Hive Pro

Threat Level

Amber

Hiveforce Labs

# THREAT ADVISORY

## ATTACK REPORT

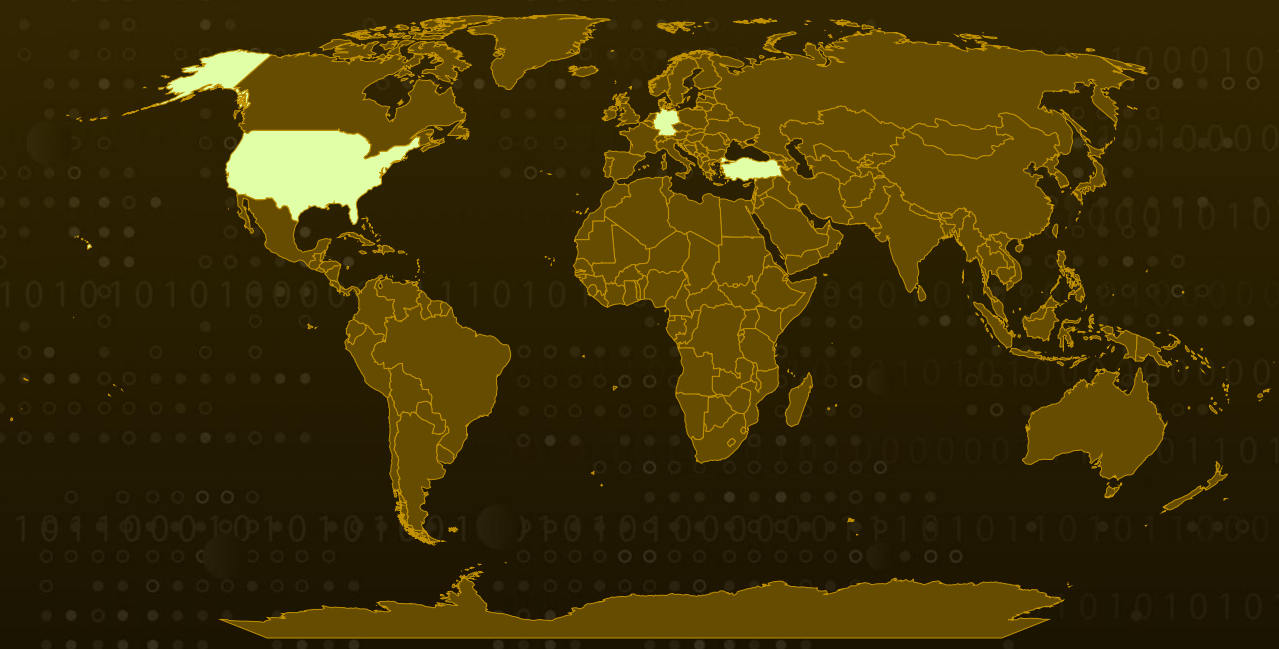
# Hpingbot Rising: The Botnet That Thinks Outside the Payload

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| July 4, 2025 | A1 | TA2025208 |

# Summary

**Attack Commenced:** June 2025
**Targeted Countries:** Germany, USA, Turkey
**Affected Platforms:** Windows, Linux, IoT
**Malware:** Hpingbot
**Attack:** Hpingbot is a stealthy, cross-platform botnet that's rapidly spreading across Linux, Windows, and IoT devices. Built in Go and leveraging tools like Pastebin and hping3, it's designed for flexibility, launching DDoS attacks, downloading malicious payloads, and maintaining long-term access. What makes it especially dangerous is its modular design, silent behavior, and constant evolution, suggesting a skilled team behind it. With SSH brute-force as its main entry point and frequent updates to evade detection, Hpingbot represents a growing, sophisticated threat in today's cyber landscape.

## Attack Regions



# Attack Details

**#1** Hpingbot is a newly emerging and rapidly evolving botnet family that has cross-platform capabilities and innovative use of existing technologies. Developed in the Go programming language, Hpingbot is compatible with both Windows and Linux, IoT environments and supports multiple processor architectures. Hpingbot leverages platforms like Pastebin to distribute its payloads and utilizes the command-line network tool hping3 to conduct DDoS attacks. Additionally, it can download and executing arbitrary payloads, making it a versatile threat often used by APT and ransomware groups.

**#2** One of the key characteristics of Hpingbot is its silent but persistent behavior. Monitoring data reveals that it issues DDoS commands sparingly only a few hundred attacks have been recorded since June 17, primarily targeting systems in Germany. It has been observed participating in broader DDoS campaigns alongside other emerging botnets, collectively launching over 15,000 attacks against a single monitored IP address hosting the NetData monitoring tool.

**#3** Hpingbot's infrastructure is designed for flexibility and modularity. Its propagation is primarily driven by SSH brute-force attacks, though the SSH module remains separate from the main payload to conceal propagation logic and protect key components. The botnet uses Pastebin to host and distribute payload URLs, and includes a dedicated installer that manages downloading, persistence, and execution. Hpingbot ensures long-term presence on compromised devices using various persistence techniques, such as creating services through Systemd, SysVinit, or setting up Cron jobs.

**#4** The botnet's DDoS capabilities are built around the hping3 tool, which is automatically installed using the command apt -y install hping3 on supported Linux systems. Once installed, Hpingbot leverages hard-coded commands to configure and launch over ten types of DDoS attacks, offering flexibility through adjustable parameters. However, this method is limited in Windows environments, where apt is not supported. The botnet's architecture includes multiple hard-coded Pastebin links to streamline command retrieval and payload sharing.

**#5** A new DDoS component is being distributed through Hpingbot's infrastructure. Written in Go, it adds UDP and TCP flood capabilities and includes German debugging comments, suggesting it's still in testing. The attacker may be planning to replace or enhance the original botnet. Frequent updates, shifting C&C servers, and improved installation scripts indicate active development by a skilled team, making Hpingbot a high-priority threat to monitor.

# Recommendations

**Strengthen SSH Security:** Hpingbot spreads mainly through systems with weak SSH passwords. Make sure all servers use strong, complex passwords and, if possible, switch to key-based authentication instead of passwords. Disable SSH access where it's not needed.

**Monitor for Unusual Traffic:** Keep an eye on outgoing network traffic, especially connections to unusual Pastebin URLs or attempts to download unknown files. Use network monitoring tools to flag and investigate suspicious activity early.

**Limit Installation Rights:** Restrict who can install software or run commands like apt install. This helps prevent tools like hping3 from being installed by malware without your knowledge.

**Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

## Potential MITRE ATT&CK TTPs

| | | | |
|---|---|---|---|
| TA0042 Resource Development | TA0002 Execution | TA0003 Persistence | TA0005 Defense Evasion |
| TA0006 Credential Access | TA0007 Discovery | TA0011 Command and Control | TA0040 Impact |
| T1059 Command and Scripting Interpreter | T1059.004 Unix Shell | T1569 System Services | T1569.002 Service Execution |
| T1543 Create or Modify System Process | T1543.002 Systemd Service | T1037 Boot or Logon Initialization Scripts | T1037.004 RC Scripts |

| | | | |
|---|---|---|---|
| **T1053** Scheduled Task/Job | **T1053.003** Cron | **T1070** Indicator Removal | **T1070.004** File Deletion |
| **T1070.003** Clear Command History | **T1102** Web Service | **T1102.002** Bidirectional Communication | **T1008** Fallback Channels |
| **T1498** Network Denial of Service | **T1082** System Information Discovery | **T1583** Acquire Infrastructure | **T1583.006** Web Services |
| **T1095** Non-Application Layer Protocol | **T1110** Brute Force | **T1105** Ingress Tool Transfer | |

## Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| IPv4 | 45[.]139[.]113[.]61, 193[.]32[.]162[.]210 |
| URLs | hxxp[:]//128[.]0[.]118[.]18, hxxp[:]//93[.]123[.]118[.]21, hxxp[:]//94[.]156[.]181[.]41 |
| MD5 | F33E6976E3692CB3E56A4CC9257F5AAE |
| SHA256 | 3359037b5a331ecf79ab9aa114f673e96a227a038fdb377badfbe16b5eaa4e7f |

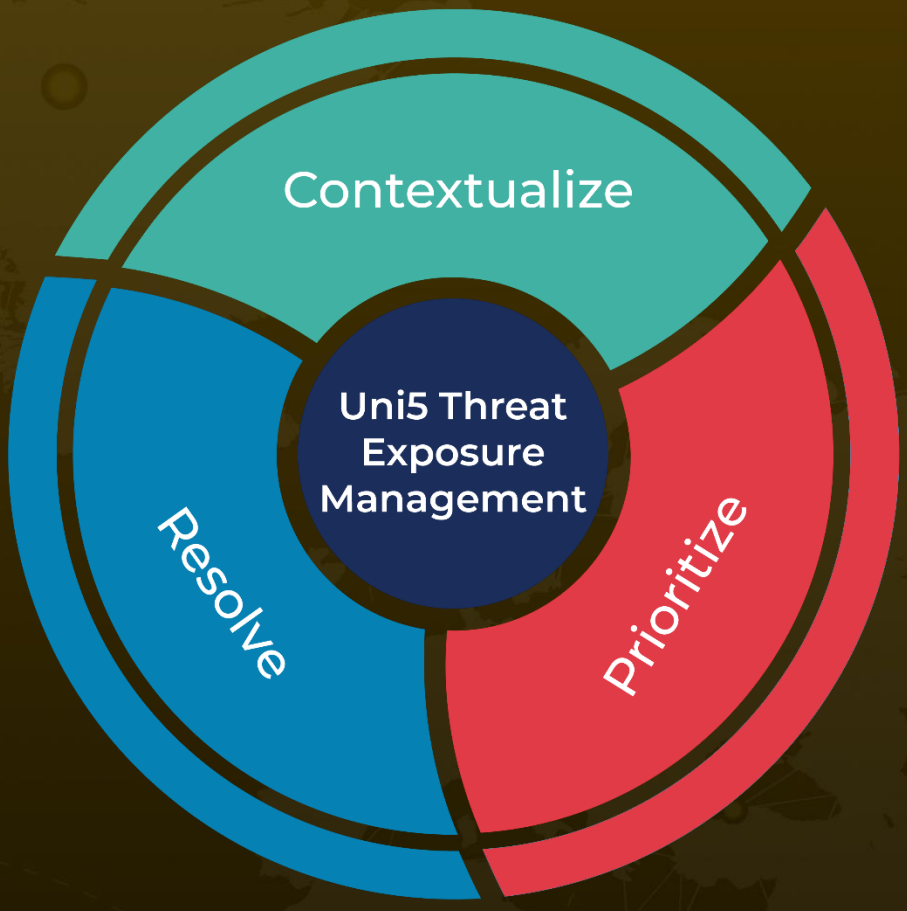
## References

https://nsfocusglobal.com/hpingbot-a-new-botnet-family-based-on-pastebin-payload-delivery-chain-and-hping3-ddos-module/

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.




REPORT GENERATED ON

**July 4, 2025 • 5:00 AM**



More at www.hivepro.com