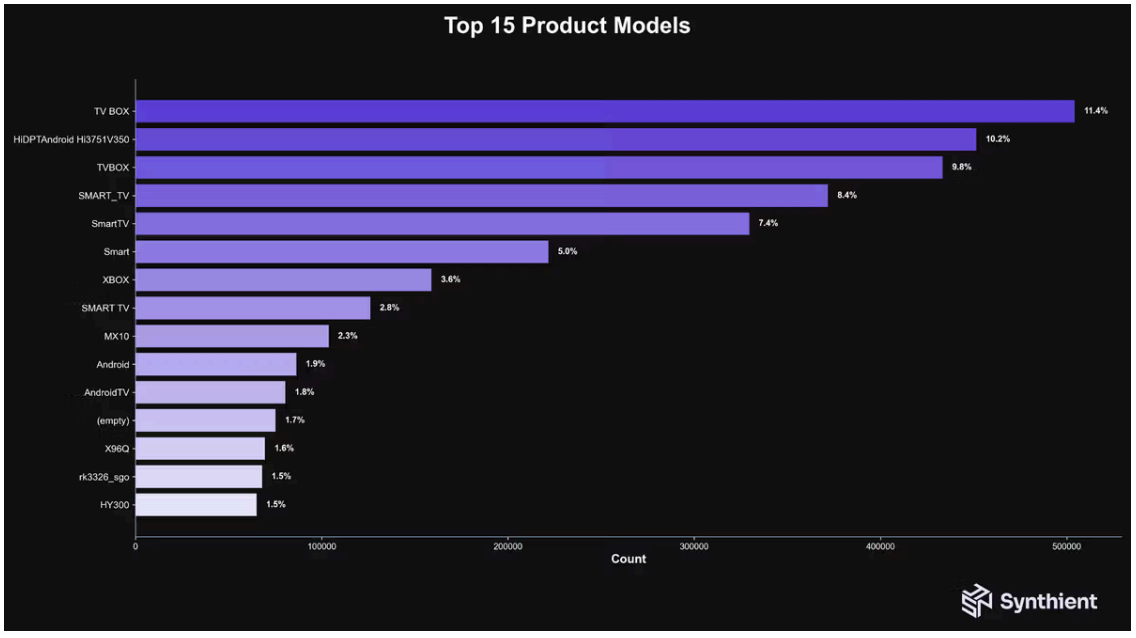
> Fig 4. Kimwolf's internal Grafana instance.

Upon analyzing exposed devices part of IPIDEAs proxy pool, we found that 67% of all Android devices are unauthenticated, leaving them vulnerable to remote code execution. From our scans, we found approximately 6 million vulnerable IPs (i.e., unique IPv6 or IPv4 addresses). These devices are often shipped pre-infected with SDKs from proxy providers. Once part of the residential proxy pool, Kimwolf will have scanned and exploited the device within minutes.



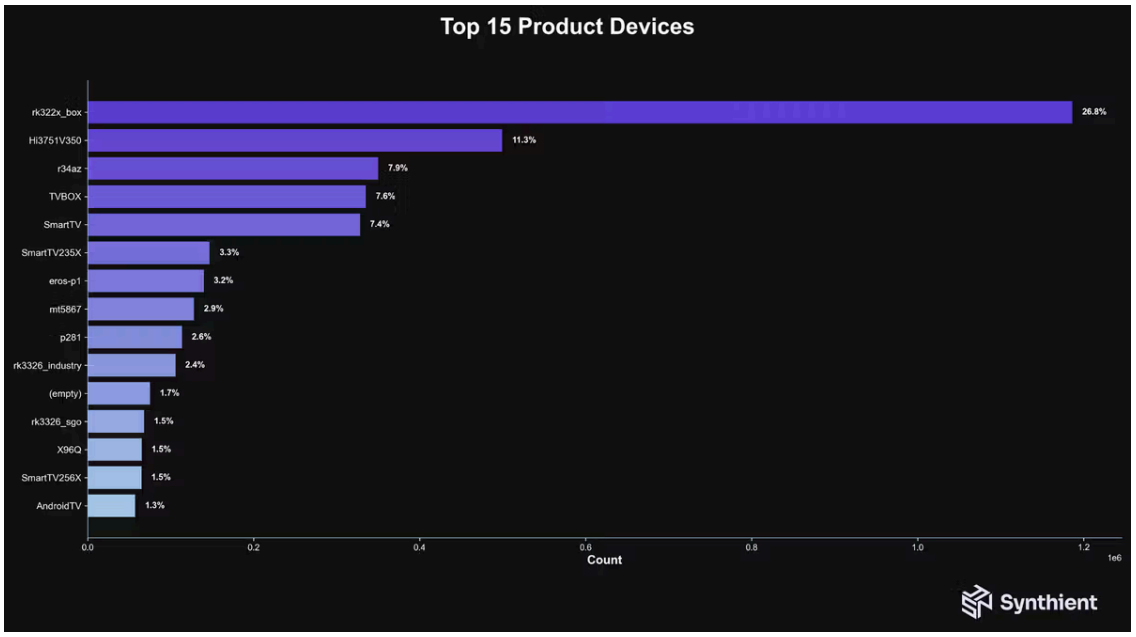
> Fig 5. 67% of connected devices responding as unauthenticated.

An analysis of the infected device's product name (ro.product.name) yields the following stats. TV BOX, HiDPTAndroid, and SMART_TV are among the top compromised devices.



> Fig 6. Top compromised product models.

Analyzing the device name (ro.product.device), we see the following breakdown. The over-representation of devices indicates they arrive pre-infected. Synthient's Research Team purchased several devices from the list, which corroborated this theory, showing that the devices were already running a malicious proxy SDK.



> Fig 7. Top compromised product devices.

A complete breakdown of impacted devices can be found here.

Kimwolf Analysis

XLab has published a comprehensive analysis of both V4 and V5 of the Kimwolf botnet. We refer to their publication for a complete analysis, as we will only cover changes to the latest Kimwolf botnet. Synthient received its final payload on December 27th before IPIDEA implemented a security patch. Due to IPIDEA's rapid deployment of the security patch, the final payload from December 27th was successfully mitigated before a full binary capture could be completed. As a result, the latest Kimwolf version downloaded was from December 25th.

When the payload runs, the following script is executed. This installs the latest version of the Kimwolf binary. These binaries are installed as "botless" and "com.abcproxy.sdk". Please note that the threat actors named the binary "com.abcproxy.sdk" to associate this activity with IPIDEA, which has no involvement with the Kimwolf actors.

Both binaries are almost identical, with the rolf binary making a slight difference in its TLS implementation. Additionally, the libdevice[.]so binary uses an Android APK for delivery, whereas the botless binary is dropped to the /rolf/ directory.

```
            SDKService sDKService = (SDKService) obj;
            try {
                AbstractC0280a.m508a(new File(sDKService.getApplicationContext().getApplicationInfo().nativeLibraryDir, "libdevice.so"),
"network_task");
            } catch (Exception unused) {
            }
```

> Fig 8. Android dropper executing Kimwolf

On execution, Kimwolf uses the environment variable xdrofl123 as a poor man's mutex to prevent multiple versions of the binary from running. If the variable is present, it prevents another instance from starting.

```
flame:/data/local/tmp $ ./kimwolf_libdevice_unpacked.so
the fuck?
```

Fig 9. Running the Kimwolf binary

In this latest version, Kimwolf listens on port 40860 and connects to 85[.]234[.]91[.]247:1337 for commands.

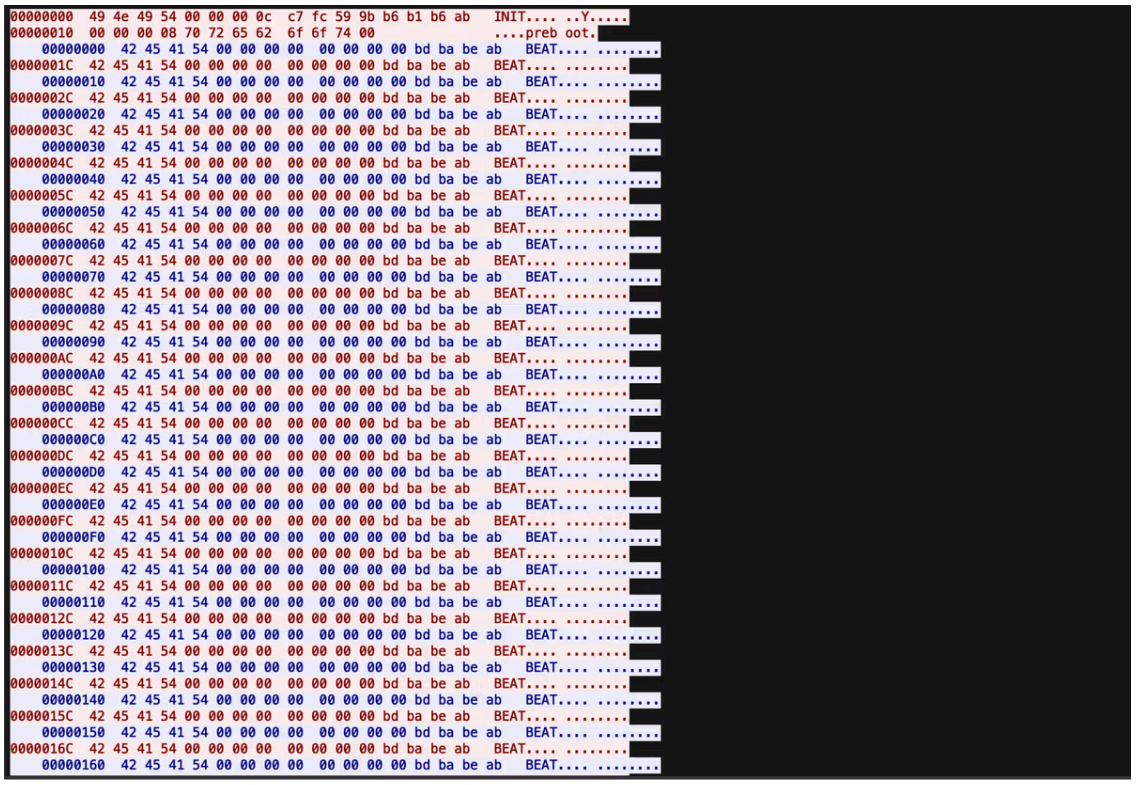


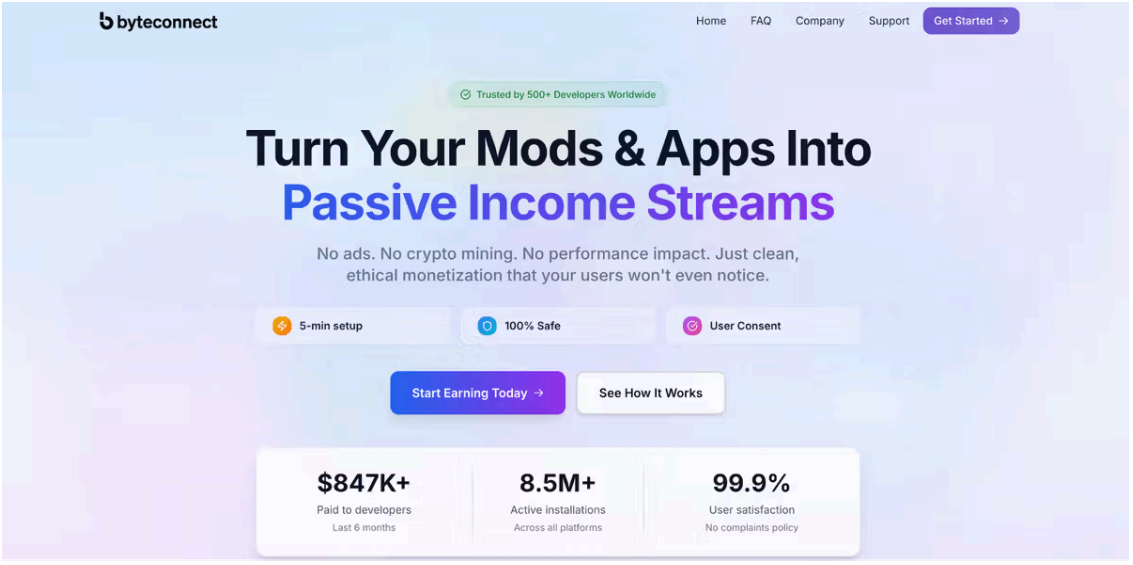
Fig 10. Initial connection and heartbeat

Another notable update includes the significant expansion of Kimwolf L7 attacks. The new attacks use the tls-client and azuretls-client Go libraries to spoof TLS fingerprints and headers. The Config for L7 attacks is as follows.

The complete Golang struct definitions for the Kimwolf botnet are documented here.

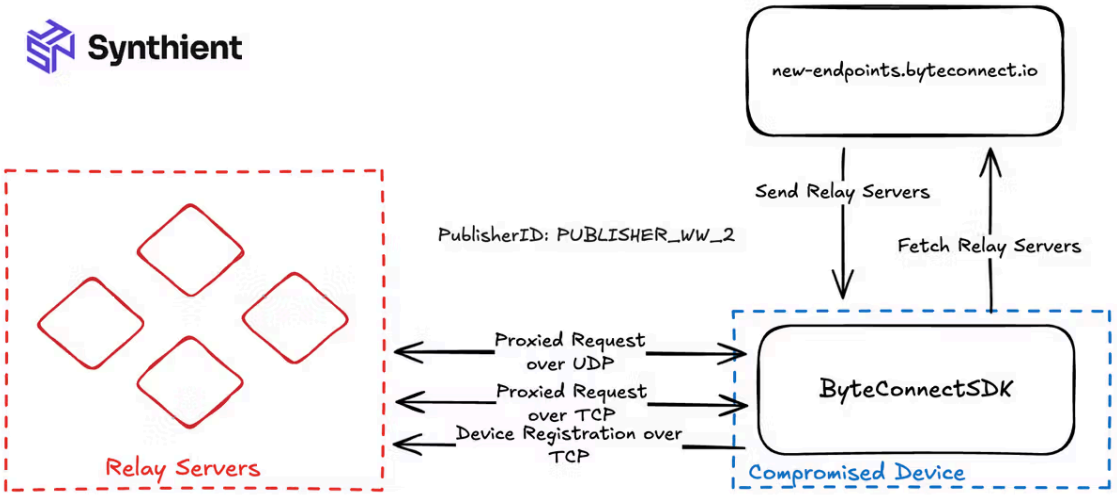
Byteconnect SDK

In addition to capturing the Kimwolf payload on December 14th, Synthient's Research Team also observed the installation of the Plainproxies Byteconnect SDK (e465e625c1f85527e7082ff70dc479b5). This SDK offers a bandwidth monetization service, indicating that Kimwolf actors received payment for performing app installs on compromised devices. This further highlights the threat actors' monetization attempts, in addition to the operation of their own proxy services.



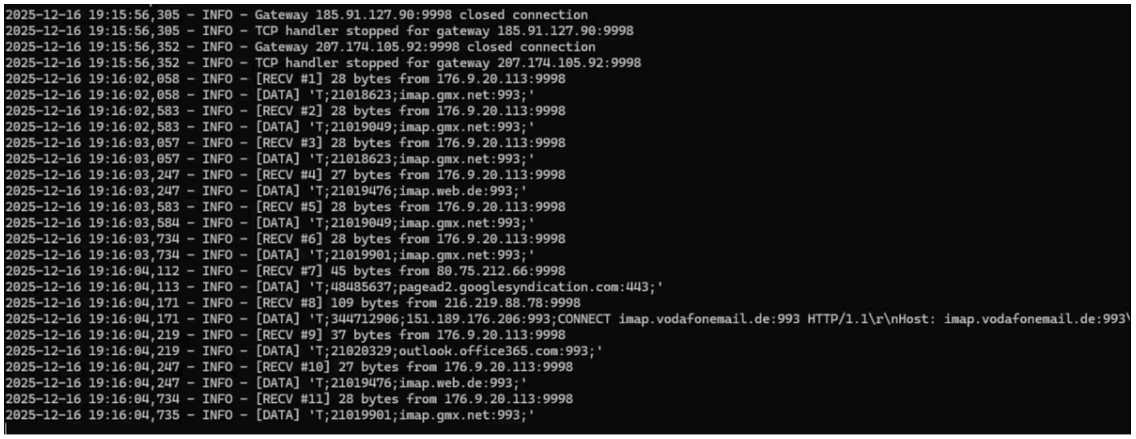
> Fig 11. A "clean, ethical monetization that your users wont even notice."

The ByteconnectSDK uses 119 relay servers that receive proxy tasks from a command-and-control server, which are then executed by the compromised device. These responses are sent back over the TCP socket.



> Fig 12. Byteconnect connection and task flow.

Upon connecting to the SDK, we observed an influx of credential-stuffing attacks targeting IMAP servers and popular online websites.



> Fig 13. Byteconnect credential stuffing.

Synthient's Research Team notified Plainproxies and has yet to receive any comment. The ByteconnectSDK continues to remain active on compromised devices.

Byteconnect Protocol

Registration Request

TCP Registration Packet

UDP Receive Task Packet

UDP Get Task Packet

Notifying Impacted Parties

Synthient notified IPIDEA, which confirmed and successfully patched the vulnerability on December 28th. This update now prevents access to local network devices and blocks access to the following sensitive ports: 21, 22, 23, 25, 69, 110, 139, 143, 161, 389, 465, 512, 513, 514, 587, 873, 993, 995, 1352, 1433, 1521, 2181, 2409, 3306, 3389, 3690, 4848, 5000, 5432, 5632, 5900, 6532, 6379, 7001, 7002, 8069, 9200, 9300, 11211, 27017, 27018, 50000, 5555, 5858, 12108, 3222, 1210, 5114.

As part of this research, we sent 11 vulnerability emails on December 17th to the top proxy providers. Each notified provider was impacted to varying degrees, with a significant portion allowing access to devices on the local network. The scale of this vulnerability was unprecedented, exposing millions of devices to attacks. Synthient's Research Team is unable to assess with confidence the complete list of targeted providers by Kimwolf. Current evidence indicates that IPIDEA was the main target because it enabled access to all ports.

The Proxy Ecosystem

Kimwolf's monetization strategy became apparent early on through its aggressive sale of residential proxies. By offering proxies as low as 0.20 cents per GB or $1.4K a month for unlimited bandwidth, it would gain early adoption by several proxy providers.

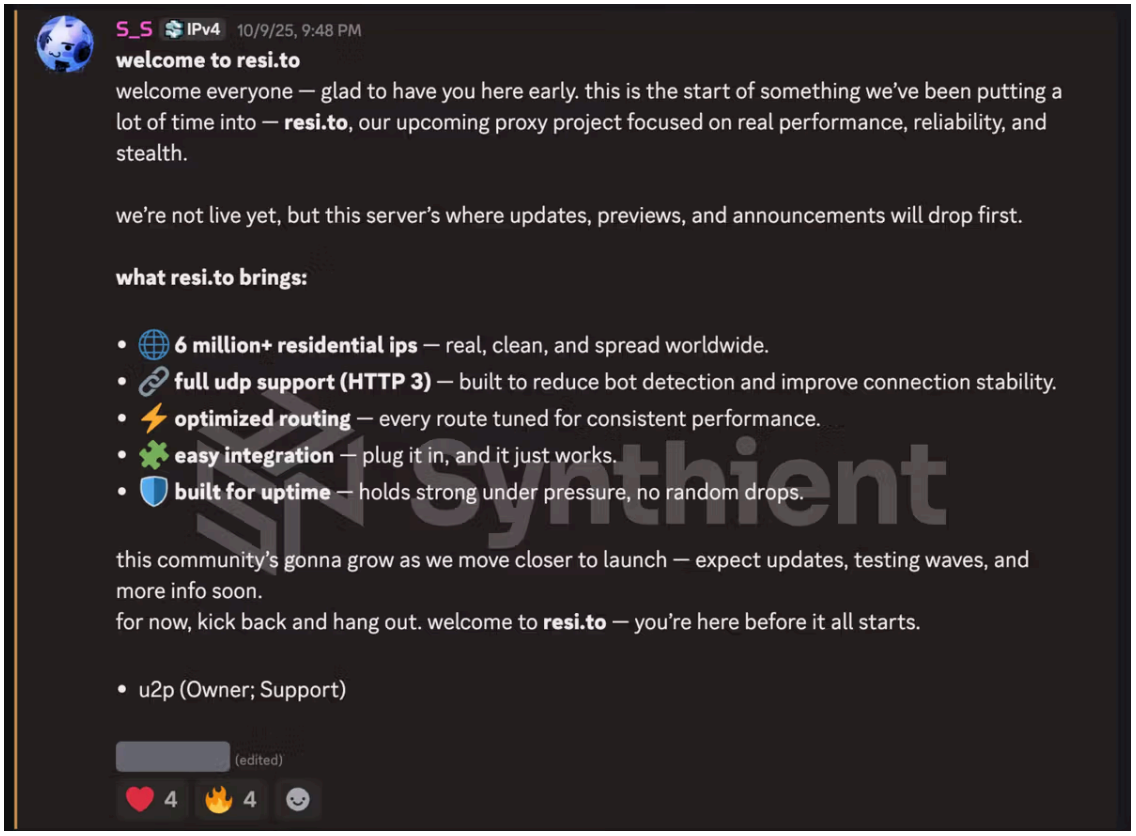


Fig 14. RESITO Discord Server and the selling of Kimwolf proxies in early October.

Synthient's Research Team received screenshots from other proxy providers showing key Kimwolf actors attempting to offload proxy bandwidth in exchange for upfront cash. This approach likely helped fuel early development, with associated members spending earnings on infrastructure and outsourced development tasks. Please note that resellers know precisely what they are selling; proxies at these prices are not ethically sourced.

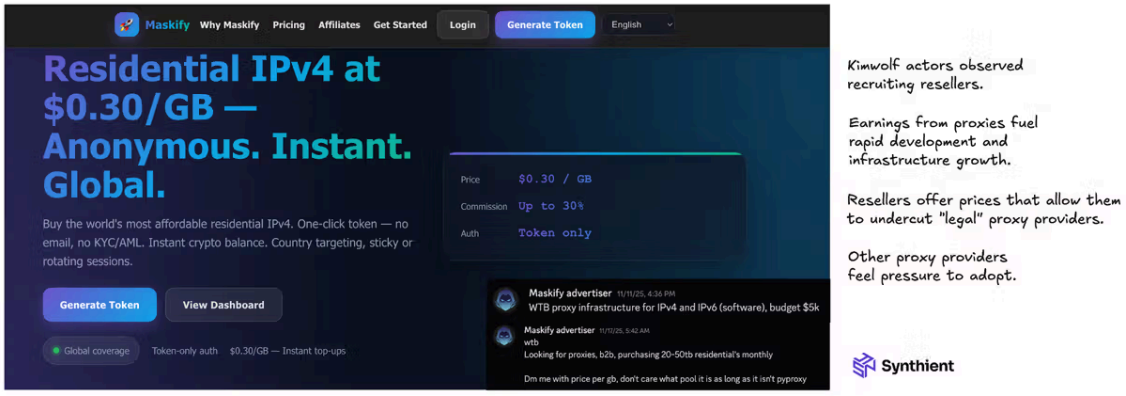


Fig 15. Maskify, another provider heavily involved in the sales of Kimwolf proxies.

The aggressive tracking of Kimwolf helped create a novel dataset, enabling clients of Synthient to mitigate both DDoS and credential-stuffing attacks targeting their platform. Synthient actively tracks Kimwolf through the following providers.

Proxy Provider	Synthient Tag	Gateway
https://discord[.]gg/ipv4	RESITO	172[.]93[.]102[.]243:80
https://discord[.]gg/ipv4	RESITO	104[.]243[.]43[.]148:80
https://discord[.]gg/ipv4	RESITO	104[.]243[.]41[.]180:80
https://discord[.]gg/ipv4	RESITO	104[.]243[.]41[.]110:80
https://discord[.]gg/ipv4	RESITO	80.75[.]212[.]10:80
https://discord[.]gg/ipv4	RESITO	193[.]25[.]217[.]66
https://maskify[.]su	MASKIFY	resi[.]maskify[.]su:80
https://ptun[.]nl	PTUNNL	resi[.]ptun[.]nl:80
https://flashproxy[.]com	FLASHPROXY_LITE	lite[.]flashproxy[.]io:6969

Several larger proxy providers have also been observed mixing in Kimwolf proxies to increase the size of their core pool.

Mitigation Strategies

Proxy Providers

If you are a proxy provider and want to test whether you are vulnerable, you can do so by issuing a request to the domain amivulnerable.synthient.com. If you see a default router page, your proxy network is vulnerable. Proxy providers should implement necessary fixes to block requests to RFC 1918 addresses.

Additionally, proxy providers should check whether they are affected by reviewing existing logs for requests to the following domains.

- localhost
- 127[.]0[.]0[.]0
- 127[.]0[.]0[.]1
- 127[.]0[.]0[.]2
- 0[.]0[.]0[.]0
- xd[.]resi[.]to
- xd[.]mob[.]to
- onetwoseven[.]14emeliaterracewestroxburyma02132[.]su
- lolxd[.]713mtauburnctcolumbusoh43085[.]st

Victims of Kimwolf

Users can check if they are a victim of the Kimwolf botnet on synthient.com/check. If flagged, we encourage the TV Box to be destroyed.

Organizations

- **Audit Network & Devices**: Reference the complete list of Indicators of Compromise (IOCs) and inspect your network traffic and hardware for signs of infection.
- **Remove High-Risk Hardware**: Avoid keeping potentially vulnerable devices, specifically TV boxes, on your network, as these are Kimwolf's primary targets.
- **Secure ADB Shells**: Lock down devices running unauthenticated ADB (Android Debug Bridge) shells to prevent unauthorized access.
- **Check for Proxy SDKs:** Verify your IP address to ensure your system isn't running a proxy SDK unintentionally.

Observables and IOCs

A complete list of observables and IOCs are available on the Synthient GitHub.

Conclusion

Kimwolf highlights the significant risks posed by residential proxy networks, along with their sophisticated operations that exploit the "gray market" of the proxy ecosystem. The botnet’s unprecedented growth to over 2 million devices is not just a failure of individual device security but a systemic vulnerability within the residential proxy supply chain.

The discovery of pre-infected TV boxes and the monetization of these bots through secondary SDKs like Byteconnect indicates a deepening relationship between threat actors and commercial proxy providers. While the collaboration with IPIDEA led to a successful patch, the broader landscape remains precarious.

Synthient assesses that the Kimwolf operation provides a blueprint for future botnets to achieve rapid, low-cost growth by bypassing traditional defenses. As long as demand for low-cost residential bandwidth continues to grow, the risk to organizations and individuals will remain high.
