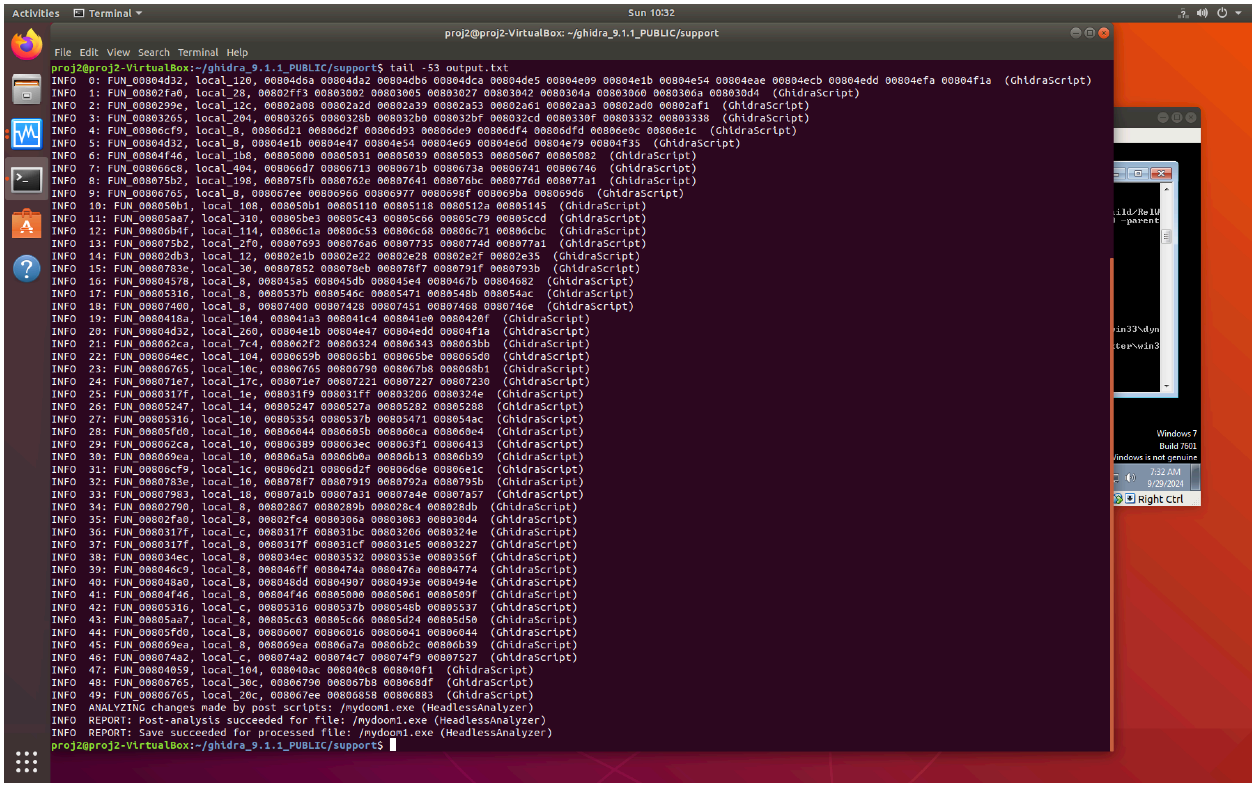
Malware Analysis Report

1. Malware1 (mydoom1.exe)

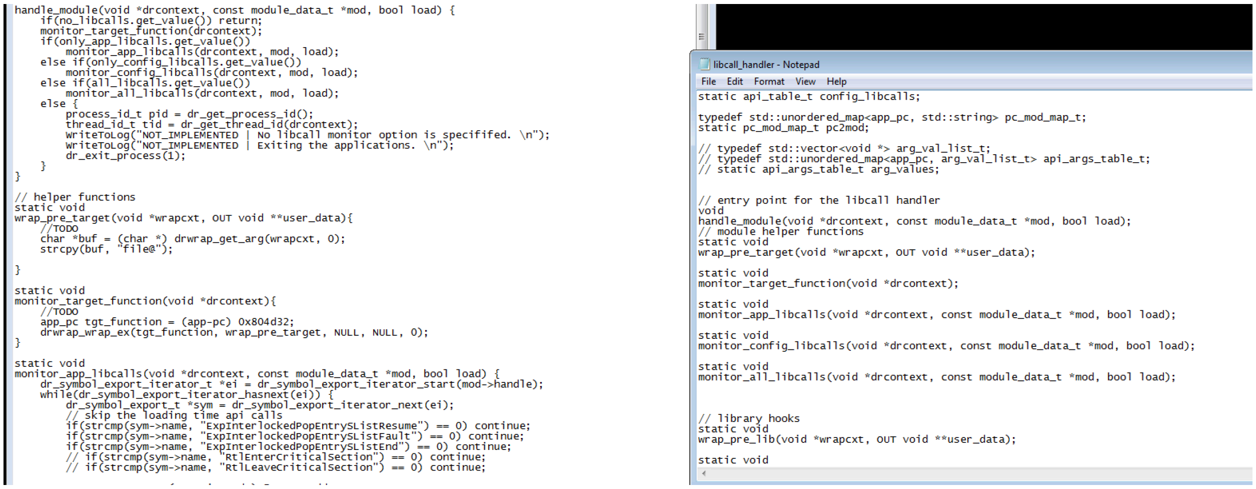
For this task, first I did static analysis and run the script that gives output top longest chain of basic blocks.



```
proj2@proj2-VirtualBox:~/ghidra_9.1.1_PUBLIC/support$ tail -53 output.txt
INFO  0: FUN_00804d32, local_120, 00804d6a 00804da2 00804db6 00804dca 00804de5 00804e09 00804e1b 00804e54 00804eae 00804ecb 00804edd 00804efa 00804f1a  (GhidraScript)
INFO  1: FUN_00802fa0, local_28, 00802ff3 00803002 00803005 00803027 00803042 0080304a 00803060 0080306a 008030d4  (GhidraScript)
INFO  2: FUN_0080299e, local_12c, 00802a08 00802a2d 00802a39 00802a53 00802a61 00802aa3 00802ad0 00802af1  (GhidraScript)
INFO  3: FUN_00803265, local_204, 00803265 0080328b 008032b0 008032bf 008032cd 0080330f 00803332 00803338  (GhidraScript)
INFO  4: FUN_00806cf9, local_8, 00806d21 00806d2f 00806d93 00806de9 00806df4 00806dfd 00806e0c 00806e1c  (GhidraScript)
INFO  5: FUN_00804d32, local_8, 00804e1b 00804e47 00804e54 00804e69 00804e6d 00804e79 00804f35  (GhidraScript)
INFO  6: FUN_00804f46, local_1b8, 00805000 00805031 00805039 00805053 00805067 00805082  (GhidraScript)
INFO  7: FUN_008066c8, local_404, 008066d7 00806713 0080671b 0080673a 00806741 00806746  (GhidraScript)
INFO  8: FUN_008075b2, local_198, 008075fb 0080762e 00807641 008076bc 0080776d 008077a1  (GhidraScript)
INFO  9: FUN_00806765, local_8, 008067ee 00806966 00806977 0080698f 008069ba 008069d6  (GhidraScript)
INFO  10: FUN_008050b1, local_108, 008050b1 00805110 00805118 0080512a 00805145  (GhidraScript)
INFO  11: FUN_00805aa7, local_310, 00805be3 00805c43 00805c66 00805c79 00805ccd  (GhidraScript)
INFO  12: FUN_00806b4f, local_114, 00806c1a 00806c53 00806c68 00806c71 00806cbc  (GhidraScript)
INFO  13: FUN_008075b2, local_2f0, 00807693 008076a6 00807735 0080774d 008077a1  (GhidraScript)
INFO  14: FUN_00802db3, local_12, 00802e1b 00802e22 00802e28 00802e2f 00802e35  (GhidraScript)
INFO  15: FUN_0080783e, local_30, 00807852 008078eb 008078f7 0080791f 0080793b  (GhidraScript)
INFO  16: FUN_00804578, local_8, 008045a5 008045db 008045e4 0080467b 00804682  (GhidraScript)
INFO  17: FUN_00805316, local_8, 0080537b 0080546c 00805471 0080548b 008054ac  (GhidraScript)
INFO  18: FUN_00807400, local_8, 00807400 00807428 00807451 00807468 0080746e  (GhidraScript)
INFO  19: FUN_0080418a, local_104, 008041a3 008041c4 008041e0 0080420f  (GhidraScript)
INFO  20: FUN_00804d32, local_260, 00804e1b 00804e47 00804edd 00804f1a  (GhidraScript)
INFO  21: FUN_008062ca, local_7c4, 008062f2 00806324 00806343 008063bb  (GhidraScript)
INFO  22: FUN_008064ec, local_104, 0080659b 008065b1 008065be 008065d0  (GhidraScript)
INFO  23: FUN_00806765, local_10c, 00806765 00806790 008067b8 008068b1  (GhidraScript)
INFO  24: FUN_008071e7, local_17c, 008071e7 00807221 00807227 00807230  (GhidraScript)
INFO  25: FUN_0080317f, local_1e, 008031f9 008031ff 00803206 0080324e  (GhidraScript)
INFO  26: FUN_00805247, local_14, 00805247 0080527a 00805282 00805288  (GhidraScript)
INFO  27: FUN_00805316, local_10, 00805354 0080537b 00805471 008054ac  (GhidraScript)
INFO  28: FUN_00805fd0, local_10, 00806044 0080605b 008060ca 008060e4  (GhidraScript)
INFO  29: FUN_008062ca, local_10, 00806389 008063ec 008063f1 00806413  (GhidraScript)
INFO  30: FUN_008069ea, local_10, 00806a5a 00806b0a 00806b13 00806b39  (GhidraScript)
INFO  31: FUN_00806cf9, local_1c, 00806d21 00806d2f 00806d6e 00806e1c  (GhidraScript)
INFO  32: FUN_0080783e, local_10, 008078f7 00807919 0080792a 0080795b  (GhidraScript)
INFO  33: FUN_00807983, local_18, 00807a1b 00807a31 00807a4e 00807a57  (GhidraScript)
INFO  34: FUN_00802790, local_8, 00802867 0080289b 008028c4 008028db  (GhidraScript)
INFO  35: FUN_00802fa0, local_8, 00802fc4 0080306a 00803083 008030d4  (GhidraScript)
INFO  36: FUN_0080317f, local_c, 0080317f 008031bc 00803206 0080324e  (GhidraScript)
INFO  37: FUN_0080317f, local_8, 0080317f 008031cf 008031e5 00803227  (GhidraScript)
INFO  38: FUN_008034ec, local_8, 008034ec 00803532 0080353e 0080356f  (GhidraScript)
INFO  39: FUN_008046c9, local_8, 008046ff 0080474a 0080476a 00804774  (GhidraScript)
INFO  40: FUN_008048a0, local_8, 008048dd 00804907 0080493e 0080494e  (GhidraScript)
INFO  41: FUN_00804f46, local_8, 00804f46 00805000 00805061 0080509f  (GhidraScript)
INFO  42: FUN_00805316, local_c, 00805316 0080537b 0080548b 00805537  (GhidraScript)
INFO  43: FUN_00805aa7, local_8, 00805c63 00805c66 00805d24 00805d50  (GhidraScript)
INFO  44: FUN_00805fd0, local_8, 00806007 00806016 00806041 00806044  (GhidraScript)
INFO  45: FUN_008069ea, local_8, 008069ea 00806a7a 00806b2c 00806b39  (GhidraScript)
INFO  46: FUN_008074a2, local_c, 008074a2 008074c7 008074f9 00807527  (GhidraScript)
INFO  47: FUN_00804059, local_104, 008040ac 008040c8 008040f1  (GhidraScript)
INFO  48: FUN_00806765, local_30c, 00806790 008067b8 008068df  (GhidraScript)
INFO  49: FUN_00806765, local_20c, 008067ee 00806858 00806883  (GhidraScript)
INFO  ANALYZING changes made by post scripts: /mydoom1.exe (HeadlessAnalyzer)
INFO  REPORT: Post-analysis succeeded for file: /mydoom1.exe (HeadlessAnalyzer)
INFO  REPORT: Save succeeded for processed file: /mydoom1.exe (HeadlessAnalyzer)
proj2@proj2-VirtualBox:~/ghidra_9.1.1_PUBLIC/support$
```

Then after modifying the sample_inputs.py for mydoom1.exe malware to print all the commands at one run.

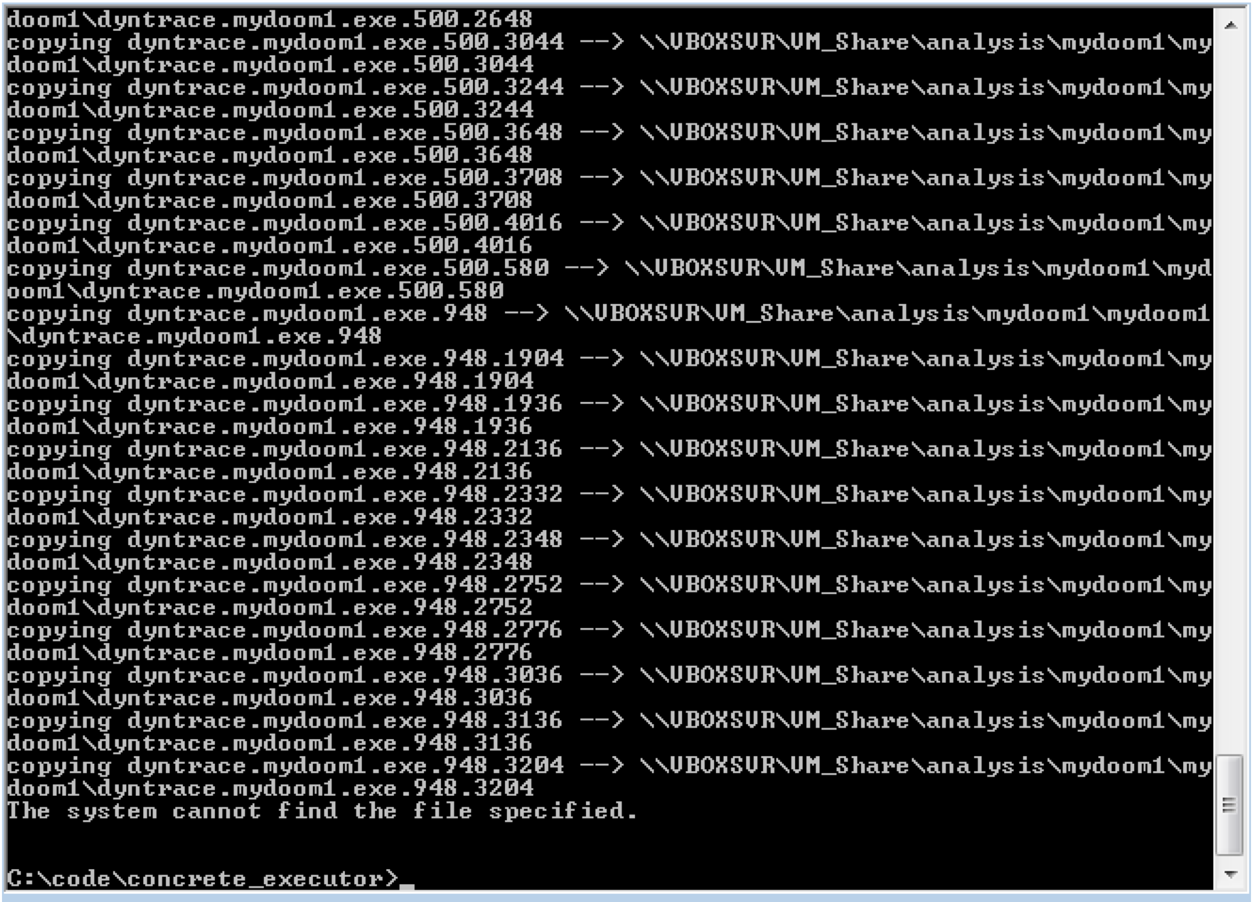
After that, I did Dynamic Analysis in win7 vm. I change the code in libcall_handler for helper functions.



```
handle_module(void *drcontext, const module_data_t *mod, bool load) {
    if(no_libcalls.get_value()) return;
    monitor_target_function(drcontext);
    if(only_app_libcalls.get_value())
        monitor_app_libcalls(drcontext, mod, load);
    else if(only_config_libcalls.get_value())
        monitor_config_libcalls(drcontext, mod, load);
    else if(all_libcalls.get_value())
        monitor_all_libcalls(drcontext, mod, load);
    else {
        process_id_t pid = dr_get_process_id();
        thread_id_t tid = dr_get_thread_id(drcontext);
        WriteToLog("NOT_IMPLEMENTED | No libcall monitor option is specifed. \n");
        WriteToLog("NOT_IMPLEMENTED | Exiting the applications. \n");
        dr_exit_process(1);
    }
}

// helper functions
static void
wrap_pre_target(void *wrapcxt, OUT void **user_data){
    //TODO
    char *buf = (char *) drwrap_get_arg(wrapcxt, 0);
    strcpy(buf, "file@");

}

static void
monitor_target_function(void *drcontext){
    //TODO
    app_pc tgt_function = (app-pc) 0x804d32;
    drwrap_wrap_ex(tgt_function, wrap_pre_target, NULL, NULL, 0);
}

static void
monitor_app_libcalls(void *drcontext, const module_data_t *mod, bool load) {
    dr_symbol_export_iterator_t *ei = dr_symbol_export_iterator_start(mod->handle);
    while(dr_symbol_export_iterator_hasnext(ei)) {
        dr_symbol_export_t *sym = dr_symbol_export_iterator_next(ei);
        // skip the loading time api calls
        if(strcmp(sym->name, "ExpInterlockedPopEntrySListResume") == 0) continue;
        if(strcmp(sym->name, "ExpInterlockedPopEntrySListFault") == 0) continue;
        if(strcmp(sym->name, "ExpInterlockedPopEntrySListEnd") == 0) continue;
        // if(strcmp(sym->name, "RtlEnterCriticalSection") == 0) continue;
        // if(strcmp(sym->name, "RtlLeaveCriticalSection") == 0) continue;
```

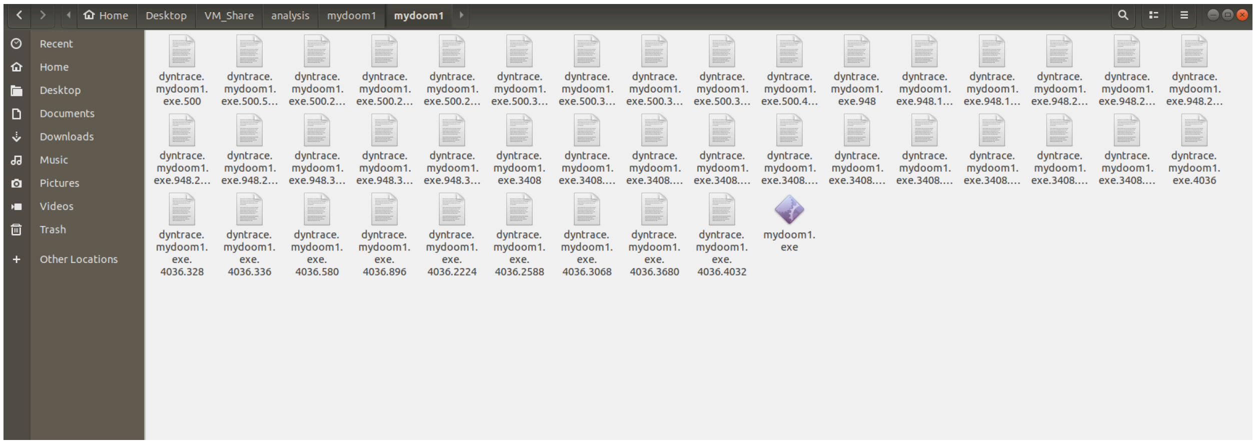
```
static api_table_t config_libcalls;

typedef std::unordered_map<app_pc, std::string> pc_mod_map_t;
static pc_mod_map_t pc2mod;

// typedef std::vector<void *> arg_val_list_t;
// typedef std::unordered_map<app_pc, arg_val_list_t> api_args_table_t;
// static api_args_table_t arg_values;


// entry point for the libcall handler
void
handle_module(void *drcontext, const module_data_t *mod, bool load);
// module helper functions
static void
wrap_pre_target(void *wrapcxt, OUT void **user_data);

static void
monitor_target_function(void *drcontext);

static void
monitor_app_libcalls(void *drcontext, const module_data_t *mod, bool load);

static void
monitor_config_libcalls(void *drcontext, const module_data_t *mod, bool load);

static void
monitor_all_libcalls(void *drcontext, const module_data_t *mod, bool load);



// library hooks
static void
wrap_pre_lib(void *wrapcxt, OUT void **user_data);

static void
```

After changing the code, I change the file name and path and remove the Done form mv.analysis file for mydoom1. Run the python run.py in win7 for concrete_executor.



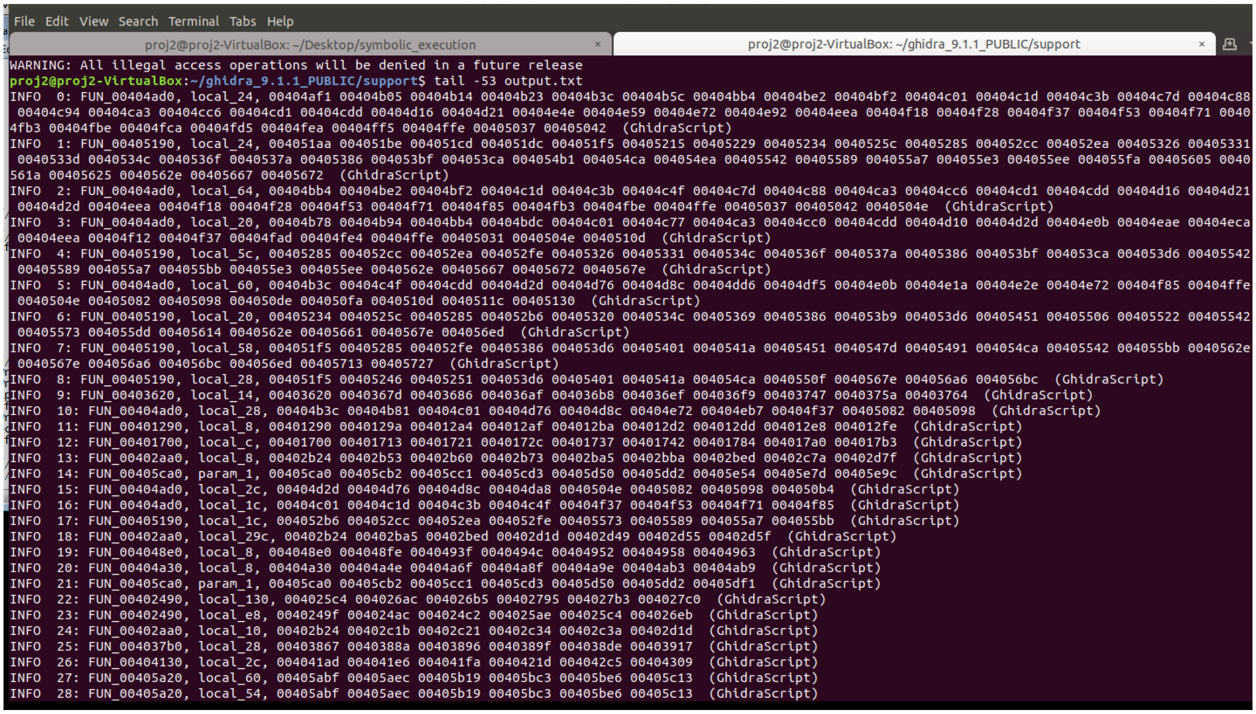
```
doom1\dyntrace.mydoom1.exe.500.2648
copying dyntrace.mydoom1.exe.500.3044 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.500.3044
copying dyntrace.mydoom1.exe.500.3244 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.500.3244
copying dyntrace.mydoom1.exe.500.3648 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.500.3648
copying dyntrace.mydoom1.exe.500.3708 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.500.3708
copying dyntrace.mydoom1.exe.500.4016 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.500.4016
copying dyntrace.mydoom1.exe.500.580 --> \\VBOXSVR\VM_Share\analysis\mydoom1\myd
oom1\dyntrace.mydoom1.exe.500.580
copying dyntrace.mydoom1.exe.948 --> \\VBOXSVR\VM_Share\analysis\mydoom1\mydoom1
\dyntrace.mydoom1.exe.948
copying dyntrace.mydoom1.exe.948.1904 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.1904
copying dyntrace.mydoom1.exe.948.1936 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.1936
copying dyntrace.mydoom1.exe.948.2136 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.2136
copying dyntrace.mydoom1.exe.948.2332 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.2332
copying dyntrace.mydoom1.exe.948.2348 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.2348
copying dyntrace.mydoom1.exe.948.2752 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.2752
copying dyntrace.mydoom1.exe.948.2776 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.2776
copying dyntrace.mydoom1.exe.948.3036 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.3036
copying dyntrace.mydoom1.exe.948.3136 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.3136
copying dyntrace.mydoom1.exe.948.3204 --> \\VBOXSVR\VM_Share\analysis\mydoom1\my
doom1\dyntrace.mydoom1.exe.948.3204
The system cannot find the file specified.

C:\code\concrete_executor>_
```

After running the python program, it did copy the trace file for mydoom1 to the shared folder.


Home
Desktop
VM_Share
analysis
mydoom1
mydoom1
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Trash
Other Locations
dyntrace.mydoom1.exe.500
dyntrace.mydoom1.exe.500.5…
dyntrace.mydoom1.exe.500.2…
dyntrace.mydoom1.exe.500.2…
dyntrace.mydoom1.exe.500.2…
dyntrace.mydoom1.exe.500.3…
dyntrace.mydoom1.exe.500.3…
dyntrace.mydoom1.exe.500.3…
dyntrace.mydoom1.exe.500.3…
dyntrace.mydoom1.exe.500.4…
dyntrace.mydoom1.exe.948
dyntrace.mydoom1.exe.948.1…
dyntrace.mydoom1.exe.948.1…
dyntrace.mydoom1.exe.948.2…
dyntrace.mydoom1.exe.948.2…
dyntrace.mydoom1.exe.948.2…
dyntrace.mydoom1.exe.948.2…
dyntrace.mydoom1.exe.948.2…
dyntrace.mydoom1.exe.948.3…
dyntrace.mydoom1.exe.948.3…
dyntrace.mydoom1.exe.948.3…
dyntrace.mydoom1.exe.3408
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.3408.…
dyntrace.mydoom1.exe.4036
dyntrace.mydoom1.exe.4036.328
dyntrace.mydoom1.exe.4036.336
dyntrace.mydoom1.exe.4036.580
dyntrace.mydoom1.exe.4036.896
dyntrace.mydoom1.exe.4036.2224
dyntrace.mydoom1.exe.4036.2588
dyntrace.mydoom1.exe.4036.3068
dyntrace.mydoom1.exe.4036.3680
dyntrace.mydoom1.exe.4036.4032
mydoom1.exe

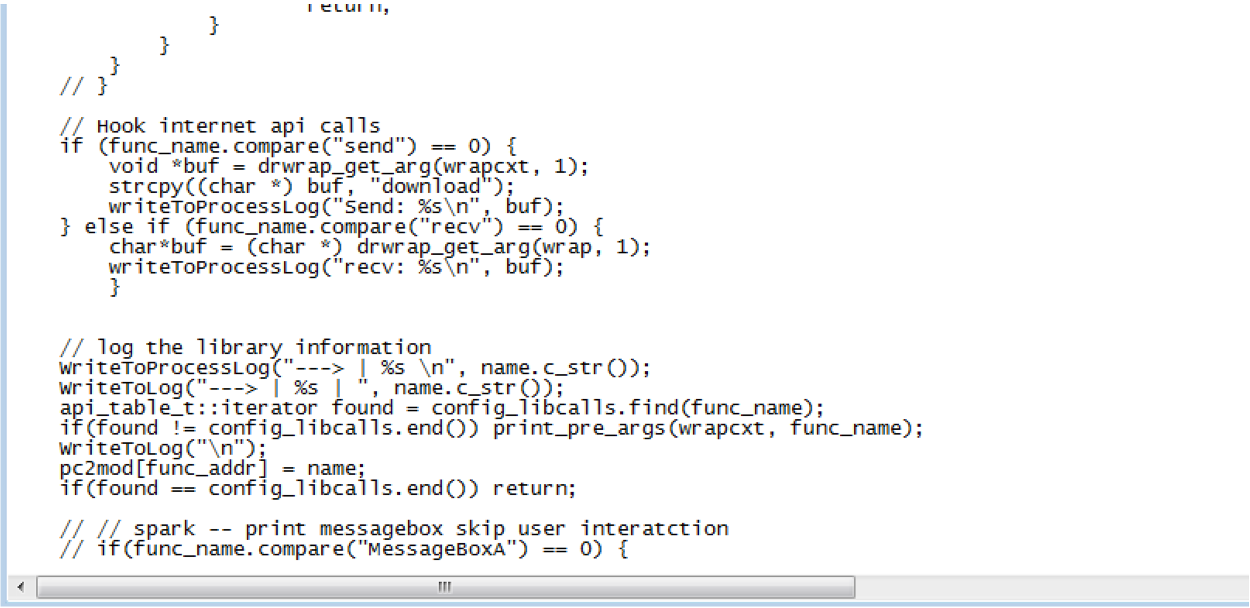
2. Malware2 (wun33.exe)

Run python script to get top longest chain output. Then tried to change the python program to get all command at one run.


File Edit View Search Terminal Tabs Help
proj2@proj2-VirtualBox: ~/Desktop/symbolic_execution
proj2@proj2-VirtualBox: ~/ghidra_9.1.1_PUBLIC/support

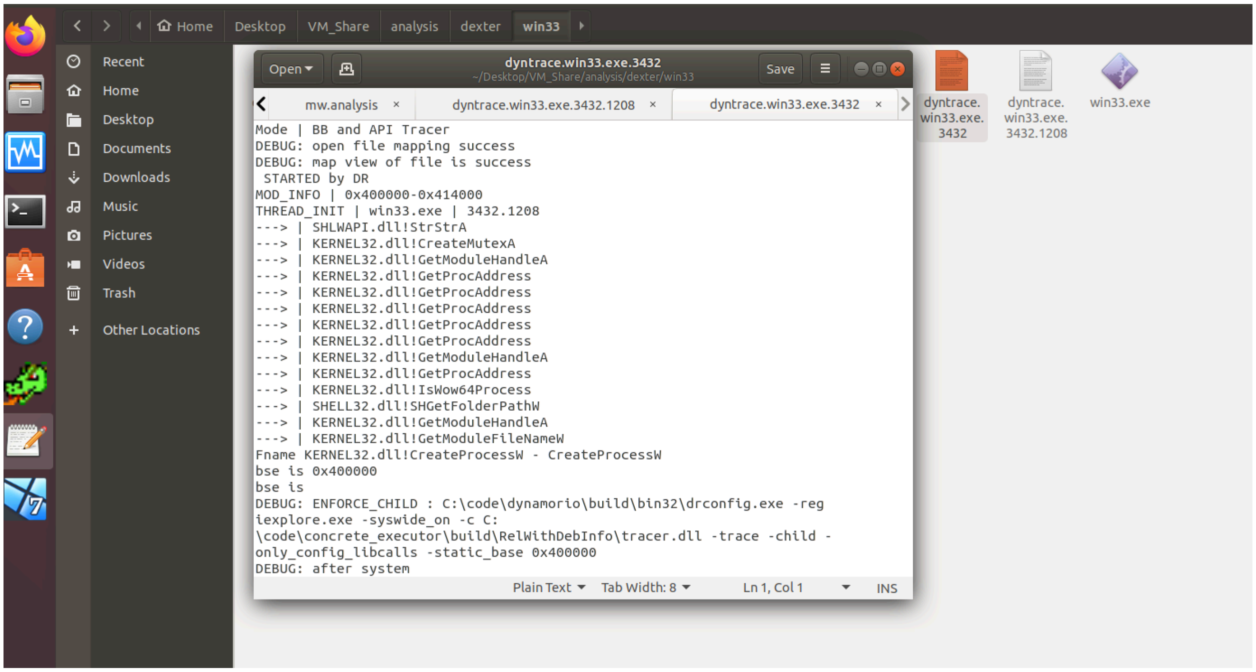
```
WARNING: All illegal access operations will be denied in a future release
proj2@proj2-VirtualBox:~/ghidra_9.1.1_PUBLIC/support$ tail -53 output.txt
INFO  0: FUN_00404ad0, local_24, 00404af1 00404b05 00404b14 00404b23 00404b3c 00404b5c 00404bb4 00404be2 00404bf2 00404c01 00404c1d 00404c3b 00404c7d 00404c88
 00404c94 00404ca3 00404cc6 00404cd1 00404cdd 00404d16 00404d21 00404e4e 00404e59 00404e72 00404e92 00404eea 00404f18 00404f28 00404f37 00404f53 00404f71 0040
4fb3 00404fbe 00404fca 00404fd5 00404fea 00404ff5 00404ffe 00405037 00405042  (GhidraScript)
INFO  1: FUN_00405190, local_24, 004051aa 004051be 004051cd 004051dc 004051f5 00405215 00405229 00405234 0040525c 00405285 004052cc 004052ea 00405326 00405331
 0040533d 0040534c 0040536f 0040537a 00405386 004053bf 004053ca 004054b1 004054ca 004054ea 00405542 00405589 004055a7 004055e3 004055ee 004055fa 00405605 0040
561a 00405625 0040562e 00405667 00405672  (GhidraScript)
INFO  2: FUN_00404ad0, local_64, 00404bb4 00404be2 00404bf2 00404c1d 00404c3b 00404c4f 00404c7d 00404c88 00404ca3 00404cc6 00404cd1 00404cdd 00404d16 00404d21
 00404d2d 00404eea 00404f18 00404f28 00404f53 00404f71 00404f85 00404fb3 00404fbe 00404ffe 00405037 00405042 0040504e  (GhidraScript)
INFO  3: FUN_00404ad0, local_20, 00404b78 00404b94 00404bb4 00404bdc 00404c01 00404c77 00404ca3 00404cc0 00404cdd 00404d10 00404d2d 00404e0b 00404eae 00404eca
 00404eea 00404f12 00404f37 00404fad 00404fe4 00404ffe 00405031 0040504e 0040510d  (GhidraScript)
INFO  4: FUN_00405190, local_5c, 00405285 004052cc 004052ea 004052fe 00405326 00405331 0040534c 0040536f 0040537a 00405386 004053bf 004053ca 004053d6 00405542
 00405589 004055a7 004055bb 004055e3 004055ee 0040562e 00405667 00405672 0040567e  (GhidraScript)
INFO  5: FUN_00404ad0, local_60, 00404b3c 00404c4f 00404cdd 00404d2d 00404d76 00404d8c 00404dd6 00404df5 00404e0b 00404e1a 00404e2e 00404e72 00404f85 00404ffe
 0040504e 00405082 00405098 004050de 004050fa 0040510d 0040511c 00405130  (GhidraScript)
INFO  6: FUN_00405190, local_20, 00405234 0040525c 00405285 004052b6 00405320 0040534c 00405369 00405386 004053b9 004053d6 00405451 00405506 00405522 00405542
 00405573 004055dd 00405614 0040562e 00405661 0040567e 004056ed  (GhidraScript)
INFO  7: FUN_00405190, local_58, 004051f5 00405285 004052fe 00405386 004053d6 00405401 0040541a 00405451 0040547d 00405491 004054ca 00405542 004055bb 0040562e
 0040567e 004056a6 004056bc 004056ed 00405713 00405727  (GhidraScript)
INFO  8: FUN_00405190, local_28, 004051f5 00405246 00405251 004053d6 00405401 0040541a 004054ca 0040550f 0040567e 004056a6 004056bc  (GhidraScript)
INFO  9: FUN_00403620, local_14, 00403620 0040367d 00403686 004036af 004036b8 004036ef 004036f9 00403747 0040375a 00403764  (GhidraScript)
INFO  10: FUN_00404ad0, local_28, 00404b3c 00404b81 00404c01 00404d76 00404d8c 00404e72 00404eb7 00404f37 00405082 00405098  (GhidraScript)
INFO  11: FUN_00401290, local_8, 00401290 0040129a 004012a4 004012af 004012ba 004012d2 004012dd 004012e8 004012fe  (GhidraScript)
INFO  12: FUN_00401700, local_c, 00401700 00401713 00401721 0040172c 00401737 00401742 00401784 004017a0 004017b3  (GhidraScript)
INFO  13: FUN_00402aa0, local_8, 00402b24 00402b53 00402b60 00402b73 00402ba5 00402bba 00402bed 00402c7a 00402d7f  (GhidraScript)
INFO  14: FUN_00405ca0, param_1, 00405ca0 00405cb2 00405cc1 00405cd3 00405d50 00405dd2 00405e54 00405e7d 00405e9c  (GhidraScript)
INFO  15: FUN_00404ad0, local_2c, 00404d2d 00404d76 00404d8c 00404da8 0040504e 00405082 00405098 004050b4  (GhidraScript)
INFO  16: FUN_00404ad0, local_1c, 00404c01 00404c1d 00404c3b 00404c4f 00404f37 00404f53 00404f71 00404f85  (GhidraScript)
INFO  17: FUN_00405190, local_1c, 004052b6 004052cc 004052ea 004052fe 00405573 00405589 004055a7 004055bb  (GhidraScript)
INFO  18: FUN_00402aa0, local_29c, 00402b24 00402ba5 00402bed 00402d1d 00402d49 00402d55 00402d5f  (GhidraScript)
INFO  19: FUN_004048e0, local_8, 004048e0 004048fe 0040493f 0040494c 00404952 00404958 00404963  (GhidraScript)
INFO  20: FUN_00404a30, local_8, 00404a30 00404a4e 00404a6f 00404a8f 00404a9e 00404ab3 00404ab9  (GhidraScript)
INFO  21: FUN_00405ca0, param_1, 00405ca0 00405cb2 00405cc1 00405cd3 00405d50 00405dd2 00405df1  (GhidraScript)
INFO  22: FUN_00402490, local_130, 004025c4 004026ac 004026b5 00402795 004027b3 004027c0  (GhidraScript)
INFO  23: FUN_00402490, local_e8, 0040249f 004024ac 004024c2 004025ae 004025c4 004026eb  (GhidraScript)
INFO  24: FUN_00402aa0, local_10, 00402b24 00402c1b 00402c21 00402c34 00402c3a 00402d1d  (GhidraScript)
INFO  25: FUN_004037b0, local_28, 00403867 0040388a 00403896 0040389f 004038de 00403917  (GhidraScript)
INFO  26: FUN_00404130, local_2c, 004041ad 004041e6 004041fa 0040421d 004042c5 00404309  (GhidraScript)
INFO  27: FUN_00405a20, local_60, 00405abf 00405aec 00405b19 00405bc3 00405be6 00405c13  (GhidraScript)
INFO  28: FUN_00405a20, local_54, 00405abf 00405aec 00405b19 00405bc3 00405be6 00405c13  (GhidraScript)
```

After that I change the lib handler to hook up the internet API calls in wrap_pre_lib() functions.



```
                    return;
            }
        }
    }
// }

// Hook internet api calls
if (func_name.compare("send") == 0) {
    void *buf = drwrap_get_arg(wrapcxt, 1);
    strcpy((char *) buf, "download");
    writeToProcessLog("Send: %s\n", buf);
} else if (func_name.compare("recv") == 0) {
    char*buf = (char *) drwrap_get_arg(wrap, 1);
    writeToProcessLog("recv: %s\n", buf);
    }


// log the library information
WriteToProcessLog("---> | %s \n", name.c_str());
WriteToLog("---> | %s | ", name.c_str());
api_table_t::iterator found = config_libcalls.find(func_name);
if(found != config_libcalls.end()) print_pre_args(wrapcxt, func_name);
WriteToLog("\n");
pc2mod[func_addr] = name;
if(found == config_libcalls.end()) return;

// // spark -- print messagebox skip user interatction
// if(func_name.compare("MessageBoxA") == 0) {
```

Then run run.py in command prompt to get traces of win33.exe malware.



```
Mode | BB and API Tracer
DEBUG: open file mapping success
DEBUG: map view of file is success
 STARTED by DR
MOD_INFO | 0x400000-0x414000
THREAD_INIT | win33.exe | 3432.1208
---> | SHLWAPI.dll!StrStrA
---> | KERNEL32.dll!CreateMutexA
---> | KERNEL32.dll!GetModuleHandleA
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!GetModuleHandleA
---> | KERNEL32.dll!GetProcAddress
---> | KERNEL32.dll!IsWow64Process
---> | SHELL32.dll!SHGetFolderPathW
---> | KERNEL32.dll!GetModuleHandleA
---> | KERNEL32.dll!GetModuleFileNameW
Fname KERNEL32.dll!CreateProcessW - CreateProcessW
bse is 0x400000
bse is
DEBUG: ENFORCE_CHILD : C:\code\dynamorio\build\bin32\drconfig.exe -reg
iexplore.exe -syswide_on -c C:
\code\concrete_executor\build\RelWithDebInfo\tracer.dll -trace -child -
only_config_libcalls -static_base 0x400000
DEBUG: after system
```

3. Maware3 (unknown.exe)
For this task, I simply used ghidra to analyze functions and fil the excel form.