Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

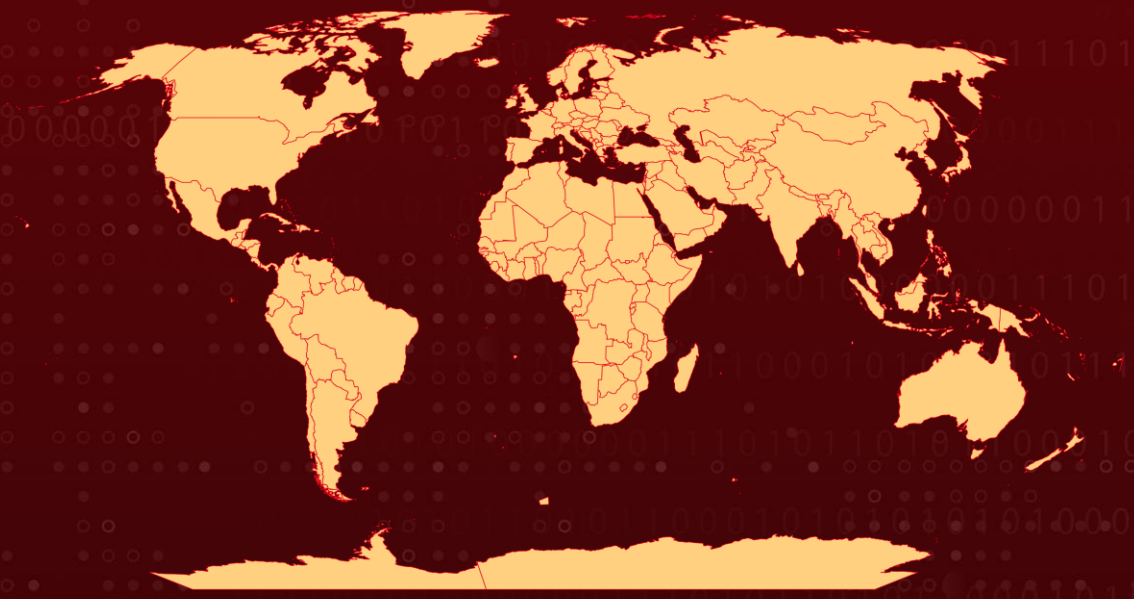
FritzFrog Expanding Its Lethal Reach with Frog4Shell

Date of Publication	Admiralty Code	TA Number
February 7, 2024	A1	TA2024046

Summary

First Seen: 2020
Malware: FritzFrog Botnet
Attack Region: Worldwide
Attack: The recent activities surrounding the FritzFrog Golang-based botnet reveal in its iterations, the employment of an exploit called 'Frog4Shell,' capitalizing on the Log4Shell vulnerability.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-4034	PwnKit (Polkit's Privilege Escalation Vulnerability)	Polkit pkexec utility	✗	✓	✓
CVE-2021-44228	Log4Shell (Apache Remote Code Execution Vulnerabilities)	Apache Log4j: 2.0 - 2.14.1	✓	✓	✓

Attack Details

#1 In recent developments the FritzFrog botnet has exploited the Log4Shell vulnerability discovered in 2021. Initially identified in 2020, this sophisticated, Golang-based peer-to-peer botnet was designed to support AMD and ARM-based machines. The actively curated FritzFrog has undergone iterative enhancements over time, progressively incorporating and refining its capabilities.

#2 Traditionally, FritzFrog has targeted its victims by utilizing SSH brute-force attacks on Internet-facing servers with weak passwords. This method has proven highly successful, resulting in over 20,000 recorded FritzFrog attacks and impacting more than 1,500 victims. Notably, recent iterations of FritzFrog have introduced a new exploit called 'Frog4Shell,' taking advantage of the Log4Shell vulnerability.

#3 FritzFrog's approach to identifying potential Log4Shell targets involves scanning for HTTP servers on ports 8080, 8090, 8888, and 9000. In its propagation strategy, the malware now aims to compromise all hosts within the internal network.

#4 Another significant modification is the integration of a privilege escalation tactic, exploiting CVE-2021-4034, a memory corruption vulnerability in Polkit. This vulnerability enables FritzFrog to manipulate pkexec into loading and executing a library controlled by the attacker, leading to code execution with root privileges.

#5 The persistence and adaptability of FritzFrog underscore the determination of sophisticated adversaries who continuously refine their techniques. The observed Log4Shell capabilities in FritzFrog highlight the ongoing and potent threat it poses, persisting for years beyond the initial disclosure of the vulnerabilities it exploits.

Recommendations

Keep Software and Systems Updated: Regularly update operating systems, antivirus software, and applications to patch known vulnerabilities. Ensure that security patches from software vendors are promptly applied to mitigate the risk of exploitation.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control
T1587.004 Exploits	T1190 Exploit Public-Facing Application	T1018 Remote System Discovery	T1059 Command and Scripting Interpreter
T1110 Brute Force	T1588.006 Vulnerabilities	T1055 Process Injection	T1584.005 Botnet
T1083 File and Directory Discovery	T1082 System Information Discovery	T1211 Exploitation for Defense Evasion	T1105 Ingress Tool Transfer
T1659 Content Injection			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f77ab04ee56f3cd4845d4a80c5817a7de4f0561d976d87563deab752363a765d, fb3371dd45585763f1436afb7d64c202864d89ee6cbb743efac9dbf1cefcc291, 52b11d3fa9206f51c601bd85cb480102fd938894b7274fac3d20915eb3af44f8, 85cb8ceda7d2a29bc7c6c96dd279c43559797a624fc15d44da53ca02379afe01, 0b95071c657f23d4d8bfa39042ed8ad0a1c1bceb6b265c1237c12c4c0818c248

Patch Details

https://access.redhat.com/security/vulnerabilities/RHSB-2022-001

https://logging.apache.org/log4j/2.x/security.html

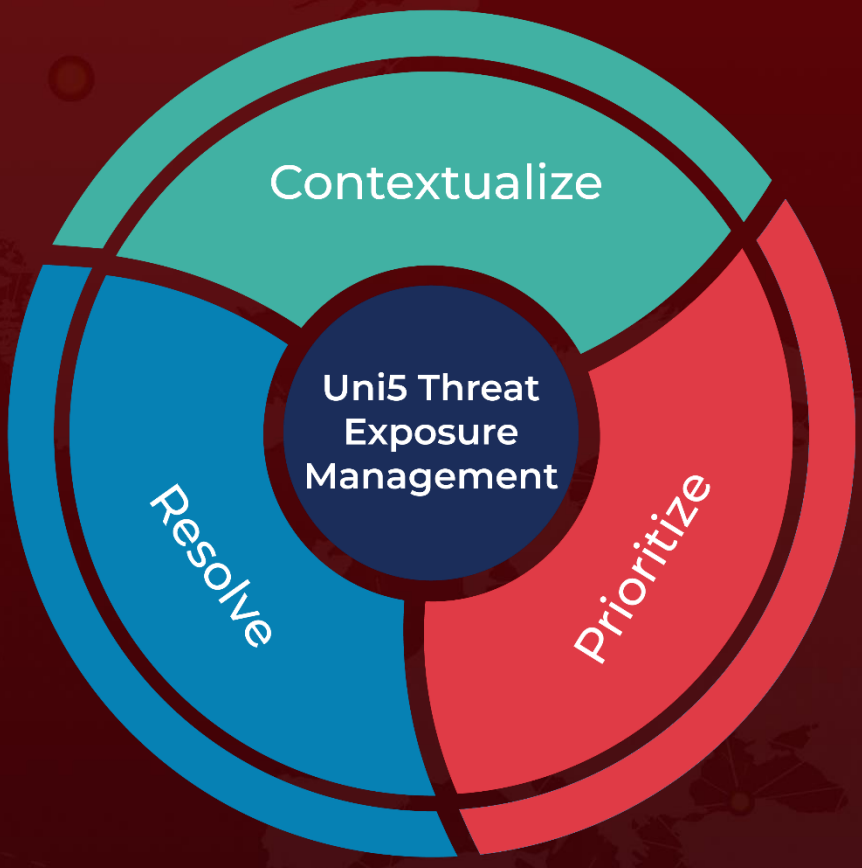
References

https://www.akamai.com/blog/security-research/fritzfrog-botnet-new-capabilities-log4shell

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

February 7, 2024 • 4:15 AM

More at www.hivepro.com