Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Unveiling ChinaZ DDoS Threat Landscape

Date of Publication	Admiralty Code	TA Number
March 27, 2023	A1	TA2023161

Summary

First appeared: 2014
Malware: ChinaZ or ChinaZ DDoSClient
Threat Actor: ChinaZ
Attack Region: Worldwide
Attack: ChinaZ, a Chinese threat group, is infamous for using DDoS botnets known as “ChinaZ” or “ChinaZ DDoSClient” to target both Windows and Linux systems.

Attack Regions

Attack Details

#1

The ChinaZ threat group, discovered in 2014, installs ChinaZ or ChinaZ DDoSClient bots on Windows and Linux systems, likely using stolen account credentials from scanners and SSH Brute Force malware. Once logged in, the group disables iptables and deploys the malware, built for x86 and x64 architectures, using wget. ChinaZ installs the malware as the root user in the /root directory.

#2

ChinaZ DDoSClient, after being executed, camouflages itself as "declient". It first utilizes the CSocketManager::GetOnlineInfo() method to gather essential details of affected systems, which are then sent to the C&C server. The majority of ChinaZ's supported commands are commonly used for DDoS attacks.

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

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	TA0040 Impact	T1110 Brute Force
T1498 Network Denial of Service	T1057 Process Discovery	T1546 Event Triggered Execution	T1021 Remote Services
T1499 Endpoint Denial of Service	T1027 Obfuscated Files or Information	T1027.005 Indicator Removal from Tools	T1129 Shared Modules
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c69f5eb555cc10f050375353c205d5fa c9eb0815129c135db5bbb8ac79686b9a 2ec7348e6b6b32d50a01c3ffe480ef70
URLs	hxxp[:]//45.113.163[.]219/linux32 hxxp[:]//45.113.163[.]219/linux64 hxxp[:]//45.113.163[.]219/win32
IPV4:PORT	45.113.163[.]219:29134
Domains	www[.]911ddos[.]com

References

https://asec.ahnlab.com/en/50316/

https://www.intezer.com/blog/malware-analysis/chinaz-relations/

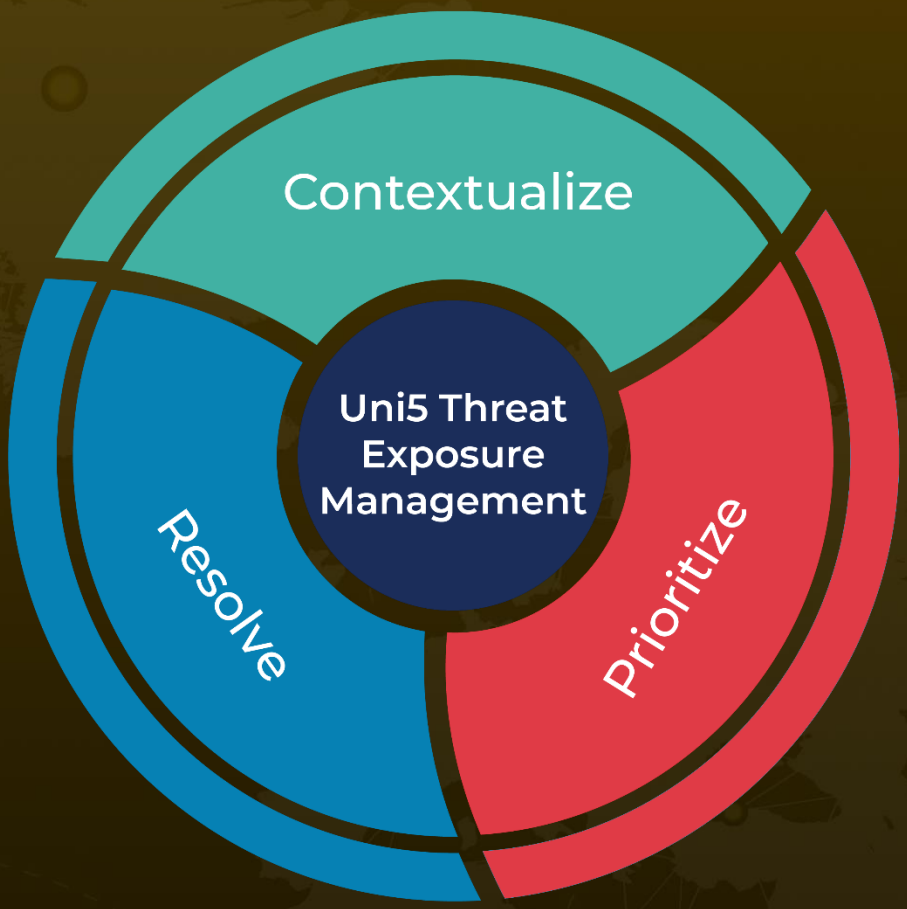
https://www.virusbulletin.com/virusbulletin/2019/12/vb2019-paper-exploring-chinese-ddos-threat-landscape/#ref5

https://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html

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

March 27, 2023 • 2:33 AM

More at www.hivepro.com