

Bulk De-obfuscation and Analysis of PowerShell Malware with PowerDrive

Jeff Malavasi

Dept. of Computing Security
Rochester Institute of Technology
Email: jm3378@rit.edu

I. TOOL ANALYSIS

PowerShell is an extremely useful and robust scripting language that is primarily used to administer Windows computers and servers at scale. Recently, it has even expanded to be cross compatible with Unix systems. One of the reasons that the language is so popular is due to it's ability to be extremely forgiving. For example, aliases are automatically created for all MS-DOS commands for backwards compatibility and cmdlets are able to fill in incomplete instructions. Due to this ability to call the same command in multiple ways, PowerShell is also extremely useful to bad actors, as obfuscation becomes part of the language.

When creating a malicious PowerShell script, threat actors often use multiple layers of obfuscation including reordering strings, encoding and compression. Being able to properly deobfuscate these scripts is extremely important as it allows analysts to detect potential files or URLs in the code as well as determine the attackers goals. One tool that can be used to deobfuscate PowerShell scripts is called PowerDrive [1]. It was created in 2019 and is able to deobfuscate multi-layer scripts using both static and dynamic analysis. The module takes an input file as a parameter and starts by using a set of functions to determine the number of layers in the file. For example the script could use sting manipulation before encoding the entire file. During this stage PowerDrive stores each of the layers in an array. The majority of the rules are accomplished using Regex filters. The next stage, pre-processing works by linting the file and will remove any syntax errors, endless loops, try-catch blocks, null redirection, and sleep functions. Next, the script is deobfuscated using a series of functions including a Base64 decoder. Additionally, PowerDrive relies on the automatic decoding ability of Invoke-Expression. When this cmdlet is called PowerShell automatically deobfuscates the provided string. PowerDrive uses cmdlet override in order to capture this data. Additionally, the module also overrides Invoke-WebRequest and Invoke-Rest in order to protect the analyzing system and intercept web traffic. Next, in the final stage, the script is executed for dynamic analysis. Finally, the script returns a string output with each of the layers written out like the below example:

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

II. LIMITATIONS

While PowerDrive is extremely effective at analyzing a single malicious file it has a few limitations. Firstly, the module returns string output which is difficult to parse or analyze programmatically. This makes the tool difficult to scale and be useful for a large enterprise. PowerShell has the ability to create custom objects, which can be passed through the pipeline for further analysis. Additionally, the tool does not return any information about the results of the dynamic analysis besides whether or not the remote URL is still active. It fails to tell the analyst which type of obfuscation techniques were used, if anti-debugging was employed, or what actions the malware took during execution. Finally, provided with the tool is an example dataset, however all the files are grouped together and requires manual extraction and conversion to PowerShell.

III. PROPOSED IMPROVEMENTS

An updated version of PowerDrive was created and uploaded to Github [2]. The code was written and tested on a Windows 10 virtual machine in a contained network.

A. Custom PSObject

In order to address the output limitation, a custom PSObject was created that stores the results of the analysis both before and after the change (below). This object stores the number of layers, all techniques used by the threat actor, as well as a behavioral analysis of the execution. Additionally, this output can be redirected using the PowerShell pipeline in order to store the results in a CSV that could be ingested by a SIEM for automatic detection and alerting.



B. Bulk Analysis Script

The next improvement that was made was the creation of a bulk analysis script (Invoke-PowerDriveAnalysis). Instead of scanning a single file, the script recursively scans a directory for all PowerShell files and stores the results in a CSV. This script can be run as a scheduled task and can be deployed to many machines in order to use PowerDrive at scale.

[illegible]

- [1] D. Ugarte, D. Maiorca, F. Cara, and G. Giacinto, "Powerdrive: Accurate de-obfuscation and analysis of powershell malware," 2019.
- [2] J. Malavasi, "Powerdrive," <https://github.com/ursaMaj0r/PowerDrive>, 2023.
- [3] M.-H. Tsai, C.-C. Lin, Z.-G. He, W.-C. Yang, and C.-L. Lei, "Powerdp: De-obfuscating and profiling malicious powershell commands with multi-label classifiers," *IEEE Access*, vol. 11, pp. 256–270, 2023.
- [4] S. Choi, "Malicious powershell detection using attention against adversarial attacks," *Electronics*, vol. 9, no. 11, 2020. [Online]. Available: <https://www.mdpi.com/2079-9292/9/11/1817>