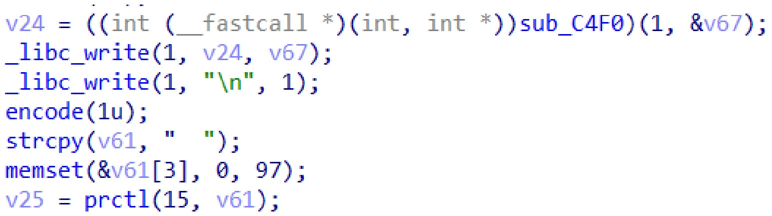
关于 变种 僵尸网络大规模传播的风险提示

一、 概述

二、 僵尸网络分析

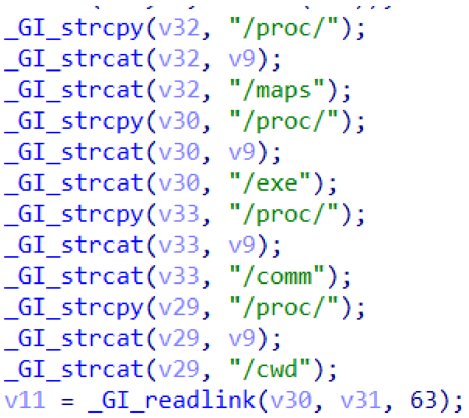
4	4
XI4	HF E H DFKL FIID MHG J M M 4
4	Y 4GFA 4 V4 4U 4
WF4	FBIJBIJBEJF4



```
v24 = ((int (__fastcall *)(int, int *))sub_C4F0)(1, &v67);
_libc_write(1, v24, v67);
_libc_write(1, "\n", 1);
encode(1u);
strcpy(v61, "  ");
memset(&v61[3], 0, 97);
v25 = prctl(15, v61);
```

4

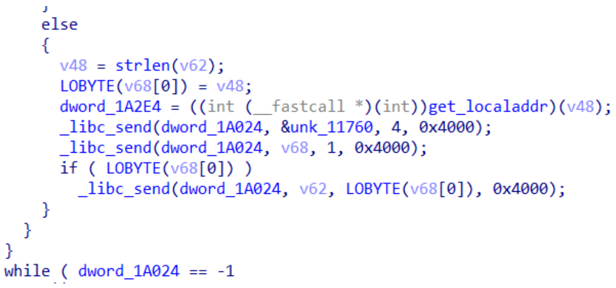
4



```
_GI_strcpy(v32, "/proc/");
_GI_strcat(v32, v9);
_GI_strcat(v32, "/maps");
_GI_strcpy(v30, "/proc/");
_GI_strcat(v30, v9);
_GI_strcat(v30, "/exe");
_GI_strcpy(v33, "/proc/");
_GI_strcat(v33, v9);
_GI_strcat(v33, "/comm");
_GI_strcpy(v29, "/proc/");
_GI_strcat(v29, v9);
_GI_strcat(v29, "/cwd");
v11 = _GI_readlink(v30, v31, 63);
```

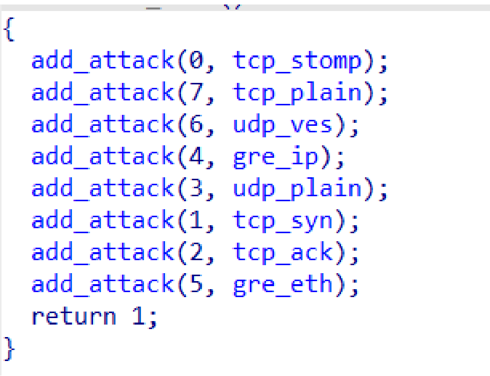
4

4



```
    else
    {
      v48 = strlen(v62);
      LOBYTE(v68[0]) = v48;
      dword_1A2E4 = ((int (__fastcall *)(int))get_localaddr)(v48);
      _libc_send(dword_1A024, &unk_11760, 4, 0x4000);
      _libc_send(dword_1A024, v68, 1, 0x4000);
      if ( LOBYTE(v68[0]) )
        _libc_send(dword_1A024, v62, LOBYTE(v68[0]), 0x4000);
    }
  }
}
while ( dword_1A024 == -1
```

4



```
{
  add_attack(0, tcp_stomp);
  add_attack(7, tcp_plain);
  add_attack(6, udp_ves);
  add_attack(4, gre_ip);
  add_attack(3, udp_plain);
  add_attack(1, tcp_syn);
  add_attack(2, tcp_ack);
  add_attack(5, gre_eth);
  return 1;
}
```

4

E 4	4	4
4	FG FGFG4	D JF4
4	FG FGFG4	4
	FF FFFF4	
	W YAFDEKAMEDD4	
	W YAFDEKAEKFEI4	
	W YAFDEMAEEGMM4	
WF4	EHFBMGBFFMBEMM4	
4	EHFBMGBFFMBEMM4 GKBDBEEBEJL4	
4	FDFF H J I EK 4	

44

F 4	4	4
4	FG FGFG4	4
	FF FFFF4	4

4	FG FGFG4	
	W YAFDEKAMEDD4	
	W YAFDFFAFMIME4	
	XA 4X ALFG 4 EBDF4VDI 4	
	W YAFDEMAEEGMM4	
	4 4 Y 4U 4	
	U 4X 4V 4IIII4	
WF4	FBIJBIJBEJF4 EHFBMGBFFMBEMM4 HJBEMBEGKBID4 EMIBILBGLBFIG4 GEBKBILBEJF4	
4	FBIJBIJBEJF4 ELIBFLBGMBEEM4 HJBEMBEGKBID4 EMIBILBGLBFIG4 EMHBGEBMLBFDI4 GEBKBILBEJF4	
4	FDFF H EG 4	

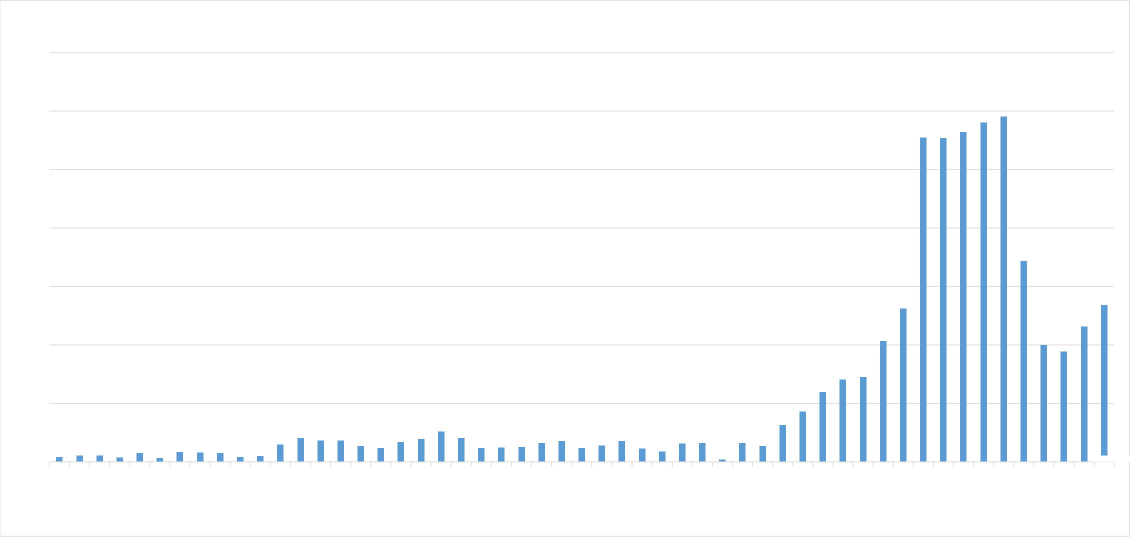
44

G 4	4	4
4	FG FGFG4	D G4
4	FF FFFF4	4
	W YAFDFFAFFMJI4	
	FG FGFG4	
	W 4IGHEG 4	
	W YAFDFFAFMIME4	
	W YAFDEKAMEDD4	
	W YAFDEKAEKFEI4	
	W YAFDFFAFMHJH4	
	XA 4X ALFG 4 EBDF4VDI 4	
	W YAFDFEAGIGMI4	
	4 4 Y 4U 4	
WF4	EKMBHGBEIJBFEH4	
4	EKMBHGBEIJBFEH4	
4	FDFF H FL 4	

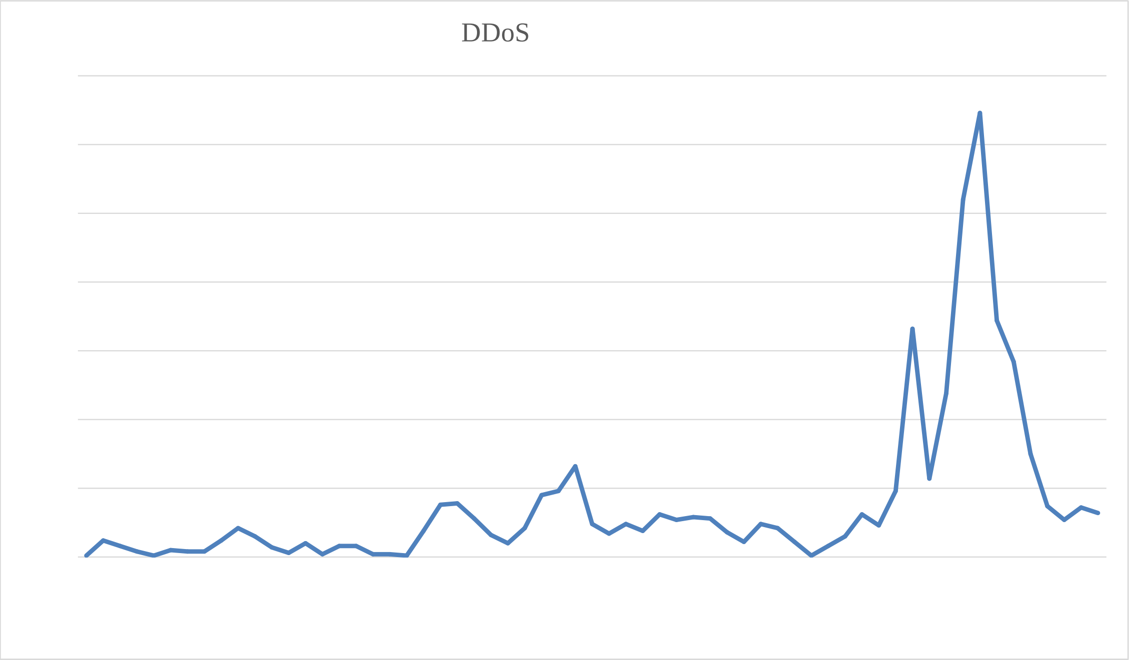
4	4
W YAFDEKAMEDD4	4GBDH4 4XA 4X AJDD 4 4
W YAFDEKAEKFEI4	IGF GKFEI 4
W YAFDEMAEEGMM4	Y X 4 Y AJIEV 4FBDHVE Y AJIFV 4GBDH DE4 4 Y AJIFV 4EBDD EF4 4
W YAFDFEAGIGMI4	4 4 X 4 FB 4 4 GBHBEHV 4
W YAFDFFAFMIME4	4 M4 4FFBDGBDFBED 4
W YAFDFFAFFMJI4	4 X 4M 4 4 4 W4 4 4 ▾— 4 4
W YAFDFFAFMHJH4	4 4 4 F4 4 W Y 4
XA 4X ALFG 4 EBDF4VDI 4	4C U E 4
4 4 Y 4U 4	4
W 4IGHEG 4	C IGHEG X 44
U 4X 4V 4IIII4	IIII 4

E		F		G	
					MM
					IFE
		U	U	KKEDE	
					TFG
L	L				L
L	L		EFGHIJ		J
					F
			EFGH		
			EFGH		
				U	U
		L	L		
	EDDE	L	L		EFGHIJ
					EFGH
					EFGH
	TFGHMILIM				
	EFG				
	LELF			L	L
			EDDE	L	L
			TFGHMILIM		
			EFG		
			LELF		
					EDDE
					TFGHMILIM
					EFG
					LELF

三、 僵尸网络感染规模



四、 僵尸网络攻击动态



五、 防范建议

六、 相关