The Art of Domain Deception: Bifrost's New Tactic to Deceive Users

By Anmol Maurya, Siddharth Sharma

Published: 2024-02-29 · Archived: 2026-04-05 16:51:41 UTC

Executive Summary

We recently found a new Linux variant of Bifrost (aka Bifrose), showcasing an innovative technique to evade detection. It uses a deceptive domain, download.vmfare[.]com, which mimics the legitimate VMware domain. This latest version of Bifrost aims to bypass security measures and compromise targeted systems.

First identified in 2004, Bifrost is a remote access Trojan (RAT) that allows an attacker to gather sensitive information, like hostname and IP address. In this article, along with exploring Bifrost, we'll also showcase a notable spike in Bifrost's Linux variants during the past few months. This spike raises concerns among security experts and organizations.

Palo Alto Networks customers are better protected from the threats discussed in this article through our Next-Generation Firewall with Cloud-Delivered Security Services, including Advanced WildFire. Advanced URL Filtering and DNS Security. Cortex XDR can help detect and prevent Bifrost and related malicious behavior. If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Introduction

Attackers typically distribute Bifrost through email attachments or malicious websites. Once installed on a victim's computer, Bifrost allows the attacker to gather sensitive information, like the victim's hostname and IP address.

The latest version of Bifrost reaches out to a command and control (C2) domain with a deceptive name, download.vmfare[.]com, which appears similar to a legitimate VMware domain. This is a practice known as typosquatting. By leveraging this deceptive domain, the threat actors behind Bifrost aim to bypass security measures, evade detection, and ultimately compromise targeted systems.

As of late February, the deceptive domain has so far been undetected on VirusTotal as shown below in Figure 1.

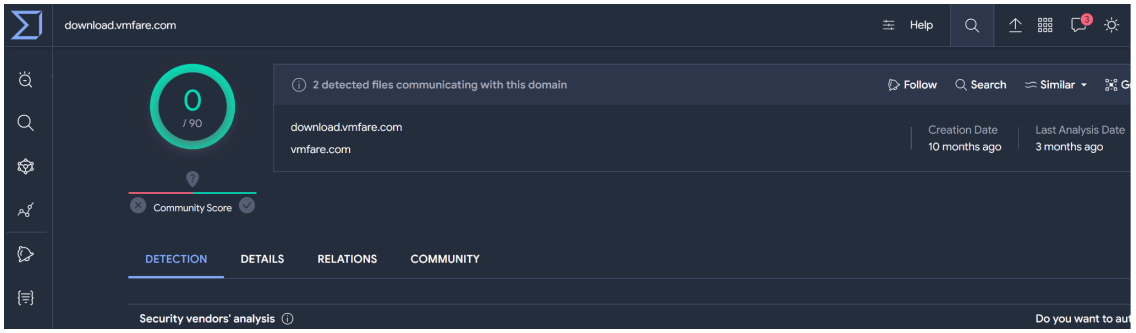

Figure 1. VirusTotal score for download.vmfare[.]com.

Malware Overview: Bifrost

We found the latest sample of Bifrost (SHA256 hash: 8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00250a4a2fe4729) hosted on a server at 45.91.82[.]127.

The sample binary is compiled for x86 and seems stripped. A stripped binary is one from which debugging information and symbol tables have been removed. Attackers usually use this technique to hinder analysis.

Figure 2 shows the sample's file type using the file command from a terminal window in a Linux environment.

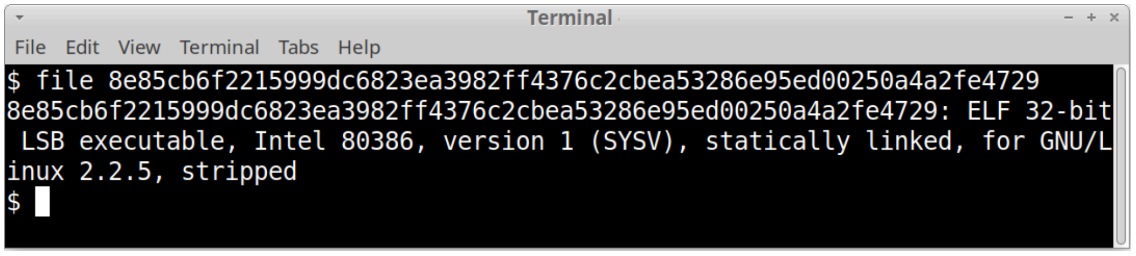

Figure 2. Stripped binary.

To better understand how this latest version of Bifrost functions, we viewed the recent sample in a disassembler. The malware first creates a socket via a setSocket function to establish communications, then it collects the user data and sends it to the attacker's server. The disassembled code illustrating this is shown below in Figure 3.

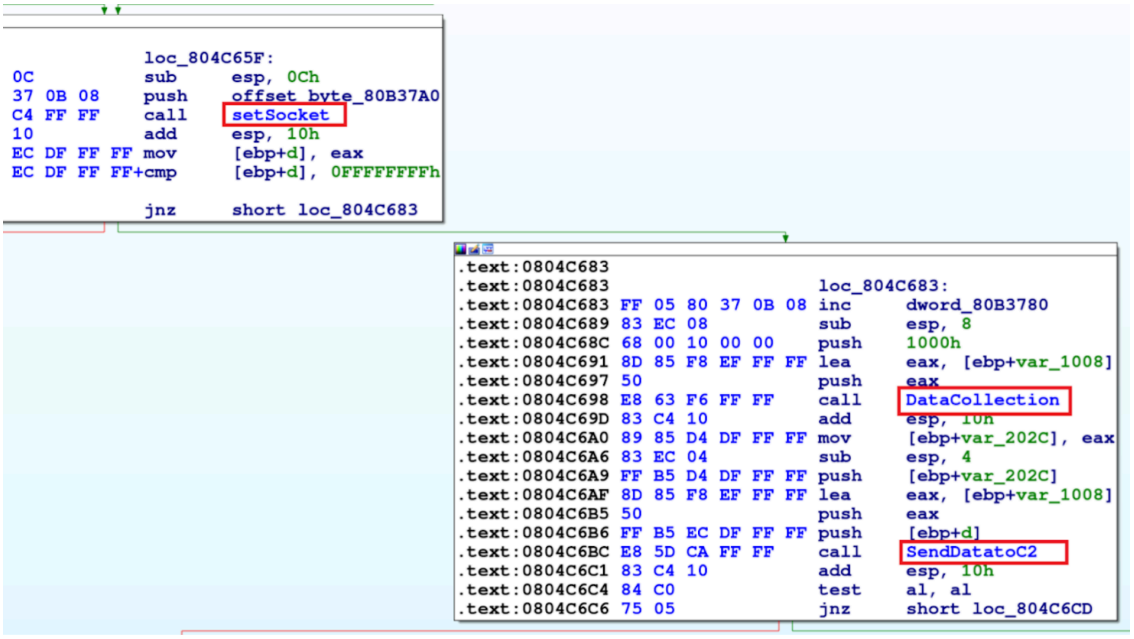

Figure 3. Code flow of the malware seen in a disassembler.

A snippet of code for the setSocket function is shown below in Figure 4, where the code pushes three values onto the stack and later calls sys_socket(0x8063A80):

- push 2: This corresponds to the socket domain, which is AF_INET (IPv4 Internet Protocols).
- push 1: This corresponds to the socket type, which is SOCK_STREAM (TCP).
- push 6: This corresponds to the socket protocol, which is IPPROTO_TCP (TCP).

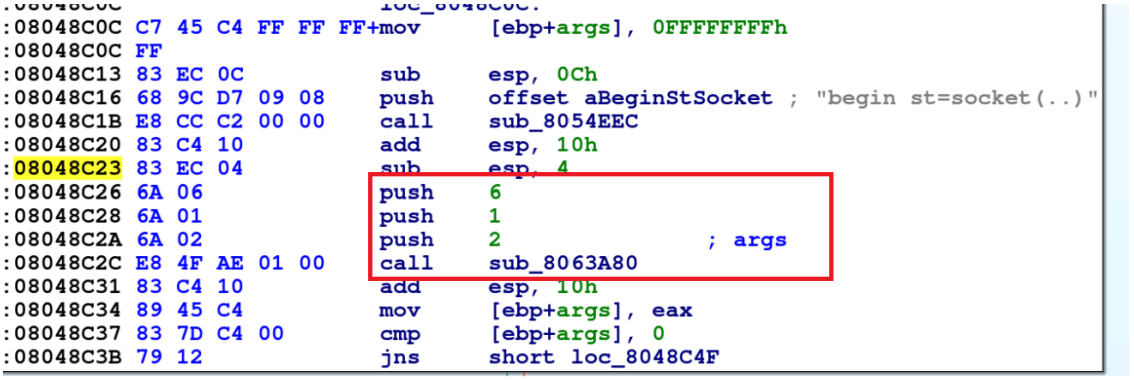

Figure 4. Disassembler view of code for socket creation in the Bifrost sample.

After socket creation, the malware collects user data as shown below in Figure 5, to send it over to the attacker's server.

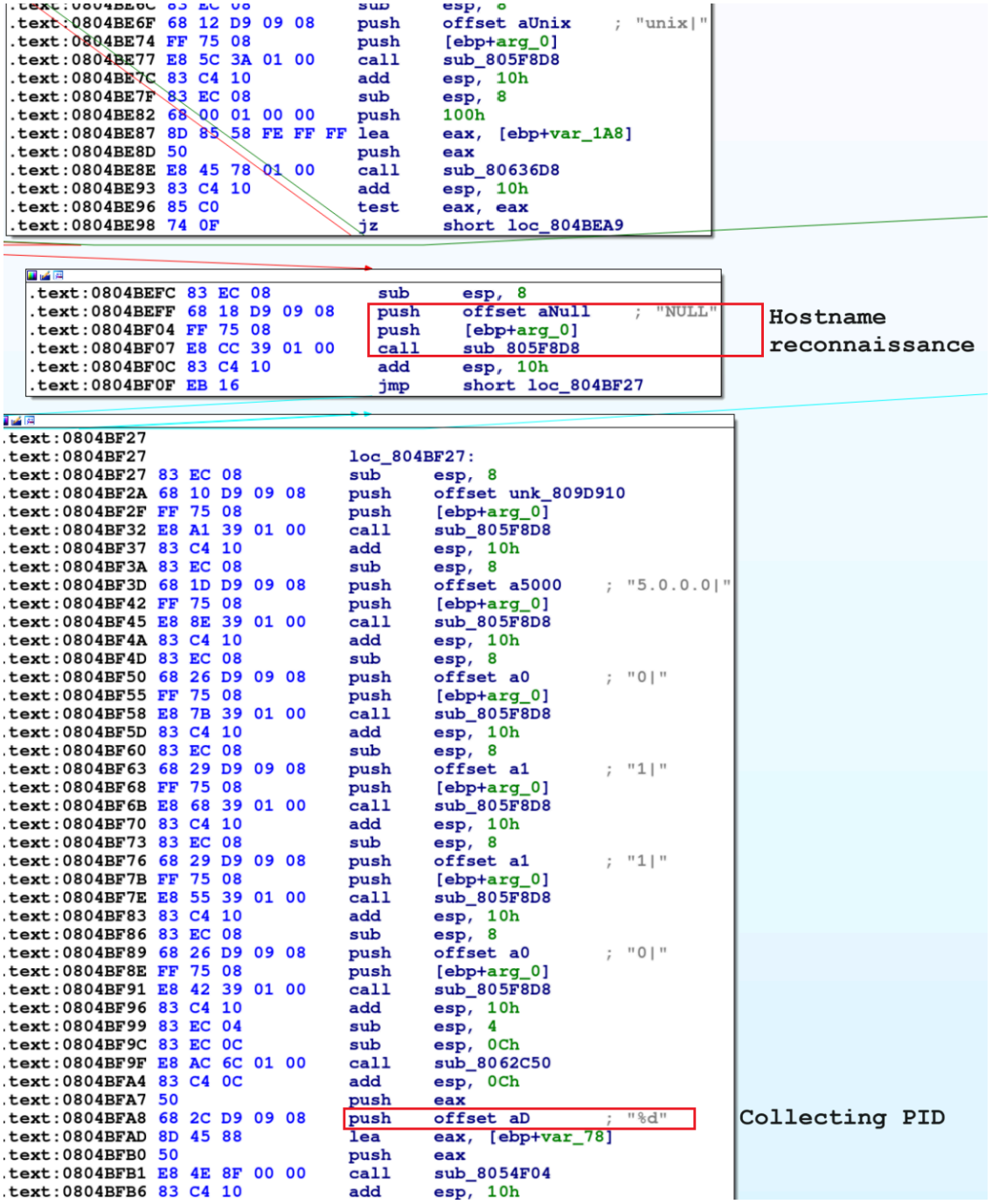

Figure 5. Disassembled code showing how Bifrost collects victim data.

This recent sample uses RC4 encryption to encrypt collected victim data as shown below in Figure 6. Compared to previous Bifrost samples, we find small changes, like bitwise AND operations in the encryption process, depending on the particular instance being studied.

```
.text:080483FD                and     eax, 0FFh
.text:08048402                mov     al, [eax+ebp-128h]
.text:08048409                mov     [ebp+var_1A], al
.text:0804840C                mov     al, [ebp+var_19]
.text:0804840F                mov     dl, [ebp+var_1A]
.text:08048412                add     edx, eax
.text:08048414                mov     al, 0FFh
.text:08048416                and     eax, edx
.text:08048418                mov     [ebp+var_1A], al
.text:0804841B                movzx   eax, [ebp+var_1A]
.text:0804841F                mov     al, [eax+ebp-128h]
.text:08048426                mov     [ebp+var_19], al
.text:08048429                mov     al, 80h
.text:0804842B                and     eax, [ebp+var_18]
.text:0804842E                test    al, al
.text:08048430                jnz     short loc_8048468
```

Figure 6. Disassembled code from the most recent Bifrost sample, indicating potentially modified RC4 encryption.

Subsequently, the malware tries to make contact with a Taiwan-based public DNS resolver with the IP address 168.95.1[.]1 shown below in Figure 7.

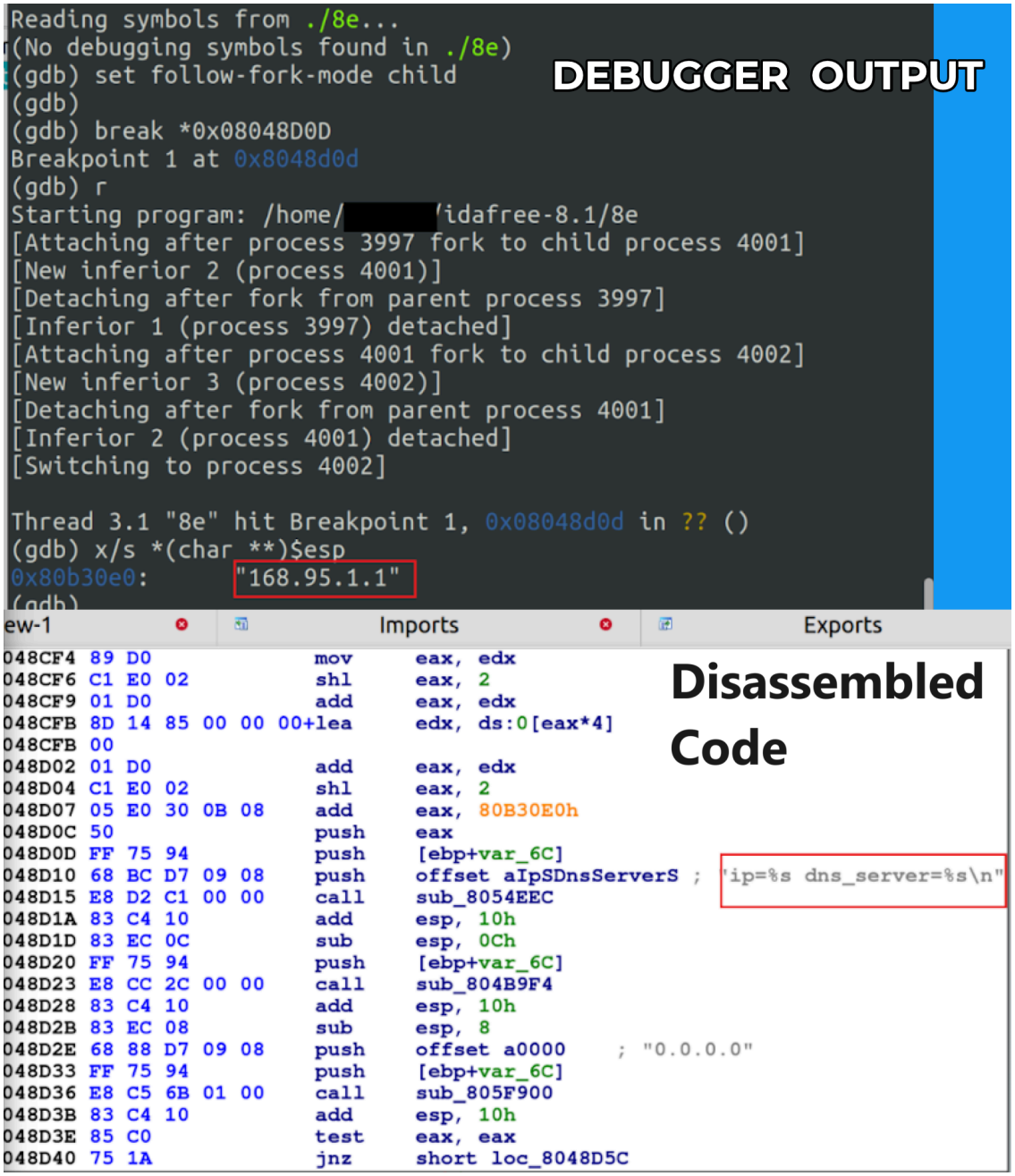

Figure 7. Debugger output and disassembled code revealing the malware contacting a public DNS resolver at 168.95.1[.]1.

As evidenced by the logs in Figure 8, the malware initiates a DNS query to resolve the domain download.vmfare[.]com by employing the public DNS resolver at 168.95[.]1.1. This step is crucial in ensuring that the malware can successfully connect to its intended destination.

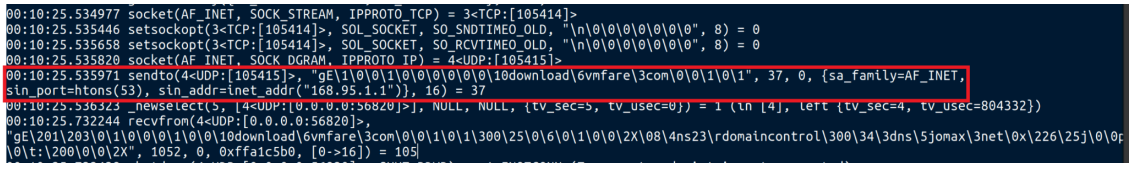

Figure 8. Malware initiating a DNS query to resolve the domain download.vmfare[.]com.

The malware often adopts such deceptive domain names as C2 instead of IP addresses to evade detection and make it more difficult for researchers to trace the source of the malicious activity.

Expanding Attack Surface

Upon checking, we found that the malicious IP address at 45.91.82[.]127 hosts an ARM version of Bifrost as well. The presence of this version indicates that the attacker is trying to expand their attack surface.

The ARM version functions the same as the x86 version we've analyzed in this article. By providing an ARM version of the malware, attackers can expand their grasp, compromising devices that may not be compatible with x86-based malware. As ARM-based devices become more common, cybercriminals will likely change their tactics to include ARM-based malware, making their attacks stronger and able to reach more targets.

Capturing Bifrost

Palo Alto Networks Advanced WildFire detected a recent spike in Bifrost activity. For the last few months, WildFire detected more than 100 instances (hashes) of Bifrost samples, as illustrated below in Figure 9.

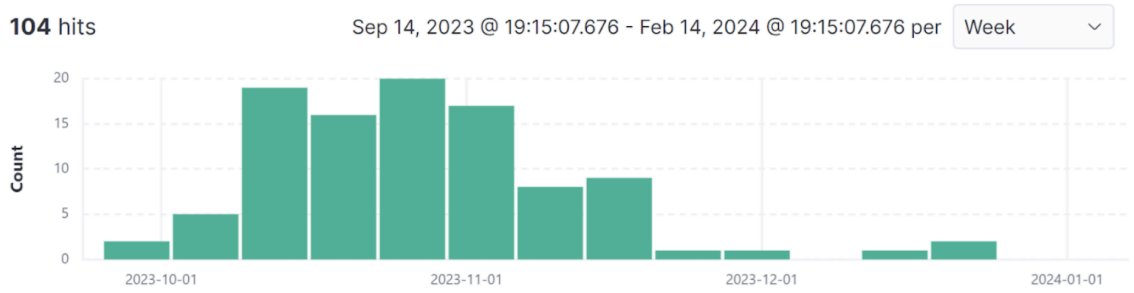

Figure 9. Advanced WildFire report of Bifrost sample detections from October through January 2024.

Conclusion

The Bifrost RAT remains a significant and evolving threat to individuals and organizations alike. With new variants that employ deceptive domain strategies like typosquatting, a recent spike in Bifrost activity highlights the dangerous nature of this malware.

Tracking and counteracting malware like Bifrost is crucial to safeguarding sensitive data and preserving the integrity of computer systems. This also helps minimize the likelihood of unauthorized access and subsequent harm.

Palo Alto Networks customers are better protected from the threats discussed in this article through our Next-Generation Firewall with Cloud-Delivered Security Services, including Advanced WildFire, Advanced URL Filtering and DNS Security. Cortex XDR can help detect and prevent Bifrost and related malicious behavior.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared our findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Acknowledgments

We would like to thank Bradley Duncan for his valuable input and suggestions that helped shape up this article.

Indicators of Compromise

Malware Samples

SHA256 Hash	Architecture
8e85cb6f2215999dc6823ea3982ff4376c2cbea53286e95ed00250a4a2fe4729	x86
2aeb70f72e87a1957e3bc478e1982fe608429cad4580737abe58f6d78a626c05	ARM

Domain and IP Addresses

- download.vmfare[.]com
- 45.91.82[.]127

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