Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

New Linux Variant of Bifrost RAT Utilizes Deceptive Domain for Evasion

Date of Publication	Admiralty Code	TA Number
March 4, 2024	A1	TA2024084

Summary

Attack Began: February 2024
Targeted Countries: Worldwide
Malware: Bifrost (aka Bifrose)
Affected Platform: Linux
Attack: A new Linux variant of the Bifrost RAT evades detection using a deceptive VMware domain, aiming to compromise systems. This persistent threat spreads through malicious emails and sites, harvesting sensitive data and now includes an ARM version, emphasizing the need for vigilant countermeasures to safeguard against evolving malware.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1 A new Linux variant of the Bifrost remote access Trojan (RAT) has emerged, utilizing innovative techniques to avoid detection. First identified two decades ago, Bifrost persists as a significant RAT threat, spreading through malicious email attachments or payload-dropping sites and harvesting sensitive data from infected hosts.

#2 The latest version of Bifrost employs a deceptive domain, download.vmfare[.]com, resembling a legitimate VMware domain, in an attempt to trick users into downloading the malware, to bypass security measures and compromise targeted systems. This technique is known as typosquatting.

#3 Bifrost utilizes RC4 encryption to encrypt collected victim data, with slight modifications compared to previous versions. It communicates with a Taiwan-based public DNS resolver to resolve the deceptive domain, ensuring successful connection to its intended destination.

#4 Furthermore, the malware has expanded to include an Advanced RISC Machine (ARM) version hosted on the IP address 45.91.82[.]127, indicating an expansion in targeting to ARM-based architectures increasingly prevalent in various environments.

#5 Bifrost is linked to the BlackTech APT Group, a cyber actor group known for using custom malware payloads and remote access tools (RATs) to target victims' operating systems. Counteracting malware like Bifrost is critical to protecting sensitive data and maintaining the security of computer systems, underscoring the importance of continuous monitoring and mitigation efforts.

Recommendations

Update Security Measures: Ensure that all security measures, including antivirus software, firewalls, and intrusion detection systems, are up to date. Regularly update security patches and definitions to detect and block known threats, including variants of Bifrost.

Email Security Awareness: Educate employees about the risks associated with email attachments and links from unknown or suspicious sources. Encourage them to exercise caution when opening attachments or clicking on links, especially if they appear unexpected or unfamiliar.

Enhanced DNS Monitoring: Monitor DNS traffic for any attempts to resolve suspicious or deceptive domains associated with Bifrost. Implement DNS filtering and blocking to prevent connections to known malicious domains.

Web Filtering: Implement web filtering solutions to block access to malicious websites that may distribute Bifrost or other malware variants. Monitor web traffic for suspicious activity and block access to deceptive domains like download.vmfare[.]com.

Behavior-Based Detection: Employ behavior-based detection techniques to identify and block unusual or suspicious activity on endpoints and network devices. Monitor for signs of unauthorized access, data exfiltration, or abnormal system behavior that may indicate the presence of Bifrost or similar threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0011 Command and Control	TA0002 Execution
TA0042 Resource Development	TA0005 Defense Evasion	T1027 Obfuscated Files or Information	T1573.001 Symmetric Cryptography
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204.002 Malicious File	T1204.001 Malicious Link
T1204 User Execution	T1071 Application Layer Protocol	T1573 Encrypted Channel	T1071.004 DNS
T1583.001 Domains	T1583 Acquire Infrastructure	T1036 Masquerading	T1027.008 Stripped Payloads

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	download.vmfare[.]com
IPv4	45.91.82[.]127
SHA256	8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00250a4a2fe4729, 2aeb70f72e87a1957e3bc478e1982fe608429cad4580737abe58f6d78a626c05

References

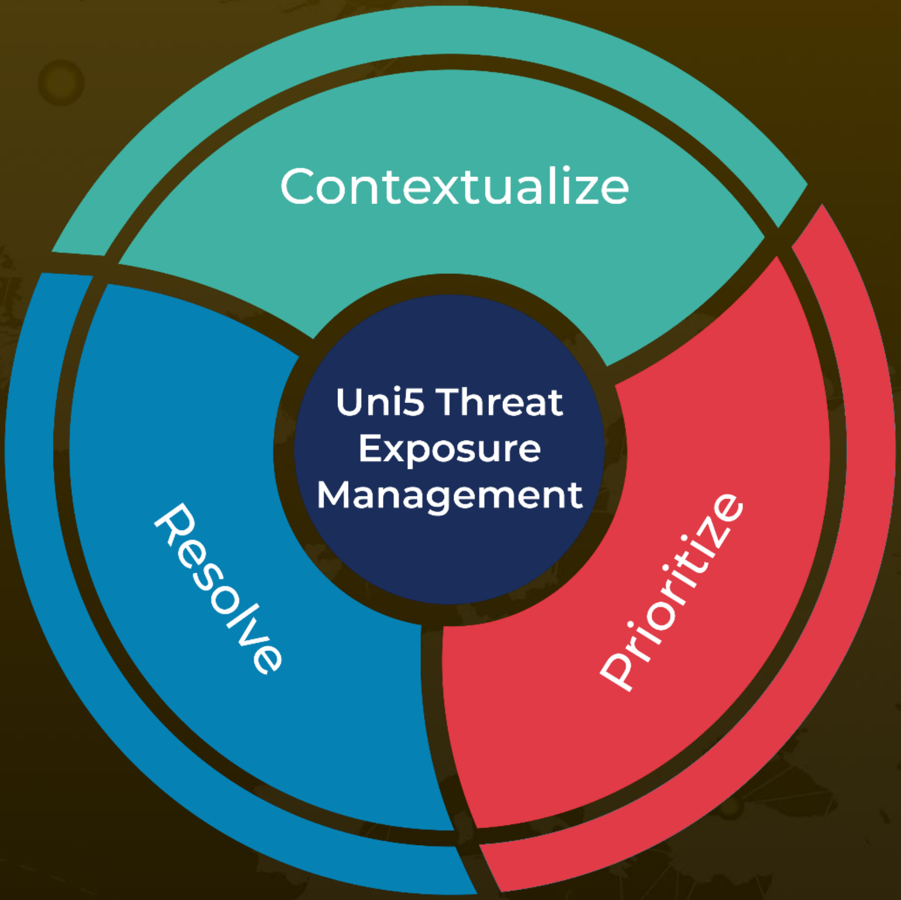
https://unit42.paloaltonetworks.com/new-linux-variant-bifrost-malware/

https://www.hivepro.com/threat-advisory/blacktech-china-linked-cyber-actors-exploit-router-firmware/

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 4, 2024 • 4:30 AM

More at www.hivepro.com