

Computer Science 491/691

Malware Analysis

Homework 5

Assigned: April 10, 2019

Due: April 17, 2019

Submitted by: Sai Sasaank Srivatsa Pallerla

ID: HG13015

How to turn this in for grading: You can edit your answers right into this file. Email it to the TAs as described in class. Make sure your name appears in the body of the document.

Hint: Chapters 9, 11, and 15 of your Practical Malware Analysis textbook are useful references! In addition, the "Malware Behavior and the Windows API" PowerPoint will be helpful.

Download hw5.7z and extract it. The password is "infected". Answer the following questions:

1) What is unusual about the assembly code from 0x4019AA to 0x4019C1? Why might the malware be doing this? (10 pts)

4019AA is the start function: The programs execution starts here. We can see that the malware is adding data to the stack pointer and pushing some data into the edx register, then immediately popping the stack and register. At the end of the function we can see two jump statements JZ and JNZ which jump to the same address, i.e., 40198C. By looking at these jump statements, we can say the malware wants to execute the code/call the function at 40198C.

Later at 40198C we can see the function 401520 is enclosed between two null-functions. Few more things to notice is that all of the assembly instruction are in .CODE segment and the main (start) is in the end. The malware might be doing this throw off the antivirus or distract the analyst.

- 2) What is the value of lpServiceName when the malware calls OpenServiceA at 0x4016C1? (5 pts)

Value of lpServiceName at 4016C1 (call OpenserviceA) is BITS

The screenshot shows the Immunity Debugger interface. The CPU window displays assembly instructions, and the Register window shows the value of EAX as 'BITS'. The instruction at 0x4016C1 is 'CALL 0x4016C1', which corresponds to the OpenServiceA function. The value of EAX is 'BITS', which is the lpServiceName parameter.

- 3) What is the value of the first argument to the call to CreateFileA at 0x4012AA? What is the desired access mode? (Expecting the name of the access mode, not an integer) (5 pts)

The value of the first argument at 4012AA (call CreateFileA): d3dxd1a.dll

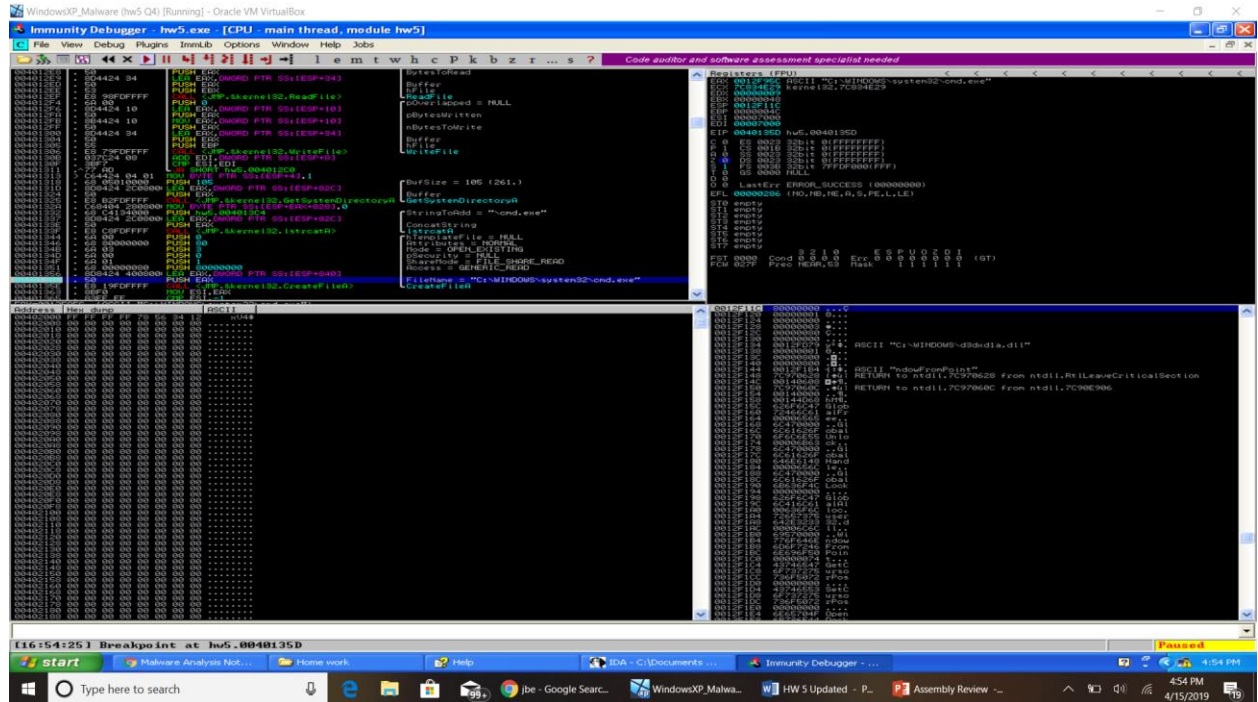
The desired access mode is GENERIC_READ:GENERIC_WRITE

The screenshot shows the Immunity Debugger interface. The CPU window displays assembly instructions, and the Register window shows the values of EAX and ECX. The instruction at 0x4012AA is 'CALL 0x4012AA', which corresponds to the CreateFileA function. The value of EAX is 'd3dxd1a.dll', which is the lpFileName parameter. The value of ECX is 'GENERIC_READ:GENERIC_WRITE', which is the dwDesiredAccess parameter.

4) What is the value of the first argument to the call to CreateFileA at 0x40135E? What is the desired access mode? (Expecting the name of the access mode, not an integer) (5 pts)

The value of the first argument at 40135E (call CreateFileA): cmd.exe

The desired access mode is GENERIC_READ



5) What is happening from 0x40136A to 0x401395? (12 pts)

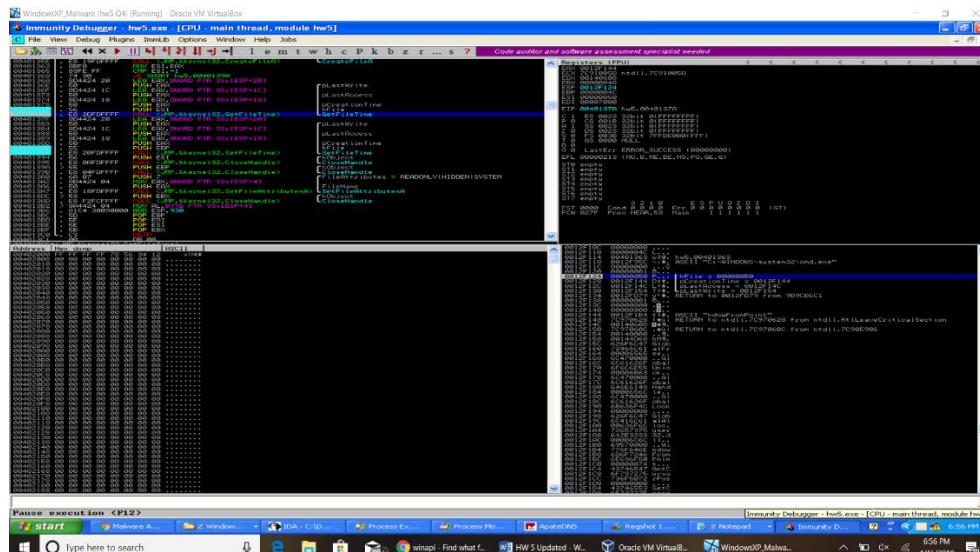
At 40137A the malware calls GetFileTime for which the parameters are

LastWrite: 0012F154

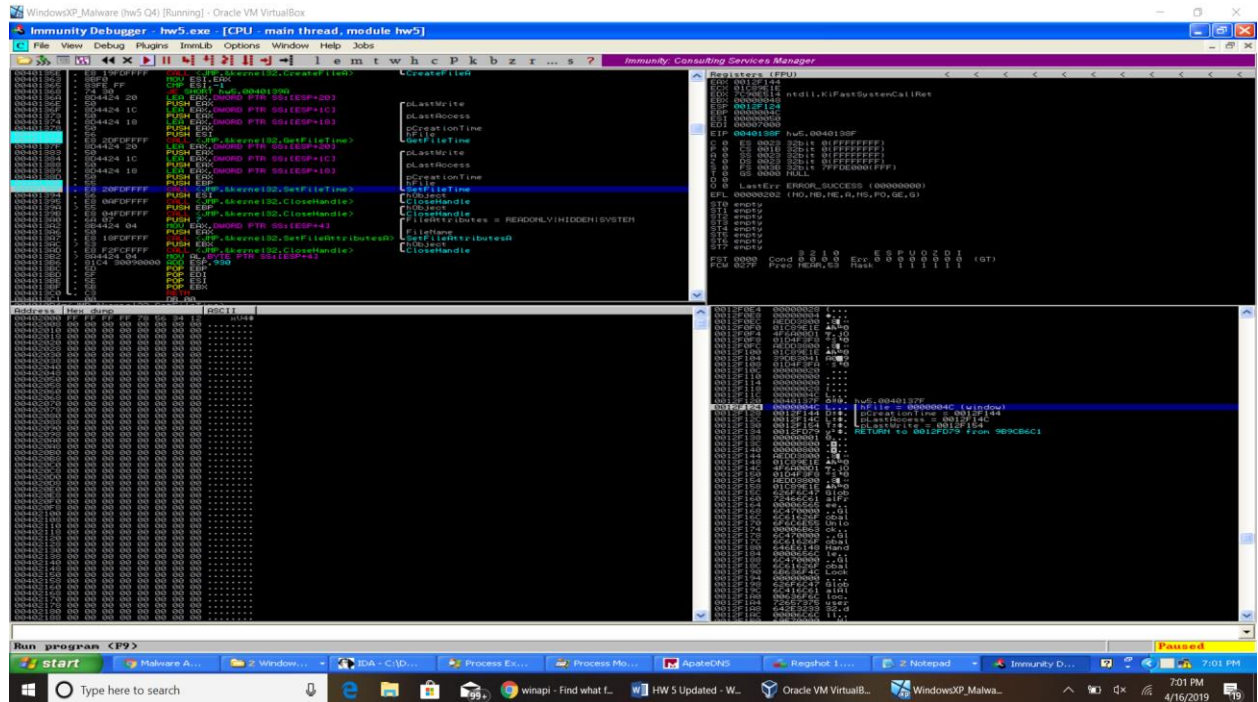
LastAccess: 0012F14C

CreationTime: 0012F144

hfile: 50



At 40138F the malware calls SetFileTime for which the parameters are
LastWrite: 0012F154
LastAccess: 0012F14C
CreationTime: 0012F144
hfile: 4C



WindowsXP_Malware (hw5 04) [Running] - Oracle VM VirtualBox

Immunity Debugger hw5.exe [CPU: main thread, module hw5]

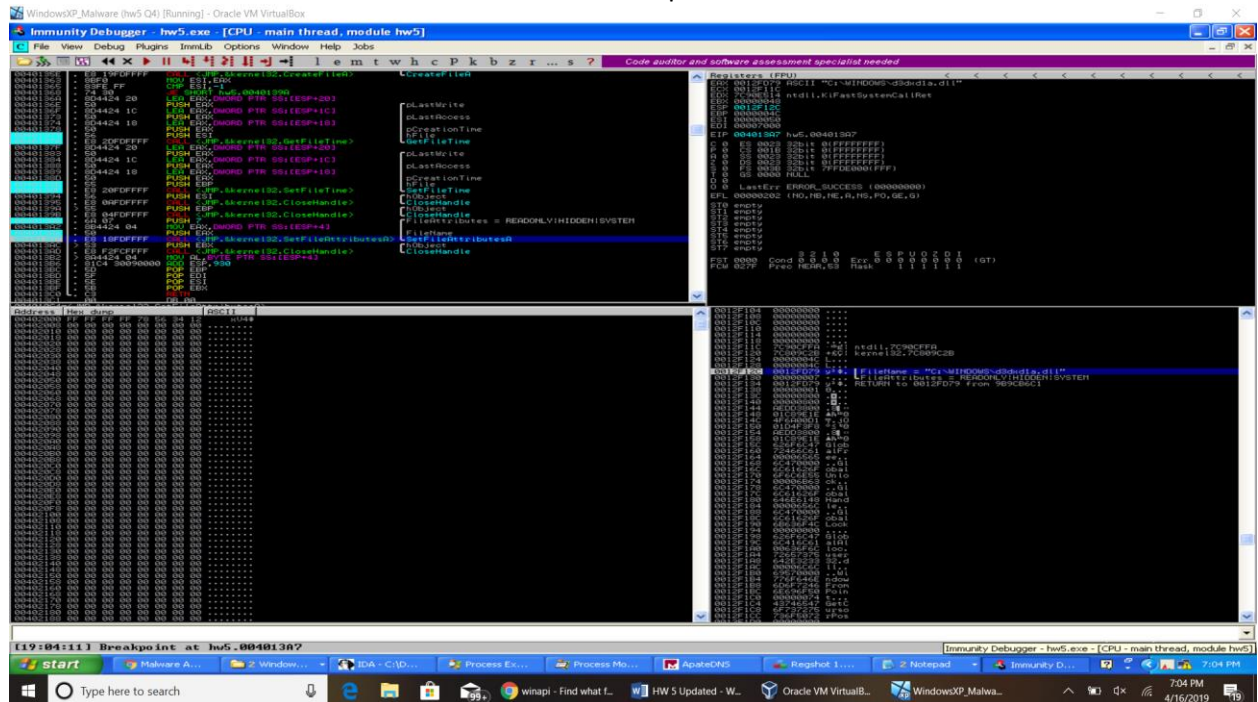
Disassembly:

```
0040138F 55 push ebp
00401390 8B EC mov ecx, esi
00401391 5D pop ebp
00401392 5E pop esi
00401393 5F pop edi
00401394 5G pop esi
00401395 5H pop ebx
00401396 5I pop edx
00401397 5J pop ecx
00401398 5K pop eax
00401399 5L pop edi
0040139A 5M pop esi
0040139B 5N pop ebx
0040139C 5O pop edx
0040139D 5P pop ecx
0040139E 5Q pop eax
0040139F 5R pop edi
004013A0 5S pop esi
004013A1 5T pop ebx
004013A2 5U pop edx
004013A3 5V pop ecx
004013A4 5W pop eax
004013A5 5X pop edi
004013A6 5Y pop esi
004013A7 5Z pop ebx
004013A8 5AA pop edx
004013A9 5AB pop ecx
004013AA 5AC pop eax
004013AB 5AD pop edi
004013AC 5AE pop esi
004013AD 5AF pop ebx
004013AE 5B0 pop edx
004013AF 5B1 pop ecx
004013B0 5B2 pop eax
004013B1 5B3 pop edi
004013B2 5B4 pop esi
004013B3 5B5 pop ebx
004013B4 5B6 pop edx
004013B5 5B7 pop ecx
004013B6 5B8 pop eax
004013B7 5B9 pop edi
004013B8 5BA pop esi
004013B9 5BB pop ebx
004013BA 5BC pop edx
004013BB 5BD pop ecx
004013BC 5BE pop eax
004013BD 5BF pop edi
004013BE 5C0 pop esi
004013BF 5C1 pop ebx
004013C0 5C2 pop edx
004013C1 5C3 pop ecx
004013C2 5C4 pop eax
004013C3 5C5 pop edi
004013C4 5C6 pop esi
004013C5 5C7 pop ebx
004013C6 5C8 pop edx
004013C7 5C9 pop ecx
004013C8 5CA pop eax
004013C9 5CB pop edi
004013CA 5CC pop esi
004013CB 5CD pop ebx
004013CC 5CE pop edx
004013CD 5CF pop ecx
004013CE 5D0 pop eax
004013CF 5D1 pop edi
004013D0 5D2 pop esi
004013D1 5D3 pop ebx
004013D2 5D4 pop edx
004013D3 5D5 pop ecx
004013D4 5D6 pop eax
004013D5 5D7 pop edi
004013D6 5D8 pop esi
004013D7 5D9 pop ebx
004013D8 5DA pop edx
004013D9 5DB pop ecx
004013DA 5DC pop eax
004013DB 5DD pop edi
004013DC 5DE pop esi
004013DD 5DF pop ebx
004013DE 5E0 pop edx
004013DF 5E1 pop ecx
004013E0 5E2 pop eax
004013E1 5E3 pop edi
004013E2 5E4 pop esi
004013E3 5E5 pop ebx
004013E4 5E6 pop edx
004013E5 5E7 pop ecx
004013E6 5E8 pop eax
004013E7 5E9 pop edi
004013E8 5EA pop esi
004013E9 5EB pop ebx
004013EA 5EC pop edx
004013EB 5ED pop ecx
004013EC 5EE pop eax
004013ED 5EF pop edi
004013EE 5F0 pop esi
004013EF 5F1 pop ebx
004013F0 5F2 pop edx
004013F1 5F3 pop ecx
004013F2 5F4 pop eax
004013F3 5F5 pop edi
004013F4 5F6 pop esi
004013F5 5F7 pop ebx
004013F6 5F8 pop edx
004013F7 5F9 pop ecx
004013F8 5FA pop eax
004013F9 5FB pop edi
004013FA 5FC pop esi
004013FB 5FD pop ebx
004013FC 5FE pop edx
004013FD 5FF pop ecx
004013FE 600 pop eax
004013FF 601 pop edi
00401400 602 pop esi
00401401 603 pop ebx
00401402 604 pop edx
00401403 605 pop ecx
00401404 606 pop eax
00401405 607 pop edi
00401406 608 pop esi
00401407 609 pop ebx
00401408 60A pop edx
00401409 60B pop ecx
0040140A 60C pop eax
0040140B 60D pop edi
0040140C 60E pop esi
0040140D 60F pop ebx
0040140E 610 pop edx
0040140F 611 pop ecx
00401410 612 pop eax
00401411 613 pop edi
00401412 614 pop esi
00401413 615 pop ebx
00401414 616 pop edx
00401415 617 pop ecx
00401416 618 pop eax
00401417 619 pop edi
00401418 61A pop esi
00401419 61B pop ebx
0040141A 61C pop edx
0040141B 61D pop ecx
0040141C 61E pop eax
0040141D 61F pop edi
0040141E 620 pop esi
0040141F 621 pop ebx
00401420 622 pop edx
00401421 623 pop ecx
00401422 624 pop eax
00401423 625 pop edi
00401424 626 pop esi
00401425 627 pop ebx
00401426 628 pop edx
00401427 629 pop ecx
00401428 62A pop eax
00401429 62B pop edi
0040142A 62C pop esi
0040142B 62D pop ebx
0040142C 62E pop edx
0040142D 62F pop ecx
0040142E 630 pop eax
0040142F 631 pop edi
00401430 632 pop esi
00401431 633 pop ebx
00401432 634 pop edx
00401433 635 pop ecx
00401434 636 pop eax
00401435 637 pop edi
00401436 638 pop esi
00401437 639 pop ebx
00401438 63A pop edx
00401439 63B pop ecx
0040143A 63C pop eax
0040143B 63D pop edi
0040143C 63E pop esi
0040143D 63F pop ebx
0040143E 640 pop edx
0040143F 641 pop ecx
00401440 642 pop eax
00401441 643 pop edi
00401442 644 pop esi
00401443 645 pop ebx
00401444 646 pop edx
00401445 647 pop ecx
00401446 648 pop eax
00401447 649 pop edi
00401448 64A pop esi
00401449 64B pop ebx
0040144A 64C pop edx
0040144B 64D pop ecx
0040144C 64E pop eax
0040144D 64F pop edi
0040144E 650 pop esi
0040144F 651 pop ebx
00401450 652 pop edx
00401451 653 pop ecx
00401452 654 pop eax
00401453 655 pop edi
00401454 656 pop esi
00401455 657 pop ebx
00401456 658 pop edx
00401457 659 pop ecx
00401458 65A pop eax
00401459 65B pop edi
0040145A 65C pop esi
0040145B 65D pop ebx
0040145C 65E pop edx
0040145D 65F pop ecx
0040145E 660 pop eax
0040145F 661 pop edi
00401460 662 pop esi
00401461 663 pop ebx
00401462 664 pop edx
00401463 665 pop ecx
00401464 666 pop eax
00401465 667 pop edi
00401466 668 pop esi
00401467 669 pop ebx
00401468 66A pop edx
00401469 66B pop ecx
0040146A 66C pop eax
0040146B 66D pop edi
0040146C 66E pop esi
0040146D 66F pop ebx
0040146E 670 pop edx
0040146F 671 pop ecx
00401470 672 pop eax
00401471 673 pop edi
00401472 674 pop esi
00401473 675 pop ebx
00401474 676 pop edx
00401475 677 pop ecx
00401476 678 pop eax
00401477 679 pop edi
00401478 67A pop esi
00401479 67B pop ebx
0040147A 67C pop edx
0040147B 67D pop ecx
0040147C 67E pop eax
0040147D 67F pop edi
0040147E 680 pop esi
0040147F 681 pop ebx
00401480 682 pop edx
00401481 683 pop ecx
00401482 684 pop eax
00401483 685 pop edi
00401484 686 pop esi
00401485 687 pop ebx
00401486 688 pop edx
00401487 689 pop ecx
00401488 68A pop eax
00401489 68B pop edi
0040148A 68C pop esi
0040148B 68D pop ebx
0040148C 68E pop edx
0040148D 68F pop ecx
0040148E 690 pop eax
0040148F 691 pop edi
00401490 692 pop esi
00401491 693 pop ebx
00401492 694 pop edx
00401493 695 pop ecx
00401494 696 pop eax
00401495 697 pop edi
00401496 698 pop esi
00401497 699 pop ebx
00401498 69A pop edx
00401499 69B pop ecx
0040149A 69C pop eax
0040149B 69D pop edi
0040149C 69E pop esi
0040149D 69F pop ebx
0040149E 6A0 pop edx
0040149F 6A1 pop ecx
004014A0 6A2 pop eax
004014A1 6A3 pop edi
004014A2 6A4 pop esi
004014A3 6A5 pop ebx
004014A4 6A6 pop edx
004014A5 6A7 pop ecx
004014A6 6A8 pop eax
004014A7 6A9 pop edi
004014A8 6AA pop esi
004014A9 6AB pop ebx
004014AA 6AC pop edx
004014AB 6AD pop ecx
004014AC 6AE pop eax
004014AD 6AF pop edi
004014AE 6B0 pop esi
004014AF 6B1 pop ebx
004014B0 6B2 pop edx
004014B1 6B3 pop ecx
004014B2 6B4 pop eax
004014B3 6B5 pop edi
004014B4 6B6 pop esi
004014B5 6B7 pop ebx
004014B6 6B8 pop edx
004014B7 6B9 pop ecx
004014B8 6BA pop eax
004014B9 6BB pop edi
004014BA 6BC pop esi
004014BB 6BD pop ebx
004014BC 6BE pop edx
004014BD 6BF pop ecx
004014BE 6C0 pop eax
004014BF 6C1 pop edi
004014C0 6C2 pop esi
004014C1 6C3 pop ebx
004014C2 6C4 pop edx
004014C3 6C5 pop ecx
004014C4 6C6 pop eax
004014C5 6C7 pop edi
004014C6 6C8 pop esi
004014C7 6C9 pop ebx
004014C8 6CA pop edx
004014C9 6CB pop ecx
004014CA 6CC pop eax
004014CB 6CD pop edi
004014CC 6CE pop esi
004014CD 6CF pop ebx
004014CE 6D0 pop edx
004014CF 6D1 pop ecx
004014D0 6D2 pop eax
004014D1 6D3 pop edi
004014D2 6D4 pop esi
004014D3 6D5 pop ebx
004014D4 6D6 pop edx
004014D5 6D7 pop ecx
004014D6 6D8 pop eax
004014D7 6D9 pop edi
004014D8 6DA pop esi
004014D9 6DB pop ebx
004014DA 6DC pop edx
004014DB 6DD pop ecx
004014DC 6DE pop eax
004014DD 6DF pop edi
004014DE 6E0 pop esi
004014DF 6E1 pop ebx
004014E0 6E2 pop edx
004014E1 6E3 pop ecx
004014E2 6E4 pop eax
004014E3 6E5 pop edi
004014E4 6E6 pop esi
004014E5 6E7 pop ebx
004014E6 6E8 pop edx
004014E7 6E9 pop ecx
004014E8 6EA pop eax
004014E9 6EB pop edi
004014EA 6EC pop esi
004014EB 6ED pop ebx
004014EC 6EE pop edx
004014ED 6EF pop ecx
004014EE 6F0 pop eax
004014EF 6F1 pop edi
004014F0 6F2 pop esi
004014F1 6F3 pop ebx
004014F2 6F4 pop edx
004014F3 6F5 pop ecx
004014F4 6F6 pop eax
004014F5 6F7 pop edi
004014F6 6F8 pop esi
004014F7 6F9 pop ebx
004014F8 6FA pop edx
004014F9 6FB pop ecx
004014FA 6FC pop eax
004014FB 6FD pop edi
004014FC 6FE pop esi
004014FD 6FF pop ebx
004014FE 700 pop edx
004014FF 701 pop ecx
00401500 702 pop eax
00401501 703 pop edi
00401502 704 pop esi
00401503 705 pop ebx
00401504 706 pop edx
00401505 707 pop ecx
00401506 708 pop eax
00401507 709 pop edi
00401508 70A pop esi
00401509 70B pop ebx
0040150A 70C pop edx
0040150B 70D pop ecx
0040150C 70E pop eax
0040150D 70F pop edi
0040150E 710 pop esi
0040150F 711 pop ebx
00401510 712 pop edx
00401511 713 pop ecx
00401512 714 pop eax
00401513 715 pop edi
00401514 716 pop esi
00401515 717 pop ebx
00401516 718 pop edx
00401517 719 pop ecx
00401518 71A pop eax
00401519 71B pop edi
0040151A 71C pop esi
0040151B 71D pop ebx
0040151C 71E pop edx
0040151D 71F pop ecx
0040151E 720 pop eax
0040151F 721 pop edi
00401520 722 pop esi
00401521 723 pop ebx
00401522 724 pop edx
00401523 725 pop ecx
00401524 726 pop eax
00401525 727 pop edi
00401526 728 pop esi
00401527 729 pop ebx
00401528 72A pop edx
00401529 72B pop ecx
0040152A 72C pop eax
0040152B 72D pop edi
0040152C 72E pop esi
0040152D 72F pop ebx
0040152E 730 pop edx
0040152F 731 pop ecx
00401530 732 pop eax
00401531 733 pop edi
00401532 734 pop esi
00401533 735 pop ebx
00401534 736 pop edx
00401535 737 pop ecx
00401536 738 pop eax
00401537 739 pop edi
00401538 73A pop esi
00401539 73B pop ebx
0040153A 73C pop edx
0040153B 73D pop ecx
0040153C 73E pop eax
0040153D 73F pop edi
0040153E 740 pop esi
0040153F 741 pop ebx
00401540 742 pop edx
00401541 743 pop ecx
00401542 744 pop eax
00401543 745 pop edi
00401544 746 pop esi
00401545 747 pop ebx
00401546 748 pop edx
00401547 749 pop ecx
00401548 74A pop eax
00401549 74B pop edi
0040154A 74C pop esi
0040154B 74D pop ebx
0040154C 74E pop edx
0040154D 74F pop ecx
0040154E 750 pop eax
0040154F 751 pop edi
00401550 752 pop esi
00401551 753 pop ebx
00401552 754 pop edx
00401553 755 pop ecx
00401554 756 pop eax
00401555 757 pop edi
00401556 758 pop esi
00401557 759 pop ebx
00401558 75A pop edx
00401559 75B pop ecx
0040155A 75C pop eax
0040155B 75D pop edi
0040155C 75E pop esi
0040155D 75F pop ebx
0040155E 760 pop edx
0040155F 761 pop ecx
00401560 762 pop eax
00401561 763 pop edi
00401562 764 pop esi
00401563 765 pop ebx
00401564 766 pop edx
00401565 767 pop ecx
00401566 768 pop eax
00401567 769 pop edi
00401568 76A pop esi
00401569 76B pop ebx
0040156A 76C pop edx
0040156B 76D pop ecx
0040156C 76E pop eax
0040156D 76F pop edi
0040156E 770 pop esi
0040156F 771 pop ebx
00401570 772 pop edx
00401571 773 pop ecx
00401572 774 pop eax
00401573 775 pop edi
00401574 776 pop esi
00401575 777 pop ebx
00401576 778 pop edx
00401577 779 pop ecx
00401578 77A pop eax
00401579 77B pop edi
0040157A 77C pop esi
0040157B 77D pop ebx
0040157C 77E pop edx
0040157D 77F pop ecx
0040157E 780 pop eax
0040157F 781 pop edi
00401580 782 pop esi
00401581 783 pop ebx
00401582 784 pop edx
00401583 785 pop ecx
00401584 786 pop eax
00401585 787 pop edi
00401586 788 pop esi
00401587 789 pop ebx
00401588 78A pop edx
00401589 78B pop ecx
0040158A 78C pop eax
0040158B 78D pop edi
0040158C 78E pop esi
0040158D 78F pop ebx
0040158E 790 pop edx
0040158F 791 pop ecx
00401590 792 pop eax
00401591 793 pop edi
00401592 794 pop esi
00401593 795 pop ebx
00401594 796 pop edx
00401595 797 pop ecx
00401596 798 pop eax
00401597 799 pop edi
00401598 79A pop esi
00401599 79B pop ebx
0040159A 79C pop edx
0040159B 79D pop ecx
0040159C 79E pop eax
0040159D 79F pop edi
0040159E 7A0 pop esi
0040159F 7A1 pop ebx
004015A0 7A2 pop edx
004015A1 7A3 pop ecx
004015A2 7A4 pop eax
004015A3 7A5 pop edi
004015A4 7A6 pop esi
004015A5 7A7 pop ebx
004015A6 7A8 pop edx
004015A7 7A9 pop ecx
004015A8 7AA pop eax
004015A9 7AB pop edi
004015AA 7AC pop esi
004015AB 7AD pop ebx
004015AC 7AE pop edx
004015AD 7AF pop ecx
004015AE 7B0 pop eax
004015AF 7B1 pop edi
004015B0 7B2 pop esi
004015B1 7B3 pop ebx
004015B2 7B4 pop edx
004015B3 7B5 pop ecx
004015B4 7B6 pop eax
004015B5 7B7 pop edi
004015B6 7B8 pop esi
004015B7 7B9 pop ebx
004015B8 7BA pop edx
004015B9 7BB pop ecx
004015BA 7BC pop eax
004015BB 7BD pop edi
004015BC 7BE pop esi
004015BD 7BF pop ebx
004015BE 7C0 pop edx
004015BF 7C1 pop ecx
004015C0 7C2 pop eax
004015C1 7C3 pop edi
004015C2 7C4 pop esi
004015C3 7C5 pop ebx
004015C4 7C6 pop edx
004015C5 7C7 pop ecx
004015C6 7C8 pop eax
004015C7 7C9 pop edi
004015C8 7CA pop esi
004015C9 7CB pop ebx
004015CA 7CC pop edx
004015CB 7CD pop ecx
004015CC 7CE pop eax
004015CD 7CF pop edi
004015CE 7D0 pop esi
004015CF 7D1 pop ebx
004015D0 7D2 pop edx
004015D1 7D3 pop ecx
004015D2 7D4 pop eax
004015D3 7D5 pop edi
004015D4 7D6 pop esi
004015D5 7D7 pop ebx
004015D6 7D8 pop edx
004015D7 7D9 pop ecx
004015D8 7DA pop eax
004015D9 7DB pop edi
004015DA 7DC pop esi
004015DB 7DD pop ebx
004015DC 7DE pop edx
004015DD 7DF pop ecx
004015DE 7E0 pop eax
004015DF 7E1 pop edi
004015E0 7E2 pop esi
004015E1 7E3 pop ebx
004015E2 7E4 pop edx
004015E3 7E5 pop ecx
004015E4 7E6 pop eax
004015E5 7E7 pop edi
004015E6 7E8 pop esi
004015E7 7E9 pop ebx
004015E8 7EA pop edx
004015E9 7EB pop ecx
004015EA 7EC pop eax
004015EB 7ED pop edi
004015EC 7EE pop esi
004015ED 7EF pop ebx
004015EE 7F0 pop edx
004015EF 7F1 pop ecx
004015F0 7F2 pop eax
004015F1 7F3 pop edi
004015F2 7F4 pop esi
004015F3 7F5 pop ebx
004015F4 7F6 pop edx
004015F5 7F7 pop ecx
004015F6 7F8 pop eax
004015F7 7F9 pop edi
004015F8 7FA pop esi
004015F9 7FB pop ebx
004015FA 7FC pop edx
004015FB 7FD pop ecx
004015FC 7FE pop eax
004015FD 7FF pop edi
00401600 800 pop esi
00401601 801 pop ebx
00401602 802 pop edx
00401603 803 pop ecx
00401604 804 pop eax
00401605 805 pop edi
00401606 806 pop esi
00401607 807 pop ebx
00401608 808 pop edx
00401609 809 pop ecx
0040160A 80A pop eax
0040160B 80B pop edi
0040160C 80C pop esi
0040160D 80D pop ebx
0040160E 80E pop edx
0040160F 80F pop ecx
00401610 810 pop eax
00401611 811 pop edi
00401612 812 pop esi
00401613 813 pop ebx
00401614 814 pop edx
00401615 815 pop ecx
00401616 816 pop eax
00401617 817 pop edi
00401618 818 pop esi
00401619 819 pop ebx
0040161A 81A pop edx
0040161B 81B pop ecx
0040161C 81C pop eax
0040161D 81D pop edi
0040161E 81E pop esi
0040161F 81F pop ebx
00401620 820 pop edx
00401621 821 pop ecx
00401622 822 pop eax
00401623 823 pop edi
00401624 824 pop esi
00401625 825 pop ebx
00401626 826 pop edx
00401627 827 pop ecx
00401628 828 pop eax
00401629 829 pop edi
0040162A 82A pop esi
0040162B 82B pop ebx
0040162C 82C pop edx
0040162D 82D pop ecx
0040162E 82E pop eax
0040162F 82F pop edi
00401630 830 pop esi
00401631 831 pop ebx
00401632 832 pop edx
00401633 833 pop ecx
00401634 834 pop eax
00401635 835 pop edi
00401636 836 pop esi
00401637 837 pop ebx
00401638 838 pop edx
00401639 839 pop ecx
0040163A 83A pop eax
0040163B 83B pop edi
0040163C 83C pop esi
0040163D 83D pop ebx
0040163E 83E pop edx
0040163F 83F pop ecx
00401640 840 pop eax
00401641 841 pop edi
00401642 842 pop esi
00401643 843 pop ebx
00401644 844 pop edx
00401645 845 pop ecx
00401646 846 pop eax
00401647 847 pop edi
00401648 848 pop esi
00401649 849 pop ebx
0040164A 84A pop edx
0040164B 84B pop ecx
0040164C 84C pop eax
0040164D 84D pop edi
0040164E 84E pop esi
0040164F 84F pop ebx
00401650 850 pop edx
00401651 851 pop ecx
00401652 852 pop eax
00401653 853 pop edi
00401654 854 pop esi
00401655 855 pop ebx
00401656 856 pop edx
00401657 857 pop ecx
00401658 858 pop eax
00401659 859 pop edi
0040165A 85A pop esi
0040165B 85B pop ebx
0040165C 85C pop edx
0040165D 85D pop ecx
0040165E 85E pop eax
0040165F 85F pop edi
00401660 860 pop esi
00401661 861 pop ebx
00401662 862 pop edx
00401663 863 pop ecx
00401664 864 pop eax
00401665 865 pop edi
00401666 866 pop esi
00401667 867 pop ebx
00401668 868 pop edx
00401669 869 pop ecx
0040166A 86A pop eax
0040166B 86B pop edi
0040166C 86C pop esi
0040166D 86D pop ebx
0040166E 86E pop edx
0040166F 86F pop ecx
00401670 870 pop eax
00401671 871 pop edi
00401672 872 pop esi
00401673 873 pop ebx
00401674 874 pop edx
00401675 875 pop ecx
00401676 876 pop eax
00401677 877 pop edi
00401678 878 pop esi
00401679 879 pop ebx
0040167A 87A pop edx
0040167B 87B pop ecx
0040167C 87C pop eax
0040167D 87D pop edi
0040167E 87E pop esi
0040167F 87F pop ebx
00401680 880 pop edx
00401681 881 pop ecx
00401682 882 pop eax
00401683 883 pop edi
00401684 884 pop esi
00401685 885 pop ebx
00401686 886 pop edx
00401687 887 pop ecx
00401688 888 pop eax
00401689 889 pop edi
0040168A 88A pop esi
0040168B 88B pop ebx
0040168C 88C pop edx
0040168D 88D pop ecx
0040168E 88E pop eax
0040168F 88F pop edi
00401690 890 pop esi
00401691 891 pop ebx
00401692 892 pop edx
00401693 893 pop ecx
00401694 894 pop eax
00401695 895 pop edi
00401696 896 pop esi
00401697 897 pop ebx
00401698 898 pop edx
00401699 899 pop ecx
0040169A 89A pop eax
0040169B 89B pop edi
0040169C 89C pop esi
0040169D 89D pop ebx
0040169E 89E pop edx
0040169F 89F pop ecx
004016A0 8A0 pop eax
004016A1 8A1 pop edi
004016A2 8A2 pop esi
004016A3 8A3 pop ebx
004016A4 8A4 pop edx
004016A5 8A5 pop ecx
004016A6 8A6 pop eax
004016A7 8A7 pop edi
004016A8 8A8 pop esi
004016A9 8A9 pop ebx
004016AA 8AA pop edx
004016AB 8AB pop ecx
004016AC 8AC pop eax
004016AD 8AD pop edi
004016AE 8AE pop esi
004016AF 8AF pop ebx
004016B0 8B0 pop edx
004016B1 8B1 pop ecx
004016B2 8B2 pop eax
004016B3 8B3 pop edi
004016B4 8B4 pop esi
004016B5 8B5 pop ebx
004016B6 8B6 pop edx
004016B7 8B7 pop ecx
004016B8 8B8 pop eax
004016B9 8B9 pop edi
004016BA 8BA pop esi
004016BB 8BB pop ebx
004016BC 8BC pop edx
004016BD 8BD pop ecx
004016BE 8BE pop eax
004016BF 8BF pop edi
004016C0 8C0 pop esi
004016C1 8C1 pop ebx
004016C2 8C2 pop edx
0
```


6) What is the value of the second argument to the call to SetFileAttributesA at 0x4013A7? What is the name of the file that SetFileAttributesA modifies, and why is this significant? (Expecting the names of the attributes, not an integer) (10 pts)

The value of second argument at 4013A7 (call SetFileAttributesA) is READONLY:HIDDEN:SYSTEM
Name of the file that SetAttributesA modifies is d3dxd1a.dll

Considering the modified value, READONLY:HIDDEN:SYSTEM, and the file, DLL, its not suspicious that its READONLY because we don't want anybody changing or adding function in the library, but the suspicious part is the HIDDEN:SYSTEM. Any legitimate program wouldn't try to hide the execution of a DLL which makes d3dxd1a.dll and the modification suspicious.



7) In a few sentences, describe what sub_4011B4 does. (12 pts)

This function is responsible for creating registry keys (RegCreateKey - Creates the specified registry key. If the key already exists, the function opens it.) and setting values to the registry key (RegSetValue - Sets the data and type of a specified value under a registry key).

RegCreateKey

Syntax

```
C++
Copy

LSTATUS RegCreateKeyEx(
    HKEY          hKey,
    LPCSTR        lpSubKey,
    DWORD         Reserved,
    LPSTR         lpClass,
    DWORD         dwOptions,
    REGSAM        samDesired,
    const LPSECURITY_ATTRIBUTES lpSecurityAttributes,
    PHKEY         phkResult,
    LPDWORD       lpdwDisposition
);
```

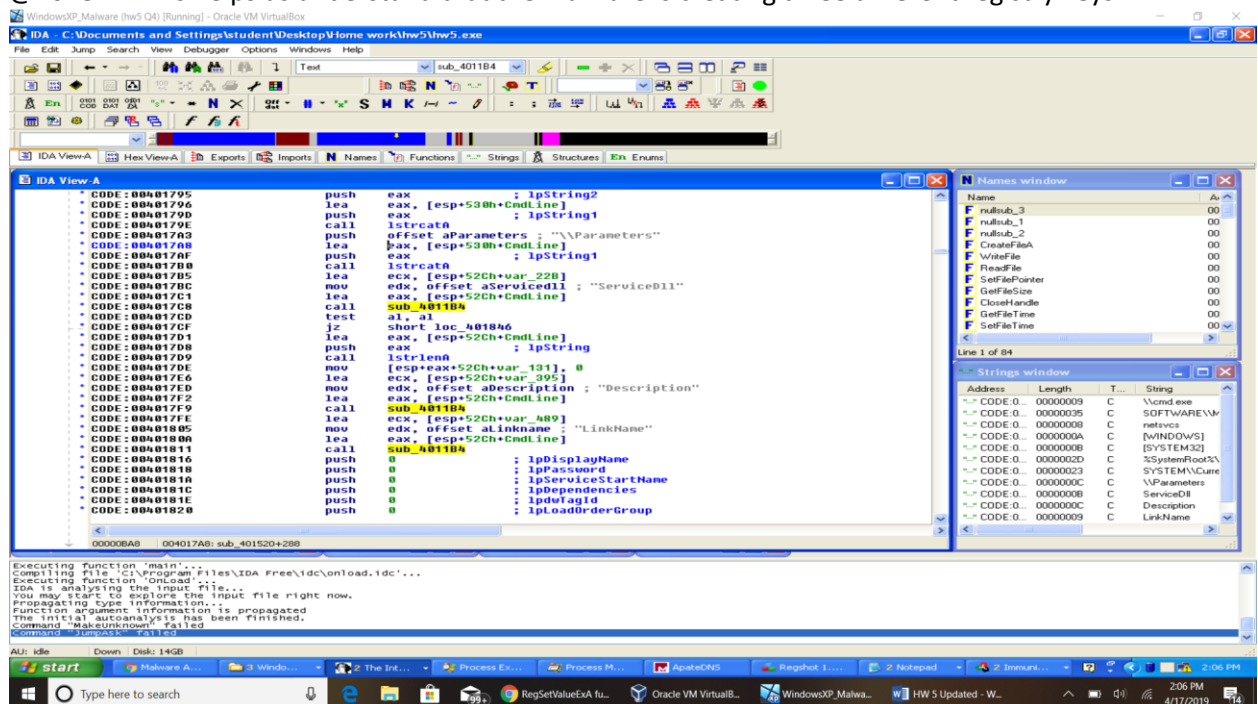
RegSetValue Syntax

C++

Copy

```
LSTATUS RegSetValueEx(  
    HKEY    hKey,  
    LPCSTR  lpValueName,  
    DWORD   Reserved,  
    DWORD   dwType,  
    const BYTE *lpData,  
    DWORD   cbData  
);
```

This function takes two input parameters `hkey` and `dwDisposition`. When called, `hkey` is stored in `ecx` and `dwDisposition` is stored in `eax`. This function is called three times: `@4017C8`, `@4017F9`, and `@401811`. This helps us understand that the malware is creating three different registry keys.



8) What is the value of the second argument to `RegSetValueExA` when `sub_4011B4` is called at the following locations? (9 pts)

- a) At `0x4017C8`?: ServiceDll
- b) At `0x4017F9`?: Description
- c) At `0x401811`?: LinkName

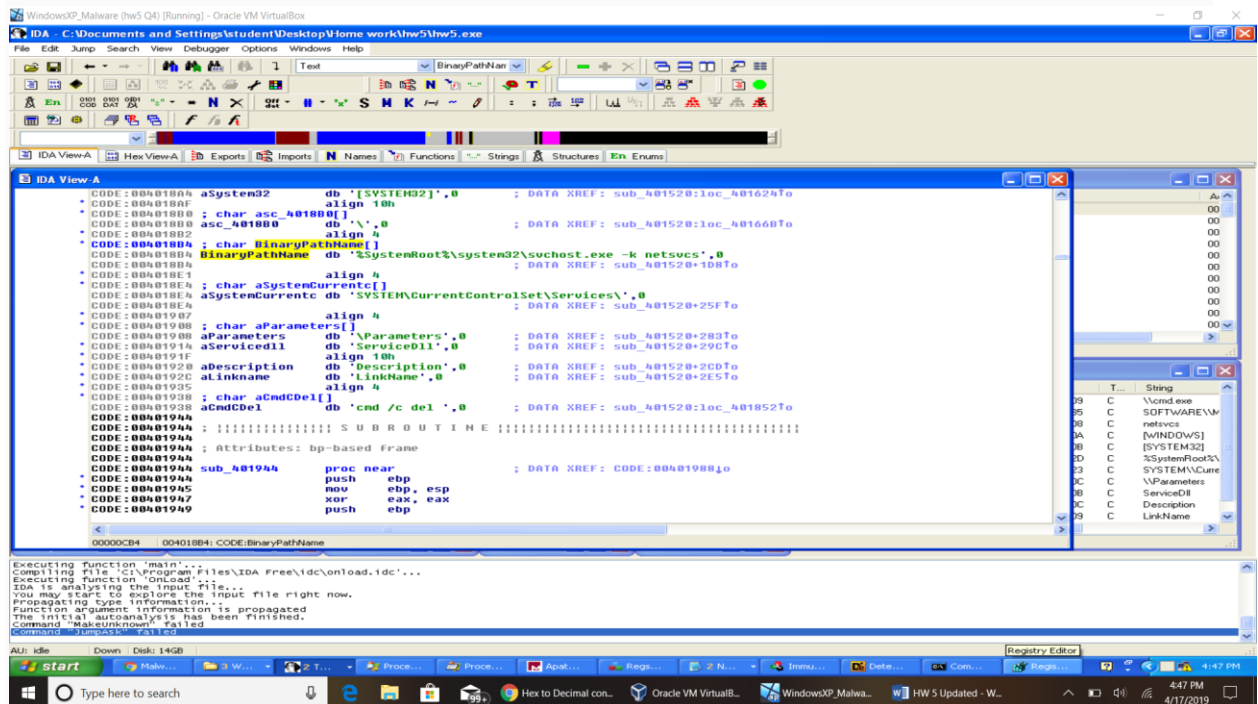
9) How does the malware gain persistence? (8 pts)

HKLM\System\CurrentControlSet\Services\SharedAccess

The keys located here get loaded by the Service Controller at various times during the operation of the computer. Some are loaded at system startup and others are loaded on demand or when triggered by other events. The attackers want to load at startup so that even if no user logs in they can connect to the computer. This is where the "Share Process" DLLs are configured to be loaded by the host process, SvcHost.exe. This has been the most common location for attackers to locate their remote access tools, often called "RATs" by response investigators.

Installing malware for persistence as an *svchost.exe* DLL makes the malware blend into the process list and the registry better than a standard service.

The malware to blend in the network, uses the netsvcs. We get this by this value by looking at %SystemRoot%\System32\svchost.exe -k GroupName, where group name is netsvcs.

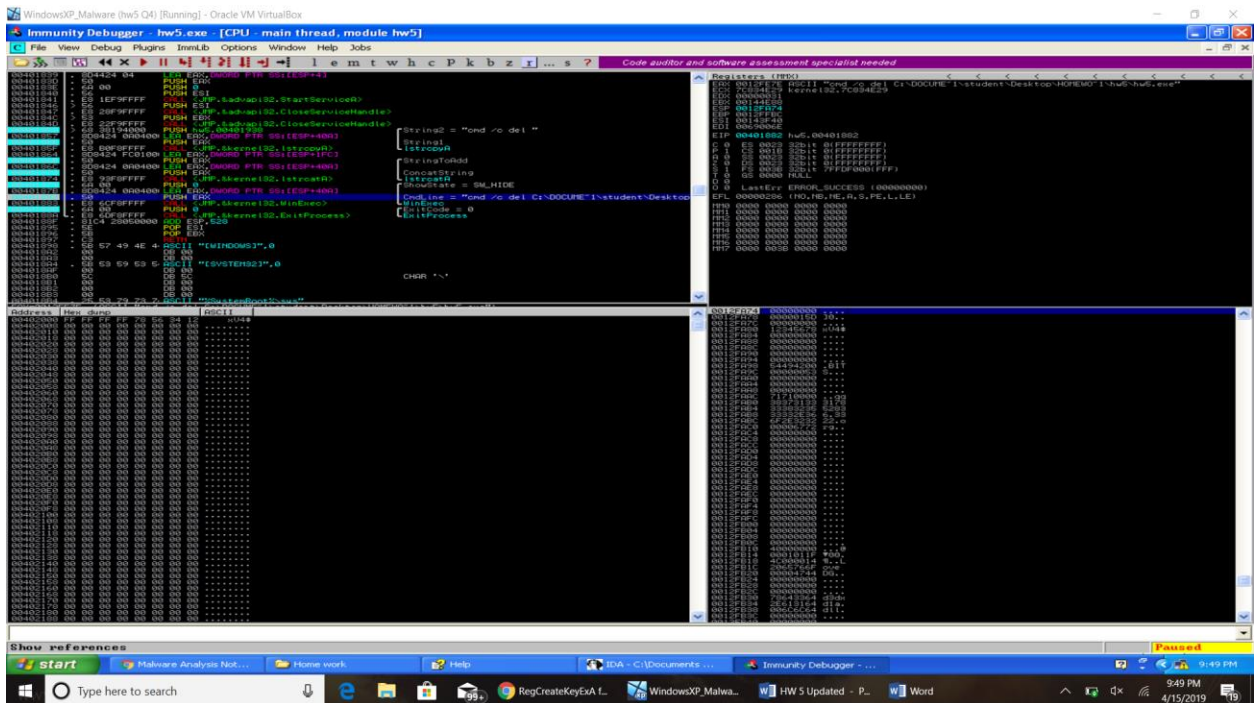


10) What is the value of the first argument to WinExec at 0x401883? What does the call to WinExec do? (9 pts)

First Argument at 401883 (call WinExec) is

"cmd /c del C:\Student\dersktop\HOMEWORK\hw5\hw5.exe"

This command when entered in command prompt deletes hw5.exe



11) Investigate the file created during question 3 (Hint: The file may have some unusual attributes that make it difficult to find). Using any type of analysis you wish, list 3 malicious behaviors you suspect this file can perform. Justify your answers. Extra credit will be awarded if very good analysis is provided. (15 pts)

a) Process Injection Taking a look at the imports in DLL, we can see VirtualAlloc, WriteProcessMemory and CreateRemoteThread. VirtualAlloc - Allocates spaces in an external process memory, WriteProcessMemory - Write data to allocated space (can be executed as a thread), CreateRemoteThread - Creates thread out of the written data and executes it as a thread. This combination gives away that the malware is performing process injection.

b) Polling Keylogger Taking a look at the imports in the DLL, we can see few functions – keybd_event, mouse_event, SetCursorpos, GetCursorpos, MapVirtualKey. Mouse_event is used to synthesize mouse events by applications that need to do so. It is also used by applications that need to obtain more information from the mouse than its position and button state. Using Keybd_event an application can simulate a press of the PRINTSCRN key to obtain a screen snapshot and save it to the clipboard.

Looking at the functions we can say that the malware is trying to simulate mouse clicks and press of keyboardkeys and it is all running in hidden mode without giving any access to other file. Thus, considered as malicious behavior.

c) RunTime Linking Taking a look at the imports in DLL, we can see few function – LoadLibrary and GetProcAddress. LoadLibrary loads the address of the DLL into the memory and GetProcAddress gets the address of the function from DLL in memory. So this combination of imports show that

the malware is performing runtime linking.