

# 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.

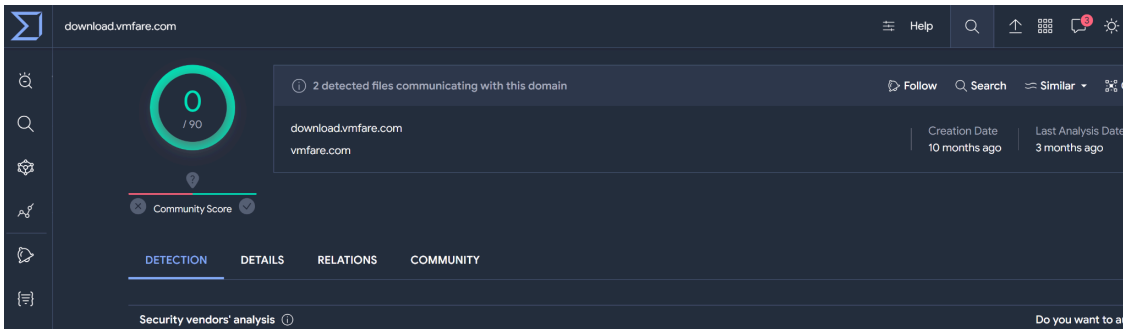


Figure 1. VirusTotal score for download.vmfare[.]com.

## 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.

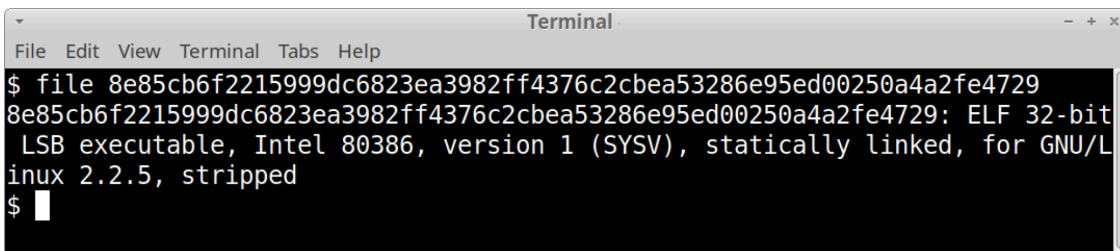


Figure 2. Stripped binary.

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.

```

loc_804C65F:
0C      sub     esp, 0Ch
37 0B 08  push  offset byte_80B37A0
C4 FF FF  call   setSocket
10      add     esp, 10h
EC DF FF FF  mov    [ebp+d], eax
EC DF FF FF+cmp [ebp+d], 0FFFFFFFh
                               jnz    short loc_804C683

.text:0804C683
.text:0804C683      loc_804C683:
.text:0804C683  FF 05 80 37 0B 08  inc    dword_80B3780
.text:0804C689  83 EC 08          sub    esp, 8
.text:0804C68C  68 00 10 00 00    push  1000h
.text:0804C691  8D 85 F8 EF FF FF  lea   eax, [ebp+var_1008]
.text:0804C697  50              push  eax
.text:0804C698  E8 63 F6 FF FF   call  DataCollection
.text:0804C69D  83 C4 10          add    esp, 10h
.text:0804C6A0  89 85 D4 DF FF FF  mov    [ebp+var_202C], eax
.text:0804C6A6  83 EC 04          sub    esp, 4
.text:0804C6A9  FF B5 D4 DF FF FF  push  [ebp+var_202C]
.text:0804C6AF  8D 85 F8 EF FF FF  lea   eax, [ebp+var_1008]
.text:0804C6B5  50              push  eax
.text:0804C6B6  FF B5 EC DF FF FF  push  [ebp+d]
.text:0804C6BC  E8 5D CA FF FF   call  SendDatatoC2
.text:0804C6C1  83 C4 10          add    esp, 10h
.text:0804C6C4  84 C0            test   al, al
.text:0804C6C6  75 05            jnz   short loc_804C6CD
    
```

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).

```

:08048C0C  C7 45 C4 FF FF FF+mov [ebp+args], 0FFFFFFFh
:08048C0C  FF
:08048C13  83 EC 0C          sub    esp, 0Ch
:08048C16  68 9C D7 09 08    push  offset aBeginStSocket ; "begin st=socket(..)"
:08048C1B  E8 CC C2 00 00    call  sub_8054EEC
:08048C20  83 C4 10          add    esp, 10h
:08048C23  83 EC 04          sub    esp, 4
:08048C26  6A 06            push  6
:08048C28  6A 01            push  1
:08048C2A  6A 02            push  2 ; args
:08048C2C  E8 4F AE 01 00    call  sub_8063A80
:08048C31  83 C4 10          add    esp, 10h
:08048C34  89 45 C4          mov    [ebp+args], eax
:08048C37  83 7D C4 00      cmp    [ebp+args], 0
:08048C3B  79 12            jns   short loc_8048C4F
    
```

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.

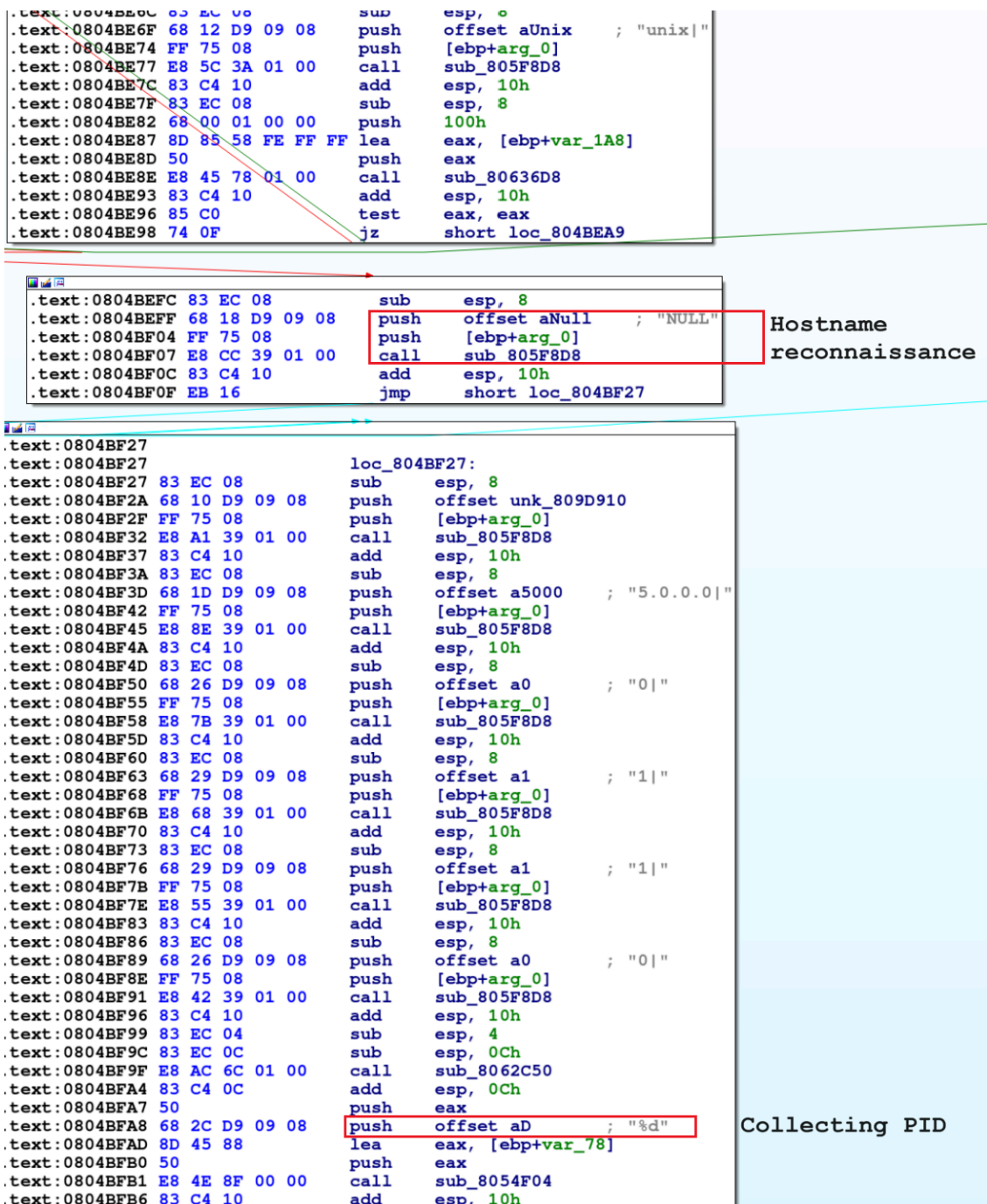


Figure 5. Disassembled code showing how Bifrost collects victim data.

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      inzb   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.

```

Reading symbols from ./8e...
(No debugging symbols found in ./8e)
(gdb) set follow-fork-mode child
(gdb)
(gdb) break *0x08048D0D
Breakpoint 1 at 0x8048d0d
(gdb) r
Starting program: /home/.../idafree-8.1/8e
[Attaching after process 3997 fork to child process 4001]
[New inferior 2 (process 4001)]
[Detaching after fork from parent process 3997]
[Inferior 1 (process 3997) detached]
[Attaching after process 4001 fork to child process 4002]
[New inferior 3 (process 4002)]
[Detaching after fork from parent process 4001]
[Inferior 2 (process 4001) detached]
[Switching to process 4002]

Thread 3.1 "8e" hit Breakpoint 1, 0x08048d0d in ?? ()
(gdb) x/s *(char **) $esp
0x80b30e0: "168.95.1.1"
(gdb)

```

## DEBUGGER OUTPUT

ew-1					Imports	Exports
048CF4	89	D0		mov	eax, edx	
048CF6	C1	E0	02	shl	eax, 2	
048CF9	01	D0		add	eax, edx	
048CFB	8D	14	85 00 00 00	lea	edx, ds:0[eax*4]	
048CFB	00					
048D02	01	D0		add	eax, edx	
048D04	C1	E0	02	shl	eax, 2	
048D07	05	E0	30 0B 08	add	eax, 80B30E0h	
048D0C	50			push	eax	
048D0D	FF	75	94	push	[ebp+var_6C]	
048D10	68	BC	D7 09 08	push	offset aIpSDnsServerS ; "ip=%s dns_server=%s\n"	
048D15	E8	D2	C1 00 00	call	sub_8054EEC	
048D1A	83	C4	10	add	esp, 10h	
048D1D	83	EC	0C	sub	esp, 0Ch	
048D20	FF	75	94	push	[ebp+var_6C]	
048D23	E8	CC	2C 00 00	call	sub_804B9F4	
048D28	83	C4	10	add	esp, 10h	
048D2B	83	EC	08	sub	esp, 8	
048D2E	68	88	D7 09 08	push	offset a0000 ; "0.0.0.0"	
048D33	FF	75	94	push	[ebp+var_6C]	
048D36	E8	C5	6B 01 00	call	sub_805F900	
048D3B	83	C4	10	add	esp, 10h	
048D3E	85	C0		test	eax, eax	
048D40	75	1A		jnz	short loc_8048D5C	

## Disassembled Code

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.

```

00:10:25.534977 socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) = 3<TCP:[105414]>
00:10:25.535446 setsockopt(3<TCP:[105414]>, SOL_SOCKET, SO_SNDTIMEO_OLD, "\n\0\0\0\0\0", 8) = 0
00:10:25.535658 setsockopt(3<TCP:[105414]>, SOL_SOCKET, SO_RCVTIMEO_OLD, "\n\0\0\0\0\0", 8) = 0
00:10:25.535820 socket(AF_INET, SOCK_DGRAM, IPPROTO_IP) = 4<UDP:[105415]>
00:10:25.535971 sendto(4<UDP:[105415]>, "gE\1\0\1\0\0\0\0\0\10download\6vmfare\3com\0\1\0\1", 37, 0, {sa_family=AF_INET, sin_port=htons(53), sin_addr=inet_addr("168.95.1.1")}, 16) = 37
00:10:25.536323 newselect(s, [4<UDP:[0.0.0.0:56820]>], NULL, NULL, {tv_sec=5, tv_usec=0}) = 1 (tn [4], left {tv_sec=4, tv_usec=804332})
00:10:25.732244 recvfrom(4<UDP:[0.0.0.0:56820]>, "gE\201\203\0\1\0\0\1\0\0\10download\6vmfare\3com\0\1\0\1\300\25\0\6\0\1\0\0\2X\08\4ns23\rdomaincontrol\300\34\3dns\5jomax\3net\0x\226\25j\0\0\0\t\200\0\0\2X", 1052, 0, 0xffa1c5b0, [0->16]) = 105

```

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.

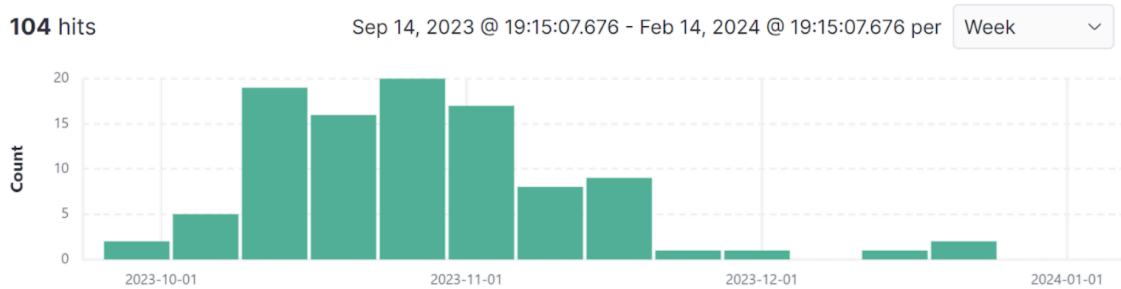


Figure 9. Advanced WildFire report of Bifrost sample detections from October through January 2024.

## 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/>