

中國駭客 HUAPI 的惡意後門程式 BiFrost 分析

By Global Support & Service

Published: 2020-04-15 · Archived: 2026-04-02 10:42:05 UTC

關鍵字：HUAPI、PLEAD、GhostCat、CVE-2020-1938、Linux、BiFrost、RC4、RAT

前言

TeamT5 近期接獲情資，於台灣某學術網路的圖書館網站上發現存有惡意程式。經過 TeamT5 研究員分析調查發現，該網站系統使用 Tomcat 7.0.73 作為網頁伺服器且開啟 8009 通訊埠，TeamT5 研究員驗證網站具有 Ghostcat (CVE-2020-1938) 漏洞，詳見下圖。

 圖一、Nmap 掃描結果

駭客利用 Tomcat 網頁伺服器預設開啟的 AJP 服務（預設為 8009 通訊埠），可達到遠端指令執行（Remote Code Execution, RCE）之目的並上傳檔案。於該案例中，駭客疑似透過 Ghostcat 漏洞上傳 BiFrost 惡意程式，使該圖書館系統成為惡意程式下載站（Download Site）。

惡意程式分析

該惡意程式 (8fd3925dadf37bebcc8844214f2bcd18) 於 2020 年 1 月 31 日被上傳至 Virustotal 平台，當時的各家防毒軟體的偵測率並不佳，僅有 6 家防毒軟體能夠有效識別，詳見下圖。

Engine	Signature	Version	Update
Ad-Aware	-	3.0.5.370	20200131
AegisLab	-	4.2	20200131
AhnLab-V3	-	3.17.0.26111	20200131
ALYac	-	1.1.1.5	20200131
Antiy-AVL	-	3.0.0.1	20200131
Arcabit	-	1.0.0.869	20200131
Avast	-	18.4.3895.0	20200131
Avast-Mobile	-	200130-00	20200130
AVG	-	18.4.3895.0	20200131
Avira	-	8.3.3.8	20200131
Baidu	-	1.0.0.2	20190318
BitDefender	-	7.2	20200131
BitDefenderTheta	-	7.2.37796.0	20200120
Bkav	-	1.3.0.9899	20200122
CAT-QuickHeal	-	14.00	20200131
ClamAV	-	0.102.1.0	20200130
CMC	-	1.1.0.977	20190321
Comodo	-	32027	20200131
Cyren	-	6.2.2.2	20200131

圖二、惡意程式於一月底上傳至 VirusTotal 且一開始防毒軟體的偵測率並不佳

TeamT5 取得該惡意後門程式並進行分析，該惡意後門程式檔名為 md.png，但檔案格式為 UNIX ELF 執行檔，推測是利用 PNG 副檔名偽裝在 Tomcat 網站伺服器上，詳見下圖。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	7F	45	4C	46	01	01	01	00	00	00	00	00	00	00	00	00	ELF
00000010	02	00	03	00	01	00	00	00	10	81	04	08	34	00	00	00	4
00000020	AC	BE	08	00	00	00	00	00	34	00	20	00	05	00	28	00	4 (
00000030	1A	00	19	00	01	00	00	00	00	00	00	00	00	80	04	08	€
00000040	00	80	04	08	E0	AB	08	00	E0	AB	08	00	05	00	00	00	€ à« à«
00000050	00	10	00	00	01	00	00	00	00	B0	08	00	00	30	0D	08	° 0
00000060	00	30	0D	08	E4	0A	00	00	A4	4E	00	00	06	00	00	00	0 ä ðN
00000070	00	10	00	00	04	00	00	00	D4	00	00	00	D4	80	04	08	Ô Ô€
00000080	D4	80	04	08	20	00	00	00	20	00	00	00	04	00	00	00	Ô€
00000090	04	00	00	00	07	00	00	00	00	B0	08	00	00	30	0D	08	° 0
000000A0	00	30	0D	08	14	00	00	00	44	00	00	00	04	00	00	00	0 D
000000B0	04	00	00	00	51	E5	74	64	00	00	00	00	00	00	00	00	Qãtd
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	06	00	00	00	
000000D0	04	00	00	00	04	00	00	00	10	00	00	00	01	00	00	00	
000000E0	47	4E	55	00	00	00	00	00	02	00	00	00	06	00	00	00	GNU

圖三、偽裝為 PNG 的 ELF 執行檔

使用 TeamT5 的 ThreatSonar 惡意威脅鑑識系統可有效辨識出該惡意程式並可以偵測到中繼站 IP 位址 (107.191.61.247)，詳見下圖。

The screenshot displays the ThreatSonar interface for a system scan. At the top, it shows the computer name 'Ubuntu' with a search icon and a threat level of '威脅等級 5'. The scan started on '2020/03/30 16:09:27 CST'. System details include '系統: Ubuntu 16.04.6 LTS (i686)', '使用者名稱: root', 'IP: 192.168.152.129', and 'Connect ip: 192.168.152.129'. Below this, there are tabs for '威脅', '連線狀態', '時間軸', '事件紀錄', and '資訊'. The main content area shows a file path '/tmp/md.png' and a list of threat indicators: 'APT_L..._00', 'Apt Malware', 'Suspicious Elf Ext', 'Exec In Suspicious Dir', 'Unique File Owner', 'Exec Cmd', 'Dpkg Md5 Not Found', 'Enum Process', 'Exec Perm', 'Network Ability', 'Tty Not Exist', 'Cmdline Exist', 'ELF32', 'Hardlink Not Exist', 'Softlink Not Exist', 'Underscore Env Exist', and 'X11 Display'. A 'Memory Block Inspector' is also visible. The SHA256 hash is '3CAD20318F36B020CF4D6B44320EB5A6DAE0A78339A0FDC3A1FE5E280A8507F1' and the C&C address is '107.191.61.247'.

圖四、ThreatSonar 偵測畫面

經過逆向分析，該惡意後門程式具有上傳/下載/列舉/刪除/搬移檔案 (File)、執行/結束程序 (Process)、開啟/關閉遠端命令列介面程式 (Remote Shell) 等功能，其中惡意後門程式與中繼站的連線內容會使用修改過的 RC4 演算法進行加密，此專屬特徵可用來辯認出此惡意程式，詳見下圖。

```
13 for ( i = 0; i <= 255; ++i )
14     v7[i] = i;
15 for ( i = 0; i <= 255; i += a4 )
16 {
17     for ( j = 0; j < a4 && i + j <= 255; ++j )
18         v6[j + i] = *(_BYTE *)(a3 + j);
19 }
20 j = 0;
21 for ( i = 0; i <= 255; ++i )
22 {
23     v13 = v7[i];
24     v12 = v6[i];
25     j = (unsigned __int8)(j + v13 + v12);
26     v12 = v7[j];
27     v7[i] = v12;
28     v7[j] = v13;
29 }
30 v10 = a5;
31 j = 0;
32 for ( i = 0; ; ++i )
33 {
34     result = i;
35     if ( i >= a2 )
36         break;
37     v11 = v7[(unsigned __int8)(i + 1)];
38     j = (unsigned __int8)(j + v11);
39     v7[(unsigned __int8)(i + 1)] = v7[j];
40     v7[j] = v11;
41     v12 = v7[(unsigned __int8)(i + 1)];
42     v12 += v11;
43     v11 = v7[v12];
44     if ( v10 & 0x80 )
45     {
46         v11 ^= *(_BYTE *)(a1 + i);
47         *(_BYTE *)(a1 + i) = v11 + v10;
48     }
```

圖五、惡意後門程式使用

修改後的 RC4 加密演算法

攻擊族群分析

該惡意程式為 Linux 版本的 BiFrost 後門程式，其版本號為 5.0.0.0。根據 TeamT5 長期研究的情資顯示，該惡意程式為中國駭客組織 HUAPI（又名為 PLEAD）慣用的後門程式。HUAPI 駭客組織自 2007 年開始活躍至今，攻擊台灣超過 10 年的時間。TeamT5 觀察到 HUAPI 所開發的惡意程式有時會使用加殼來阻擋研究人員分析，且通常會使用修改後的 RC4 演算法來加密傳輸。HUAPI 長期攻擊政府、高科技、電信或研究智庫單位，根據 TeamT5 的統計結果，超過 5 成的受害單位為政府機關，受害國家包含台灣、美國、日本及南韓，其中針對台灣政府機關進行入侵攻擊的為多。

影響與建議

若用戶有使用 Tomcat 服務作為網頁伺服器，且版本為以下之一者：

- Apache Tomcat 9.x < 9.0.31
- Apache Tomcat 8.x < 8.5.51
- Apache Tomcat 7.x < 7.0.100
- Apache Tomcat 6.x

TeamT5 建議需要立即進行版本更新，避免遭到駭客利用 Ghostcat 漏洞進行遠端控制，甚至上傳惡意檔案。

另外，若用戶若遭遇針對性進階持續威脅（Advanced Persistent Threat, APT）時，則需要使用如 TeamT5 的 ThreatSonar 惡意威脅鑑識系統，IT 管理者可以在最短時間內偵測並回應這類的惡意威脅。TeamT5 建議可將下方威脅指標（Indicator of Compromise, IOC）匯入到各式資安設備中偵測與識別威脅。

- 107.191.61.247
- 8fd3925dadf37bebcc8844214f2bcd18
- Yara Rule

```
rule RAT_BiFrost_UNIX
{
  meta:
    description= "HUAPI UNIX BiFrost RAT"
    author = "TeamT5"
    date = "2020-04-15"

  strings:
    $hex1 = {25 ?? 00 00 00 85 C0 75 37 8B 45 F0 89 C1 03 4D 08 8B 45 F0 03 45 08 0F B6 10 8B 45 F8 01 C
    $hex2 = {8B 45 F0 03 45 08 0F B6 00 30 45 FD 8B 45 F0 89 C1 03 4D 08 8B 45 F8 89 C2 02 55 FD B8 FF F

  condition:
    all of them
}
```

外部參考資料

- 1.