Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

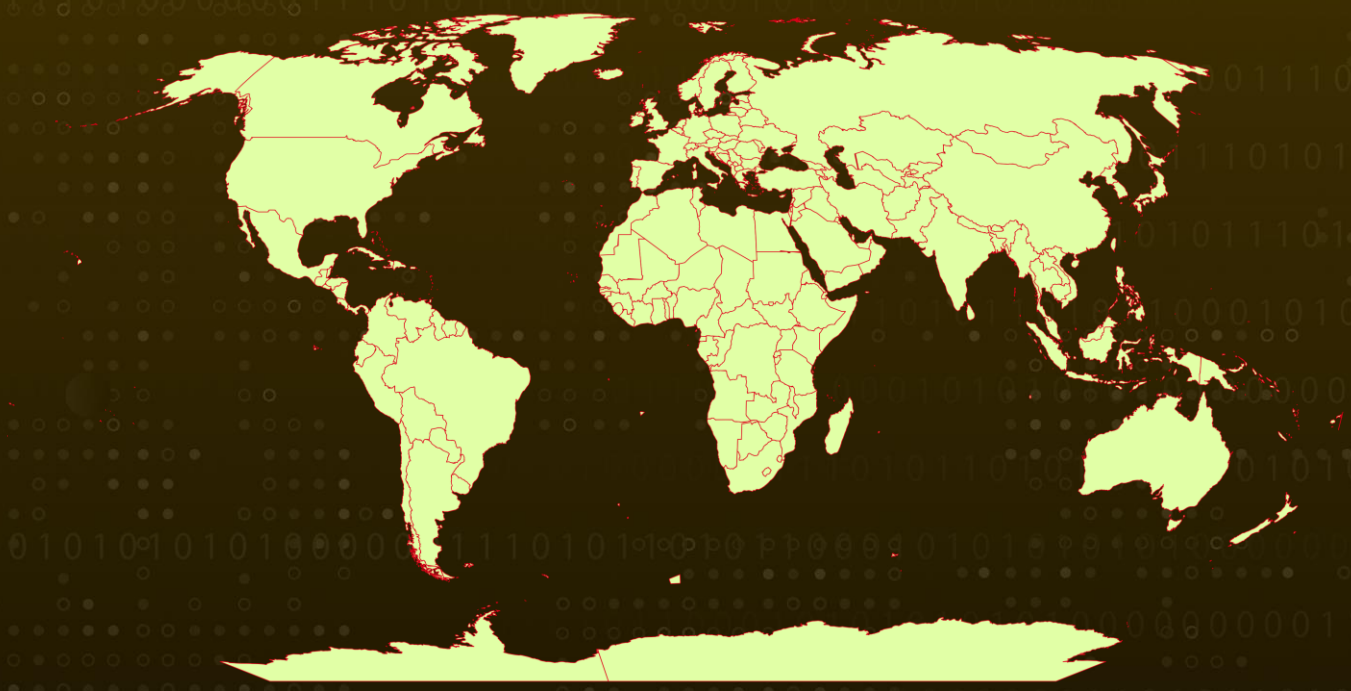
RapperBot Campaign Launches DDoS Attacks on Game Servers

Date of Publication	Admiralty Code	TA Number
November 18, 2022	A1	TA2022265

Summary

Date: October 2022
Attack Region: Worldwide
Attack: DDoS attack allows remote attackers to take control of susceptible systems.

Attack Regions



Attack Details

#1

The new RapperBot malware version creates a botnet capable of launching Distributed Denial of Service (DDoS) attacks. The latest version can launch Telnet brute-force strikes, DoS attacks using the Generic Routing Encapsulation (GRE) tunneling protocol, and UDP floods against game servers.

#2

After it has gained access, it communicates the credentials used, the compromised device's IP address, and its architecture to the C2 server via a different port (5123). Before executing the payload, the bot downloads its payload using software such as ftpget, wget, curl, or tftp installed on the infected device.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	TA0011 Command and Control	TA0040 Impact	T1110 Brute Force
T1003 OS Credential Dumping	T1499 Endpoint Denial of Service	T1102 Web Service	

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	3d5c5d9e792e0a5f3648438b7510b284f924ab433f08d558b6e082e1d5414a03,7afcac5f71e9205879e0e476d3388898a62e7aa4a3e4a059884f40ea36cfd57f,8ec79a35700f6691f0d88d53647e9f2b75648710ecd119e55815331fc3bdd0b5,a12ad4bc394d60bc037271e1c2df1bd2b87bdaaba85f6c1b7d046341f027cc2d,f000bf482040b48595badee1fc56afb95449ac48b5dc35fe3a05542cbf18f658,4aa9175c1846557107ec197ea73d4cc8dbe6d575a8fd86ae214ff9b3a00e438b,f98261eb7dc122449c158118cc9c660683206983a9e90ff73eb88c4705e0c48e
URLs	hxxp://185[.]216[.]71[.]149/armv4l hxxp://185[.]216[.]71[.]149/armv5l hxxp://185[.]216[.]71[.]149/armv6l hxxp://185[.]216[.]71[.]149/armv7l hxxp://185[.]216[.]71[.]149/mips hxxp://185[.]216[.]71[.]149/mipsel hxxp://185[.]216[.]71[.]149/powerpc hxxp://185[.]216[.]71[.]149/sparc hxxp://185[.]216[.]71[.]149/sh4 hxxp://185[.]216[.]71[.]149/bot_arm4_el hxxp://185[.]216[.]71[.]149/bot_mips_eb hxxp://185[.]216[.]71[.]149/bot_mips_el hxxp://185[.]216[.]71[.]149/bot_sh_el
IP Address	185[.]216[.]71[.]149

References

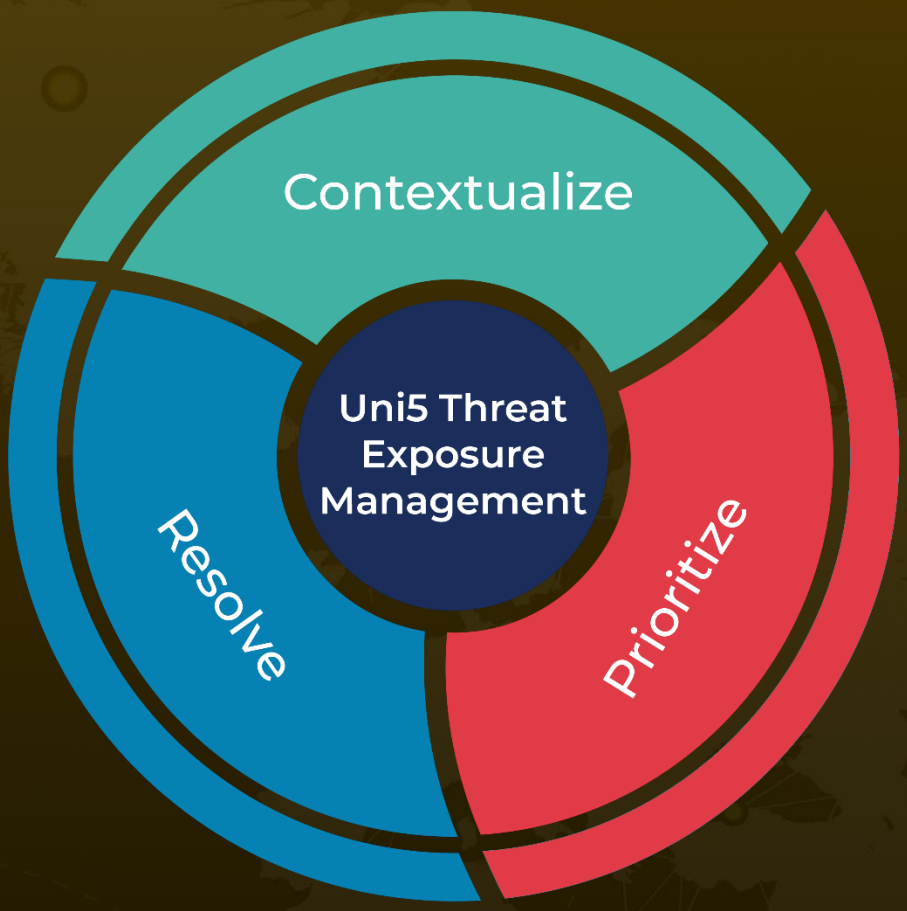
https://www.fortinet.com/blog/threat-research/new-rapperbot-campaign-ddos-attacks

https://thehackernews.com/2022/11/warning-new-rapperbot-campaign-aims-to.html

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 18, 2022 . 2:58 AM

More at www.hivepro.com